BOWING TO QUIRINUS: COMPROMISED NODES AND CYBER SECURITY IN EAST ASIA

by

CAMERON JAY ORTIS

B.A., University of Northern British Columbia, 1999
M.A., McMaster University, 1999

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE

DOCTOR OF PHILOSOPHY

in

THE FACULTY OF GRADUATE STUDIES

(Political Science)

THE UNIVERSITY OF BRITISH COLUMBIA

August 2006

Abstract

An increasing amount of scholarly work in International Relations is being devoted to reconsidering traditional concepts about what constitutes security in an era of information technologies. Yet the discipline has focused this re-examination almost exclusively on the Internet as a communications technology; a technology that allows for the ability to exchange complex forms of data – the ability to talk at a distance. Viewing the Internet through the prism of a communications media largely ignores its more potent dimension – the ability to act from a distance. This study seeks to examine the relationship between rapid Internet diffusion and the emergence of new threats and the digitization of traditional threats.

The study outlines a compromised-node framework. At the core of this level of analysis is the argument that the compromised node on the Internet is the central problem in a digitizing world both in physical and theoretical terms. Other approaches used in International Relations to study security and the information revolution commonly employ more traditional frameworks built around the international system or the state and more recently the "network" level of analysis. In more theoretical terms, using a node-based level of analysis allows for a contribution to the 'broadening of security' project that has occupied much of the International Relations literature recently and at the same time grounds the research in the technical realities that are often overlooked or misunderstood.

Utilizing different methodological tools and data forms to illuminate the multi-faceted nature of the problem, this study is organized into two parts. Part one examines the distribution of compromised nodes cross-nationally in order explore the relationship between the level of Internet insecurity and key socio-economic, political and infrastructural

factors. Part two examines transnational organized crime as a high-tech threat to firms and state organizations in East Asia.

The insecurities of the digital world call into question the efficacy and legitimacy of traditional state-based security when applied to new Internet based threats. But for the foreseeable future the state remains the only actor with the authority, legitimacy, resources and governance tools to address these issues.

Table of Contents

List Tables

List of Figures

Acronyms

APEC – Asia Pacific Economic Cooperation

ASEAN – Association of Southeast Asian Nations

BGP – Border gateway protocol

BSD – Berkeley Service Distribution

CCP – Chinese Communist Party

CSE – Communications Security Establishment (Canada)

DoD – Department of Defense (US)

DnD – Department of National Defence (Canada)

FCC – Federal Communications Commission (US)

FinCEN – American Financial Crimes Enforcement Network (US)

GDP – Gross domestic product

GIS – Geographic information system

GPS – Global positioning System

IDS – Intrusion detection system

ITU – International Telecommunications Union (UN)

IP – Internet protocol

ISP – Internet service provider

KISA – Korea Information Security Agency (ROK)

LAN – Local area network

LCD – Lowest common denominator format

NGO – Nongovernmental organization

NSA – National Security Agency (US)

OECD – Organization for Economic Cooperation and Development

PRC – People's Republic of China

RIAA – Recording Industry Association of America

RBL – Real time blacklist

SCADA – Supervisory control and data acquisition

TCP – Transmission control protocol

VPN – Virtual private network

WAN – Wide Area Network

Glossary

Chained relay – a series of compromised Internet devices linked together.

Cracker – a network intruder.

Encryption - is the process of obscuring information to make it unreadable without special knowledge. This is usually done for secrecy, and typically for confidential communications. Encryption can also be used for authentication.

Exploit – a program written to take advantage of a vulnerability.

Firewall – a hardware or software device designed to restrict inbound and outbound network traffic.

Hacker – in common public usage refers to an individual that breaks into computer systems or network. In fact, a hacker actually refers to an individual that takes things apart to understand, modify or improve a machine.

Linux - is the name of a computer operating system and its kernel. The name *Linux* strictly refers only to the linux kernel, but it is commonly used to describe entire unix-like operating system.

Open relay – a computer or sever that performs electronic mail handling. A relay is a form of open proxy which is an Internet proxy server which is accessible by unauthorised users, specifically those from elsewhere on the internet.

Polymorphic shell code – is code or programs that act like chameleons by changing their form autonomously to avoid detection. Currently, in computer security there is no known defense against this type of program.

Port scan - refers to checking for services presented on port addresses, usually as part of a cracking attempt or computer security scan. Port scans are performed both by attackers and systems administrators attempting to check the security of their systems.

Scale free topology – refers to the general structure of the Internet on an aggregate scale. Originally, the concept was applied to computer networks by Albert-Laslo Barabasi at the University of Notre Dame, in Indiana. Until 1999, the standard way of modelling the Internet was to use randomly generated graphs, in which routers were represented by points and the links between them by lines. But it turns out that such random graphs are a poor approximations because they miss two important features. The first is that links in the net are "preferentially attached": a router that has many links to it is likely to attract still more links; one that does not, will not. The second is that the Internet has more clusters of connected points than random graphs do. Scale-free topologies are thought to be resistant to random failures.

Script kiddie – a cracker with a low skill level, in other words without a deeper understanding of science and engineering behind the code. Generally thought to be responsible for the majority of the known Internet attacks.

Server – a computer software application that carries out some task on behalf of its user. The most common types are file servers and applications servers. Web, email and database servers are the most commonly used for the Internet.

Social engineering – in the computing community context it refers to the act of manipulating humans to divulge privileged information. It should not be confused with its meaning in social thought.

Source code – is a series of statement written in some human readable computer programming language. Source code can be in one or more text files that are then converted by software into computer executable form.

TCP/IP stack – TCP/IP is the Internet protocol suite. It is the set of protocols that implement the protocol stack on which the Internet runs. It is sometimes called the TCP/IP protocol suite, after the two most important protocols in it: the transmission control protocol (TCP) and the Internet protocol (IP). The internet protocol suite can be described by analogy to a layered stack which describes the layers of a protocol stack. In a protocol stack, each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the higher layers. Higher layers are logically closer to the user and deal with more abstract data, relying on lower layers to translate data into forms that can eventually be physically manipulated. Any device that can "connect" to the Internet must have a TCP/IP stack.

Trojan horse – is a program that is secretly placed on a computer or network device to perform various tasks.

Uberhacker – a slang term used in reference individuals with the highest level of cracking or hacking expertise.

Unix - is a portable, multi-task and multi-user computer operating system originally developed by a group at AT&T and Bell Labs

Virus - is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus which spreads by inserting itself into living cells.

Vulnerabilities – flaws in computer or network systems that are either known or unknown which can be taken advantage of by exploits to compromise the machine.

Windows – an operating system created and sold by Microsoft.

Worm - is a self-replicating computer program similar to a computer virus. A virus attaches

itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.

Zombie – in computer security a zombie can be either a machine that has been taken over by a cracker to attack other machines or a program that remains running on a computer after it has received a termination command.

Preface

Quirinus was a Roman god of the state and war. His origins are often traced back to the protector god of the fields before being associated with Romulus' apotheosis toward the end of the Roman Empire. Most of what is known of both Quirinus and the cult that worshiped him is derived from a time period when myths were being reworked to fit into the Roman political ideology (Cook, 1905; Quirinus, 2006). The Romans themselves often wondered about Quirinus because he was seen as mysterious, often being depicted in both clerical and military clothing, and set as a lesser god against Jupiter and Mars (Cook 1905). Yet they continued to worship him even though they were not really sure why it was important to do so.

The impact of the cyber infrastructure on international security is a lesser problem when compared to economic and military security issues. It is interesting then that cyber infrastructure security is still assumed to be of some importance by academics and policy makers even though they are often not sure exactly why. The politics of cyber infrastructure security can be clothed in either clerical or military garb. This dissertation does not try to argue that Quirinus is equal to Mars and Jupiter. Rather, the argument is that the state now sees the cyber infrastructure increasingly in traditional security terms. Or couched in the metaphor above, Jupiter and Mars are beginning to take much more than a passing interest in the affairs of Quirinus.

There are two problems that are the analytical focus of the study. The first is the general gap between threat perception and reality in the cyber infrastructure. The objective here is to use a unique large-N data set to show that one of the current assumptions regarding the sources of infrastructure instability across countries is without empirical merit. The second

analytical problem is the adaptation space between the state and transnational organized crime groups in East Asia. A series of short case studies are developed that focus in on specific social and political processes of the state's response to cyber security issues. The dissertation takes an unusual approach to the two analytical problems by using two distinct research designs that both keep the analysis rooted in the technical realities of the infrastructure, exemplified and centered on compromised nodes, while situating the state in an emerging virtual realism.

Acknowledgements

This dissertation would not have been written without the unwavering support and encouragement of my parents.

I would also like to thank my research supervisor Dr. Brian Job, professor of Political Science at the University of British Columbia (UBC) and director of the Centre of International Relations. His guidance and comments on the many drafts made the dissertation possible. In particular, I would like to thank Dr. Job for allowing me to take on an unusual topic and approach to the study of the impact of technology on international security in the East Asia region.

In addition to my supervisor, other members of the dissertation committee were invaluable. I would like to thank Dr. Paul Evans, professor in the Faculty of Graduate Studies at UBC and co-CEO of the Asia Pacific Foundation of Canada in Vancouver for the intellectual guidance and constant reminder that writing a dissertation is a marathon not a sprint. Dr. Evans also helped to provide contacts in East Asia for the field research. Dr. Fred Cutler, assistant professor in the Department of Political Science at UBC, also a member of my committee, spent one-on-one time with me hunched over a computer pouring over statistical results.

I would also like to thank Tom Ngi, a software engineer living in Vancouver, whose technical skills made Part One of the dissertation possible. Mr. Ngi graciously volunteered his time on the project and re-wrote the software that processed the data for the quantitative sections.

My friends and family members should also be acknowledged for their understanding during the many absences while I completed this project and for their help celebrating its

conclusion.

I must also thank the anonymous individuals in East Asia and North America who graciously agreed to speak on the issues addressed in this study. Without their participation during many trips to the region, Part Two of the dissertation would not have been written.

I would also like to acknowledge Dr. Heather Smith, associate professor of International Studies at the University of Northern British Columbia, whose mentoring during my undergraduate years laid the groundwork for a continuing interest and passion for the study of international relations.

The work received financial support from the Charles C.C. Wong Memorial Fellowship through St. John's College at UBC. The research also benefited from financial support from the Social Sciences and Humanities Research Council of Canada. The Centre of International Relations at UBC provided office space and other logistical support at various points between 2001 and 2005.

Dedication

To my parents.

Introduction

Introduction: scope of study

Drawing on the recent research of various scholars and social scientists working in and around the debate in International Relations over the meaning of the information revolution, this study outlines a compromised-node theory of security. At the core of this theory is the argument that the compromised node on the Internet is the central problem in a digitizing world both in a physical and theoretical sense. The coevolutionary behavior between those trying to secure nodes and those trying to compromise them can be likened to a series of asymmetrical arms races of attack-defense where offensive adaptations are countered by defensive adaptations. This study's conclusions are in general agreement with Herrera's theory that, as is mostly the case in coevolutionary processes, the outcome is indeterminate as long as the environment, or in this case infrastructure in which these dynamics play out, continues to evolve and change.[1] In more theoretical terms, using a node-based level of analysis allows for a contribution to the 'broadening of security' project that has occupied much of the International Relations literature recently and at the same time grounds the research in the technical realities that are often overlooked or misunderstood. It also allows for a contribution to the securitization literature and its attempts to understand the linkages between perceived existential threats and performative acts.

Organization of the study

Focusing on the East Asian region, this study is broken down into two investigations that explore two dimensions of Internet security. Utilizing different methodological tools and data forms to illuminate the multi-faceted nature of the problem of the compromised

[1] See Herrera (2002).

node, I will show in the following pages that there is a coherent theme and fundamental problem that connects the two approaches. Two distinct methodologies are used in this dissertation. Both the indicator of cyber infrastructure instabilities and the locus of transnational organized crime's usage of cyber space are centered on compromised nodes. Thus, the study is broken down into two components. The first looks at the aggregate cross-national distribution of compromised nodes. The second component focuses on how the number of compromised nodes continue to grow and support untoward uses of the infrastructure. Both designs are meant to better situate the state as an imperfect actor in an increasingly complex technological environment.

Building upon the introductory chapter and the theoretical discussion in Chapter Two, Chapters Three, Four, and Five of the dissertation examine the variation of compromised nodes both globally and specifically in East Asia. Using unique data obtained from a widely distributed logging system, Chapters Three and Four of Part One examine multiple hypotheses on the relationship between these patterns and several socio-political, economic and infrastructural variables. To my knowledge, this is the first study to address this problem from an international perspective using quantitative data collected via intrusion logs from networks distributed throughout the world. The primary objective here will be to develop a quantitative description of Internet incidents – specifically from compromised machines – by country and explain the variations in these patterns on a state oriented basis.

Part Two also takes as its starting point the problem of the compromised node on the Internet. Here I examine transnational organized crime as a high-tech threat to firms and state organizations in the East Asia; a problem that many in the Internet security community consider to be the most serious Internet based threat. By looking at the

coevolutionary adaptive gap between sophisticated, well organized criminal elements and state response mechanisms used to confront this threat, the analysis focuses on how far the adaptation space has widened. Chapter Eight develops a series of three short case studies from Hong Kong, Japan and Singapore that examine two dimensions of the impact the organized crime groups are having on the cyber infrastructure. The central question is: if the evolutionary adaptive gap between criminal innovators and enforcement response is widening, can it be narrowed?

Research for Part Two is based primarily on field work plus documentation from scholarly journals and media reports. Over the last four years I have conducted 31 interviews with government officials, engineers, and members of the 'hacker community' in 8 cities in Asia as well as with individuals in Canada and the United States. Interviews with government officials and security practitioners yielded valuable information on new and emerging Internet threats that states and firms face from organized crime. It was also valuable to get firsthand accounts on the policies and strategies that have been implemented in national settings in order to get a sense of what has worked what has not worked in the past and why. Field interviews also provided a unique opportunity to speak with individuals in the "underground" community. While access to this population was limited when compared to government policy makers and network engineers working at large firms, enough qualitative data was gathered to gain some insight into general behavioral trends.

The East Asia cases were chosen as the focus for this study for three reasons.[2] The first

[2] For the remainder of this study the term 'East Asia' is taken to mean the regions: Southeast Asia which includes Brunei, Myanmar, Cambodia, Indonesia, Lao, Malaysia, Philippines, Singapore, Thailand, Vietnam (as well as New Zealand and Australia); and East Asia which includes, China, Hong Kong SAR, Japan, North Korea, S. Korea (Northeast Asia) and Taiwan. I will largely ignore both: Central Asia which includes Mongolia, Afghanistan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan; and South Asia which includes Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, Sri Lanka.

is that the region provides a certain kind of diversity of actors. There is no other region in the world where there is such extreme variability – deep and shallow – in Internet diffusion patterns and where there are both non-democratic and democratic regimes. Along side state actors in the region, and often at odds with them, are a host of non-state actors that are taking advantage of rapid Internet diffusion. Second, this particular regional context is unique from others in the sense that there has been a nascent socio-political impact of the Internet. Finally, East Asia has a growing reputation as a breeding ground for software piracy, crackers, virus writers and lackadaisical system administrators. The region plays host to the most advanced use of the Internet by organized crime groups.

The role of the state is extensive in most East Asian countries and this is particularly true with respect to the Internet. Early experimentation with computer networks occurred in the scientific or academic sector, but the central government has been the major player in any Internet development beyond the experimental level. Like their counterparts in advanced industrial democracies, many authoritarian governments have instituted security plans, created special Internet governance committees, or reorganized bureaucracies to deal more effectively with the Internet and resulting security dilemmas. State Internet security policies and governance structures are often outgrowths of older regulatory regimes of the armed forces, intelligence and law enforcement agencies. As in any country -- especially where the role of the state is strong -- policy will have an important influence on the myriad of ways in which Internet security issues are approached and framed.

There is, of course, room to quibble with the use of 'East Asia' to mean 'Southeast' and 'East' Asia alone, and the addition of New Zealand and Australia. I define the regions largely based on a cyber infrastructural perspective, which also takes into account geopolitical and cultural influences. In two of the following chapters, for technical reasons to facilitate data analysis, I do expand the regional definitions to include India, New Zealand and Australia.

The final chapter of the dissertation is a summary that returns to the theoretical or analytical framework fleshed out in Chapter Two and empirically assessed in Part One and Part Two. It reassesses the utility of a node-based approach in understanding the efficacy of setting the context of cyber security within purely territorial or non-territorial frameworks. The concluding chapter will also return to the description of specific usages of Internet technologies by non-state actors and subsequent state responses as a coevolutionary process. The state does appear to be adapting in the short run even though much of the adaptation gap remains tenuously uneven. Over the long run, however, this gap may begin to widen. In East Asia, this will put increasing pressure on states to securitize cyber infrastructures as opposed to criminalizing nefarious uses of this environment. New node-based security actors behave as both a threat to the state, as in the case of organized crime usage of computing technologies, and as a surrogate to the traditional role of state-based providers of security. International Relations might be applied and its conceptual apparatus yield insights; but it too requires serious rethinking as both the phenomena and conceptual frameworks of the cyber infrastructure are novel. International security studies will play an important role both by conceptualizing the nature of these 'new' threats and assessing the response by state and non-state actors. It is to this subject that the dissertation now turns.

Chapter One: The Origins of the Cyber Infrastructure

The Internet

This introduction begins with an historical overview of the development of the Internet. The focus here will be on the technologies themselves because these are the evolutionary engines of the Internet that are driven by technological developments. The social, economic and political environments of the mid to late twentieth century provided fertile ground for their growth. The second section moves to a discussion of the literature on the social impact of technology in more general terms. Here the focus is on the intellectual heritage that scholars in International Relations have drawn upon in the study of the impact of the Internet on international politics. The third and fourth sections of the chapter outline current Internet security issues and begin to place the state within this context. The central theme here is: why should students of international security care about the Internet? The final section of this chapter briefly outlines the objectives of this study.

The *Internet* is often taken to mean loosely connected computer networks. *Cyber space* is shorthand for not only Internet space but other forms of electronic or digital domains that can be reached via computer networks. Cyber space, a term first used in science fiction, is much broader in the sense that it describes not just the Internet but other architectures, applications and spaces that can be accessed from, and send data through the Internet. These electronic spaces have evolved into a much more complex infrastructure – primarily in the Western world – and taken together the Internet, intranets, cyber spaces now provide a digital environment for both control of machines and communications between humans, and between humans and machines.

What is the Internet and where did it come from?

The Internet is one dimension of an immensely complex electronic universe. The categories of electronic media and information technology range from radios, cellular phones, wireless Internet-enabled devices to distributed computing networks that form a kind of Internet-based supercomputer (Wong, 2001:67-68). For the purpose of this study, the Internet and computer networks are taken to mean both the hardware and software necessary for the control and communication of information that has been reduced to binary form. Hardware refers to computing and networking components. Software includes applications and protocols that allow for various kinds of control and communication functions to take place via an emerging global web of computer networks that can now be considered as a cyber infrastructure. For the purpose of this dissertation, an Internet node refers to the connection of any machine that possesses a transmission control protocol and Internet protocol (TCP/IP) stack; in other words any device that can use the common protocols for communicating with other nodes in the cyber infrastructure. Any Internet device whether it is a router, server or a personal computer is a node that is theoretically accessible though a large and increasingly complex connection of very large networks.

The idea of an *inter-net* was first articulated by Joseph Licklider, a psychologist working at the Massachusetts Institute of Technology (MIT) in the late 1950s and early 1960s. Licklider, in 1962, wrote about the concept of a "Galactic Network" and 'thinking center' concept (Liener *et al.*, 2003). His idea was essentially a globally connected set of computers through which anyone could send and receive data and programs from any site in an efficient and reliable manner. By the 1950s and into the early 1960s computers were already wide spread enough for researchers at major universities to have access and

begin working them into research designs (Liener *et al.,* 2003). The driving factors were the emergence of several technologies and ideas in the United States where a technology friendly environment existed. The internationalization of economic markets encouraged firms and the US government to respond positively to new technologies that appeared to stimulate interconnection (Zacher, 2002:190-191).

The emergence and adoption of the telegraph, telephone, radio, and computer laid the groundwork for what Leiner *et al* observed was an "unprecedented integration of capabilities" (2003:1). New networking concepts demanded new technologies, or more precisely, new ways of thinking about networks. Computers themselves had been invented a decade before any serious thought was applied to thinking about how to connect them.[3] Until the early 1960s, networks, such as the telephone system, were circuit switched. In the mid-1960s Leonard Kleinrock published the first paper on packet switching. This was a fundamentally different way of networking. Instead of switching based on the idea of circuits Kleinrock envisioned packet based switching.[4] The central difference is that data would traverse a network individually based on a routing algorithm that allows for individual packets to 'find' the best path to destination available.

This move from theoretical idea to electronic reality was not, however, taking place in isolation. Researchers were proceeding in parallel without either knowing about each others' work. As these separate groups of researchers became aware of one another, the focus of packet switching congealed around the US ARPANET. After a research center at Stanford was connected, the first host-to-host data was sent between the two locations. Two more nodes were added by the end of 1969. Thus, four host computers were connected together to form the initial ARPANET – the genesis of the Internet. But the

[3] For more on the history of computing see Edwards (1994) and Mahoney (1988:113-125).
[4] For more on telecommunications see Rockstrom and Zdebel (1998:36: 36-40).

new network form needed a reliable, agreed upon way to exchange data, one that would allow differing architectures, network environments, and interfaces to communicate with one another. Other researchers moved to develop a new version of the protocol which could meet the needs of an 'open' architecture network. This early collection of protocols would evolve into the Transmission Control Protocol/Internet Protocol (TCP/IP). In an friendly-to-different-hardware-forms network, with the TCP/IP suite of protocols, all participating networks could be of different design and each may have its own unique interface but yet still participate.[5]

The issue at this point in the evolution of the Internet was how to get the protocols out to as many computers as possible. The US Defense Advanced Research Projects Agency (DARPA) decided to support the University of California at Berkeley to see if these changed could be added to the unix operating system, which already included the TCP/IP suite of protocols. The addition of TCP/IP into the unix Berkley System Distribution (BSD) marked an important point in the diffusion of the necessary Internet software protocols to the broader research world.[6] This strategy of incorporating Internet protocols into an operating system for the research community was an important ingredient in the widespread adoption of the Internet (Liener *et al.,* 2003). The universal protocols for inter-networking were thus built directly into computer operating systems. At this stage in the evolution of the Internet there existed an evolving hardware (packet switching) and software (TCP/IP protocols) which provide an all-new-comers-welcome concept of interconnected networks. By 1983, the ARPANET was being used by a significant

---

[5] For a complete overview and history refer to the original paper authored by Cerf and Kahn (1974) and also Clark (1998).

[6] For more on protocols see Stallings (1993:17-56). This is essentially an overview of network concepts based upon the ISO Reference Model of Open System Interconnection (OSI). The OSI model consists of seven layers of protocols: 1) physical 2) data link 3) network 4) transport 5) session 6) presentation and finally 7) the application layer.

number of US governmental agencies and organizations.

By the mid-1980s the Internet was already well established in both the US defence community and university environments.[7] What spurned this growth was the emergence of a 'killer application' – electronic mail (email). The utility and efficiency of email was immediately apparent to users on the relatively small nascent Internet. While other applications of the early Internet were making an impact in tucked away corners of specialized communities, it was email that was the common form of communication that, in many ways, helped to justify reasons to connect.

The Internet's evolution accelerated in the 1980s with the invention of Ethernet and the personnel computer (PC). Ethernet, originally invented in the 1970s, was being adopted as a common hardware approach to connecting machines. As opposed to tokin-rings, a competing technology backed by IBM in the early 1980s, Ethernet, back by 3Com, allowed for true local area networks. This is important. The idea here was that Ethernet 'cards' could be added to a device, any device, to allow it to physically join a network and exchange data. While most personnel computers in the 1980s did not have Ethernet cards, the use of local area networks in university, government, and large corporate environments meant that computers that could understand TCP/IP were beginning to connect disparate local area networks (LAN).

By the early-mid 1990s the Internet begins to look and act more like the infrastructure we see today rather than simply a collection of interesting interconnected technologies. This is an important genesis point for security. Cyber infrastructure security today includes not only the technologies themselves but also the social, political, economic and psychological factors that influence both security technologies and policy (Denning,

[7] For more on data networks please see Bertsekas and Gallager (1991).

2003:26).[8] During the 1990s the growth in LANs drove massive increases in Internet traffic as firms of all sizes began to rely on Internet technologies to stay competitive, reduce costs, manage supply chains and explore new ways to create demand for products and services.[9] Internet diffusion patterns – the spread and adoption of Internet infrastructures and technologies – begin to impact rural areas and the lesser developed economies. Two Internet applications, email and the World Wide Web (WWW), become standard communication mediums.[10] These developments begin to 'feed' off of one another as firms, governments and individuals begin to utilize Internet technologies in ways the university and military environments had scarcely envisaged.[11]

Current overview of Internet and infrastructure

Today there are four networking architectures or general models that utilize both computer hardware and software. The first, and still most commonly seen, is the client-server model. A client-server is a network application architecture that separates the client, usually through some type of interface, from the server. Through client software a user can send requests to a server to perform some sort of task and then the server sends the results back to the client. The second networking model is a multi-tier framework which builds upon the client-server concept. A multi-tier or n-tier environment exists when an application server stores data on a third machine, known as a database server.

---

[8] Throughout this study I will refer to both the cyber infrastructure and the Internet. The former is a broader, more ecological definition in line with Denning (2003). Internet security refers to the technologies themselves and as such is a subset of cyber infrastructure security. More on this below.

[9] For more on local area networks see Vargo and Hunt (1996). It is often difficult to understand the early impact of intra and inter networks on businesses. For a good case study which describes the evolution of the American Hospital Supply and Baxter information systems see Short and Venkatramen (1992).

[10] For more on wide area networks see "The Worldwide Web and Internet Technology" (1998).

[11] For more on the Internet's impact on commerce and business see Porter (2001:63-78). Porter argues that the Internet does not change the old rules of doing business but rather that the "old rules" are also the "new rules." See also Venkatraman (1994:73-87) for more on the different ways in which Internet technologies can impact and transform a business. Venkatraman focuses on business impact after the dot.com market depression in 2000. Did these technologies really improve the productivity of organizations? Did they create new kinds of organizations? For an alternative perspective where Internet technologies were critical for a firm please see the following case study on how firms connect disparate global operations in Ross (1995).

As opposed to the more generic client-server architecture, in general, an n-tier architecture may deploy any service using any number of intermediate servers as helpers doing specific tasks.

The third model is a peer-to-peer (P2P) computer network. This is a network that relies on the computing power and bandwidth of the participating nodes in the network rather than relying on a few servers as in the client-server or n-tier cases. In a P2P network there is no real concept of clients and servers, but rather peer nodes that operate as both "clients" and "servers" at the same time. A P2P network is typically used for connecting nodes via ad hoc connections. Such networks are useful for many purposes. Sharing content files (file sharing) containing audio, video, data or anything in digital format, as well as real time data such as telephone traffic is also passed using P2P technology. The term "P2P network" can also be employed to act as a grid computer where the computing power of many individual machines is harnessed for large number crunching tasks.[12]

Finally there is the web services model. This is a more software focused model than the previous three architectures discussed above. It is a 'system of software systems' designed to support machine-to-machine interaction over a network – without human intervention. Applications written in different programming languages and using different technologies can use web services to exchange data over any type of computer network in the same way as an inter-process communication on a single computer.[13] Web services allow machines to communicate with other machines, thus it is theoretically capable of removing any remaining barriers between disparate nodes, networks and devices.

Into early 2000 and 2001, these four networking models allowed for a vast array of

---

[12] For more on grid computing see Waldrop (2002).

[13] It is important to point out that the word "web" in web services is a bit of a misnomer and should not be confused with the World Wide Web (WWW) which is an application built 'on top' of the Internet. For more on web services see Vaughan-Nichols (2002); Hansen, Madnick, and Siegel (2002); and Seetharaman (1998).

human activities to migrate to the Internet: from personal banking and manufacturing assembly plants to modern military applications. Military functions such as command, control, communications and intelligence now rely on computer networks as do an increasing amount of government services.[14] Home entertainment systems from gaming to movies, scientific research and education, traffic control systems, infrastructures such as sewage treatment, water, and electrical grids now rely on Internet based technologies to evolve and function efficiently. In the near future, voice-over-Internet Protocol (VOIP) will begin to replace the plain-old-telephone system (POTS) in many organizations allowing for voice communication to be digitized and travel over the Internet and be processed like any other form of digital information.

This growing reliance on and use of the Internet in real-world applications signals a shift from the Internet as merely a collection of useful technologies to a cyber infrastructure capable of absorbing and integrating other technologies (Denning, 2003). Increasingly, economies – especially advanced industrial and post-industrial economies – can not maintain current growth levels and competitive market positions without the cyber infrastructure. The complexities of this infrastructure can be understood as a kind of ecosystem or cyber ecology complete with its own species variation, environmental conditions, pathogens, population growth and decline patterns.

For many, however, the Internet and cyber infrastructure is merely an interface to a computing machine to which instructions can be given through a keyboard and then information is retrieved and presented through a monitor. This gives the mistaken impression that the interaction is unidirectional: from the real world to the digital world.

[14] There have been claims by the US Department of Defense that the US military does not use the public Internet for anything other than unclassified, routine tasks. This is not entirely true. A considerable amount of classified data used by militaries around the world zips through cyber space along side ordinary email and other data. The difference is that these organizations open encrypted tunnels through the public Internet which allow the data to safely get to its destination.

From this vantage point the cyber infrastructure is seen as purely a communications and information retrieval technology. But beginning in the mid-1990s the cyber infrastructure began to take on omni-directional characteristics: the digital world could interact and control the real world. This adds the dimension of using the Internet and the cyber infrastructure as a control technology to interface with real world objects like manufacturing robots, sensor monitoring, and other control systems. The computing machines that can perform these tasks (not so different from a typical personal computer or email server) are called supervisory control and data acquisition devices or simply SCADA.

When SCADA equipment is 'plugged into' the cyber infrastructure the host computer allows for 'supervisory level' control of a remote site and can acquire data from that site. The bulk of the site control is actually performed automatically by instructions programmed into the computer that allow it to operate without human intervention using various types of artificial intelligence set according to predefined rules. The diffusion and adoption of SCADA equipment accessible via the cyber infrastructure across sectors and industries is arguably the current growth stage in the evolution of the Internet as infrastructure.

Diffusion of the cyber infrastructure

The global diffusion of the Internet can be best described as a hub-and-spoke formation where the hub is the United States and the spokes are the other parts of the world. Diffusion patterns are neither uniform nor symmetrical (Luke, 1998:120-122; CAIDA, 2001; Kirkman *et al.*, 2002:11-12). The lack of uniformity can be explained by the high variance in the growth of the Internet around the world. It is asymmetrical because the various social and technological dimensions of Internet diffusion in any

country vary in breadth, depth, rate and penetration. For example, some statistics point to an increasing number of hosts in a geographical region but upon closer examination the vast majority of these hosts are likely personal computers where the primary use is only in a few applications. This type of diffusion may be wide but it is not very deep. Deeper diffusion exists when critical infrastructures such as health, electrical systems, government services, manufacturing and production, apply Internet technologies.

Internet diffusion patterns globally remain profoundly uneven. Much of the cyber infrastructure is concentrated in North America, Western Europe and parts of East Asia. For example, many countries that are currently seeing rapid diffusion patterns – such as much of East Asia -- must still rely on the peering relationships between large networks called autonomous systems that are concentrated in North America or Western Europe to achieve connectivity with the rest of the world. This reliance of periphery countries on the United States drives much of the international security politics of the Internet. Many governments are profoundly uncomfortable with the idea that their data traffic will often travel through distrusted cyber space in order to reach its destination.[15]

Regional diffusion patterns

Internet diffusion patterns in East Asia are unique. There is no other region where the variation in diffusion is as high. Singapore, Hong Kong SAR, Japan and South Korea represent typical cases where diffusion patterns are both broad and deep. At the other end of the spectrum are several countries where there is virtually no use of the Internet, for

[15] With regard to the politics of peering it should be noted that an autonomous system can simply cut off a country on its own by refusing to handle data traffic. If a stoppage were to take place this would not stop traffic from going between computers attached to these ISPs. It merely stops the data from going to its destination directly; it will most likely travel via other providers. This will take longer but it will eventually get there. This is the essence of packet switching technology and the reason why the Internet tends to see political censorship and other forms of control as a kind of damage and routes around it. For a very interesting example of the peering relationship see <https://www.linx.net/www_public/our_members/peering_matrix/>. This informative table shows the peering matrix at the London Internet Exchange and nicely illustrates the complexity of Internet topology.

example North Korea and Burma, and a variety of countries somewhere in between. In political terms there are a variety of regime types; in economic terms there is an equal range of systems and levels of development. There are additional differences that make this region unique when comparing cyber infrastructures and diffusion patterns. For example, Wong argues that "while Asian countries in the past have captured a disproportionately high share of global production of ICT goods, [they] have as a group been laggard in the adoption of ICT in comparison to non-Asian countries" (Wong, 2002:167).

This lag means that North America and to a lesser extent Europe have a considerable advantage from an infrastructural perspective. The more interesting infrastructural disparities are highlighted bold in Table 1.1 below. Beginning with the number of autonomous systems (ASs are the largest networks that connect to each other to allow global connectivity and are owned primarily by firms) in 2001 59 out of the roughly 95 ASs were located in North America (NA). Thus, while NA had only 7% of the world's population it had a significantly higher proportion of the controlling infrastructure. Asia, which had roughly 28% of the world's population – and the fastest cyber infrastructure growth rates – possessed a paltry 11 autonomous systems. The imbalance is even more striking when the number of prefixes and address (IPv4) space is compared.

Table 1.1 Static Internet diffusion by region (%)

Region	NA	Asia	EU	SA	Africa
Area	12	28	6	5	20
Population	7	59	10	3	13
GDP	27	35	24	3	3
Telephones	24	35	29	2	2
ISPs	75	9	13	1	1
ASs	**59**	**11**	**23**	**2**	**0.5**
Prefixes	**69**	**8**	**12**	**2**	**1**
Addresses	**68**	**8**	**20**	**1**	**0.5**

Source: Cooperative Association of Internet Data Analysis (CAIDA) (2001).[16]

It is easy to see why policy makers and strategic analysts in Beijing, for example, are eager to address this infrastructural imbalance. Simply adding more 'users' and nodes to the Internet in a country does not necessarily mean that infrastructure robustness will follow. This imbalance leaves the periphery dependent on the core and is at the heart of many of the international political disputes surrounding Internet governance.[17] This sense of imbalance is in part the impetus for calls from the international community that the US should relinquish control over the governance of parts of the Internet to allow it to elevate to an international institution like the United Nations (UN).

Internet and computing security: situating the state

Accompanying this diffusion has been an increase in Internet security incidents that threaten the integrity and security of the digital networks that drive an increasingly digitized international system.[18] States, firms, civil society groups and individuals face

[16] An Internet Service Provider (ISP) is a firm that provides the 'last mile' connections for most home and corporate users to the backbones of the Internet. An AS is an autonomous system (defined earlier). Prefixes are the first set of digits in a telephone number which are not a country code or area code. Addresses are IP addresses, pools of numbers (IPv4) that are given out by country.

[17] Internet governance, in general, falls well beyond the scope of this study. For more see Mueller (2002). The book provides an introduction to the role of the US in 'governing' the Internet as well as the role of epistemic communities and non-governmental organizations.

[18] I will use the term "Internet security" to refer to a set of issues that surround network integrity. The term "security" by itself will refer to the academic field "international security" which can be thought of as a sub-field of International Relations. The term "computer security" will refer to the academic study of securing networks and computers that draws from computer science and engineering.

uncertainties as their reliance on the Internet and its constituent components and applications continues to deepen. The nation-state in particular is in a unique dilemma as it faces challenges to its autonomy not only from the overt spread of communications and information technologies but also to its traditional function of security provision. Covert challenges to national security from network intruders have increased steadily since the early 1990s.[19]

The central theme or question in the International Relations literature with regard to the cyber infrastructure is: how does the state fit in? The short answer is: not easily. The long answer requires recognizing the multidimensional role that the state plays; as the object of increasing reliance on the cyber infrastructure, the protector of this infrastructure, the initial investor, the sometimes unwilling and at other times willing regulator, and of course a major beneficiary of these new technologies. The state can also be an obstacle seeing this type of technology as a threat to its existence. The state is the ultimate, although often contested, source of authority in cyber space. While the Internet evolved to be self-governing and organic, it is still the state that has both the authority and legitimacy to un-plug. But state capacity and autonomy in cyber space is not necessarily about extremes, it is more about the ability to allow the cyber infrastructure to grow and take advantage of the resulting benefits while at the same time managing the risks associated to this dependence.

Two brief illustrations of the differential effects of network intrusions are a useful

---

19 I will avoid the use of the term "hacker" when referring to those that perpetrate network intrusions. The term is an unfortunate casualty of media hyperbole. The term "cracker" is more apt in the sense that it captures the act of cracking the code to reveal vulnerabilities in machines which can then be exploited either directly or indirectly by a program called an "exploit." An "intrusion" will be used in this study to refer to a clear evidence-based case where a network or machine has been compromised. Furthermore, an "Internet incident" or just "incident" will refer to either an *actual* or *attempted* intrusion by a human or machine.

starting point.[20] First, consider the results from research done on network intrusions at major firms in Western economies. Firms that publicly announced security breeches lost an average 2.1 percent of their market value - a US$1.65 billion loss on average in market value - within two days after reporting incidents.[21] Increasingly the effects of serious network intrusions are not restricted to the targeted firm. After the incidents are reported, the market values of security firms specializing in the technologies to protect organizations in cyber space tend to go up on average of US$1.06 billion (Huseyin *et al.*, 2002). There are interesting questions, therefore, about reporting effects as opposed to intrusion effects not only for firms, but states as well.

Second, consider a more traditional state-based national security target. Beginning at some point in or around 1998 an extended organized pattern of intrusions and probing was discovered taking place against the Pentagon, major US research labs, and other US military sites.[22] These incidents referreds to collectively as "Moonlight Maze", involved the systematic reading and copying of tens of thousands of files over an extended period. During field research for this dissertation government officials from two other countries acknowledged similar cases of serious breaches against military or highly sensitive research sites – some originating internally via a "trusted insider" others externally from remote sites.[23] Unlike the first illustration, the costs associated with this type of Internet incident are very difficult to quantify but are quite easy to conceptualize.

---

[20] A discussion of the tactics, strategies and techniques of system intrusion is well beyond the scope of this study. For more information see Denning (1990) for a good introduction to system intruders, hackers, crackers and culture. Of additional interest is The Knightmare (1994) which is a "how to" manual on breaking into computer systems. The book argues that system intrusions are sometimes more a matter of dumpster diving rather than technical mastery. See also "hacker" based websites: <http://www.phrack.org/> ; <http://www.binrev.com/> ; <http://vx.netlux.org/29a/main.html> ; <http://www.2600.com/> ; <http://www.rootkit.com/index.php> ; and for more general security websites see <http://www.securityfocus.com/> ; and <http://www.securitypronews.com/>.

[21] For more on computer crime issues see <http://www.farcaster.com/sterling/contents.htm>

22 Some reports indicate accidental discovery.

23 Confidential Interviews, August-September 2003.

Cyber infrastructure security incidents

The forms of conflict on the Internet can range from information attacks to the promotion of violent ideologies (Ballard *et al.*, 2002:1007).[24] Adapting a cyber-incident typology used by Ballard *et al* to study cyber terrorism, there are four general types of Internet incidents or attacks. As noted in Table 1.2, an information attack is the use of the Internet directly or as a "force-multiplier" to alter or destroy systems or files. This is the most common objective and result of systems intrusions, and the primary concern for firms that rely heavily on the integrity of data files. Infrastructure attacks are designed to destroy or disrupt actual hardware in communications or control systems.[25] This category of cyber incident is often analyzed in conjunction within broader notions of critical infrastructure protection.

Table 1.2 Cyber Security Typology

Category	Description
Information attacks	Altering, destroying, or stealing electronic files
Infrastructure attacks	Altering or destroying hardware, platforms, and control systems
Facilitation of attacks	Communications to plan attacks or facilitate non-Internet based activities
Disruption	Intention not to destroy or alter but to slow and frustrate

Source: Adapted from Ballard *et al.*, 2002

Facilitation is the most common form of cyber incident that uses the Internet as a communications tool. By using such techniques as encryption via the WWW, email, anonymous ftp servers and Internet relay chat servers, the destructively minded can

24 Large parts of this section appeared in Ortis and Evans (2003).
25 For example, a process management system or supervisory control and data acquisition system (SCADA).

communicate for purposes of coordinating cyber or physical attacks.[26] In East Asia, most incidents involve considerably less spectacular events than high-profile intrusions. I have added disruption to the Ballard *et al* typology to encompass a common form of cyber incident that can be even more costly to an economy than other forms of intrusion. Internet disruption includes the creation and proliferation of viruses and worms that are not necessarily designed to destroy or alter files and data. For example, firms that use an open-mail relay on mail servers to flood the Internet with 'spam' can be classified as disruptions (Ortis and Evans, 2004:253-254).

The frequency of Internet incidents – the attempted or actual compromise of nodes - by either direct human attacks or the creation of artificial attacks (viruses, worms and malicious bots) is steadily increasing. In the early 1990s it sparked the creation of computer emergency response teams (CERTs) around the world which in theory are designed not only to monitor national incidents but to cooperate internationally with other CERTs. In East Asia, for example, there are thirteen nationally-based CERTs with loose regional coordination taking the form of an annual Internet response coordination conference. The US-based computer emergency response team (CERT/CC) published a

[26] Encryption, both the science and politics of, is a vast topic unto itself. For the most part, this dissertation does not deal directly with the politics, international relations, and national security issues surrounding these technologies. This study does, however, presuppose some knowledge by the reader of the use of encryption in cyber infrastructure security. For more on encryption and the politics of code, see as a general introduction to the different algorithms by Ferguson and Schneier (2003). For a textbook introduction see Stinson (1995). One of the most frequently asked questions of the author of this dissertation during field work in Asia and North America was: has the US government (or their own governments) put secret "backdoors" into any of the most frequently used encryption algorithms? My response was invariably "I have no idea." Further to my field response, it should be pointed out that while some US government cryptography and encryption policies have been controversial there is no evidence of secret backdoors or exploitable weaknesses. Users, however, should always adhere to community recommendations on safe encryption. Of course, the only known provably secure encryption technique is the 'one-time' pad. A one-time pad is provably secure in a certain academic sense. However, it is not practical for use in the cyber infrastructure because it needs long keys that can never be repeated and if not used correctly in practice one-time pads can be very insecure because an individual can intercept the message and alter it without the intended recipient noticing - *cautum intransit*. The 'community' standards for secure hashing is SHA-256 (MD5 has been broken, SHA-1 is not far behind); and for a block cipher AES-128 or Triple-DES (with AES preferred), in either CBC or CTR mode; and for private-key authentication HMAC-SHA1; and finally, for public-key encryption and signatures there is DH/DSA or RSA.

report outlining both incident and vulnerability trends for the period 1990-2002 but these trends do not allow for motive or source of incidents. Table 1.3 shows a steady increase of incidents and vulnerabilities until 1998 and then a dramatic increase in 1999, 2000 and 2001. The kinds of vulnerabilities that networks face are also increasing. Despite a renewed effort on the part of software companies to control poor programming practices leading to costly holes in both network protocols and applications, software engineers believe that the number of incidents will continue to increase.

Table 1.3 US Reported Incidents and Vulnerabilities 1995-2005

Year	Reported incidents	Vulnerabilities reported
1995	2412	171
1996	2573	345
1997	2134	311
1998	3734	262
1999	9859	417
2000	21756	1090
2001	52658	2437
2002	82094	4129
2003	137529	3784
2004	-	3780
2005	-	5990

Source: (CERT/CC, 2006)

The data do not show where these incidents took place and against whom. Not all cyber or Internet incidents are random or opportunistic events perpetrated by the archetypal anonymous intruder as conceived in the early and mid-1990s. In an increasing number of instances, the intrusion is deliberate and has a specific target in mind. A recent study by the security firm Riptech shows that the ratio between "targeted" and "opportunistic" system intrusions and attacks may be more even than previously thought. This indicates not just a quantitative difference but also a qualitative shift in the behaviour underlying Internet incidents. It appears to affirm the CERT/CC results

presented in Table 1.3 that attacks are increasingly both in frequency and magnitude (Belcher *et al.*, 2002:13).

The Riptech results are suggestive even if the methodology of its study is rather obscure. It is very difficult to differentiate targeted versus opportunistic intrusions. It is equally difficult to pinpoint the origin of attack, even when employing a combination of passive and active tracing. Specific industries suffered significantly different rates of attack, measured both by intensity and severity. Financial services, media/entertainment, technology companies and power and energy enterprises showed the highest number of attacks per firm with each averaging more than 700 attacks per case over a six-month period. A top-tier group of countries was the source of the vast majority of the attacks. Attacks originating from the U.S. accounted for 30%, from South Korea 9%, and finally China 8%. East Asian countries populated half of the top-ten in this category.

Objectives and limitations of study

This study examines the relationship between rapid Internet diffusion and the emergence of new threats, the digitization of traditional threats and new security actors that are beginning to take advantage of the ability to act at a distance using the cyber infrastructure. I will introduce the securitization-desecuritization puzzle and its application to the Internet's impact on security. In particular, by examining the emergence of new threats, the digitization of traditional threats, and new security actors, I will assess why some Internet security issues make it onto state security agendas while others do not. A main argument in this study is that approaching the Internet's impact on security through the prism of the Internet as a communications media largely ignores its other dimension – the ability to act from a distance.

My objective in this study is to put forward a node-based level of analysis allowing for

a contribution to the 'broadening of security' project that has occupied much of International Relations recently. As opposed to a "network" or "state" level of analysis, a compromised-node framework grounds the research in the technical realities of the Internet that are often overlooked or misunderstood. Finally, I assess these findings against the securitization-desecuritization puzzle in an attempt to understand the linkages between the existential threats posed by the Internet and the performative acts that articulate Internet security issues in several states in East Asia.

To do this, the study is broken down into two parts. Part One will characterize cyber infrastructure security incidents from an international perspective. A quantitative analysis is used to assess claims that there are links between cyber infrastructure events cross-nationally and socio-political instabilities. The roles of state capacity and stability are the primary concepts through which the research situates the state in, what I will argue, is an emerging virtual realism in the cyber infrastructure. Part Two examines the role of cyber infrastructure events more closely by directly examining the non-state and state actors engaged in competitive defensive-offensive strategies. This is interesting because it examines the manner by which states in East Asia 'see' security when confronted with a non-traditional security issue - one that is often treated as a more traditional, often territorially based threat.

Chapter two begins by providing a general introduction to the theoretical issues and the central problem that are the focus of this study: the relationship between Internet based threats, the digitization of traditional threats and the new security actors. The analytical framework and problem under study here is somewhat unusual in International Relations. Given this, a significant amount of the following chapter is devoted to situating this study within the recent literature and outlining the general problem of

increasing Internet security incidents globally. As will be shown below, this study explores security and the cyber infrastructure from the perspective of the compromised node rather than that of the system, state, or network levels of analysis.

Chapter Two: Theorizing Cyber Infrastructure Security

Introduction

This study examines the relationship between rapid Internet diffusion and the emergence of new threats, the digitization of traditional threats and new security actors that are beginning to take advantage of the ability to act at a distance. This chapter begins by suggesting that technology is treated differently in International Relations than it is in other modes of social inquiry. The chapter then moves to a discussion of the dual notions of security in cyber space by making the distinction between Internet technologies as a mode of communications and a mode of control – a control technology that allows for security actors to act from a distance. This ability to act from a distance is influencing a territorialization of the cyber infrastructure along geopolitical lines and how state actors understand or 'see and perceive' security in cyber space.

A key issue is what states see as the referent object of security. Is it geographical territories of information spaces, networks, or individual nodes? The chapter concludes by arguing that a virtual realism is emerging in a digital environment where the gap between threat perception and reality is widening. Explicit empirical claims are being made which link cyber infrastructure instabilities to geopolitical spaces, even though the threats from the cyber infrastructure originate from both state and non-state actors. The question that emerges for state actors is, can the constructs of security in the cyber infrastructure be changed or adapted enough to meet these challenges? Here the chapter introduces the idea of an adaptation space and argues that cyber security incidents and threats are best understood as coevolutionary competitive processes.

Studying the social impact of the Internet

The literature and debate surrounding the impact of the Internet on human behaviour

covers numerous fields and disciplines. In many ways the study of the Internet or cyber infrastructure and social systems has grown out of the study of technology in general and the impact of computers and telecommunications more specifically.[27] Debates over the impact of technology on social, political and economic systems often boiled down to utopian versus dystopian perspectives, community versus social isolation, or of modernity versus post-modern ideas and their associated claims of the death of modernity and the rise of a post-industrial landscapes. Because of this intellectual legacy, it is worth summarizing the key debates and questions raised in this literature in order both to better situate the state in its 'place' in the evolution of the infrastructure and to review how this has been approached by scholars in International Relations.

The role of technology in the transition from the industrial world of the twentieth century to a post-industrial twenty-first century are central themes in the scholarly work the deals with the impact of technology on society. For example, Daniel Bell's research on the post-industrial economy highlighted theoretical and conceptual issues revolving around the emergence of an 'information society'. This concept challenged dominant theories in sociology and economics which were still using the idea of an 'industrial society' to frame research questions. This academic debate over the transition into an 'information society' has informed a number of competing perspectives on the political and economic implications of the cyber infrastructure (Bell, 1999; Miles, 1996; Castells, 2000).

Research on the impact of technology has an intellectual lineage and the studies that it produces are often critiqued for not including the political and economic factors that feedback into the evolution as well as the initial impact of technology. An empirical case

[27] See for example Mesthene (1969) and de Sola (1977:1-9).

can be made that technologies, like the emergence of a cyber infrastructure, make a linear difference simply by shaping patterns of reliance and dependency (Rochlin, 1997), accelerating and enabling globalization (Castells, 2000) and by creating domestic political issues of access to technology and privacy (Dutton, 1999). The impact of technologies such as the Internet also concerns scholars in Communications who ask more basic questions of certain applications of the Internet such as the World Wide Web (WWW). For example, are there inherent biases to electronic modes of communication? Are electronic modes somehow inherently more democratic than older forms of media and modes of communication?

Visions of cyber democracy have been promoted since the 1960s with each new media form renewing debate over the opportunities and threats posed by technology in democratic institutions (Deutsch, 1959, 1963). A key question in this literature is: what are the factors that are important to electronic democracy in areas like government, politics, and the infrastructures of public access to information (Dutton, 1999:173-202; Castells, 2001)?[28] The changes in government and public service delivery have become a focus of policy at many levels and across states.[29] Inventions like direct democracy, for example, is now an accepted topic for experimental policy, and with them comes an increasing reliance on the cyber infrastructure.[30]

The debates in the social sciences seem to shift continuously from deterministic perspectives to technological and organizational paradigms of the networked society (Freeman, 1996; Hiltz, 1978; Teich, 1999; Shapiro, 2000). Questions relevant to students

---

[28] See also Laudon (1977), and Becker and Slaton (2000).

[29] This is especially true in countries such as Canada. There, the federal government has been quietly moving as many services to the WWW as possible (i.e. employment insurance, taxation, human services, and so on). For more see the main portal to the Government of Canada at <http://www.canada.gc.ca>.

[30] For more on governing and public service delivery in the 'information' age, see Bellamy and Taylor (1998), Raab *et al.* (1996), Tsagarousianou, Tambini, and Bryan (1998), and Taylor *et al.* (1999).

of political science and international relations have also been addressed. For example, to what degree are political vicissitudes designed into technology? Is policy embedded in technology? What variables effect their development and diffusion? How can we study the shaping of technological change? This is where the treatment of 'technology' in general, and the cyber infrastructure more specifically, is different in International Relations when compared to other fields of social inquiry. Instead of the utopian-disutopian frameworks, International Relations treats technology as enabling or disabling international actors and processes. It can enable non-state actors like organized crime and civil society groups or enable process based phenomenon like globalization. Specific collections of technologies like the cyber infrastructure can also disable actors like the state or individuals.

International Relations

Consideration of the cyber infrastructure is not entirely new to the study of International Relations.[31] Since the early 1990s there have been continuous efforts to address the effects of the Internet and other information communications technologies on international politics (Latham, 2005; Herrera, 2002; Rosenau, 2002, 1998; Singh, 2002; Deibert, 1997; Papp and Alberts, 1997; Zacher and Sutton, 1996; Frederick, 1993; Krasner, 1991). Long before the broad diffusion of computing, scholars have debated the impact of science and technology on national security (Deutsch, 1959). Technological innovation and transference was seen as an important factor in order to understand change – primarily as a result of war (Gilpin, 1981).

More recently, this focus began to shift toward the Internet and computing and its consequential impact on international order and security (Deibert, 2002a; Arquilla and

31 Throughout this study I will use the upper-case "International Relations" when referring to the academic discipline and the research therein. A lower-case "international relations" refers to actual relations between modern states and events that take place in the international system.

Ronfeldt, 2001; Keohane and Nye, 1998; Castells, 1998; Mathews, 1997). From the earliest theoretical explorations it was recognized that the growth of information technologies would bring about some sort of transformation. James Rosenau pointed out that there are profound shifts taking place in the international system but "students of global politics have not begun to take account of transformations at work within societies" (Rosenau, 1997:17). Falling marginal costs, the spread of digital technologies and the rise of network forms of organization have all contributed to the rapid diffusion of the Internet which in turn has fed back into and spurned the former (Singh, 2002).

But several research questions surrounding the impact of the cyber infrastructure and IR theory remain, not least of which is, as Robert Latham puts it: should "fields like International Relations provide theories for the formation of global [cyber] infrastructures" (Latham, 2005:146)? Latham, the former director of the US Social Science Research Council's Information Technology and International Cooperation Program, argues that the "crucial factor in thinking about the infrastructure logic of the Internet is the *relations among networks*" (2005:149). Latham makes a kind of level of analysis distinction between the network level and the internetwork level (2005:173). Ultimately then, the starting point is not necessarily international politics or international system processes but the infrastructure logic itself - though it should be noted that the ultimate goal is to work up to the former from the later.

If social meaning, laws, norms and behaviour are not defined at the aggregate level of the inter-networking process that is constantly occurring in cyber infrastructure then "the form and character of the Internet will be a function of (1) the interaction of the information and purposes of the networks and organizations that compose it; and (2) the patterns of aggregation [which] favor concentration and power via back-bones and hubs"

(Latham, 2005:174). Herein lies a flip-side to Herrera's notion of indeterminancy (discussed below) - the logic model put forward by Latham seems to suggest that the evolution of the Internet did not really have an overarching social purpose or rationale built into it, and thus is open to contestation of many purposes by all actors in the international system. Latham's model is useful in exploring the historical evolution of the infrastructure, especially the interconnectivity between states, but brings researchers in international security studies only incrementally closer to a *modus operandi* for a working theory of the cyber infrastructure.[32]

Theorizing the cyber infrastructure and International Security

As the Internet has evolved over the last decade its impact on security has been multidimensional and controversial. Threats from cyber space have garnered much popular speculation in the media. The speculation is sometimes insightful but often prone to hyperbole. Scholarly research on the subject has generally employed two distinct approaches. The first is to assess the security implications on technical-behavioral grounds. The second is to understand the way the problem is rhetorically framed and how it is eventually perceived through discourse. Ralf Bendrath has argued that most researchers working in the social sciences have chosen to work the ground of the latter rather than the former.[33] This is not surprising given the background required to

[32] To be fair, this was not the purpose that Latham (2005) set out for in this particular line of his research. Latham appears to be after a kind of genetic logic of the infrastructure which could then help explain the scale up problem. Here, Latham draws heavily on Metcalfe's theory of network effects $V = N^2$ to illustrate an underlying logic of interconnection between states. Briefly, Metcalfe's formulation suggests that the value of a network (V) is equal to the number of nodes (N) connected to it. The number of nodes (N) is squared in order to capture the maximum amount of interaction between nodes. Latham builds onto Matcalfe's formula by adding the interaction of information (I) to a network to get $V = N(I)$. Thus, Latham's modification can better account for the reality that not all network interactions are maximized (2005:158-161, 171). This relationship sits at the core of Latham's attempt to explain transboundary *internetwork* formation. The question of how transboundary connections scale up, however, remains elusive because, as Latham admits, the logic of infrastructure formation appears to be ill equipped to move beyond the network level of analysis (2005:173).

33 This interdisciplinary or transdisciplinary problem produces a tricky pedagogical dilemma: how to train

build research designs to explain a very technically driven set of security dilemmas (Bendrath, 2003:52-53).

Immediately after World War I it became clear that technological change and war are closely related and that many technological advances come as a result of military requirements demanded by the state (Ogburn, 1949). Beginning with research in the mid-twentieth century the work of Karl Deutsch, whose rich quantitative research and ground breaking measurement of information flows, serves as a starting point (Deutsch, 1963, 1966). Deutsch approached the subject of technology and security cautioning against the overestimation of its potential impact on international politics without first systematically observing technological change itself (1959:669-670, 680-681). For Deutsch, technology played a subordinate role to politics. He concluded that the state's capacity to deal with subsequent national security problems would likely adapt and evolve over time.

By the late 1960s and early 1970s theories of war and conflict in International Relations began to draw heavily from Geography. Geopolitical theories suggested that as technology both develops and diffuses throughout the international system – together with other factors such as population growth – states would begin to seek greater access to resources and as a consequence the likelihood of armed conflict would increase. But the impact of technology always appeared to be a two-way street: the potential for conflict along with possibilities for peace. Even at this early juncture, electronic communications and computing technology were beginning to 'blink' faintly on scholarly radar.

Quincy Wright, who underscored the association between political and technological change and its impact on war, postulated that technology narrowed the communication

---

students in the social sciences whom generally have very little background in computer science or engineering? See Nielsen and Welch (2003).

distance between societies. Technology becomes an important 'factor' in understanding the growth of state power and therefore technology's potential to contribute to both the growth of states and the shrinking of distance between peoples, but also increases demand for more resources. In other words, for Wright and others technology makes it more necessary that conflict be resolved through means other than war (Cohen, 1973:28-32).

Two groups of general arguments that emerged in the late 1990s are relevant to this study. The first see the Internet and information technologies as a type of fundamental change that is rendering the state less capable of managing security. As an example, Rosenau attempts to situate technology and its transformative capabilities when looking for a causal dynamic in broader processes like globalization. He writes "it is technology that has profoundly altered the scale in which human affairs take place ... it is technology in short, that has fostered the interdependence of local, national and international communities" (Rosenau, 1990:17). If technology is an important driving force behind the processes like globalization, then the Internet 'fits' into the etiology by reinforcing and enabling its effects such as undermining governments and state borders. Information flows freely and information is power. For Rosenau the Internet has helped to trigger a long process of change, by which the lines between nation-states are currently fragmenting, a process that could play out toward the emergence of what he calls spheres of authority (SOAs). Thus, by implication, it appears that state-centric models alone can no longer explain international phenomenon.

If state-centric models of security are less powerful, is there something more appropriate to replace or supplant them? One such effort by Ron Deibert compares four competing images of security in the context of rapid Internet diffusion: private security,

state security, national security and network security (2002). The preservation of information between communications and control systems like the Internet becomes more important than state-centric perspectives and instead favors a network-centric "image" of security. Arquilla and Ronfeldt, while not after a new level of analysis for International Relations and security studies, support similar network centric ideas of what constitutes security (2001, 2003).

Deibert, Arquilla and Ronfeldt have this in common: the Internet has the inherent capability of increasing state vulnerability. For Deibert, working in an activist mode, this is a good thing which represents a window of opportunity to use the Internet's unique architecture to develop applications that circumvent state control. For Arquilla and Ronfeldt, this could be a bad thing. Arquilla's most recent openly available work with the US Navy at the Monterey Institute is designed to protect the state and its agencies from the darker side of the Internet by finding ways to defeat cyber adversaries be they other states or non-state actors (Arquilla, 2001, 2003).

The most important commonality in this vein of the literature is the observation that there are an increasing number of actors that have been enabled by information technologies. The Internet and its constituent components and applications have increased the importance of non-state actors in matters of national and international security. The assumption here is that these actors become both challengers and new providers of security usually because they have adapted to the new network environment faster than state institutions and organizations (Pool, 1990; Castells, 1998; Arquilla and Ronfeldt, 2001; Deibert, 2002; Deibert and Stein, 2003). Still an even stronger form of this argument, although increasingly in the minority, suggests that the rise of the "virtual state" and the primacy of network forms of organization mean a decline in state-to-state

violence and a gradual reduction for the role of state-based security provision (Rosecrance, 1996). This reduction, however, comes with the potential for an increase in non-state violence directed either at the state or at other non-state actors, or both. It is important to emphasize that the perspectives in the previous theoretical "camp" do not necessarily predict the demise of the state. Rather that the changes brought about by technologies such as the Internet require a re-thinking of the strict state-centric models of security. This is not a new mantra in International Relations.

The second group of perspectives on the Internet and security pick up where the more abstract theoretical discussions of the former group leave off. In contradistinction to the first group, the second approach the problem of security by first considering the technological environment in which these contending forces play out and their potential to affect and effect real, physical spaces. Their general conclusion is that Internet-based security threats are over-blown. An example is the argument that Internet security enabled issues like cyber terrorism are simply "synthetic issue[s], easily correctable, and not deserving of the attention forced on the public by the press and would-be solution mongers" (Desouza and Hensgen, 2003:386). The security purist here would contend that unless the instruments of the cyber world can be used as the primary tool to cause direct damage it can not be considered as part of hard security threat environments and more broadly, a direct threat to national security (Libicki 1997, Denning 2001, Desouza and Hensgen, 2003:386). Internet based threats do not yet have the capacity to kill – in large numbers - but they can certainly cause great economic damage (Bendrath, 2003; Denning, 2003).

Others make similar arguments that the potential uses of cyber warfare by the state and cyber terrorism by non-state actors do not constitute a real threat to security or, at the

very least, that these network based threats are overstated (Embar-Seddon, 2002). But a closer examination of both the definitions commonly employed to form typologies of cyber terrorism and their prognostication for the potential for acts of cyber terror reveal that the infrastructure – at present – would be used more as a potent force multiplier than a method for directly causing death and destruction (Ballard *et al.*, 2002: 990-993). Uses of the cyber infrastructure by anti-state forces aim to achieve a means to an end by facilitating terror activities in an environment where the state security apparatus appears flat-footed and weak (Stanton, 2002). Here, the state is not just an imperfect actor, it is an incompetent one.

Dual notions of cyberspace and security

The key here is to view this new environment and its constituent technologies both as a communications and control technology.[34] Students of International Relations – especially security studies – should appreciate this distinction and thus the historical uniqueness of these technologies. Never before has the ability to remotely control material objects rested with so many. The Internet allows for ordinary individuals to possess the capability that was once the domain of the state or very wealthy individuals, often connected in someway to the function of the state, to destroy remote locations. This leveling of the playing field using the cyber infrastructure raise important questions, not least of which is: in an era of growing cyber technologies does the idea of security also enlarge and change for the state? Analytically, should the state be considered an object of security or a provider; or both?

The broadening of security to incorporate the Internet and 'cyber space' must be more than adding technology and then stirring. Treating the cyber infrastructure as a new

[34] On historical evolution of communications technology versus control technology see Hall (2000:22-31).

dimension or layer of international security requires a new framework to address it. Such a cumulative analytical process will keep technology like the Internet as an exogenous variable without allowing for a new assessment of the referent objects and providers of security. A more extreme analytical stance would see the state taken out completely as new/old questions about security "for whom?" and "what is being secured" are redux to become the "what and where is the threat?". The more careful analytical approach would be to remain open to a broadening of the notion of security but keep the focus on empirical evidence and the referent object the state. There are good reasons for this.

First, very little is actually known about the 'real' threats to cyber infrastructures themselves. A who's-who list of both state and non-state actors has been identified to have malicious or threatening intent, ranging from bored teenagers to other states. The result has been a wide gap between threat perception and reality. Claims made regarding threats often pay little or no attention to the infrastructure itself. Can the technology really facilitate such threats? Is the infrastructure itself becoming more amenable to actors who wish to use it as a platform? How would we know if more of the infrastructure's nodes were being compromised by new or old security actors?

Critical infrastructure protection is another dimension of the Internet's impact on security and here again one that finds similar theoretical polarities. For example, Lewis's analysis of critical infrastructure vulnerabilities from Internet based attacks used a unique methodological approach to compare infrastructural vulnerability issues with routine failures in the past, drawing from the strategic bombing literature. He argued that computer network vulnerabilities are an increasingly serious economic problem but that their threat to national security has been vastly overstated (Lewis, 2002).[35] Critical

[35] For example, Matthew and Shambaugh (2005) use network theory to study the ways in which networks limit the breadth of non-traditional challenges to state security. It is resiliency, they argue, that favors the

infrastructures, especially in market economies are more heterogeneous making them less vulnerable to Internet based attack. In most cases, Lewis argues, cyber attacks are less effective and less disruptive than physical attacks. Their only advantage is that they are cheaper to carry out (2002). What Lewis fails to account for is that under increasing free market pressure much of the cyber infrastructure is beginning to concentrate and centralize. This is an unexpected result of the externalities of market economies: instead of many smaller infrastructure stakeholders (embryonic stage of the Internet) there are now fewer, larger owners of national cyber infrastructures (current stage of Internet).

Geoffrey Herrera's argument more clearly illustrates the hesitation in the literature. For Herrera, as the Internet continues to evolve it will slowly reduce both relative state capacity and autonomy (Herrera, 2002). Herrera frames this process as relative to other actors but attaches an important caveat: the real effects of Internet diffusion, he argues, are actually quite indeterminate for two reasons. First, the technology itself is far from complete; and second, the technology itself is "inextricably intertwined" with politics (2002:120-121). Herrera argues that increasingly transnational efforts to deal with the problems poised by insecurity in the digital world will be developed.[36] Responding, in part to the first group of perspectives reviewed above, Herrera and others have grown increasingly frustrated with theories that fundamentally misunderstand the nature of the digital environment and in doing so assume prematurely that the architecture is beyond the reach of state-based organizations to control and regulate. This, they argue, is not the case (Herrera, 2002; Lessig, 1999). This perspective appears to echo Deutsch's much

---

defender and past a certain threshold, actually hinders the coordination of attacks. Matthew and Shambaugh conclude that over the long-run, challenges to state security from various non-traditional and traditional network-based threats such as cyberwarfare and infectious diseases and terrorist strikes are overstated.

36 There is increasing evidence to suggest that Herrera may indeed be correct. A recent example from the Asia region is the 12-nation multilateral talks taking place in Australia in June 2004. These meetings, involving countries from Europe and North America, are laying the ground work for increasing inter-governmental cooperation on Internet security issues like critical infrastructure protection and cyber crime.

earlier observation and caution regarding the state's ability to cope with technological change. The state is adapting its role – however slowly - as supreme provider of security in the digital world (Fountain, 2001).

The Return of the State

The starkly defined positions both in the theoretical and policy literatures miss an important development in international relations: the Internet has gone through or is currently going through a period of "securitization" (Eriksson, 2001a and 2001b; Williams, 2003). It is becoming an infrastructure in its own right (Denning, 2003; Bendrath, 2003). In this sense, cyber infrastructures are physical things that have a territorial existence. The securitization of the Internet means, among other things, that the state and other actors see threats to the cyber infrastructure as originating from "outside" their territory – even if the threats often originate from within. In geo-strategic terms the Internet actually becomes an invaluable "overlay" on geography (Gray, 1996a:251-252; 1996b:276). Threats from the Internet and to the Internet are no longer associated with the stateless cyber geographies of the "hacker" but from real, often geopolitical, territories. The result is the territorialization along geopolitical lines of the cyber infrastructure and how state actors understand it. Many governments are beginning to frame the problem within context of territorial integrity and therefore assume that technology does not make geography irrelevant – a distinct shift from the thinking in the early to mid 1990s.

This territorialization of the cyber infrastructure and subsequent responses to threats to information territory heralds the emergence of virtual realism.[37] Virtual realism means

[37] Michael Heim (1998) appears to be the only one to use the term virtual realism Heim's concept is based on an artistic interpretation of utopian (idealist) and disutopian visions of virtual reality. It is not, as far as I can tell, based in IR or political realist thought. Heim argues that there should be balance between the cyber idealist's enthusiasm for computerized life and more deep grounding in primary reality. This "uneasy

that states treat threats to and from the cyber infrastructure in a more traditional manner. Almost every country makes some sort of commitment to constructing information infrastructures that are considered empowering. Yet states are at some level aware of the potential danger that the growth of the cyber infrastructure produces negative externalities and therefore look for ways to regulate this space. Virtual realism mirrors the precepts of IR realism. Virtual realism assumes the worst and that international relations, where the cyber infrastructure is concerned, are fundamentally conflictual. In cyber space, states seek to maximize national interests; and the primary actors are, in the end, other states. The structure of cyber space strongly informs the behaviour of states acting as both an enabler and a restrictor. International institutions that inform and influence the cyber infrastructure are important actors in and of themselves; but they are reflections of states pursuing their own interests. *A priori*, then, the various institutions and mechanisms that have shaped the cyber infrastructure are only relevant in the sense that states have just begun to take an active interest in them.

This is an important insight for this study. The nature of the infrastructure is such that traditional approaches to security studies because of their territorial orientation meet with mixed results. This is, of course, due to the digital environment. Network intruders can appear to be originating from anywhere and then from nowhere. Yet, there have been cyber infrastructure security constructs that rely heavily on the link between territory and threat. These constructs or ideas of security threats come from state actors and corporations that supply cyber infrastructure security knowledge and information to policy makers. One example is particularly stark. During a recent conference on cyber infrastructure security held at Oxford's Internet Institute (OII) in February 2005 an

---

balance" he calls virtual realism (Heim, 1998). I cannot find this term after searching the IR and Political Science literature, after having searched of my own files and online databases of journals, and the ISA conference paper archive.

interesting development in the discourse on cyber security emerged. DK Matai the executive director of mi2g -- a private company that specializes in cyber security and intelligence gathering -- gave a talk in which the claim was made that there are links between cyber attacks and 'real' world cross-national factors. Drawing on mi2g's proprietary databases and research, Matai argued "when we [mi2g] overlay digital attack data with physical attack information, interesting patterns begin to emerge." The patterns, according to Matai, link aggregate socio-political features of states, such as regime type and stability, to the preponderance and timing of cyber attacks and infrastructure instability. He went further arguing that the "higher the number of digital attacks originating per capita the greater the political and social instability in that country. Russia, Turkey, Brazil, Saudi Arabia, Egypt, Morocco and Pakistan all fall into this category" (Matai, 2005). This study returns to empirically assess this conjecture in later chapters using non-proprietary large-N data.

The security of the cyber infrastructure is often a confusing mix of threat perceptions and rhetoric combined with underlying uncertainties surrounding the growth and evolution of technologies used in the infrastructure. International Relations does have some theoretical tools that can be applied here. The Copenhagen school first introduced the idea of securitization in the early to mid-1990s (Buzan, 1991; Waever, 1995). Here security is an idea that is rhetorically articulated rather than just existing as a material thing. An existential threat is usually identified or discovered rather than constructed in a particular way which can then be followed by action(s) that are required to protect from the threat – sometimes justifying the use of extraordinary measures. The utility of this approach when applied to the Internet and security is that it allows for a more precise articulation of perceptions of Internet threats on security relations. The approach is very

close to both Deibert's notion of security images and Bendrath's exploration of memetic change and evolution in the rhetorical uses of "cyber security". Similar to Williams' general conclusions on security studies, the process of securitization of the Internet has fused the political with the "production" and "transmission" of Internet security images. Therefore, studying the Internet's impact on security requires more than a focus on speech-acts or network security images. It requires efforts be devoted to understanding the mediums and structures themselves (Williams, 2003:512).

Returning briefly to the two "camps" discussed above, Deibert, Herrera and Bendrath, while arriving at differing conclusions, share this indeterminancy of threat ideas that are tied to the infrastructure. The crucial issue for securitization theory and the Internet's impact on security is assessing the links between the "performative" acts and the existential threats themselves (Williams, 2003:526). In other words, the threats to cyber infrastructure are often constructed in a particular way to be threats to national security as opposed to economic or individual security. This, in turn, allows for governments to securitize rather than criminalize cyber infrastructure incidents and also expands the range of policy tools that can be employed against potential threats.

Internet based threats are more prone to securitization than traditional threats because they are difficult to understand, hard to measure, and even more abstruse to anticipate. This uncertainty is the central conundrum that motivates the exploration of the two dimensions of cyber infrastructure security that were chosen for this study. The first dimension is the distribution of compromised nodes. This is essentially a look at the structural or global network environment in order to examine the distribution of threats cross-nationally and within a particular regional security context. The second dimension seeks to assess the threats posed by non-state or uncivil society actors. Here the study

continues in the East Asian security context to look at the digitization of transnational organized crime. This is particularly useful because it allows for a better understanding of how state capacity is responding to a specific group of Internet enabled non-state actors – a group that some have argued should be viewed as a threat to security because of their rapid adaptation to the cyber environment. In short, as opposed to viewing cyber infrastructural security as either a strictly territorial or strictly non-territorial problem, the technology has created security dilemmas that exist as both simultaneously.

This idea of a duality in impact of 'cyber space' on security is close to Herrera's notion of an emerging "double-move" in international politics. Herrera argues that one can "observe in international politics today a simultaneous double-move: the territorialization of cyberspace and the deterritorialization of state security. In other words, the claims for the placelessness of cyberspace are overstated. This double-move is neither inevitable, nor necessarily desirable. But it is clearly in evidence in contemporary world politics and its existence exposes the fallacies of traditional ways of thinking about technology and its relationship to international politics" (Herrera, 2006:2). This thesis will argue that there is indeed a territorialization of the cyber infrastructure, but that this has not necessarily changed the way states 'see' security nor does the cyber infrastructure require a complete, as Hererra puts it, "deterritorialization of state security"(2006). In other words, there is both a simultaneous deterritorialization and territorialization of security in the cyber infrastructure – not one or the other.

Coevolutionary competitive processes and compromised nodes

Regardless of where one is positioned in the debate it is safe to assume that the Internet brings some sort of pressure to bear on the functions of the state: i.e. to provide national security, to regulate economic activities, and to protect and promote civic and

moral values. Clearly individuals have access to a wealth of information and influences more so now than at any other time in human history. Various applications of the Internet are responsible for this process. Electronic mail, databases, and the World Wide Web (WWW), to name only a few, have all contributed to the relative decline in capacity with which the state can protect and promote civic and moral values and control information.

The contemporary escalation of incidents and the vast array of technologies and strategies being developed and deployed by states, firms, civil society groups, and individuals, to combat the problem of compromised Internet nodes would have shocked early Internet pioneers. Firewalls, intrusion detection systems, network telescopes, artificially intelligent servers and topologies, self-healing networks, honey nets, and biometrics are all evolving to keep the good information flowing and the bad guys out. The behavior between systems intruders and those that design policies, strategies and technologies to defeat them can be described as a continuing series of coevolutionary competitive processes analogous to arms races. The battle to keep the nodes safe takes on the characteristics of an asymmetric arms race of attack-defense where offensive adaptations are countered by defensive adaptations. Nodes are compromised, strategies and technologies are developed to harden them which in turn spurns on more sophisticated counter moves.[38]

It is important to note that the definitions and uses of symmetrical and asymmetrical competitive processes vary between those of international security studies (i.e. military arms races) and those of evolutionary theory being considered. Symmetrical arms races emerge when two actors compete at the same thing, for example, the nuclear arms race

[38] A more recent and specific example is the development of polymorphic shell coding used to avoid intrusion detecting systems (Confidential Interviews, Vancouver 2005-2006).

between the Soviet Union and the United States during the Cold War.[39] According to Langlois and Catherine (2005) an asymmetrical arms race emerges when there is predatory behaviour against primarily defensive adaptations.[40] The nature of cyber infrastructure security is predominantly populated by asymmetrical arms races between those trying to secure infrastructure and those trying to compromise that same infrastructure. The former group is almost always on the defensive while the latter has the luxury of always being on the offensive. Both states and non-state actors can find themselves in either position – often simultaneously.[41] Upon closer examination, however, there are specific peculiarities of adaptation patterns of both state and non-state actors in cyber environments.

The most important peculiarity for defensive adaptation groups – state actors – is that during an asymmetrical arms race the fastest adaptation will only produce a static outcome. In other words, it takes all the effort of an actor just to keep up with the threats. Thus, the adaptation space, or gap between offensive and defensive actors, remains constant, neither widening nor shrinking if the defender is 'running' flat out. In evolutionary theory this is referred to as the Red Queen effect. The "Red Queen" hypothesis – the Red Queen is taken from the children's story 'Alice in Wonderland' - is used to describe two ideas. The first is that coevolution could lead to situations for which the probability of extinction, or failure to adapt, is relatively constant over time. The second, a species has to "run" and evolve in order to stay in the same place or maintain

---

[39] It is important to point out here that there are few, if any, pure symmetrical arms races left in the contemporary international system. There are, however, still asymmetric arms races such as PRC-Taiwan, Pakistan-India.

[40] For an example of how researchers in International Relations define arms races please see Langlois and Catherine (2005:506). It is important to point out that no real deterrence effect exists in cyber infrastructure security and that part of my objective here is to demonstrate – if only in an informal manner - the existence of inefficient equilibria.

[41] An example would be the state which is trying to adapt to pressures to its cyber infrastructures while at the same time developing offensive cyber warfare tactics and strategies.

ground.[42] One of the impacts of the Red Queen effect is that it makes it very difficult to assess whether or not any real progress is being made in an actor's strategy. Many coevolutionary processes are susceptible to the "Red Queen effect" and the relationship between those trying to secure Internet nodes and protect them, often succumb to this effect.[43]

In an asymmetrical arms race the implication for states, firms and other actors is that stamping out Internet security threats or obtaining victory against network intrusions is unlikely. The optimal strategy is to find a temporarily stable equilibrium point. A simple example would be state based property rights enforcement and subsequent attempts to stamp out online file sharing or peer-to-peer networking strategies. Firm-based organizations like the US Recording Industry Association of American (RIAA) have developed a set of novel approaches drawn from pollution strategies where the networks are loaded with bad files to a point where file sharers get frustrated and leave. In other instances they have built robots that will seek out and destroy a users machine that have a certain quantity of "pirated" data. But because this is a coevolutionary type of process where the red queen effect is present the RIAA strategies to achieve complete disruption of P2P networks is an improbable outcome. The optimal point or outcome will likely be some sort of stable equilibrium or a "mediocre stable-state" which is not, over the long run, self-sustaining. The Red Queen effect might suggest that this is a result of a moving equilibrium because of adaptive counter-strategies. These type of pursuit strategies and evasion strategies in the realm of Internet security lead to outcomes which are acceptable but far from optimal for all actors.

---

[42] Keep in mind that in evolutionary theory adaptation involves generational sequences. And that evolution selects on populations not individuals. My purpose here is to adapt these concepts to describe, in general terms, how this dynamic behaviour in cyber infrastructures takes place.

[43] During many confidential interviews with law enforcement personnel and policy makers in East Asia conducted for this study the sense of never being able to get ahead was often expressed.

When systems administrators take measures to secure nodes that are not necessarily optimal, or software and hardware vendors issue patches that are not preemptive, mediocre stable-states emerge. These are sub-optimal for a plethora of socio-economic and political reasons. One of which is political where the state pursues adaptive strategies that address cyber security threats in part to try to satisfy domestic stakeholders (individuals, corporations, and other state agencies) but does not pursue full maximization strategies in either a domestic or international context.[44] This typically results in slowing the adaptation pace for network intruders but only for a finite period of time -- a type of Nash equilibrium called a collusive equilibria.[45] The cyber infrastructure relies on its 'internationalness' to provide benefits to the state. Both the international system and the cyber infrastructure itself -- from the perspective of the Internet -- are essentially anarchical.

A set of important questions emerges from this discussion. First, how do competitive, selfish processes like this end when they are deeply embedded in both the technologies and socio-political processes themselves? Second, how are they won or is it even possible to win? One possible answer is that there are three general outcomes to coevolutionary processes: they simply 'peter-out' over time; they are won or lost, or a kind of détente is reached.[46] Using the same ecological metaphor Anil Somayaji, a professor of computer science, argues that the "best we can hope for is to stay in the

---

[44] This is basically a problem of two-level games that policy makers must often play. In predominantly Western countries this also involves tensions between securing cyber infrastructures while at the same time preserving privacy and freedoms.

[45] Interestingly, Nash equilibriums can also be observed in the infrastructure as well as, and not just from, social processes that emerge from its use. For example, a data flow in the cyber infrastructure is at Nash equilibrium when all are routed on a minima latency path called a Nash flow (Roughgarden, 2003). But research in network engineering suggests that Nash flows do not minimize total latency because of network anarchy in the cyber infrastructure. Instead, a Nash flow is the outcome of selfish routing, trying to get the best out of the infrastructure. The price of this anarchy, as Roughgarden shows, is completely independent of the current network topology (2003:341).

[46] Through the modern and contemporary international system arms races have usually 'petered-out' and not led to conflict.

game no matter how the adversaries change and adapt because we're faced with adversaries that can potentially deploy attacks faster than we can deploy defenses, even if we use automated update systems [including artificial intelligence]" (Somayaji, 2004:70, 71). Somayaji argues that it may be desirable to pursue radically new strategies to change the game entirely by adapting evolutionary theory ideas of propagation and death to the cyber infrastructure (2004:72). At this point, the Red Queen effect begins to dissipate. While it may, in the future, be possible for scientists and engineers to adopt radical new strategies that can, on technological grounds, "change the game", the state and other non-state actors are not in a position – do not yet have the capacity – to change the nature of the game. But can the constructs of security in the cyber infrastructure be changed or adapted enough to meet these challenges? The adaptation space between state responses and threat perception can be in several positions: either widening, nominal or narrowing. One of the keys to understanding this process is to clearly identify what is being secured: Is it the state, the nation, the corporation,[47] the individual, the network, or the individual node in cyber space? This study will begin with individual nodes in the infrastructure, the subject to which the chapter now turns.

Studying Compromised Nodes

The "network" is an abstraction. When a network is "hacked" it is a node that is compromised which in turn may or may not compromise the more abstract connections of nodes called a network. Networks are generally concerned with securing against threats and attacks from outside the network. However, they also are increasingly designed to secure against compromised machines that are inside a network. By definition if a node inside a network is compromised the rest of the nodes inside that network are at much

[47] The firm level (corporation) is added to this list because most of the cyber infrastructure is owned by corporations, not by states, a point that is often understated in discussions of 'critical infrastructure protection' more broadly.

greater risk. Internet security incidents are really compromises of firewalls, servers, SCADA[48] or other devices. These devices are nodes which in turn communicate with other nodes producing a network. The communicative sense tends to dominate the "discourse" of re-inventing security in an "information age". Yet IR has focused this re-examination almost exclusively on the Internet as a communications technology; a technology that allows for the ability to exchange complex forms of data – the ability to talk at a distance. Viewing the Internet through the prism of a communications media largely ignores its other dimension – the ability to act at a distance.

The network level of analysis used by Deibert and Arquilla represents an interesting and useful advancement in the study of the Internet and its impact on security. Network levels of analysis draw from social network analysis in sociology, network analysis in engineering, and graph theory in mathematics.[49] One of the beneficial claims that is made to justify this level of analysis is that it may be applied to "hacking" terrorist networks and improving network centric warfare in order to 'fight back'(Deibert and Stein, 2003; Arquilla and Ronfeldt, 2002). In the face of threats from both physical and social networks it is argued that "we need appropriate conceptual language to understand what a network is, how it operates, how it thrives, and how it withers, if we are not to misunderstand the threat or misconceive the response" (Deibert and Stein, 2003:157). Network levels of analysis share one common feature across disciplines and applications: they are pure structural approaches, which tend to ignore individual agents or actors.

A compromised node level of analysis begins with the assumption that networks are

[48] Recall that SCADA is an acronym for supervisory control and data acquisition. These devices are essentially machines that can control the physical world from within the cyber infrastructure. For example, SCADA are often found in electricity grids.

[49] In military and intelligence circles the term Nodal analysis is used to mean the determination of linkages and relationships among disparate entities. The intellectual lineage here is social network analysis used in sociology. It is a very structural approach which allows the observer to, in theory, look for patterns based on no observations of previous activity. In intelligence analysis, nodal analysis allows the analyst to deal with individual names of people in order to try to understand vulnerability and linkages.

not attacked; nodes are attacked. It is the node not the network that is both the vulnerability and the opportunity in Internet security. Conceiving the network as actors or agents unto themselves suggests an unnecessary equality among a distribution of nodes. Deibert and Stein make this error when they argue that "in the pure model of the network, such as the Internet, eliminating one node of a network does not imperil other nodes" (Deibert and Stein, 2003:160). This is not the case. Some nodes are more important than others. The Internet is full of critical nodes whose failure can place many other nodes in immediate peril. In the wide area network (WAN) sense if a border gateway protocol router fails (BGP) it can "blackhole" any number of local area networks. In the local area network (LAN) sense failure or compromise of a firewall, IDS, or router can immediately open other nodes to peril. This is the central dilemma of Internet security; when one node fails or is compromised it immediately threatens others. This "inside" "outside" problem is often rhetorically grafted onto national cyber security issues by framing the problem as threat from outside the state's geographical border.

The Internet – recall from the introductory chapter, is a collection of networks – is "scale free" in structure and form which comes with a certain amount of redundancy. Indeed, it is very difficult to imagine a threat to the Internet infrastructure itself. One cannot "hack the Internet" in its present form or "take it down".[50] This does not contradict the notion of vulnerability presented above. It simply means that while individual networks are vulnerable once a key node has been compromised, no one set of networks or nodes can be seen as critical to the Internet's operation.

Conclusion

The motivation for using this level of analysis does not originate from a need or desire

50 In theory, even if all of the root domain name servers – part of the Internet's plumbing -- were to somehow be compromised, the Internet, or more specifically applications of the Internet like the WWW, would still have some level of functionality.

to replace other security frameworks or theories but seeks to add to the current analytical tools available to researchers in a cumulative manner. In this sense, the framework presented here is necessarily incomplete. The rapid deep diffusion of computer networks and the rise of the compromised node have produced new security dilemmas and amplified the role of new security actors. These new node-based security actors behave as both a threat to the state, as in the case of organized crime usages of computing technologies, and as surrogates to the traditional role of state-based providers of security. Does the distribution of compromised nodes reinforce territorial based perspectives on security? Or does the data point to a world where security in the cyber infrastructure knows no boundaries or border? It is to these questions that the dissertation now turns.

Chapter Three: Examining the Distribution of Compromised Nodes

Introduction

The link that Matai suggests between social, political and economic instabilities and cyber infrastructure security events is a particularly tempting one for practitioners and policy makers responsible for securing cyber space. It raises the possibility of better predictive power: as social-institutional instabilities increase so to does the threat to cyber infrastructures from these states. Another implication for cyber security theory is that by linking factors like wealth, regime type, and levels of social stability to the integrity and behaviour of the cyber infrastructure theoretical concepts like cyberterrorism gain a conceptual cantilever to move from the abstract hyperbole level to the concrete - usually via inferences made from *prima facia* cases. Matai's OII talk generated controversy and has renewed debate over the connection between geopolitical instabilities, state capacity, cross-national factors and cyber security.

Cyber security practitioners and former intelligence policy makers were quick to respond. Richard Clarke, the former White House cyber security advisor, criticized Matai's use of the term cyberterrorism and the link between seemingly disparate factors. Bruce Schneier, chief technology officer of Counterpane Internet Security echoed Clarke's critique of Matai's theory (Ilet, 2005; Sturgeon, 2005). So, why the concern regarding a hypothesis articulated at an academic event? In short, cyber security is a field – especially threat forecasting – which can influence policy; thus assertions like the Matai conjecture. One media response to his OII talk illustrates this point more clearly. The interviewed source quipped, "we could just laugh this off as barmy, were it not for the fact that government, the City and now Oxford University actually take this self-appointed guru seriously. That's where I stop laughing and start worrying about the

direction things are going" (Sturgeon, 2005). Indeed, Matai's conjecture is a significant departure from conventional wisdom which suggests that there is no link between territorial geography and cyber infrastructure instabilities like attacks. But Matai makes it quite clear that mi2g has in its possession the empirical data to support the conjecture using in part "profile databases on over 7,500 hacking groups across the world" which draw from "the world's largest digital attack database" (Matai, 2005). But, the problem is that their data remains proprietary, closed and not available to other researchers or to policy makers.

Closing the gap between threat perception and reality in cyber space is well beyond the scope of this study. It is, however, possible to test parts of the Matai conjecture to look for links between real world instabilities and cyber security events. Using unique data obtained from a widely distributed logging system, Chapters Three, Four, and Five of Part One test for the suggested relationship between incident patterns and several socio-political, economic and infrastructural variables. This is the first study to address this problem from an international perspective using openly available quantitative data collected via intrusion logs from networks distributed throughout the world. The primary objective here will be to develop a snapshot of Internet incidents – specifically from compromised machines – by country and to explain the variations in these patterns.

Territorial integrity and securitization of cyber infrastructures

The nature of the Internet is such that traditional territorial-based approaches to security studies meet with mixed results. This is, of course, due to the environment. Network intruders can appear to be originating from anywhere and then from nowhere. Yet, there are often geographical patterns to Internet incidents in an environment that is assumed to be non-territorial. Countries that experience high levels of Internet incidents

and have high levels of Internet technology diffusion tend to be more concerned about the impact that network intrusions have on their security. An increase in the number of compromised nodes in a country's cyber infrastructure is associated with an increase in the number of Internet incidents globally. The problem is that while reducing the number of compromised nodes in a geographic domain, like a state, may decrease the number of incidents both in the immediate geography and globally, it does not, however, reduce the threat from compromised nodes that exist in other states. Alone, domestic efforts to reduce the number of compromised nodes have resulted in only marginal reductions in Internet incidents.

These features of the Internet point to an important problem: the digital insecurity in one state contributes to the insecurity of other states. This is a security dilemma that, interestingly, emerges from a non-traditional asymmetric threat. An increasing number of compromised nodes in one country produce security pressures on others. In this environment, the threats from "cyberspace" can be couched in actor-based frameworks. Terms like "cyber warfare" and "cyber terrorism" allude to threats from the state and non-state actors. It is difficult, however, to determine which actors pose the greatest threat from their untoward use of the Internet. This has led to a large gap between threat perception and reality. In the United States, for example, there have been shifts in who or what constitutes a threat in cyber space which has translated into wild policy gyrations and "sharp bends in the threat perception" (Bendrath 2003:68). The first shift, according to Ralf Bendrath, was from the "cyber terrorists" of the Clinton administration to the state-based threats during the early days of the Bush administration. After the events of September 11, 2001 attention shifted abruptly back to non-state actors and their potential to use the Internet to launch attacks or incorporate cyber tactics as a force multiplier.

Securitization of "cyberspace" is a confusing mix of threat perception and reality. There are no clear standards for judging the threat. Individual networks may be able to discern when particular nodes are threatened, which in turn may allow systems technicians to monitor and accumulate anecdotal evidence in order to defend their "sites" from intrusion attempts. However the majority of organizations – firms and state agencies – do not look outside their firewalls in order assess the threat from the 'outside'. Yet while there have been "qualitative changes in the discourse, that two times in the last two years has moved from terrorists to states", it is still not possible to assess the variation in the threat language against actual changes in the "real world" (Bendrath 2003:70-71). In other words, there is a disconnect between perceived Internet-based threats and actual threats.

While there have been substantively significant shifts in the cyber threat perception of other states, they have not been as sharp and frequent as in the US case. As Bendrath rightly points out, the number of rapid changes in US policy language point to a serious problem (2003:69). Have the nature of cyber threats oscillated that much? Or is there simply no link between security perception and reality in cyber space? Bendrath concludes that is unlikely that there is a link between cyber threat perception within the policy community of the United States and the realities in cyber infrastructures. He argues instead that the cyber threat is treated as a "wild card" which is attached to the primary "hard" security threat (state or non-state actors) in order to amplify the capability of the "enemy" (2003:72). This amplification, and subsequent multiplicative effect, is securitization. The threat perception discourse has increased in sophistication and tempo but our understanding of the real nature of the problem remains limited.

These issues begin to look much like a problem being framed, or being directed

toward framing, within the context of territorial integrity. Therefore one that assumes that technology does not make geography entirely irrelevant – a distinct shift from thinking in the early to mid 1990s. In strategic terms the Internet actually can become an invaluable "overlay" on geography (Gray, 1996a:251-252; 1996b:276). Threats from cyber space and to the infrastructure are no longer associated with the stateless geography of the "hacker" but from real, often geopolitical, spaces. The result is the territorialization of the Internet and how state actors understand it. The Matai conjecture is perhaps the most explicit manifestation of this analytical trend.

In East Asia, in addition to cyber threats from external actors, perceptions and performative acts are usually couched in language that points to threats from "within". Most of the discourse in the region remains actor-based rather than capabilities-based. Beyond this observation, the generalization breaks down according to groups of countries that utilize threat perception not necessarily as a "wild card" as in the US case but toward the key areas that are seen to be traditional security priorities for their respective regimes. In Singapore, for example, the threat from cyber space is to the economy and stability. In China, protecting social harmony from online cyber dissent is a priority in its securitization discourse. In each country there is an undercurrent of threat perceptions that run along side the public discourse. In China, for example, policy makers and technical elites quietly worry equally about the lack of integrity in their cyber infrastructure stemming from a growing number of compromised nodes that are fueling everything from theft of proprietary knowledge via network intrusions against regional high technology competitors, to piracy and spam.[51]

It is easy to understand pleas for international cooperation between states, firms and

[51] However, it should be noted that this concern often runs concurrent with inaction and even encouragement of these activities (Confidential Interview, Hong Kong 2002). This has produced a kind of boomerang effect or cyber blowback for security practitioners in China.

nongovernmental organizations to reduce the number of nodes on the Internet that have been compromised or are at risk of compromise due to poor Internet security practices. The absence of Internet security in one state contributes to the insecurity of all others and in real-time. One of the dilemmas that face proponents of international cooperation is the variation in the number of compromised nodes cross-nationally and the nature of Internet diffusion patterns. This is, of course, in addition to traditional obstacles to international cooperation such as the variation in legal systems, interests, values, regulatory quality, rule of law, wealth and power.

Shifting the focus from incidents and actors to a compromised node framework can be thought of as an examination of the other side of the same coin. A node-based framework introduced in the previous chapter takes as its starting point the integrity of machines and devices on the Internet. In order to better understand the impact that the Internet has on security, describing the global distribution of compromised nodes is the first step. Part One examines the variation of compromised nodes both globally and in the East Asia region in order to assess the Matai conjecture and other assumptions regarding 'real' world instabilities and cyber security events. Using unique data obtained from a widely distributed logging system this chapter tests multiple hypotheses on the relationship between these patterns and several socio-political, economic and infrastructural variables. This is the first study to address this problem from an international perspective using quantitative data collected via intrusion logs from networks distributed throughout the world.

Hypotheses

The central question for Part One of this study is: across an upper stratum of countries with the highest level of cyber infrastructure diffusion, what factors best explain the variation in compromised nodes? Controlling for both the size of economy and the level of Internet technology diffusion, does democracy or institutional capacity matter? Or is the cross-national distribution of compromised nodes simply a function of the level of Internet technology diffusion? It could be that the more Internet there is, the more incidents there will be and other socio-economic and political factors do not matter.

While conducting interviews for this study a policy maker was asked why some East Asian countries had a serious problem with cyber infrastructural instabilities while others, with similar levels of GDP per capita and Internet diffusion, did not. He argued that "we have a better government and people follow the rules" (Confidential Interview, Tokyo, August 2003). There is also a clear sense that the level of "openness" and "freedoms" in general contribute to the number of Internet incidents in a country. This is not because of "hackers" attacking national Internet topologies from the outside but because of various motivations from the "inside" taking the form of political dissent using "hacktivism", the growth of peer-to-peer networks for file sharing, or simply poor security practices in industry and government.

Could there be a link between instabilities in a state and the number of Internet incidents as DK Matai suggests? To explore this, the study will test the following hypotheses.

H1: There is a relationship between rule of law and the number of compromised nodes 'located' in each state's territory
H2: There is a difference between democratic and non-democratic states and the number of compromised nodes located within each of them

The null hypothesis the would be that the distribution of compromised nodes can be best

explained by the level of Internet diffusion in a country alone and that diffusion is a function of wealth or other characteristics.[52]

As will be described below the cases chosen for this cross-national analysis are from the top stratum of "IT" economies. Adding countries that have little or near zero Internet diffusion would artificially skew the results. In general, the analysis will use explanatory variables from four "baskets": general diffusion metrics, economic indicators, Internet security indicators, and socio-political indicators – some of which will be used as proxy measures of institutional capacity. It is important to note that the following analysis does not make claims regarding causation. Statistical modeling using observational data, especially cross-sectional, can only hope to point to associations between factors. Apart from experimentation, which is clearly not feasible, a time-series model would dramatically improve inferential power, but this falls well beyond the scope of this study.

Existing work

One study in particular stands out and is worth summarizing. Vinod Yegneswaran, Paul Barford and Johannes Ullrich investigated a range of characteristics of global intrusion activity by analyzing data from Dshield.org a globally distributed monitoring system. They studied the daily volume of intrusion attempts, the sources and destinations of intrusion attempts, and specific types of intrusion attempts (Yegneswaran *et al.*, 2003). What they found is important. First, the goal of their study was to focus on the distribution, typology and prevalence of intrusion activity globally. Not surprisingly they found that both a large quantity and wide variety of types of intrusions take place daily; typically around 25 billion per day.[53] This is a much better "picture" of Internet incidents

[52] It may be useful at a later date to run the model on Internet diffusion characteristics alone – as a kind of stand-alone null hypothesis. More on this in Chapter Four.

[53] This number is difficult to compare as an overall percentage of cyber infrastructure activity. It is, however, a substantively significant level of activity. It should be pointed out that the 'type' of intrusion

than previously available. Yegneswaran *et al* also found that the source IPs of typical intrusions are uniformly distributed throughout the Autonomous System (AS) space (Yegneswaran *et al.*, 2003).[54] Of particular interest for security studies was that their team found evidence that a significant proportion of the activity is coordinated.[55] This indicates that much of the intrusion activity is much more sophisticated than conventional wisdom suggests and that this non-worm activity represents a much larger proportion of over-all intrusion activity.

The work by Yegneswaran *et al* was designed in part to try and reduce the "noise" in the global sample in order to delineate between serious and non-serious attempts. In other words, every effort was made to filter out worm traffic.[56] For example, they found that the distribution of source IP addresses of the non-worm intrusions as a function of the number of attempts followed Zipf's law (2003). A small number of source IPs were found to be responsible for a significant amount of serious intrusion attempts and that these particular trends showed a type of cliquing or patterning – more on this below.

This is important for the work presented here for two reasons. First, very little noise reduction was performed on the data used for my study.[57] As will be explained below, this study focuses on the distribution of compromised-nodes globally be they household PCs that have been infected with Code Red (a worm) or a more serious type of intrusion activity. Second, the uniform distribution of source IPs used to provide the incident data is "reasonably" well distributed across AS space and geographic space. This is key to assuring a good sample of typical global activity is used in the analysis. The global

---

activity is not related to the incident typology outlined in Chapter One which is based on motivation rather technical variation.

[54] Recall that autonomous systems are the largest 'networks' on the Internet that provide global connectivity.

[55] The Yegneswaran *et al.* (2003) study determined this by analyzing the signatures of non-worm scans, and then comparing the temporal pattern and consistency of source IPs.

[56] Not methodologically relevant for this analysis.

[57] This is the same data as Yegneswaran *et al.* (2003) study.

distribution of ASs is nonuniform; skewed toward North America and Western Europe. If the distribution of source IPs from provider networks were skewed it would add a layer of bias in the data meaning that certain geographies would be over represented.

Similar research efforts have focused on Internet incidents other than serious intrusion attempts. Moore *et al* studied distributed-denial-of-service attacks and Staniford *et al* focused on particular types of worm activity in order to prognosticate on future outbreaks (Moore *et al.*, 2001; Staniford *et al.*, 2002). Using a more aggregate level of analysis, Cowie *et al* examined instabilities in the global border gateway protocol (BGP) system in order to understand how worm propagation creates instabilities in the Internet globally (Cowie *et al.*, 2001). Finally, other than the commercial offerings on the international distribution of attacks which were presented above and discussed in Ortis and Evans (2003), there are also studies employing microanalysis techniques to study intrusion behaviour.

One of these, the Honeynet Project developed a method that uses "fake" networks to lure network intruders in without detection in order to study their behavior. A "honey-net" or "honey-pot" consists of machines deployed on the Internet with no real purpose other than to look like a common network that could be in use by an organization. This in turn has inspired the use of so called "Dark Nets" which conduct a similar type of research on micro-behaviour only on a much larger scale. Dark networks are network telescope that are used to gather data on emerging threats to the cyber infrastructure – especially from worms. Network telescopes are large expanses of unused globally routable IP space. The Yegneswaran *et al* study (2003) compared data gathered from a network telescope with the DShield project and discovered evidence which suggests that

non-worm traffic exhibits spatial geographical characteristics.[58] While this finding is suggestive for the present work, the only way to confirm this is to compare the DShield data with a set of geographically distributed set of network telescopes.[59] To date, however, no study has looked at the link between cyber infrastructure instabilities on non-technical factors.

Data

It is also important to note that for the purposes of this project, total source IP data (*tsource*) is an overall indicator of the overall stability of a national infrastructure topology rather than a specific understanding of hacking or cracking patterns cross-nationally. In other words, no inference can be made from the data regarding the type of intrusion activity or its purpose. The source data is the measure of compromised nodes. In order to focus in on particular types of illegal activity the amount of noise in the data would have to be reduced substantially. As will be discusses below, not all portscans (source IP data) are indicative of a compromised node. Target data was excluded from this study for two reasons. First, the distribution is skewed heavily toward a handful of states making statistical analysis unreliable. Second, because of the nature of the target data, at the time this research was conducted liability and confidentiality issues had not been adequately resolved.

The idea of measuring the "health" and stability of a country rather than specific categories of Internet incidents is controversial. In order to capture the matrix of security dilemmas that states face as a result of the rapid and multidimensional diffusion of Internet technologies excluding worms in favor of the more sinister images of professional "crackers" would be premature. There are, of course, trade-offs here.

---

[58] Any traffic observed on a dark net is inherently suspicious.
[59] For a more capable and technically correct explanation see Yegneswaran *et al.* (2003) discussion of network telescopes and global incident prevalence.

Capturing a cross-national picture of compromised nodes by broadening the definition of an "incident" requires accepting a higher amount of noise in the data. From the perspective of a policy maker and the systems administrator these distinctions may be superficial given that the number of compromised machines is a considerable problem, one that is increasing. I am, in effect, assuming a similar distribution pattern of compromised nodes across countries. More on this below.

The data for this study, as in the Yegneswaran *et al* research, was obtained from firewall logs of portscans collected over a two year period from over 20,000 firewall administrators distributed throughout the world.[60] The log files provide a lowest common denominator (LCD) summary of portscan activity obtained from various firewall/IDS systems. This includes BlackIce Defender, CISCO PIX Firewalls, ZoneAlarm, Linux IPchains, Portsentry, Snort and FreeBSD's IP firewall. The data, submitted to Dshield.org significantly increases coverage across the Internet and reduces reliance on individual firewall or IDS interpretation of events. It is comprised of log files submitted by a very diverse series of networks which include 7 class B networks and over 45 full class C sized networks and a wide variety of smaller subnetworks. Table 3.1 below shows the format of an example LCD log entry. The date and time fields are standardized to GMT and the provider hash[61] allows for aggregation by country of source IP addresses that belong to the same administrative network.

---

[60] As indicated earlier, there is always the danger of bias in a 'global' data set. In this case, the participating networks that gather the data are fairly evenly distributed throughout both IP and geographical spaces. If there is a bias in the provider networks (sensors) it will be of little consequence for this study because the sensors collect data which themselves do not discriminate based on geography. Although it is helpful to ensure that if there is spatial trends and patterns the more evenly distributed the sensors the less likely bias will be a factor.

[61] Not shown – but is a part of each log entry.

Table 3.1: Sample log entries from DSHIELD portscan logs

Date	Time	Source IP + Port	Target IP + Port	Packet Flags
2002-12-09	02:39:16	000.000.000.000 1111	444.444.444.444 555	17
2002-12-09	02:34:44	111.111.111.111 2222	444.444.444.444 555	17
2002-12-09	02:35:26	222.222.222.222 3333	444.444.444.444 555	17

The dataset was obtained from Dshield.org – a research effort funded by SANS Institute as part of its Internet Storm Center. DShield's objectives include detection and analysis of new worms and vulnerabilities, notifying ISPs of exploited systems through their "fight back" initiative, and publishing blacklists of worst offenders and community support to the submitters of data in order to improve firewall configuration (DShield, 2003). The lowest common denominator (LCD) approach used by DShield provides a unique, globally diverse and stable data source -- the only data source of this kind available to the research community.

The benefit of choosing to use an LCD approach is in its simplicity and generality making analysis a much less complicated task. While there is a clear benefit to the LCD approach, there are two weaknesses. The logs do not provide information about packet headers or information about the events taking place during active connections. In other words, a detailed analysis of behaviour after the portscan activity has taken place is not possible. There is also a certain degree of vulnerability to pollution in the data through false positives by oddly configured firewalls or other exogenous factors. This inevitably leads to measurement error in the data.

Port scans, worms and global random noise

The interdisciplinary nature of this research requires balancing the need to be clear about the technical assumptions without losing sight of the goals of the study, which are strictly "social scientific". Due to the unusual nature of the data used for this section of

this study it is necessary to provide some technical information on portscans, port numbering, and worms. This section begins with a quick discussion of port assignments on servers, or nodes and moves to the issue of noise buildup in the data as a result of worm prorogation. For the most part, a "birds-eye view" of each subject should suffice.

Ports are numerically assigned values to which differing types of connections to machines are made.[62] These are not physical ports but are logical mappings of services to numbers. By custom certain applications generally use predefined port numbers. Every machine that can reach the Internet or other machines on a network does this through ports. When two machines communicate they open up one or more ports to exchange data. For example, most web servers will "listen" on port 80 for incoming connections. A typical machine that runs multiple services through software called servers will listen or keep open multiple ports. One of the first events that takes place before an intrusion, by either a human or another machine, is a scan of all open ports in order to gather information on various characteristics and attributes of the target system – be it a firewall, or server or some other device.

The Yegneswaran *et al* study researchers needed to control for machines attacking other machines in order to get at the signal through the noise. They began by looking at some worms like CodeRed and Nimda that scan port 80. What they found was that port 80 scans formed the single most dominant group of scans constituting somewhere between 20% - 60% (Yegneswaran *et al.,* 2003). Many of port 80 scans that they observed during the period between May 2002 to June 2002 were a result of either the

[62] The ports which are used in common applications and servers over the Internet (such as a web server: port 80 or 8080) are in the range 0-1023. The next range above 1023 is for registered port numbers between 1024-49151. Port numbers above 49151 in the range 49152-65535 are private or dynamic ports; those not used by any defined application but which can be opened and by any program and then closed when not in use. The total number of logical ports (including 0) would be 65536. In general, a port can be in a state that is closed, waiting, listening, and established. For a complete list see the Internet Assigned Numbers Authority (IANA) site at <http://www.iana.org/assignments/port-numbers>.

CodeRed or the Nimda – worms that were causing considerable disruption at the time and, consequently, add 'noise' in the data. The important thing to keep in mind is that some of the worm versions are used simply to cause damage, others are used to compromise machines for sending spam or building links of nodes that can be chained together in order to launch more sophisticated attacks against firms or governments while staying anonymous. Still other compromised machines are used to build "bot-networks" which are then rented out for periods of time on a kind of black-market for network intruders or other malicious users. The utility of collections of compromised nodes for the maliciously minded is varied.

In East Asia, for example, bot nets are broken down into small-blocks and big-blocks of compromised nodes. Buyers or renters usually meet with administrators or builders of bot nets in Internet Relay Chat (IRC) rooms. From that point payment is made using an online method or a barter arrangement is made whereby code for exploits is exchanged or some other type of information of value. The benefit for the renter is that he/she does not have to maintain or use a privately obtained chained-relay from which to send spam or launch attacks (Confidential Interviews, Hong Kong, 2002). A market based system also means reducing the risk of being discovered by law enforcement by providing a quick and easy method of access to these types of relays which can be recycled.[63]

The concept of a chained-relay is important here and is often the reason why it is extremely difficult to trace a cyber attack back to its true origin. Think of a chained-relay

[63] A recent case from Europe further illustrates the growing problem. The Netherlands' government arrested three individuals in October 2005 that allegedly controlled some 1.5 million computers as part of a worldwide bot net. At first, Dutch authorities thought the network of compromised nodes was around 100,000 but it turned out to be orders of magnitude larger. It is unclear how much of the bot network was stable enough to be sold to the underground for use in criminal activity. But it is clear that even if criminal were charged US$1.00 per node, the bot network creators stood to make a considerable amount of money. Cyber security researchers have found evidence in the past of other million-bot networks but this may be the first well-documented case of such an elaborate operation. See Lemos (2005). The dissertation returns to the case of bot nets in Chapter Seven.

as a series of stepping stones; the more stones that a network intruder steps through the less likely he/she will be discovered by law enforcement. The drawback is that the larger the chained-relay the more latency will exist in the path to the target machine. In other words, the more links in the chain the more delay in communication between to the start and end points. Another drawback to large chained-relays used in intrusions is that they can become unstable over short periods of time.

By convention a chained-relay is expressed as $h_1 \Leftrightarrow h_2$ (Zhang and Paxson, 2000). The symbol h_1 indicates the originating machine and h_2 the end machine where $\Leftrightarrow$ describes the bi-directional communication between the two machines which can be located anywhere (over both geographical and IP space) in the cyber infrastructure. In the set of stepping stones or chained-relay $h_1 \Leftrightarrow h_*$ the last hop before the target machine is h_* .[64] If we have a chained-relay where $h_1 \Leftrightarrow h_4$ then $h_4 \equiv h_*$ (are the same) and the probability of knowing the IP address of the originating machine h_1 is P(x), or unknown. In general, the likelihood of a large chained-relay being used is rather small when compared to the average attack which uses one or two stepping stones. The optimal safety margin for the intruder is to create chained-relays that span several jurisdictions using machines in differing ISPs and or countries. This frustrates passive and active tracing methods used by forcing law enforcement to pursue the "trail" through the weeds of

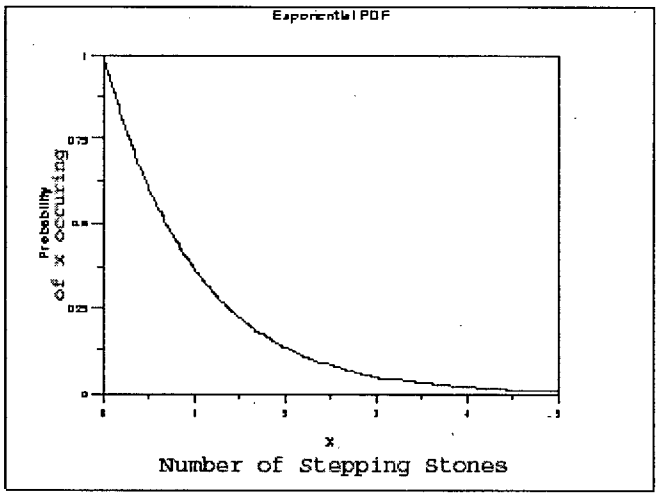
---

[64] The observation h_* is recorded or logged as a result of a port scan on the target machine running software to record the event which subsequently gets submitted to Dshield.org. Not all port scans are identical in behavior. There are essentially four different types or categories of scans (Staniford *et al.,* 2002; Yegneswaran *et al.,* 2003). The first type is a vertical scan. This is a sequential or random scan of multiple ports of a single IP address from the same source during a one hour period. The second type is a horizontal scan which takes place from a single source of several machines in a subnet aimed at the same target port, ie. the same vulnerability. The third type is a coordinated scan. This type of portscan originates from multiple sources aimed at a particular port of destinations in the same subnet within a one hour window. Finally, the fourth type is a stealth scan. Stealth scans can be horizontal or vertical scans that start with a very low frequency and are quasi-random in order to avoid detection from an intrusion detection system (IDS) (Yegneswaran *et al.,* 2003). The notation h_* is in keeping with previous work in engineering on chained-relays.

various legal environments. This is the central reason why it is often difficult for security or law enforcement to trace the attack back to its origin and the reason why cooperation across jurisdictions is so important.

We could theoretically derive from network communication theory that there a larger numbers of systems intrusion attempts (worm and non-worm) that use fewer stepping stones than those attempts that aggressively attempt to conceal their physical location using relays with many stepping stones. The probability of a large number of stepping stones tends to shrink over the observation space. The exponential probability density function in Figure 3.1 illustrates the relationship between the number of stepping stones in a chained-relay (x) and the probability of that relay length being used. Notice that there does not necessarily need to be a chained relay used in an intrusion attempt. Thus, there is no 'step' and the x axis begins at 0.

Figure 3.1: Chained-relay density function



This is a theoretical assertion with no empirical evidence other than anecdotal claims obtained through field interviewing done for this study. The purpose here is to link the concept of a chained-relay to the dependent variable source.IP. This is important because in the data used for this study a relay of unknown length $h_1 \Leftrightarrow h_k$, the observation *tsource*

(h_*) is the "last hop" or where $h_k \equiv h_*$.[65]

The provider networks represented in the DShield data are reasonably well distributed (over both geographical and IP space) and thus represent a good global sample for the top-tier countries (cases) under consideration here.[66] The point of reviewing the various technical aspects is to show that even if it is not possible to completely trace-back an attack with accuracy to the absolute source point (weed through chained-relays); a machine has still been compromised at a geographic location. In this sense, whether or not the incident was cause by another "zombied" machine, a compromised machine used in a chained relay, direct attack, or a virus is not necessarily important. All incidents are indicative of the over health of national cyberspaces and are therefore revealing.

Total source IP data (tsource) is a representation of compromised-nodes and is the dependent variable for the following analysis. It is broken down into two samples one taken from a four-month period in 2001 and the other a similar period in 2002. The sample size in 2001 is 81,035,793 and 2002 is 331,291,656. For both periods the total number of observations is 412,327,449 for 49 case countries.[67] The histogram below displays the distribution of *tsource* (h_*) data by number of incidents. The extreme observation on the far right hand side of the x axis is the United States.

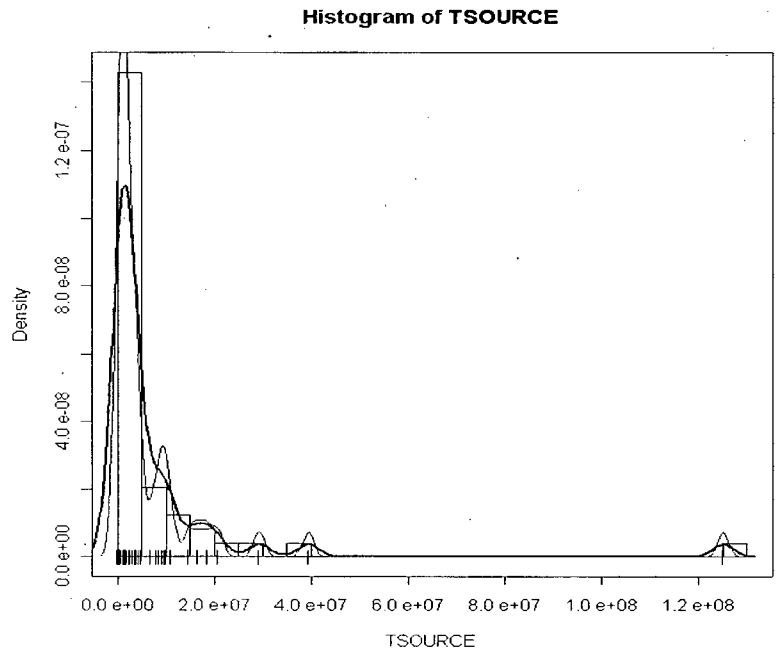
---

[65] The choice of the type of scan to be used in an attack is sometimes cited, controversially, as an indication of a strategy or motivation behind the scan. In future research it would be worth performing a limited amount of noise reduction on the data by separating two categories of ports scanned: 80 and 1433. This would help to filter out traffic from worms like sub-seven and noise due to MS Windows netbios. Noise reduction, however, reduces the accuracy of knowing the compromised-node distribution but does increase the signal of non-worm intrusion attempts. A comparison of data without noise reduction and data employing various noise reduction strategies would prove very useful in the future.

[66] Case selection is described in following chapter.

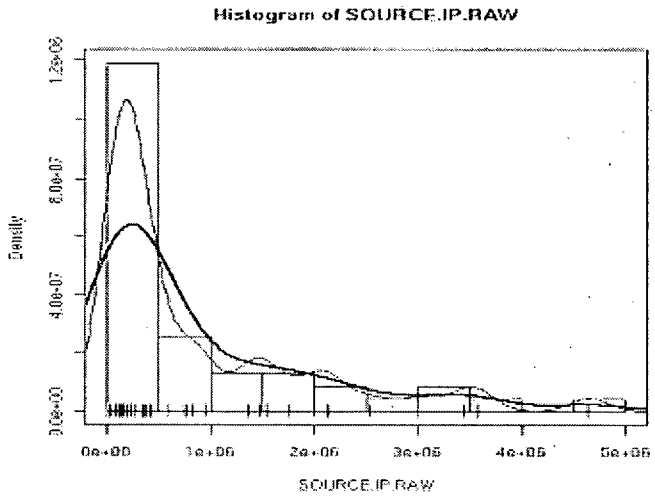
[67] The data came in two general formats: as raw log files and MySQL database files. To process the data programs had to be written to sort the data, feed it into MySQL (if it was not already in a database format) and then determine the geographic location based on the IP address using commercially available databases that map IP addresses to countries.

Figure 3.2 - Histogram of h_* for 49 upper tier countries



The histogram, Figure 3.2, with kernel density estimate lines superimposed, suggests that the raw dependent variable tsource (h_*) follows a Poisson distribution. The vast majority of the top-tier countries fall within the lower half of the distribution. The overall skew in histogram of is not surprising. From the mid-1990s a group of five countries accounted for a large portion of the Internet incidents and have consistently been home to a disproportionate number of compromised nodes. The United States is the most extreme value lying on the far right hand side of the histogram. With that case removed (Figure 3.3) the shape of the distribution becomes more pronounced.

Figure 3.3 - Histogram with US case removed



The United States consistently ranks at the top of each sample for the number of compromised nodes that generate port scans on other machines. Table 3.2 lists the top 16 worst offenders for three sample periods in 2001 and 2002. Well over one quarter of the total number of "incidents" can be attributed to compromised machines in the United States in each of the samples. There is a cast of usual suspects that accompany the US case in all three periods. China, Germany, Korea, the UK, Brazil and Canada together account for roughly 35% of the remaining counts.

Table 3.2 – Relative Country rankings

2001:3 month sample		2002a: 2 month sample		2002b: 3 month sample	
UNITED STATES	32338512 (39.90)	UNITED STATES	38830559 (26.93)	UNITED STATES	53896074 (28.80)
CHINA	4650198 (5.73)	KOREA, REPUB	13744981 (9.53)	KOREA, REPUB	22237582 (11.88)
GERMANY	3590141 (4.43)	CHINA	10730055 (7.44)	CHINA	13896358 (7.42)
KOREA, REPUB	3443155 (4.24)	GERMANY	8115244 (5.62)	TAIWAN	9152039 (4.89)
UNITED KINGDOM	3004499 (3.70)	TAIWAN	7245367 (5.02)	GERMANY	9037935 (4.83)
BRAZIL	2541728 (3.13)	BRAZIL	6805925 (4.72)	CANADA	7402730 (3.95)
TAIWAN	2145466 (2.64)	CANADA	5364278 (3.72)	BRAZIL	7366722 (3.93)
FRANCE	2129813 (2.62)	FRANCE	4096389 (2.84)	ITALY	4835819 (2.58)
CANADA	1997649 (2.46)	MEXICO	3874396 (2.68)	UNITED KINGDOM	4209723 (2.25)
ITALY	1755970 (2.16)	UNITED KING	3848402 (2.66)	JAPAN	4116433 (2.20)
JAPAN	1545967 (1.90)	ITALY	3448066 (2.39)	MEXICO	4003479 (2.13)
MEXICO	1479373 (1.82)	SPAIN	3137600 (2.17)	SPAIN	3646702 (1.94)
SPAIN	1376356 (1.69)	JAPAN	2968269 (2.05)	FRANCE	3526849 (1.88)
INDIA	1373129 (1.69)	INDIA	2808887 (1.94)	INDIA	2787927 (1.49)
TURKEY	962628 (1.18)	TURKEY	1865754 (1.29)	POLAND	2304608 (1.23)
AUSTRALIA	960661 (1.18)	POLAND	1799419 (1.24)	RUSSIAN FEDERATION	1814830 (0.97)
Total in sample	**81035793**	**Total in sample**	**144162438**	**Total in sample**	**187127981**

Notes: Figures are raw counts for top16 of 49 countries with percentage of total for sample period in brackets

Other than a consistent group of worst offenders – the US, China and South Korea – there is no immediate pattern to the rankings. Some of the countries have large populations, others small. Relative to overall population, approximately half have a high level of Internet diffusion while others such as China, India, and Brazil have relatively low levels of Internet diffusion but with rapid growth rates. The total number of observations in each sample is for all countries globally. The point here is that there is no immediate pattern to these rankings.

It is interesting to note that the United Kingdom and Taiwan are the only countries to noticeable change ranks across samples. First, the overall stability and consistency of ranks indicates that the noise reduction in the samples was intuitively effective. If the case countries in each sample were to jump around considerably than this would suggest that noise reduction used on the data had been less effective or was somehow selecting on certain countries in a biased manner. Still, it is unclear as to why the UK and Taiwan change ranks.[68]

The choice of case countries for inclusion in this analysis was made based on two distinct grounds. The first being that there was a significant break in the distribution in the raw data which indicated that many countries in the international system did not yet have 'enough' cyber infrastructure to warrant inclusion in this study. The second reason was more sociological than technical. The significant break in the raw data was compared with a socio-economic measure of Internet diffusion called the Digital Access Index to see if the break somehow coincided with a cross-national measure. It did. The rationale for case selection and the choice of independent variables is the subject to which the dissertation now turns.

[68] The next step in the research would move the design from a pooled cross section to time series. This would have the added benefit of running a number of noise reduction algorithms on the data and comparing the results.

Chapter Four: Instability and Cyber Infrastructure Security

Introduction

The link between political instability and cyber infrastructure instability – as suggested and discussed by the Matai (2005) and Bendrath (2003:69-70) – will be examined. Political-institutional factors are the focus of Part One of this study because they are proxy measures for institutional capacity and overall stability across countries. The motivation for the analysis, as discussed in Chapters Two and Three, stems directly from assumptions that are made by both network administrators and policy makers that there is a relationship between cyber incidents and general instability in a country. These assumptions inform the growing gap between cyber threat perception and reality. Second, the analysis is motivated in more general terms to examine relationships between social, political and economic instabilities, and cyber security events cross-nationally because it provides a unique look at the development of the cyber security infrastructure. Examining measures of infrastructure instability and what they might mean is important for international security studies because, as Bendrath writes "threat perception can change when the criteria for a threat are changed" (2003:70).

Case selection

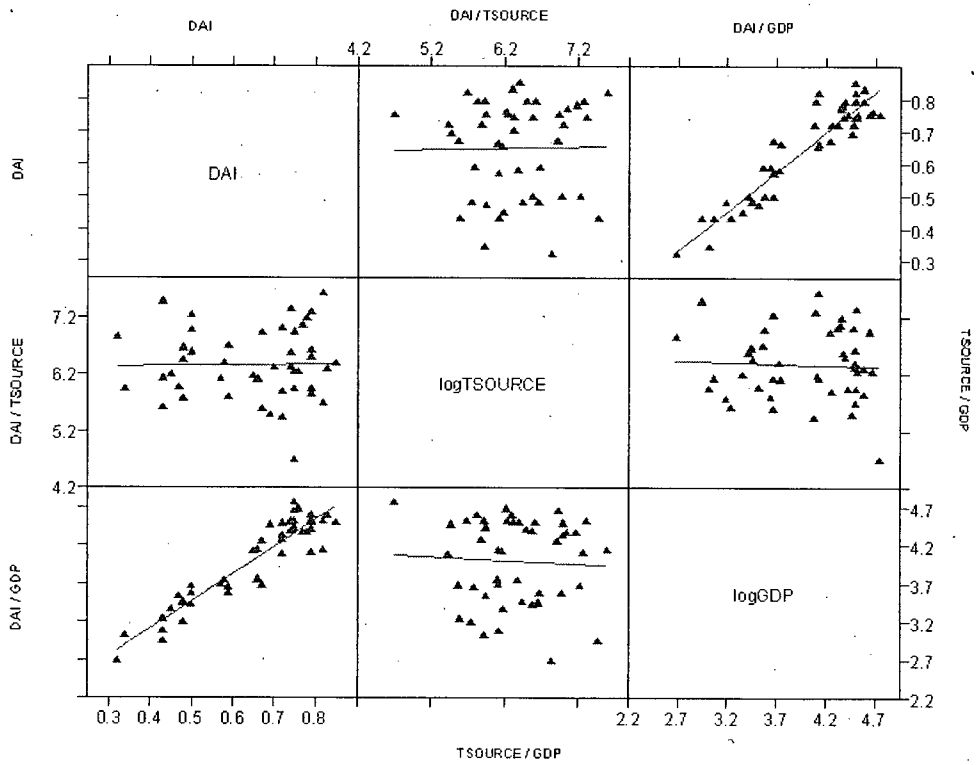
The dependent variable *tsource* or h_* is the source frequency of Internet incidents and the number of compromised nodes per country.[69] The source of the Internet incidents in the data provided an ample sample size for approximately 90 countries in the international system.[70] Only half of these countries were selected for use as cases. The

[69] As discussed in Chapter Three, the target data was excluded from this study for two reasons. First, the distribution is skewed heavily toward a handful of states making statistical analysis unreliable. Second, because of the nature of the target data, liability and confidentiality issues prevent its use in publicly accessible research. The notation h use for the dependent variable follows from Zhang and Paxon (2000).
[70] This is for the raw data. I did not subject the entire sample to the noise reduction, only the 49 countries (cases) used for this study.

selection of case countries was done in order to best capture the variation of compromised nodes globally. A minimum level of Internet diffusion had to exist in each country. Therefore, 49 countries were selected based on the upper half of the International Telecommunications Union's (ITU) Digital Access Index (DAI) which ranks all countries in terms of their potential for what the ITU calls digital development. The DAI uses a range of socio-economic and infrastructural data to assess the level of IT development. It combines eight variables, covering five areas which create an overall country score that ranges from 0 to 1. The criteria measured for the DAI are availability of infrastructure, cost of access, education levels, quality of IT services (ISPs etc.), and Internet usage.

Because the principal focus here is the variation among countries in compromised nodes the cutoff point for the cases was the median point of 0.43 – the Philippines. In Figure 4.1 below, there appears to be no relationship between the DAI and the dependent variable h_*. A log transformation was performed on the dependent variable in order to normalize the variables for visual inspection using scatter plots. The scatter plot matrix below (Figure 4.1) showing the relationship between h_*, GDP per capita and the DAI for all 49 countries illustrates this point. The solid line in each window shows a nonparametric regression of y on x.

Figure 4.1 – Scatterplot matrix of source, GDP per capita, and the DAI



It is important to point out that the DAI is a basket of IT measures of which Internet diffusion represents only a small component. The result, as shown in cell 2 above, is a weak negative relationship between h_* and the DAI. While the DAI is a good measure for case selection, it has very little relationship to h_*. Clearly, the DAI is heavily based on GDP per capita as both are strongly correlated with each other as shown in cell 3. As is the case with the DAI, cell 6 shows GDP per capita has little or no relationship with h_* .

Independent variables

The independent variables chosen for this study can be grouped into four categories: infrastructural, sociological, economic and political. The analysis is restricted to one variable in each category in order to minimize the effects of multicollinearity. Many of

the independent variables will be familiar to readers in International Relations with an exposure to cross-national research designs. However, it is useful to describe the key variables and outline why they were chosen for this analysis.[71]

1. Infrastructure measures

The first category of independent variables is general Internet diffusion. It has been show in other research that raw host counts and simple counts of Internet users are often misleading indicators of overall diffusion in a country (Zook 2000, Giacomelloa and Picci 2003: 364-365). The number of Internet users in each country is at best a guess made by national statistical agencies. In order to capture additional dimensions of diffusion in each country other aspects of Internet infrastructure must be taken into account. Measures such as the number of autonomous systems, prefixes and address space may help to adjust for other diffusion dimensions.

In order to adjust for the various indicators of Internet diffusion a composite variable was created: $C = (AS + prefixes + addresses + users + hosts) \div 5$. The individual diffusion measures are strongly associated with one another.[72] This, unfortunately, means that the composite measure may not substantially improve upon simple standalone host and user counts. The value of the consolidated measure is that it captures the variance in the individual measures across countries. Adding other measures such as teledensity and PC availability could also be incorporated into the composite measure but they suffer from significant draw backs of their own.[73]

---

[71] See Appendix A for a complete list of variables including source and measurement level.
[72] See Figure 4.2 in Appendix A.
[73] An alternative to the composite indicator is teledensity, or number of lines per 1000 inhabitants, which is a frequently used as a general telecommunication infrastructure indicator. The use of this measure alone as a proxy for availability of equipment enabling Internet diffusion only accounts for PCs as one among many various possible devices that can be used to access the Internet.

Collapsing the five variables into one composite index may not significantly improve upon host or user counts alone, but it will help to avoid multicollinearity in the analysis below. As shown in Figure 4.2 the five variables are strongly correlated. This would make an interpretation of the regression coefficients

2. Economic measures

Two economic indicators were used in the models below: PPP and total unemployment (see Appendix A for data sources). Purchasing power parity (PPP) was used to capture a country's potential total personal computer or workstation holdings. The PPP was chosen because it tends to more accurately reflect real income levels. Total unemployment was also included as a proxy for overall crime levels in each country. The theory here is that countries with higher levels of GDP per capita, a more stable economy, will see low levels of cyber infrastructure events. A recent case in point involved a study of Russian and Eastern European 'cyber crime gangs' operating fraud rings (Business Week Online, 2006). The combination of advanced education systems that train students in mathematics, engineering and computer science and very high levels of unemployment produces sophisticated cyber crime rings that are difficult to combat.

3. Crime and corruption and openness

In order to hone in on "cyber crime" a variable that measures the level of software piracy is included. The piracy variable is compiled by the Business Software Alliance (BSA). The "difference between software applications installed (demand) and software applications legally shipped (supply) equals the estimate of software applications pirated" (BSA 2003:13). The BSA values were calculated for this study by country for 2002 and used in the 2001 cross-section. The BSA piracy rate is defined as the volume of software pirated as a percent of total software installed in each country. Piracy rates, of course, vary among software applications and countries. The BSA groups the software into "three tiers and uses ratios for each tier. The tiers used were general productivity applications,

---

problematic. When multicollinearity is present, the standard errors of the coefficients estimated by OLS tend to increase, and the reliance that can be placed in the coefficient values decreases. The remedy is to take some of the correlated variables out of the model but this means a loss in precision. An alternative is to create an index which collapses all of the offending variables into one measure.

professional applications, and utilities. These were chosen because they represent different target markets and price levels, and it is believed, different piracy rates" (2003:12). The interpretation is percentage rates where .99 indicates a very high level of piracy and .01 a very low level. This was useful here because cyber crime, specifically piracy, can be positively linked to cyber infrastructure instabilities. The BSA data is not perfect, but is the only available metric that tries to directly measure aggregate cyber crime levels.

The level of corruption may also be related to the number of compromised-nodes in a country. For example, in the Korean case, the problem of open-relays was in part attributed to large scale contracts awarded by the Korean government to IT firms to install and configure servers and workstations in the education and government sectors (Confidential Interview, Korea, 2003). These contracts were often improperly implemented leaving a large number of nodes free for misuse on a large scale. Another example is the relationship between ISPs and the government of the People's Republic of China (PRC). In many cases ISPs are the second line of defense in identifying problem networks and shutting down access to the Internet until the offending sites have rectified the compromised machines. Managers and administrators at the ISP level are often paid to overlook offending networks (Confidential Interview, HKSAR, 2002). The problem at the ISP level has been found in other countries including the United States. It is not the number of ISPs that are an indicator *per se*, but the general level of societal corruption.[74] The general level of corruption can be taken as a rough indicator of the number of corrupt ISPs.

The corruption perception index (CPI) is generated by Transparency International and

[74] For an example of recent cross-national research that explores the utility of various measures of societal corruption see Xin and Rudel (2004).

is a composite index, making use of surveys of businesspeople and assessments by country analysts. It is built using a wide range of methodologies. Overall, 15 surveys are included in the CPI originating from 9 independent institutions. The CPI is interpreted on a scale of 0-10 where the higher the number the less corruption is perceived. Thus the lower the score the higher the perceived level of corruption in a state. The level of corruption is important here as a measure of institutional capacity, and hence, overall stability (see Appendix A for data source). In general, there is a strong positive correlation between the CPI and overall stability across countries in the international system.[75]

As alluded to above, one of the assumptions that is often made regarding the relationship between Internet security and the state is that more "open" states are more vulnerable or susceptible to Internet security incidents. This is not because they have less control over extraterritorial processes like "hacking" from the "outside" but rather that states that exercise controls over media have greater ability to better control internal "hacking" and enforce IT related laws with illiberal jurisprudence. A prototypical case would be Singapore. The proxy measure that was chosen to measure media freedom is the Free Press Index compiled by Freedom House. The Freedom House survey of 187 countries measures the degree to which each country permits the free flow of information. It rates countries according to whether or not the press is "Free", "Partly Free", or "Not Free". Countries scoring 0 to 30 are regarded as having "Free" media, 31 to 60, "Partly Free" media, and 61 to 100, "Not Free" media.

---

[75] The most recent data (2005) and analysis on this relationship can be found online at <http://www.foreignpolicy.com./story/cms.php?story_id=3420&page=3>. The *Failed States Index* provides a good introduction to the factors generally associated with instability. For more see Foreign Policy and the Fund for Peace report online at <http://www.foreignpolicy.com./story/cms.php?story_id=3420>.

4. Political stability measures

The final category consists of two political-institutional variables that measure level of democracy and rule of law; the proxies for stability.[76] The purpose of including the democracy variable is principally to see if there is a significant difference between democracies and non-democracies in the pattern of compromised nodes. Similar in motivation to the free press proxy, it has been suggested that democracies are more vulnerable to the spread of Internet incidents given various institutional features that restrict government involvement in industry and private affairs. What is of potential interest is whether or not the distribution of compromised nodes differs between the two regimes types.

The *democ* variable from the Polity IV project is a democracy indicator which is derived from codings of the competitiveness of political participation, the openness and competitiveness of executive recruitment, and constraints on the executive.[77] Institutionalized democracy is conceived as three interdependent elements. One is the presence of institutions and procedures through which citizens can express effective preferences about alternative policies and leaders. Second is the existence of institutionalized constraints on the exercise of power by the executive. Third is the guarantee of civil liberties to all citizens in their daily lives and in acts of political participation (PolityIV, 2003). The democracy indicator is interpreted using an eleven point ordinal scale from 0-10 where 0 is very low and 10 indicate a high level of democracy (see Appendix A).

---

[76] Other work in International Relations, especially security studies, that model stability across both time and space. These studies also draw from the Polity IV project for measures of other forms of international system instability, see Marshall and Gurr (2005), Goldstone *et al.* (2005), and Gurr, Woodward and Marshall (2005). This study uses these same measures.

[77] For a more elaborate discussion of the political stability measures see the Polity IV User Manual available online from <http://www.cidcm.umd.edu/inscr/polity/>

The second variable in this category is the level of the rule of law in a country. It is very unclear if legal environments in countries have any affect on the distribution and pattern of compromised nodes. In order to test for this relationship cross-nationally the measure for the rule of law is taken from the World Bank's Governance Matters III project. Rule of law (RoL) is comprised of several indicators which measure the extent to which people have confidence in and abide by the rules of society. The variable is constructed from 250 individual measures, gathered from 25 different sources, produced by 18 different organizations. This study uses 2000 data for 2001 and scores lie between -2.5 and +2.5, with higher scores corresponding to better rule of law.

Analysis

A full exploration of the causal mechanisms linking each explanatory variable to the number and distribution of compromised nodes in each country is well beyond the scope of this study. Not all of the explanatory variables are used in the remaining analysis. Crime, corruption and openness do not perform as well as the political-institutional variables when acting as proxies for cross-national instability. The purpose here is to identify the patterns of compromised nodes globally and try to explain this variation. Subsequent chapters in this dissertation deal with several factors in more detail. Causal mechanisms are not usually determinable through large *N* quantitative research. For this purpose, carefully conducted case studies "close the loop" between explaining variation and identifying causal relationships through various mechanisms. Following a series of correlation plots, standard multivariate regression techniques were used to analyze the data.

Both the data and modeling technique are unusual to IR research and thus a brief review is useful. The dependent variable (h_*), which is essentially counts of incidents or

compromised nodes for each country over an eight month period, follows a Poisson distribution as shown in Figure 3.1.[78] Poisson regression was chosen over ordinary least squares (OLS).[79] Comparing OLS and Poisson models indicated that the Poisson did perform slightly better than the standard model. Poisson regression, of course, is a form of the generalized linear model (GLM). GLMs fit data by using an iterated weighted least squares procedure (IWLS) which generates coefficient standard errors and maximum-likelihood estimates. These models assume that the dependent variable has a Poisson distribution and uses the log link to map onto the linear predictors. For example, in Poisson models a unit increase in X has a multiplicative impact of e^{β} on Y. Thus, if $\beta = 0$, the multiplicative effect is 1 and a unit increase in X increases $\log Y$ by β; the effect of explanatory variables on the mean becomes multiplicative. Formally, the cross-national compromised node model can be expressed as:

$$\log_{10}(h_*) = \alpha + \beta_j X_{ij} + \varepsilon_i, where \phi = 1$$

Poisson models have a dispersion parameter ϕ which is set to 1. It is very likely, however, that the model will suffer from some level of over or under dispersion - a common problem which was detected.[80] To compensate for this a quasi-Poisson[81] model

---

[78] The number of attacks from the cyber infrastructure arriving at a node (i.e. server etc.) in a time period (t) is assumed in this dissertation to have a Poisson distribution. Thus the number of cyber attacks during one time interval is assumed to be statistically independent of the frequency of attacks arriving during any other non-overlapping time interval. This is a one-dimensional Poisson process. In this case, the expected value of the number of attacks between time a and b is:

$$\int_a^b \lambda(t)dt$$

The parameter λ is the rate of attacks against a node and $\lambda(t)$ is the non-homogenous rate function.

[79] For more on the theory behind Poisson regression in Political Science see King (1988:838-863). For an application of this modeling technique in International Relations see Pollins (1996). This analysis relied heavily on Fox (2002:156, 177-180, 186-187).

[80] To clarify, over-dispersion in a Poisson model essentially means that $\sigma^2 > \mu$. When the variance is greater than the mean a quasi-Poisson model is generally thought to be more appropriate. Quasi-Poisson techniques are often chosen by researchers because a log transformation of the data may not satisfy the assumptions required by classical statistical methods. Thus, the dispersion parameter is really the variance

was specified in place of Poisson regression and allows for the dispersion parameter ϕ to "float". Formally:

$$\log_{10}(h_*) = \alpha + \beta_j X_{ij} + \varepsilon_i, where \phi \neq 1$$

A quasi-Poisson model uses a quasi-likelihood estimation that calculates estimates for an arbitrary combination of link = log and variance functions in the absence of a conditional distribution for the dependent variable that measures the number of compromised nodes cross-nationally (h_*). These estimates are similar to maximum-likelihood estimates in that they share many of the same properties. The regression coefficients in a quasi-Poisson model are not affected by allowing the dispersion parameter to float - coefficients in both a Poisson and quasi-Poisson model will be the same. What are noticeably different between the results of the two modeling techniques are the coefficient standard errors. This is because in the quasi-Poisson case the coefficient standard errors are multiplied by ϕ and thus, are much larger.[82] In short, failing to detect and remedy for over or under-dispersion can lead to very small standard errors and hence the coefficients will be "too" precise (Fox 2002:186). In a sense, using the quasi-Poisson fit slightly "penalizes" the coefficient standard errors. The result is a more cautious approach.

Partial correlation results and discussion

When a correlation exists between two variables, the association may be explained by a third variable that is correlated with both *X* and *Y*. This is almost always present to one

---

divided by the mean: $\phi = \sigma^2 / \mu$. In a Poisson model, the mean is also the variance and the canonical link is the natural log. Poisson distributions are often chosen to model counts or for data in which the variance increases with the mean.

[81] The choice to use the **R** statistical environment over S-PLUS or SPSS is directly related to the choice of modeling technique. S-PLUS does not have a quasi-Poisson family of functions and treats its Poisson family in a rather inconsistent way. SPSS cannot perform quasi-Poisson regression.

[82] The dispersion parameter ϕ is defined for each model below.

degree or another in cross-national research. A set of partial correlations is used here to control for the effect of a third variable when examining the correlation between *X* and *Y*. If the correlation between *X* and *Y* is reduced, the third variable is responsible for the effect. Before proceeding to the regression models, two separate partial correlation matrices are examined: one with Internet diffusion (*C*) controlled for, the other controlling for population.[83] This procedure not only helps to elucidate the relationships between the various socio-political and economic variables but will also serve as an indicator of colinearity.

It is possible that the strength of the composite measure is having an effect on the other variables. Table 4.1 below shows the partial correlations for the same variables but controlling for diffusion. Once the level of Internet diffusion is controlled for both the rule of law and level of democracy become more important. This also allows for other variables like population to reappear.

[83] It is important to note that the term "control" refers to statistical control not experimental control.

Table 4.1 – Partial correlations controlling for diffusion

Controlling for ... COMPOSITE

	TSOURCE	CPI	TOT_UNEM	POP	DEMOC	R_O_L	PIRACY	FREE_PRE	PPP
TSOURCE	1.0000 (0) P= .	-.2573 (35) P= .124	.2182 (35) P= .194	.6198 (35) P= .000	-.4341 (35) P= .007	-.3115 (35) P= .061	.4087 (35) P= .012	.3513 (35) P= .033	-.2498 (35) P= .136
CPI	-.2573 (35) P= .124	1.0000 (0) P= .	-.3230 (35) P= .051	-.3734 (35) P= .023	.3226 (35) P= .051	.9430 (35) P= .000	-.8233 (35) P= .000	-.5952 (35) P= .000	.7931 (35) P= .000
TOT_UNEM	.2182 (35) P= .194	-.3230 (35) P= .051	1.0000 (0) P= .	.7180 (35) P= .000	-.0697 (35) P= .682	-.2362 (35) P= .159	.2870 (35) P= .085	.2065 (35) P= .220	-.3238 (35) P= .051
POP	.6198 (35) P= .000	-.3734 (35) P= .023	.7180 (35) P= .000	1.0000 (0) P= .	-.5084 (35) P= .001	-.3683 (35) P= .025	.5234 (35) P= .001	.4794 (35) P= .003	-.3894 (35) P= .017
DEMOC	-.4341 (35) P= .007	.3226 (35) P= .051	-.0697 (35) P= .682	-.5084 (35) P= .001	1.0000 (0) P= .	.4367 (35) P= .007	-.6214 (35) P= .000	-.8574 (35) P= .000	.4467 (35) P= .006
R_O_L	-.3115 (35) P= .061	.9430 (35) P= .000	-.2362 (35) P= .159	-.3683 (35) P= .025	.4367 (35) P= .007	1.0000 (0) P= .	-.8180 (35) P= .000	-.6913 (35) P= .000	.8257 (35) P= .000
PIRACY	.4087 (35) P= .012	-.8233 (35) P= .000	.2870 (35) P= .085	.5234 (35) P= .001	-.6214 (35) P= .000	-.8180 (35) P= .000	1.0000 (0) P= .	.7730 (35) P= .000	-.7284 (35) P= .000
FREE_PRE	.3513 (35) P= .033	-.5952 (35) P= .000	.2065 (35) P= .220	.4794 (35) P= .003	-.8574 (35) P= .000	-.6913 (35) P= .000	.7730 (35) P= .000	1.0000 (0) P= .	-.6467 (35) P= .000
PPP	-.2498 (35) P= .136	.7931 (35) P= .000	-.3238 (35) P= .051	-.3894 (35) P= .017	.4467 (35) P= .006	.8257 (35) P= .000	-.7284 (35) P= .000	-.6467 (35) P= .000	1.0000 (0) P= .

(Coefficient / (D.F.) / 2-tailed Significance)

Concentrating again on the first column under tsource (h_*), the correlation between population and the number of compromised nodes jumps from .284 in the full correlation matrix to .6198 – both are significant at the 95% level. It now appears that after controlling for the composite measure of diffusion there is a moderate to strong positive relationship between population size and h_*. The population measure could be picking up on the initial relationship between the size of a countries population and Internet diffusion but the original correlation was only .157 and not significant. It is unclear as to how these two factors are linked. A simple explanation might be that if a large population has high rates of diffusion, there will likely be an associated increase in the number of

compromised nodes. But this is difficult to infer from correlations alone.

The increase in the correlations of rule of law and the level of democracy in Table 4.2 are not easily understood. After controlling for Internet diffusion, the correlation between the frequency of Internet incidents and the level of democracy jumps from being insignificant at .001 to -.4341 significant at the 0.01 level. This suggests a moderate negative relationship between the level of democracy and the number of compromised nodes in a country once the "amount" of Internet is controlled for. Rule of law, too, jumps from .091 to -.3115 but is not significant. There appears to be a weak-to-moderate negative relationship between the level of the rule of law in a country and the number of compromised nodes when controlling for diffusion.

There is a large amount of "jump" in the key independent variables when controlling for diffusion factors. In particular, population showed the greatest difference between the full and partial correlations. In order to explore this further, Table 4.3 below shows the partial correlations with population controlled. Notice the difference between the previous results for the rule of law and democracy variables and the results presented in Table 4.3; both are now indicating a much weaker, now positive, relationship with tsource, .2298 and .1625 respectively.

Table 4.3 – Partial correlations controlling for population

Controlling for ... POPULATION

	TSOURCE	CPI	TOT_UNEM	DEMOC	R_O_L	PIRACY	FREE_PRE	PPP	COMPOSIT
TSOURCE	1.0000 (0) P= .	.1900 (35) P= .260	-.0730 (35) P= .668	.1625 (35) P= .337	.2298 (35) P= .171	-.3331 (35) P= .044	-.1928 (35) P= .253	.3187 (35) P= .055	.9810 (35) P= .000
CPI	.1900 (35) P= .260	1.0000 (0) P= .	-.0818 (35) P= .630	.1996 (35) P= .236	.9358 (35) P= .000	-.7979 (35) P= .000	-.5319 (35) P= .001	.7674 (35) P= .000	.2005 (35) P= .234
TOT_UNEM	-.0730 (35) P= .668	-.0818 (35) P= .630	1.0000 (0) P= .	.4844 (35) P= .002	.0441 (35) P= .796	-.1423 (35) P= .401	-.2220 (35) P= .187	-.0627 (35) P= .712	.0076 (35) P= .964
DEMOC	.1625 (35) P= .337	.1996 (35) P= .236	.4844 (35) P= .002	1.0000 (0) P= .	.3463 (35) P= .036	-.5146 (35) P= .001	-.8199 (35) P= .000	.3557 (35) P= .031	.1997 (35) P= .236
R_O_L	.2298 (35) P= .171	.9358 (35) P= .000	.0441 (35) P= .796	.3463 (35) P= .036	1.0000 (0) P= .	-.8039 (35) P= .000	-.6502 (35) P= .000	.8116 (35) P= .000	.2561 (35) P= .126
PIRACY	-.3331 (35) P= .044	-.7979 (35) P= .000	-.1423 (35) P= .401	-.5146 (35) P= .001	-.8039 (35) P= .000	1.0000 (0) P= .	.7126 (35) P= .000	-.7072 (35) P= .000	-.3628 (35) P= .027
FREE_PRE	-.1928 (35) P= .253	-.5319 (35) P= .001	-.2220 (35) P= .187	-.8199 (35) P= .000	-.6502 (35) P= .000	.7126 (35) P= .000	1.0000 (0) P= .	-.5949 (35) P= .000	-.2117 (35) P= .208
PPP	.3187 (35) P= .055	.7674 (35) P= .000	-.0627 (35) P= .712	.3557 (35) P= .031	.8116 (35) P= .000	-.7072 (35) P= .000	-.5949 (35) P= .000	1.0000 (0) P= .	.3270 (35) P= .048
COMPOSIT	.9810 (35) P= .000	.2005 (35) P= .234	.0076 (35) P= .964	.1997 (35) P= .236	.2561 (35) P= .126	-.3628 (35) P= .027	-.2117 (35) P= .208	.3270 (35) P= .048	1.0000 (0) P= .

(Coefficient / (D.F.) / 2-tailed Significance)

This "jump" factor is cause for concern. Both the democracy and rule of law variables appear to be very sensitive to slight changes in specification suggesting, in part, that these variables be the focus of the quasi-Poisson regression models. The way in which the political-institutional variables were measured may also contribute to this hyper sensitivity.[84] This is discussed at length in Appendix A – Methodological Notes.

The results presented above are suggestive, but far from complete. The partial correlations indicate that, when population is controlled for, the level of openness as measured by the free press variable, piracy and population could be linked to the number

[84] Future research would require closer examination of the instability research done by Marshall and Gurr (2005); especially measurement and transformation issues with the Polity IV data.

of Internet incidents. This suggests that "openness" in some way contributes to a larger number of compromised machines in a territorial context. But the link, so far, is tenuous. Piracy, a proxy measure for cyber crime, has a moderate positive relationship with the number of compromised nodes as a measure of cyber infrastructure instability but this will more likely be an artifact of criminal opportunity. The remainder of the analysis will focus on the impact that political and economic instability leaving out the sociological indicators of instability.

Some consideration regarding the accuracy of the measures used in this study is worth attention. First, how well has instability and perhaps more broadly institutional capacity been captured? No measure will be perfect. But making the distinction between instability, institutional incapacity, and even state effectiveness with respect to the cyber infrastructure is important yet well beyond the scope of this study. Some states, for example, may have high levels of state institutional capacity but low effectiveness in managing cyber infrastructure instabilities. The United States, Britain and Canada are typical cases. While other states have, in general, low institutional capacity yet high levels of state effectiveness in managing the growth of the cyber infrastructure – especially in its early stages. States in the Middle East and parts of East Asia are indicative of this relationship. Indeed, there are states with many combinations of varying levels of institutional capacity, instability and state effectiveness in both East Asia and the rest of the world. What is important to note is that after an outcome such as cyber infrastructure instability is produced, there are complex relationships and etiologies that link institutional capacity and state effectiveness together; and between them is politics. Thus, these measures are proxies at best.

As will be shown below, the cases chosen for this study are heavily skewed toward

socio-economic and political stability. It is likely that it is introducing bias in the correlation results. To explore this further, Chapter Five turns to the results from the regression models and in particular 'zooms' in on the East Asia region. This is important for the work here in substantive terms but also in statistical terms because East Asia provides a diversity of states that generate enough variance in stability measures which may increase model performance. If there are links between instability, territory, and cyber infrastructure incidents they should emerge here. This will also be important for a broader understanding of the securitization of the cyber infrastructure and state responses in East Asia – the subject of Part Two of this study.

The partial correlations indicate that the level of openness as measured by the free press variable, piracy and population could be linked to the number of compromised nodes. After controlling for diffusion, there is a weak positive relationship with free press. This suggests that "openness" in some way contributes to a larger number of compromised machines in a state. This link, however, is tenuous. Piracy, a proxy measure for cyber crime, had a moderate positive relationship with the number of compromised nodes. Were cross-national crime statistics readily available and reliable, further research should be done to explore the link between electronic crimes and the increasing number of compromised machines globally. Chapters Six and Seven of this dissertation will explore this relationship in more detail by examining several case where transnational organized crime has taken advantage of, and is driving, the growing number of compromised nodes globally.[85]

Internet diffusion, however, was strongly associated with the number of compromised nodes. This was not unexpected. What is somewhat surprising is the very weak link

[85] It is not likely, however, that national crime statistics will capture the impact of transnational organized crime.

between measures of wealth (PPP) and Internet diffusion for the economies chosen for this study. This affirms the axiom that Internet diffusion general follows an 'S' curve and once past a certain point, economic factors tend to be less important. What is important in the upper stratum is that, in general, the political measures of stability are not as strongly associated with cyber infrastructure instabilities as DK Matai has suggested. The more specific model of stability in the East Asia region is the subject to which the dissertation now turns.

Chapter Five: The Level of Democracy and Rule of Law and Cyber Instability

Introduction

Cyber infrastructure security incidents take on both territorial and non-territorial characteristics. This duality of Internet security has a direct impact on the securitization of cyber space. The dissertation now turns toward the link between socio-political instability and Internet incidents that DK Matai of Mi2G and others have posited. There are two key findings: First, the level of democracy has a minimal impact on the frequency of cyber infrastructure events cross-nationally. Second, the level of the rule of law – as a proxy for state capacity and stability – can be linked to cyber infrastructure instabilities. Thus, the level of the rule of law suggests a possible weak-moderate link between the proxy variable for institutional capacity and stability but the democracy model shows that Matai's claims are overstated, or at best, imprecise. The effects of specific socio-political factors on cyber infrastructural instabilities appear to be interactive rather than direct, let alone determinative.

Chapter Five begins with a general model of stability and the role of the state for all 49 upper-tier countries. Here, the 'leading' factors that were identified in chapter four are set with two distinct measures of stability – rule of law and level of democracy. Second, the focus shifts to East Asia in order to both understand the role of state capacity and stability in the cyber infrastructure, and to place this within the broader international context. The results indicate that there are unique characteristics in East Asia that set it apart from global patterns.

Stability and Cyber Infrastructure Security

The first model focuses on the impact of the rule of law on the distribution of Internet

incidents in the cyber infrastructure cross-nationally. It includes two other variables, the composite measure of diffusion and purchasing power parity based on the results of the simple analysis of the partial correlations in the previous chapter. More formally:

$$\log(h_*) = \alpha + \beta_1 \log(composite) + \beta_2 (RoL) + \beta_3 (PPP) + \varepsilon_i, where \phi \neq 1$$

The results are presented in Table 5.1 below with the dispersion parameter ϕ set at 1714204. A couple of caveats need to be pointed out regarding interpretation. Because of the way the composite variable is measured its coefficient of 0.8707 is actually quite large. A composite unit increase leads to a large percentage increase in the number of compromised nodes. The result is significant and clearly has the largest impact in the model. The level of purchasing power parity, as measured in international dollars, appears to have only modest explanatory power. The coefficient for purchasing power parity size is 0.2381 and is not significant. Rule of law is slightly more powerful. An increase in the rule of law is associated with a moderate decrease in the number of compromised nodes at the 99% confidence level. Again, it is important to keep in mind that while the coefficients for the rule of law (-0.676) and composite (0.863) appear to be close in scale, they are not. The regression slopes (estimates) have a percentage interpretation. The coefficient indicates that, controlling for internet diffusion and purchasing power parity, an increase of 1 on the 5 point rule of law scale results in roughly a 50% reduction in compromised nodes.[86]

[86] (exp(-.67)=.51)

Table 5.1 – Quasi-Poisson regression results: rule of law

```
Deviance Residuals:
   Min      1Q  Median      3Q     Max
-2692.0  -790.6  -368.8   343.9  4078.4
-----------------------------------------------------------------------
--
Coefficients:
                Estimate  Std. Error  t value   Pr(>|t|)
(Intercept)      0.86323   2.14859    0.402    0.689802
log(composite)   0.87807   0.04541   19.338    < 2e-16    ***
R_o_L           -0.67615   0.18385   -3.678    0.000637   ***
log(PPP)         0.23813   0.24451    0.974    0.335420
-----------------------------------------------------------------------
--
Signif. codes:  0 `***' 0.001 `**' 0.01 `*' 0.05 `.' 0.1 ` ' 1
(Dispersion parameter for quasipoisson family taken to be
1714204)
    Null deviance: 867774578  on 47  degrees of freedom
Residual deviance:  72716318  on 44  degrees of freedom
AIC: NA
Number of Fisher Scoring iterations: 5
```

Every statistical model and associated tests, specifically when the data are unusual, should be accompanied by the appropriate diagnostic procedures that check to see if the model is performing well. There are two concerns. First, plotting the residuals against the fitted values shows a bell shape opening toward the high end of the linear predictor (see Appendix – Figure 5.3). This suggests that there is some heteroskedasticity in the model. Various attempts were made to correct for this but were unsuccessful. Second, both Cook's statistic plots show one, perhaps two observations that are very influential in the model; they appear at the upper right corner of both plots. Interestingly, in order to correct for this several countries were pulled out of the case list and then the model was run again followed by another set of Cook's tests. This iteration repeatedly revealed "new" influential observations each time.[87]

Returning to the first hypothesis posed at the beginning of Chapter Three (H1) it

[87] See Figure 5.3 Appendix A for detailed explanation and plots.

appears that there is a weak-moderate relationship between the frequency of incidents and rule of law. It is, however, a tentative finding given the strength of the coefficient for this and other variables. The kind of change that would be illustrative of real relationship between rule of law and cyber infrastructure instabilities would have to be much greater. Recall that because of the way in which the composite measure for Internet diffusion is constructed, it is providing the most explanatory power.

> H1: There is a relationship between rule of law and the frequency of Internet incidents $(\beta_2 \neq 0)$

The null hypothesis can be rejected but barely. The coefficient for rule of law is statistically significant at the P=.001 level. Rule of law has a negative impact on the frequency of incidents (compromised nodes), but it is a weak one. The weakness of this finding suggests that while a country with high levels of rule of law can expect to on average have lower number of compromised machines – incidents -- there are many cases where this is simply not what is seen in the cyber infrastructure. For example, of the top five states with the highest number of compromised nodes – US, China, Germany, South Korea, Taiwan, UK - half have strong legal institutional environments within well functioning political regimes. Interpreted as a proxy measure for institutional capacity and overall stability, the rule of law appears to have only a modest impact on cyber infrastructure instability as measured by h_*.[88]

---

[88] The language used in this chapter to describe h_* shifts from the frequency and distribution of Internet incidents, the number of compromised nodes, to the more general concept of cyber infrastructure instability. They are all faces of the same phenomenon. However, as discussed in previous chapters, it is important to keep in mind that there is a difference between an "Internet incident" and a "compromised node" even though one presupposes the other. Both are indicative of cyber infrastructural instability.

The second hypothesis focuses on the impact of democracy on the frequency and distribution of Internet incidents cross-nationally. The model specification changes only slightly by removing the level of the rule of law and inserting the measure of democracy. Both cannot be included because of multicollinearity. Formally:

$$\log(h_*) = \alpha + \beta_1 \log(composite) + \beta_2 (DEM) + \beta_3 (PPP) + \varepsilon_i, where \phi \neq 1$$

The dispersion parameter ϕ is 2660173. The results are presented Table 5.2 below. The coefficient indicates that, controlling for internet diffusion and purchasing power parity, and increase of 1 on the 5 point democracy scale results in only a roughly 1% reduction in compromised nodes.[89] The coefficient for the composite measure of Internet diffusion has changed little from the previous model. It still has the largest role in explaining the variance in the distribution of incidents globally. The purchasing power parity coefficient has changed substantially to -0.448, significant at the 95% level. The hyper sensitivity noted earlier during the discussion of the partial correlation results has not diminished by focusing the model on key variables only. At this point, the need to move from cross-sectional data to time-series or longitudinal research design is apparent.

The impact that the level of democracy has on the variation in the number of incidents is minimal. During field interviews for this dissertation the question asked was "what institutional features allow for governments or policy makers to address the impact that the Internet has had on security." Many of the interviewees argued that countries like Singapore have a considerable advantage because they are not restrained by liberal democratic rules and principles. This non-democratic advantage has been cited as a key factor more broadly in the impact that Internet diffusion has on authoritarian regimes.

[89] (exp(-.014)=.01)

The original notion was that complex information ecologies created by rapid Internet diffusion (i.e. WWW technologies) would erode the authoritarian state's ability to maintain its monopoly on the flow of ideas, data, and information.

During the late 1990s and into 2000 the assumption that the Internet and other information technologies would be the electronic "Trojan horses" for democratic change was largely dismissed (Latham, 2002:102-103). In fact, it began to appear that non-democratic regimes were adapting to the many dilemmas created by information technologies faster than anyone thought. Whether or not a state is democratic is not a factor mitigating against the increasing frequency of Internet incidents.

> H2: There is a difference between democratic and non-democratic states and the number of Internet incidents $(\beta_2 \neq 0)$

The hypothesis H2 can be rejected. The policy makers in democratic states may feel that their counterparts in non-democratic states have a particular 'edge' in addressing the 'health' and stability problem of national cyber infrastructures but the data do not support this. The partial list of countries noted by Matai during the OII discussion identified non-democracies, or states with weak institutions or low institutional capacity, as growing sources of intrusion attempts and, hence, a threat to global security. The results of the *democ* model (Table 5.2 below) clearly show no link between the number of compromised nodes and regime type. The rule of law model suggests a possible weak-moderate link between the proxy variable for institutional capacity and stability but the democracy model suggests that Matai's claims are overstated, or at best, imprecise.

Table 5.2 – Quasi-Poisson regression results: Democracy

```
Deviance Residuals:
   Min      1Q  Median      3Q     Max
-3157.4  -809.1  -383.7   108.6  5422.1
---------------------------------------------------------------------------
Coefficients:
                Estimate  Std. Error  t value   Pr(>|t|)
(Intercept)     7.46932   1.35159     5.526     1.78e-06  ***
log(composite)  0.86805   0.05958     14.569    < 2e-16   ***
DEMOC          -0.01429   0.04564     -0.313    0.7556
log(PPP)       -0.48809   0.21155     -2.307    0.0259    *
---------------------------------------------------------------------------
Signif. codes:  0 `***' 0.001 `**' 0.01 `*' 0.05 `.' 0.1 ` ' 1
(Dispersion parameter for quasipoisson family taken to be 2660173)
    Null deviance: 863793747  on 46  degrees of freedom
Residual deviance:  95041761  on 43  degrees of freedom
AIC: NA
Number of Fisher Scoring iterations: 5
```

The diagnostics for the democracy model suggest two important features. The first is that, as was the case with the previous model, there appears to be some heteroskedasticity. The Cook's plots indicate that there are two, perhaps three observations that are influential – the US being one. The most likely explanation is that the results from the Cook's plots and the residual plots are related: the influence of several observations. The results from the diagnostic tests indicate that the models are borderline acceptable.[90]

Regional differences: East Asia and the rest of the world

As discussed earlier, East Asia has a growing reputation among systems administrators and policy makers for being the source of too many open relays, hackers, "spammers" and other assorted cyber transgressions. In statistical terms, this generalization can be subjected to a systematic analysis by adding a regional dummy variable with interaction terms on rule of law and democracy. The countries that make

[90] See Figure 5.4 Appendix A for plot and explanation.

up the regional variable are Australia, China, Indonesia, Japan, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan, and Thailand. The base group or benchmark group against which the comparisons will be made are non-East Asia region countries.[91]

Cross-national studies that look for differences between regions among various factors are often criticized for imposing artificial boundaries, geographically and culturally, around "regions" of the world. Internet diffusion, however, often reflects regional characteristics and attributes.[92] From an infrastructural perspective, there are clear regional differences with respect to routing and the distribution of autonomous systems. This, in part, leads to unique politics of peering within regional contexts. At the user level, there is also good reason to explore regional differences. For example, one of the biggest drivers of Internet diffusion in East Asia (at the infrastructural level) has come from cell phone adoption and usage which traditionally has been significantly higher than other regions of the world. Taken together, these reasons alone may not provide convincing evidence to look at regional differences. This dissertation, however, is focused on Asia Pacific security. Thus, for no other reason than "scope" it is useful to uncover regional characteristics and attributes.

Returning to the quasi-Poisson model specified above with the added dummy interactions:

$$\log(h_*) = \alpha + \beta_j X_{ij} + \delta_0 A_i + \gamma(X_i A_i) + \varepsilon_i, where \phi = 1$$

In the model above $\delta_0 A_i$ is the additive variable for East Asia and $\gamma(X_i A_i)$ is an

[91] For model specification with binary variables this study relied heavily on Fox (2002:130-136) and Wooldrige (2003:220-222, 225-226, and 233-234).
[92] See discussion in previous chapter.

interaction term. The regional focus model looks at the differences between East Asia and the rest of the world with respect to the factors that may explain the variation in the number of compromised nodes in the region. In order to "see" the difference that rule of law and democracy have in the East Asia region, effects plots are provided for the models below.[93]

The results below (Table 5.3) show that three factors affect the frequency of incidents in the cyber infrastructure in a country: composite measure of Internet diffusion, the level of democracy, and PPP. Since $\delta_0 A_i = 1$ when a country is located in the East Asia (both in the physical sense and cyber sense) and $\delta_0 A_i = 0$ when the country is grouped in the rest of the world; the interpretation of $\delta_0 A_i$ is the difference in the number incidents between East Asian countries and the rest of the world given the same amount of diffusion, PPP and democracy. If $\delta_0 A_i < 0$ then for the same level of other factors there is a difference between East Asia and the patterns in the rest of the world (ROW), keeping in mind that the coefficients have a percentage interpretation.

The regional dummy $\delta_0 A_i$ essentially allows for different intercepts between the two groups of countries. The interaction term $\gamma(X_i A_i)$ takes this "allowance" once step further to allow for a difference in slopes. For example, we may wish to assess the regional differential with a non-constant "effect" of various factors like diffusion and PPP. Stated in other words, the dummy interactions allow for the analysis to posit that the response to a change in a continuous explanatory variable (factor) differs between the

[93] Here I omit specification and analysis of a lower order term which cannot be interpreted in a meaningful way when used with interaction terms. See Braumoeller (2004).

base group and the East Asian countries; simply put, $\gamma(X_i A_i)$ is the differential effect.

The first regional model for East Asia considers the impact of the level of democracy on the variation of compromised nodes. Table 5.3 below shows the coefficients, standard errors and *t* tests for regional quasi-Poisson regression focusing on democracy. The magnitude of the variable composite has not changed from the previous models. The *composite*, DEMOC and PPP coefficients show little movement with the addition of the dummy variable and interaction terms. The dispersion parameter $\phi = 3723292$.

The coefficient for the regional dummy variable is -4.01. It is important to understand that the base group is the ROW, so, β_{ADUM} is the difference in intercepts between the East Asia and the ROW group. The difference between the two groups – East Asia and rest of world – is shown in Table 5.3. The relationship between wealth and compromised nodes is positive in the ROW, but negative in Asia. In the ROW, for a one unit increase in PPP we would expect h_* to almost double (.98). But in Asia we would expect h_* to decrease by less than half.[94] Applying this to the DEMOC, a one-unit increase in DEMOC gives only about a 4% reduction in h_* for the ROW,[95] but a 25% reduction in Asia.[96] The difference between ROW and ASIA is minimal. None of the key coefficients are statistically significant.

---

[94] (.98 + (-.13) = .85)
[95] (exp(-.07)=.04)
[96] (exp(-.07 + -0.07)= -.14)

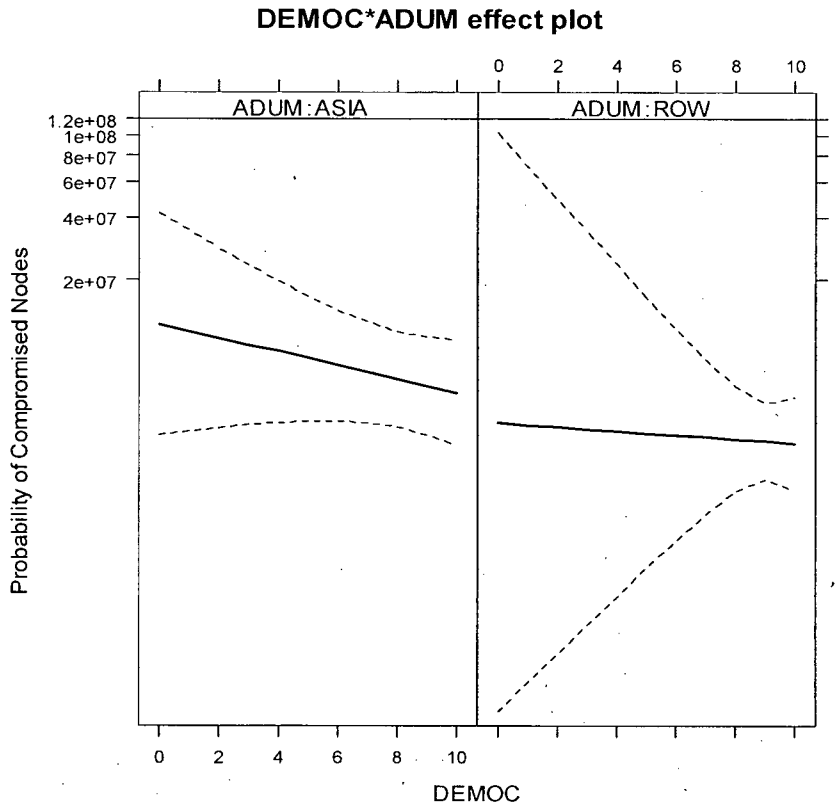
Table 5.3 – Dummy regression with interaction terms

```
glm(formula = h* ~ logCOMP + DEMOC + log(PPP) + ADUM + ADUM:logCOMP
+ ADUM:DEMOC + ADUM:log(PPP), family = quasipoisson)

Deviance Residuals:
   Min      1Q  Median      3Q     Max
-3877.5  -966.4  -255.6   348.5  6380.7

Coefficients:
                    Estimate     Std. Error     t value  Pr(>|t|)
(Intercept)         -3.14515     5.28744        -0.595   0.555574
logCOMP             1.43118      0.36754        3.894    0.000398 ***
DEMOC               -0.07621     0.06868        -1.110   0.274298
log(PPP)            0.98691      0.39147        2.521    0.016139 *
ADUMROW             -4.00859     7.09243        -0.565   0.575354
logCOMP:ADUMROW     0.62713      0.54013        1.161    0.253051
DEMOC:ADUMROW       0.05334      0.19016        0.281    0.780642
log(PPP):ADUMROW    -0.13887     0.50799        -0.273   0.786080
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for quasipoisson family taken to be 3723292)

   Null deviance: 373126841  on 44  degrees of freedom
Residual deviance: 117713921  on 37  degrees of freedom

Number of Fisher Scoring iterations: 6
```

To visualize the impact that the interaction terms have on the models, effects plots were produced. The effects plot in Figure 5.1 for the quasi-Poisson regression shows the interaction of the covariate DEMOC and the regional dummy variable for East Asia. The figure can be read as going from highest to lowest from left to right. On the graph below the vertical axis is the probability of compromised nodes in a given country. A 95% point wise confidence interval is drawn around the estimated effect. The solid effect line is sandwiched in dashed lines that represent the limits of the confidence envelope for the effect line. The confidence envelope translates statistical uncertainty in the estimation of the effect into a graphical display. Figure 5.1 confirms the numerical results in Table 5.3 that there is no differential effect of the level of democracy on the number of

compromised nodes in the East Asia region.

Figure 5.1 – Effects display for the interaction of the level of democracy and region.



In Figure 5.1 the tick marks along the vertical axis are labeled on the scale of the dependent variable – compromised nodes, the proxy for cyber infrastructure instability cross-nationally. The actual effect for East Asia and the rest of the world are plotted on the scale of the independent variable level of democracy. The level of democracy has only a slightly different relationship to the probability of cyber infrastructure instability for East Asian states and the rest of the world.[97]

The discussion now turns to the differential effect that the level of the rule of law has on the distribution of compromised nodes in East Asia. In contradistinction to the

[97] This discussion relies heavily on Fox (2003:5).

regional effect of democracy, the impact that the level of the rule of law has in East Asia is substantial. Table 5.4 below shows the results for both the regional dummy variable and the interaction effects. The dispersion parameter $\phi = 1428473$. First, the coefficient for ADUM is 21.02 significant at the P=.01 level. The difference between the two groups of countries is quite strong. There is a significant difference in the number of compromised nodes between East Asia and the ROW given the same amount of diffusion, rule of law and PPP. The relationship between wealth and compromised nodes is positive in the ROW, but negative in Asia. But this is to be expected given the *S* curve for diffusion and is consistent with the DEMOC model. In the ROW, for a one unit increase in PPP we would expect h_* to increase by about 40% (3.59). But in Asia we would expect h_* to be cut in half.[98] Applying this to the ROL, a one-unit increase in ROL gives about a 7% reduction in h_* in the ROW,[99] but a 90% reduction in Asia.[100] This is approximately 10 times greater. Confidence envelopes are nice and tight around the effect line. Results are significant at the P=.001 level.

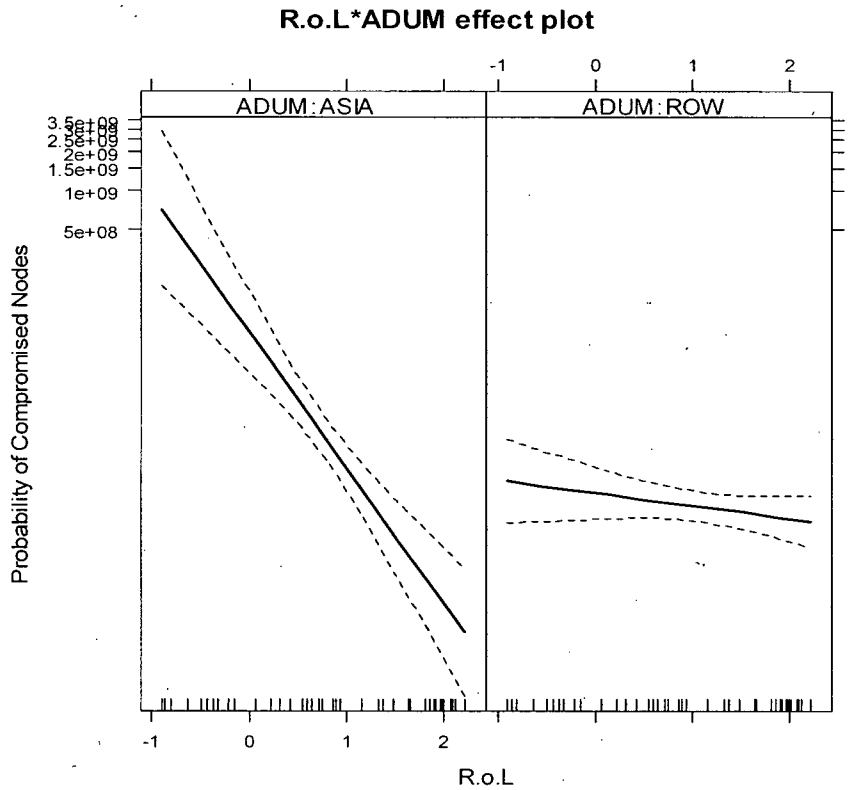
[98] (3.59 + (-2.50) = 1.09).
[99] (exp(-2.44)=7.9)
[100] (exp(-2.44 + 2.21)= -.03)

Table 5.4 - Dummy regression with interaction terms

```
glm(formula = TSOURCE ~ logCOMP + R.o.L + log(PPP) + ADUM +
ADUM:logCOMP + ADUM:R.o.L + ADUM:log(PPP), family = quasipoisson)

Deviance Residuals:
   Min      1Q  Median      3Q     Max
-2664.4  -729.0  -175.7   757.6  2534.3

Coefficients:
                      Estimate     Std. Error    t value  Pr(>|t|)
(Intercept)           -31.0039      6.6162       -4.686  3.52e-05 ***
logCOMP               2.0264        0.3255       6.225   2.79e-07 ***
R.o.L                 -2.4488       0.4022       -6.088  4.31e-07 ***
log(PPP)              3.5958        0.5182       6.939   2.98e-08 ***
ADUMROW               21.0202       7.5781       2.774   0.008541 **
logCOMP:ADUMROW       0.1044        0.4102       0.254   0.800488
R.o.L:ADUMROW         2.2144        0.4408       5.024   1.23e-05 ***
log(PPP):ADUMROW      -2.5047       0.5812       -4.309  0.000112 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

(Dispersion parameter for quasipoisson family taken to be 1428473)

   Null deviance: 374456589  on 45  degrees of freedom
Residual deviance:  54779127  on 38  degrees of freedom

Number of Fisher Scoring iterations: 5
```

To illustrate the differential effect of the rule of law interaction term, Figure 5.2 shows how the "slope" decreases as the values of the lower order term increases across the number of observations. In Figure 5.2 below, the tick marks along the vertical axis are labeled on the scale of the dependent variable – compromised nodes, the proxy for cyber infrastructure instability cross-nationally. The actual effect for East Asia and the rest of the world are plotted on the scale of the independent variable level of the rule of law. The level of the rule of law has substantially different relationship to the probability of cyber infrastructure instability for East Asian states and the rest of the world.

Figure 5.2 – Effects display for the interaction of the level of the rule of law and region



While it is clear that the level of rule of law is an important factor in the frequency and distribution of incidents in East Asia, it may be the case that this measure has a larger impact in a region that has a more variance in the level of the rule of law when compared to the cases in the rest of the world. The model was run, and effects plots produced, for other regional groupings. Other than the East Asia grouping, none indicated any significant differential effect in the level of the rule of law. Future research would see this done in the context of a time series design.

All of the problems mentioned above and in Appendix A can affect the dependent variable. This study is focused on all compromised nodes so problems like worm identification become less of an issue. Yet, there are two types of measurement error that are of particular concern here. Non-systematic measurement error occurs where the

values are sometimes too high and sometime too low. This increases inefficiency in the data but does not increase bias; and on average the value will be correct. This type of error on the dependent variable theoretically should be less of a concern because the sample for source IP is so large that the error would eventually cancel itself out. The second type of measurement error is systematic across the data. Systematic measurement error is a consistent mis-measurement of units. The only way to tell if this is happening is to acquire additional DShield data to cover more time periods (and re-sample).

Another issue is the choice of explanatory factors and the ever present possibility of omitted variable bias. For example, it was not possible to find reliable cross-national data on crime, deference to authority indicators, or measures of sudden economic shocks in high tech sectors all of which leave out a potentially powerful set of explanatory factors – even with the inclusion of several proxy variables to compensate. This could, in part, explain the heteroskedasticity found in the models above. A number of diagnostic tests were used to check for various problems in the data from heteroskedasticity to the amount of nonlinearity in the models. Both problems were found and attempts were made to compensate. There are also substantial patterns of clustering in the data.[101]

The full and partial correlations discussed above strongly suggested that the regression models would be "sensitive" to slight changes in specification. Sensitivity analysis essentially requires an estimation of the original model followed by a reasonable modification of the original. If the important conclusions change dramatically then the original specification is said to be too sensitive to be reliable. Two procedures were carried out in order to test for this. First, the independent variables were increased to

[101] See Appendix A – Methodological Notes, as well as Appendix A Figure 5.5 for contour plots of the variables rule of law and democracy.

include additional factors that could conceivably help to explain the variation in the number of compromised nodes cross-nationally. Of the key explanatory variables that had a marginal impact the coefficient signs changed from positivist to negative as expected from the partial correlations. Second, an alternative measure was used in place of DEMOC. In both cases, there was some sensitivity and subsequent research would need to explore alternative measures to other explanatory variables. For now, the "robustness" of the models is uncertain.

Finally, internal validity is, for now, impossible to assess. It would be useful to compare these results to externally verifiable data to find and validate other key patterns that affect the distribution of compromised nodes or Internet incidents and cyber infrastructural instability. This involves asking the same questions but testing the propositions using different data. For example, would there be a correlation between rule of law and compromised nodes using data gathered from other sources? Are differences between regions or between democracies and non-democracies? Unfortunately, DShield represents the only data set available to the research community.[102] In order to try and asses the internal validity of this work several commercial providers of large scale distributed intrusion detection data were contacted in 2003. None of the firms agreed to share their data or discuss their methods of analysis.

General Results and Interpretation

The purpose of Part One and the regional focus of this dissertation was to test systematically for country differences in the effects of Internet diffusion, wealth, degree

[102] There are now other research projects that can supplement the DShield.org data. For example, there is the Internet Motion Sensor at the University of Michigan <http://ims.eecs.umich.edu/> and the my|NetWatchman project <http://www.mynetwatchman.com/>. For a more thorough discussion consult the study by Bethencourt, Franklin, and Vernon (2005).

of democracy, and the level of the rule of law on the number of compromised nodes and to model this variation both globally and in East Asia. Reducing the number of compromised nodes globally will not reduce the threat of network intrusions entirely, but it will decrease the likelihood of a broad range of capabilities based threats. It will also go a long way to reducing the overwhelming amount of "noise" on the Internet that often obfuscates real attack signatures. Increasingly, digitally driven economies will also have less "drag" on them by reducing the number of compromised nodes that can be easily used in distributed denial of service attacks, spam, and other nuisances of the modern Internet environment which places undue strain on productivity and trust in the e-economy.

There are causality issues that remain unresolved. Political-institutional factors will not be important unless governments are actively trying to address Internet security problems stemming, in part, from increasing cyber infrastructural instability. With respect to causality: are lower numbers of compromised nodes influenced by the acceleration in Internet adoption patterns, or are both phenomena correlated but caused by another factor, such as wealthier, more productive economies?[103] There is no clear advantage to authoritarian regimes in controlling the number of compromised nodes and the frequency of Internet incidents. At this point, it should be clear that the ideal research design to confirm these findings would be longitudinal rather than cross-sectional.[104]

Economic factors appear to play little role in explaining cross-country differences in

[103] It is hard to conceptualize diffusion of the infrastructure as anything other than a user defined process governed by national infrastructure strategies. The observation may be self-evident and trivial.

[104] There are two points to be made with respect to the statistical robustness of the results. First, removing and adding the US case does change the results, but only slightly. Second, the models are very sensitive to specification. Changing assumptions can generate wildly differing conclusions. See Appendix A. As noted early on, the only way to 'fix' this is to move to a time-series design with sampling periods from 1999 to 2005 ($N \approx 1.75$ billion) for 51, possibly 52, cases.

the sample of 49 upper tier states. While the amount of Internet diffusion is the most powerful factor, gross domestic product per capita and purchasing power parity cannot be linked to either diffusion or the distribution in the number of compromised nodes in the upper tier countries chosen for this study. This is, in part, because Internet diffusion is not associated with increases in wealth in the upper half of the states in the digital access index. Were this study to incorporate states in the bottom tier, it is likely that economic factors would play a stronger role.

There is no evidence of a difference between democracies and non-democracies and their ability to control the number of compromised nodes. Cross-nationally, both generally and in East Asia, the level of democracy did not appear to be a factor. A key implication of this result is that non-democratic regimes do not necessarily have an "authoritarian advantage" in controlling the number of compromised nodes. While they have been increasingly successful at managing content based restrictions (primarily WWW based) and turning various applications of the Internet into a quasi-surveillance tool, there is no empirical evidence to suggest that more authoritarian regimes have a "deeper" control over Internet security matters. This conclusion is, of course, as measured by the frequency of Internet incidents sampled in each country. An alternative explanation for the result could be that no government has begun to address security at this level and thus there is no measurable difference between regime types. The latter explanation, however, is unlikely.

While reducing the number of compromised nodes has always been the weak link in national and international Internet security policy, most governments began to address this problem in early 2000. Reducing the number of compromised nodes frustrates the

creation and use of chained-relays, lessens the impact of zombies, forces spammers into ever shrinking corners of cyber space, and reduces the ability of hostile actors to "talk and control" from a distance. The number of compromised nodes and the resulting Internet incidents has been an embarrassment for some governments. In East Asia, Chinese and Korean authorities have tried – often without success – to come up with a strategy to reduce the numbers. The primary pressure has come from systems administrators from outside the region who have begun to blacklist IP spaces based up country of origin (Confidential Interview, Hong Kong SAR, 2002; China Daily, 2005).

For the first time, the problem of compromised nodes is being directly addressed by a government agency. Australia will be the first country in the world where regulators will begin notifying ISPs of infected machines using their access. In a three-month pilot program, the Australian Communications and Media Authority will identify compromised machines and ask their owners to clean them or risk being disconnected (Savvas, 2005). This new territorial focus has taken on a 'you take care of your territory and I'll take care of mine' disposition.

Internationalizing Internet security is no easy task; there are multiple actors and stake holders, converging and diverging interests, regional political dynamics that are often incommensurate. There have been a plethora of suggested international mechanisms to mitigate these frustrating factors. One such idea is to use a collective security approach to protecting cyber infrastructures (Bryen, 2002).

This international mechanism has been quietly studied by the ITU, primarily because other international efforts have done little to reduce cyber infrastructure instabilities. Bryen writes:

> In some cases, governments and organizations with substantial resources are increasingly backing such attacks. To respond properly to this threat to security and prosperity, a strong, international solution grounded in a political framework is needed: isolated technical or legal solutions will not work. Moreover, efforts to confront structured hostile threats on a national level have been less than successful, and the technology employed has not been adequate to seal the systemic vulnerabilities in the information technology-dependent critical infrastructure (2002:3).

The key ideational shift that would have to take place is that states would have to consider cyber infrastructures as part of a global infrastructure rather than a collection of national 'spaces' that are connected to one another. This, given recent trends in international politics and in the frequency and distribution of Internet incidents, is unlikely.[105]

I have emphasized the role of political institutional factors in explaining country differences in the dependent variable which measures cyber infrastructure instability. At a fundamental level, states are responsible for creating and maintaining the laws, security policies and thus, the integrity and stability of their infrastructures. Unlike the level of democracy, rule of law is linked to the dependent variable. The measure of the rule of law used in this study, from an institutional perspective, is broad. The impact of the level of the rule of law would likely become stronger in a time-series design, or at the very

[105] A recent example is the tension over US control of the domain name system (DNS). The EU is led a diplomatic effort at the World Summit on Information Society (WSIS) meetings in Tunisia 2005 to change this. Other countries, such as China and Iran are supporting this effort, albeit for different reasons than the EU. The DNS governance issue is the first, in what is likely to be a continuing series of moves to at the same time pull Internet governance 'upward' to the UN's ITU and 'downward' to individual nation-states. The US has maintained some control over Internet infrastructure (albeit very arms length) is responding to these challenges with a kind-of cyber Monroe Doctrine. Recall that the Monroe Doctrine was a unilateral declaration by the US that it would not permit European powers to establish new colonies in the Western Hemisphere. A similar policy stance has emerged from the US Commerce Department – which oversees the not-for-profit DNS agency – which tersely says no to non-US control either at the International level (i.e. UN) or devolving DNS systems to the control of individual countries. These issues are beyond the scope of this study.

least, preserve the initial results. It is important to point out, however, that a comprehensive theory of security in the cyber infrastructure would have to be multiscalar, explaining both the small scale of a sequence of Internet incidents and the larger scale of the infrastructure stability and social and political processes in which these incidents occur.

Conclusions: East Asia

The analysis done for eleven Asian countries demonstrated that some explanatory factors had more importance in a regional context than did others. First, there is no differential effect of the level of democracy on the number of compromised nodes in the East Asia. This particular result is more interesting in the regional setting given the wide range of political systems in the region when compare to the rest of the world group. Second, the level of the rule of law interaction did have a significant differential effect when compared to the base group. Institutional capacity and stability matters in this region. This is the key finding of the analysis.

The level of the rule of law has a substantially different relationship to the probability of cyber infrastructure instability for the Asia country grouping and the rest of the world. States with lower levels of the rule of law are more likely to have higher levels of cyber infrastructure instability than would states with higher levels of the rule of law, while states in the Asia grouping with high levels of the rule of law are less likely to have cyber infrastructure instabilities than states in the rest of the world grouping with a similar level of the rule of law.[106] The relationship between the level of the rule of law and the probability of cyber infrastructure instability is also much steeper for East Asian states

[106] Singapore would be a case in point.

than for the rest of the world.

In short, Matai's claimed relationship between socio-political stability and cyber infrastructure instability cannot be dismissed as easily as critics may wish but only within certain contexts. There is some evidence to support a link between cyber infrastructure events and macro-level variables. It is important to point out that DK Matai identified primarily non-democratic regimes as correlated with intrusion attempts: Russia, Turkey, Brazil, Saudi Arabia, Egypt, Morocco and Pakistan. Of this list, which presumably is not exhaustive, only Russia, Turkey, Brazil, and Saudi Arabia appear as cases for this study. Overall, however, the link between the "stability" of a country – economic, social, or political – is at best a very weak one.

The underlying goal of Part One was to demonstrate that working at the level of the compromised node holds theoretical and methodological promise but large *N* studies alone will not accomplish the task. Part Two of this dissertation continues at the level of the compromised node but moves from the aggregate perspective of the last three chapters to a more narrow set of case studies. This shift in focus is apropos given the stark regional findings presented here. Chapters Seven and Eight of Part Two examine transnational organized crime and organized collections of compromised nodes called bot nets, as a high-tech threat to firms and state organizations in the East Asia; a problem that many in the Internet security community consider to be the most serious Internet based threat. By looking at the coevolutionary adaptive gap between sophisticated, well organized criminal elements and state response mechanisms used to confront this threat the analysis focuses on how far the adaptation space has widened.

Chapter Six: Non-traditional Cyber Security Threats in East Asia

Introduction

Reconsidering traditional and non-traditional concepts about what constitutes security in an era of rapid diffusion of information technologies and infrastructures requires framing technologies such as the Internet not just as a mode of communication but also as an environment that provides the ability to act at a distance. This duality is key to realizing the positives uses of Internet technologies. It is also a source of vulnerability and insecurity that both state and non-state actors may exploit. Considerable disagreement remains over both the nature and source of the threat from the cyber infrastructure in East Asia.[107] There is, however, a growing consensus that non-state actors, especially sophisticated organized crime groups, are rapidly adopting new technologies and leveraging those that understand those technologies. This techno adaptation by organized crime in East Asia comes at a period when these groups, according to many, already pose a threat to both state and regional security. If there is evidence of a nexus between system intruders and organized crime groups in the region, two questions emerge: Is there a threat to security and stability? And can the East Asian state adapt?

The focus of the dissertation now shifts from an aggregate analysis of the relationship between state instability and compromised nodes to transnational organized crime as a high-tech threat to firms and state organizations in East Asia. There are three objectives of Part Two of this study. The first is to investigate the veracity of the claims that there is a nexus forming between traditional and non-traditional transnational organized criminal

[107] Part Two of this dissertation uses the term East Asia to collectively mean the countries of Northeast Asia (Japan, Noth Korea, South Korea), East Asia (China, Taiwan, Hong Kong SAR, Cambodia, Vietnam) and Southeast Asia (the Philippines, Singapore, Malaysia, Thailand, and Indonesia). Part One of the dissertation included parts of South Asia, but these will be ignored for the remainder of the discussion.

groups in East Asia, and systems intruders or 'hackers'. The second objective is to characterize the differing forms of organized crime in the region and revisit how these forms are treated in the security literature. The latter is important because it allows for a more thorough understanding of how a hacker-organized crime nexus might be approached from an international security studies perspective. The third objective is to situate this finding within the broader process of cyber infrastructure securitization currently taking place in the region. This securitization process, which is far from complete, provides an insight into how states in the region perceive and respond to both traditional and non-traditional security threats. By looking at the coevolutionary adaptive gap between sophisticated, well-organized criminal elements and state response mechanisms used to confront cyber threats the analysis focuses on if, and how far, the adaptation space has widened.

The remainder of chapter Six outlines the organization of Part Two of the thesis and briefly summarizes its findings. Chapter Seven begins with a brief review of the literature on transnational organized crime in East Asia and why, from time to time, researchers in International Relations and security studies re-visit this problem in order to assess its potency as a non-traditional threat to state security in the region. Chapter Eight begins by investigating the claims that there is an ever increasing overlap between traditional transnational organized criminal groups in the region and computer hackers that perform illegal systems intrusions for financial gain. The focus here is on two case studies from the Hong Kong-Shenzhen region.

What is important here is the idea that there are changing patterns of organized crime in East Asia which are distinct from the changes taking place in other regions of the world. Weak institutional capacity and a globalization of knowledge and technology are

important supporting factors. The primary research for this dissertation focuses on the organized building and use of chained compromised nodes in cyber space (bot nets) by what I call non-traditional organized crime groups in the region. The distinction is made between traditional organized crime groups in East Asia and non-traditional forms of criminal organization. Traditional organized crime (TOC) focuses on older, more hierarchical, sub-regionally based (often local) groups like the Triads and Tongs. Non-traditional organized crime groups (NTOC) are characterized as less hierarchical collections of more nimble networks that are transnational, multi-ethnic, often fleeting groups. The primary distinction from a technological perspective is the uses of the cyber infrastructure for criminal gain.

The final substantive chapter of Part Two discusses the results of the field work and sets them within the context of the cases countries in the region. Chapter Nine then turns to an assessment of the adaptation space between sophisticated organized criminal groups and state responses in East Asia. In light of the findings two central questions emerge: is there a threat to security and stability; and can the state adapt? As will be shown below, it is the absence of clear adaptation strategies and responses that are, in part, responsible for the continued securitization of the region's cyber infrastructure. Chapter Nine links the problem of transnational organized crime to security in the region and how states perceive this as part of a broader loss-of-control in cyber space. State responses to the problem of bot nets are fleshed out, assessed in light of the two cases presented in chapter seven, and tentative conclusions reached about the new 'nature' of the threat from the cyber infrastructure.

A note on methodology

The research described in the following chapters is based primarily on field work and

documentation from scholarly journals and media reports. During the period 2001-2004 I conducted 31 interviews with government officials, engineers, and members of the 'hacker community' in Tokyo, Seoul, Manila, Kuala Lumpur, Hong Kong SAR and Singapore; as well as with individuals in Canada, the United States and the United Kingdom. The field research evolved as a 'snow ball' sample where one chance encounter in Singapore in 1999 led to a shallow introduction to the 'underground' community in East Asia. From initial contacts, interviewees were asked the question "would you know of someone I could talk to about that" in order to keep the sample going.[108] Interviews with government officials and security practitioners in East Asia yielded valuable information on new and emerging Internet threats that states and firms face from organized crime. It was also useful to get firsthand accounts on the policies and strategies that have been implemented in national settings in order to get a sense of what has worked what has not worked in the past and why. Field interviews also provided a unique opportunity to speak with individuals in the "underground" community. While access to this population was limited when compared to government policy makers and network engineers working at large firms, enough qualitative data was gathered to gain provisional insight into general behavioral trends.

Given the subject matter under study here, the use of anonymous sources was unavoidable. Studying the adoption and integration of Internet technologies by TOC groups involves examining the nexus or overlap of two types of hidden social networks:

---

[108] Name generators were used during interviews. Marsden (2003) defines name generators as questions asked by an interviewer to an interviewee regarding their personal social networks (i.e. friends, family, business associates and so on). Marsden studied the interviewer effect on the use of name generators in social network analysis. His work is relevant only in the sense that interviewer effects (especially on social network questions like "do you know so-and-so") can be both statistically and substantively significant. But he cautions that even under ideal laboratory conditions respondents are less likely to reveal depth in their personal social networks and these results can vary widely across different interviewers and interview techniques used (2003). The conditions in this study were far from ideal and any information on the extent of the respondents' social network(s) is treated with a healthy dose of caution and qualm.

organized criminal groups and network intruders. At some point in the early development of the Internet these two groups were, for the most part, mutually exclusive. Over time, however, connections formed which linked sophisticated criminal enterprises with "crackers" at varying levels of capability. Unfortunately, the use of anonymous sources is often necessary simply because crucial pieces of information might never see exposure if a name had to be attached to information shared or discovered.

I adopted several informal "validity" checks when speaking with "crackers" or network intruders involved with or claimed knowledge of this nexus. First, it was necessary to somehow assess the skill level – if only at an ordinal level – of the supposed network intruder who is relaying information about changes and trends in the practices of the "underground" in East Asia. For this research I avoided Internet relay chat (IRC) encounters, pushing instead for face-to-face meetings. This was a precarious undertaking but interviewing the individual or individuals in their "laboratory" reduced the likelihood that the interviewee would turn out to be a low level "script kiddie" and thus of questionable value.[109]

Second, while doing the field research I assessed the authenticity of the interviewee by first assuming that the type of operating system distribution that they used approximated the skill level of the supposed network intruder. If the individual offered to illustrate a point on a computer it was essential to take note of this point. While many sophisticated crackers keep a variety of machines with versions of Microsoft operating systems installed it is very unlikely that it is their main "work" machine.[110] Capable

[109] It is important to point out, however, that script kiddies are still capable of a number of above average intrusions, but it is unlikely that lower level hackers have the ability to sustain themselves in the world of transnational organized crime. My trips to Asia and the subsequent interviewing that was conducted over the past few years strongly indicates that script kiddies have been "hired" to install key loggers and transmit passwords but are rarely tasked with more sophisticated sub-contracted network intrusions.

[110] In one instance, the interviewee began pointing and clicking through intrusion software downloaded on

network intruders do look for vulnerabilities on Windows machines, as well as other operating systems like IRIX, Solaris, Linux and the BSD family, but the implementation and or execution of remote hacks will invariably be constituted on some unix-like operating system with little more than an a few open terminals visible on the desktop. In a similar vein, most highly effective network intruders have some working knowledge of assembly languages and are usually "fluent" in C and or C++. If I encountered an individual struggling with a simple shell script written in a "higher" language, I assumed that it unlikely that this individual could be ranked in the upper echelons of network intruders.

It is important to point out again that even 'script kiddies' can be effectively employed by criminal elements in the organization of organized crime using the cyber infrastructure. The factors discussed above are general indicators only and assessing the authenticity of the computer skill level of the interviewee is only the first step. The second problem is characterizing the veracity of any claims of ties to organized criminal networks. This was particularly tricky as decisions on field safety and courses of action often had to be made on the fly – in one instance after what turned out to be prerequisite amounts of time spent in a pub or bar.

I make no claims here to have penetrated that murky criminal underworld in East Asia; though, it must be pointed out, that it is an environment that is not as hidden as one might think. Unlike North America, academics doing field work in East Asia sometimes have the ability to gain access to communities and populations that would otherwise be inaccessible. Being a young field researcher helped rather than hindered making contacts within this population. Superficial characteristics, such as appearance, played a key role.

---

a Windows XP laptop while we were sitting in a bar. The interviewee was trying to illustrate a new "hack", but from this information alone it was clear that he did not know as much as he had claimed.

This, from what I can guess, is a result of a large generational divide within organized criminal groups in several East Asian cities – especially ones that are actively incorporating technology as tools.

While these factors may have helped with access to the two hidden population groups and the nexus between them, it may have hindered interviews with government policy makers in the region. Policy makers and analysts were, in most cases, only able to elaborate on policies and strategies that were readily available from agency websites or existing literature. The vast majority of the policy makers and law enforcement officials in the region argued that while the threat posed by high-tech enabled TOC groups used to be significant, law enforcement and intelligence agencies were now closing the gap. There were two notable exceptions. The first is the Philippines. Here there was broad based acknowledgment that the gap was widening, an acknowledgment that came without much of the rhetoric of the official line that I was subjected to in other countries. The second exception was South Korea. Before traveling to Seoul, I sent several letters and email introductions to the relevant government agencies requesting interviews. Only one individual agreed to a brief "supervised" meeting during which I was told that there never really was a problem (Confidential Interview, Seoul, 2003).

The criminology literature does not reveal much in the way of evaluative case study information on the impact of Internet technologies on transnational crime and the impact of law enforcement efforts against this type of criminal behaviour in East Asia. What is being suggested in criminology research thus far is that a significant level of computer-related crime lies beyond the capacity of law enforcement agencies alone to address. The ideal policy response, it is generally argued, would see a mix of law enforcement, technological and market based solutions and response mechanisms (Grabosky, 2000).

Ultimately, however, in most jurisdictions, the responses are left to local law enforcement.

It is important to point out that while the criminology literature does inform this study, it is not a discipline specific exploration of crime and law enforcement issues in East Asia. This is a rethinking of the impact that non-traditional security threats such as TOC have on security not law-enforcement specifically. As such, it is a "top-down" perspective from Political Science – International Relations using two case studies-[111]; rather than a "bottom-up" approach used in Sociology - Criminology. The literature on non-traditional security threats in International Relations and security studies provide the starting point.

The Leviathan now faces additional pressures from networks forms of organization that often mimic the ranks of states in exploiting the diffusion of modern technologies (Deutsch, 1966; Rosenau, 1990; Rosenau and Czempiel, 1992; Risse-Kappen, 1995). Enabled or amplified by the cyber infrastructure, network-based threats now span the entire security spectrum (Matthew and Shambaugh, 1998; Lilley, 2003; Sageman, 2004; Deibert, 2002). As will be shown below, the emergence of new threats and new actors does not by itself provide conclusive evidence that the role of the state as the primary provider of security is in decline. On the contrary, due to the fundamental nature of the digital world, cyber enhanced security threats and the emergence of new actors are not entirely beyond the capacity or scope of state-based responses. The insecurities of the digital world may well call into question some of the efficacy and legitimacy of

[111] For the purpose of Part Two of this dissertation a case study is "an intensive study of a single unit for the purpose of understanding a larger class of (similar) units. A unit connotes a spatially bounded phenomenon - e.g., a nation-state, revolution, political party, election, or person - observed at a single point in time or over some delimited period of time" (Gerring 2004:342). The definition provided by Gerring is an 'ideal'; I am convinced that much more field work would be required before there would be sufficient evidence to make an inference or "understanding [of] a larger class of units."

traditional state-based security when applied to new Internet based threats; but for the foreseeable future the state remains the only actor with the authority, legitimacy, resources and governance tools to address these issues.

Chapter Seven: Organized Crime as Cyber Threat

Introduction

One scholar theorizes "that criminal organizations might well move from corruption and co-option of political elites to more direct control of political power" and that it is possible that "the main fissures in international politics would be that between 'outlaw states' and law-abiding states" (Williams, 1999:51). These fissures are already forming in cyber space where jurisdictional arbitrage by traditional and non-traditional TOC has meant that states with lower levels of institutional capacity and high levels of Internet diffusion (usually driven by rapid economic growth rates) are playing host to uncivil society groups seeking safe digital harbors. Does this constitute a threat to security?

This is an examination of the pressure that non-traditional security threats such as TOC place on security through illicit uses of the cyber infrastructure and as such it is a "top-down" perspective from Political Science – International Relations; rather than a "bottom-up" approach used in Sociology. The literature on non-traditional security threats in International Relations and security and the perspectives contained therein provide the starting point. I argue in this chapter that unlike other regions, East Asia are not seeing a reduction in traditional forms of organized crime as the newer non-traditional transnational organized criminal groups emerge and evolve. Rather, both are growing, each with its own characteristics and attributes and uses of technology. The effect is additive and interconnected. This has a direct impact on the nascent nexus explored in Chapter Eight.

This pattern is contrary to that which is emerging in Europe as new non-traditional networked forms of TOC are 'replacing' older hierarchical traditional organized crime. There are two general factors that explain this additive effect in East Asia. First, there

has been a weakening of institutional capacity in key regions of mainland China during a period of rapid, uneven economic growth. Second, globalization of the international system has meant cheap and easy access to advanced knowledge and technologies. The 'newer' non-traditional forms of TOC have focused attention on more sophisticated uses of technology in crime which has enabled them to create more stable black markets and connect with more traditional forms of organized crime.

Transnational organized crime in East Asia

The definition of 'organized crime' used in this thesis is behavioral rather than legal. This is, of course, due to the regional focus which presents a considerable amount of variance in legal systems, concepts of 'crime', which make a definition based on law or governmental policy not useful for this research. There is a growing international legal framework that commits states that ratify it to taking a series of measures against transnational organized crime. Transnational crime (with or without the 'organized' element) is distinct from international crimes and domestic crime – the former prosecuted under international law and the latter under national jurisdictions. An organized criminal group – whose activity is organized crime - is defined by the United Nations Convention Against Transnational Organized Crime[112] as:

> a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit (Article 2 Sec a.).

Organized crime is considered 'transnational' if it: a) it is committed in more than one state; b) is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state; c) is committed in one state but involves

[112] In December 1998 UN resolution 53/111was passed from which the General Assembly established an Ad Hoc Committee to begin the process of developing an international convention against transnational organized crime and three supporting international legal protocols. The convention was adopted by the General Assembly by Res. 55/25 in November 2000 and entered into force September 2003.

an organized criminal group that engages in criminal activities in more than one state; or d) is committed in one state but has substantial effects in another state (Article 3 Sec 2.a). The illicit activities covered by the UN Convention range widely from trafficking in drugs and humans to computer crime.

Settling on a precise, meaningful sociological definition of transnational organized crime is important because it directly scopes and informs conclusions. This is particularly important when addressing TOC relationships with other social networks like systems intruders and also when assessing substantive links to national security more generally. For example, during the international meetings to hammer out a UN TOC Convention, the most difficult task of the national representatives was to agree on what transnational organized crime is and what it is not. The end result, as shown above, is a very broad common denominator definition.

Even the term 'transnational organized crime' itself is not without its critics who argue that the international legal definition was never really designed to be useful for those actively engaged in studying or responding to it. They argue that TOC has become a catch-all repository for the bad things that happen across borders and that, more portentously the:

> concepts [organized crime and transnational organized crime] share the advantage of being easily exploited. Each can imply whatever the speaker wants it to be: a massive threat; a theatrical legacy; or petty criminals and hoodlum bikers. The police, politicians, public and media tend to see the term organized crime and alternatively transnational crime, as an undifferentiated blanket under which most 'serious' crimes can be shoved. The concept of organized crime has become mythologized to the point of total distortion, rendering it useless for anything but political mileage and the bargaining for resources by law enforcement (Beare, 2000).

This is not just a problem that can hinder cross-border cooperation or slow the progress of domestic legislation designed to conclude mutual assistance agreements, it can also create operational problems for law enforcement at all levels (Loree, 2002:73). A case in point would be the persistent struggle in formulating extradition treaties in the East Asian

region due to barriers which can often be distilled down to disagreements over the definitions of offenses.

Academic studies are not bound by such constraints and often dispose of international definitions in favor of more sociological and behavioral frameworks. For example, Finckenauer (2005) defines organized crime in terms of loose networks that share continuity across space and time. For Finckenauer, TOC has little in common with what he argues are fictional interpretations in the Western media based largely on a romanticized mid-twentieth century understanding of *la cosa nostra.*[113] Finckenauer posits that these organizations are instead "loosely affiliated networks of criminals who coalesce around certain criminal opportunities. The structure of these groups is much more amorphous, free floating, and flatter, and thus lacking in a rigid hierarchy" and that "continuity is maintained over time and across crimes, and remains an important definitional element of what is truly organized crime" (Finckenauer, 2005:65-66). This self-perpetuation, of course, presupposes some sort of sophistication, skill level of at least some of its members, and a socio-political environment conducive to survival.

A recent report published by the Council of Europe's Octopus Programme concluded that the evolution of TOC over the last decade suggests that the "notion of clearly defined hierarchical organisations is being replaced by one of criminal networks – consisting of individual criminals or cells of criminals as well as legal entities and professionals which are more or less loosely affiliated and cooperate in varying compositions for particular criminal enterprises" (2005:44). This conclusion, based on the study of TOC in Europe, would seem to be in accord with some of the more recent research on TOC in East Asia. An instructive example is the work of Zhang and Chin who studied Chinese human and

[113] La cosa nostra loosely translates to *this thing of ours.*

heroin smugglers in the United States. Based on their field interviewing they argue that there is currently a decline of traditional TOC activity and that "a different breed of organized Chinese criminals has come of age in transnational activities. These organized Chinese criminals are not affiliated with triad societies or any other traditional Chinese organized crime groups. They are freelancers" (Zhang and Chin, 2003: 469). But just because there are emerging forms of TOC does not necessarily mean that the old ones have abated in the region.

The key theme in the non-traditional TOC groups and organizations internationally is that the relationships within organized crime are expedient and functional; not necessarily rooted in the trappings of ethnic histories or familial ties. For example, Phil Williams argued that the majority of relationships or ties between drug traffickers should be understood using more trite vocabulary and that the mechanics of organized crime in the drug trade are "essentially alliances of convenience based upon strictly economic considerations rather than part of a global conspiracy" (Williams, 1995:67).[114] The key implication for law enforcement is that it is much more difficult to find critical nodes in these social networks in order to compromise or remove them. Small social networks tend to make connections with others for a short period, then detach, and connect again to another network in order to continue the pursuit of wealth. They are often *a*political, fleeting, and multinational.

In general, and more specifically in Europe, TOC is evolving into looser more fluid network forms of organization and the more traditional hierarchical, ethnically based

[114] Williams has argued more recently that organized crime, which may be transnational in scope and ambition, should be understood as both entity and activity (Williams, 2004:2). This distinction allows for conceptual ease-of-use between, for example, *la cosa nostra* and terrorist networks creating their organized crime to provide a source of financing. The former is an entity while the latter is an activity. Interestingly, Williams notes that in "some circumstances, therefore, terrorist and criminal networks will increasingly be involved with one another, albeit in competitive as well as cooperative ways" (2004:2).

groups are in decline.[115] In East Asia, the picture is different. Organized crime groups in East Asia are often categorized as traditional or non-traditional. Traditional organized crime groups include the more familiar Chinese triads based in Hong Kong, Taiwan, and Macau as well as the Japanese Yakuza or Boryokudan. Non-traditional groups often characterize more informal networks and associations such as tongs with criminal ties, triad affiliates, and common gangs located in East Asia and in countries with large East Asian communities. The activities that these groups engage in vary widely; racketeering and extortion, kidnapping, illegal gambling, prostitution, loansharking, alien smuggling, drug trafficking, financial fraud, theft of computer chips and other high tech goods, counterfeiting of computer parts, and money laundering (Finckenauer, 2002; Chin, 1996). Here the distinction is made based on formalization of ties and structure as well as longevity not on technical skills and the use of the cyber infrastructure.

In East Asia, there are also organized criminal groups that are locked into or embedded in particular social and political contexts. In addition to the traditional and non-traditional TOC groups there are also well formed municipal or metropolitan groups that are often politically active with a high cross-groups variance in level of sophistication. The most recent and extensive work on these traditional forms of TOC in East Asia is by An Chen. Chen's research examines contemporary organized crime in China. She notes that in "today's China nearly all criminal gangs are local ones" (Chen, 2005:81). The survival of organized crime over long periods of time, according to Chen, requires intimate connections with local government officials, which in turn use the "gangs" to pursue their own goals – a kind of self-reinforcing symbiotic feed-back loop,

[115] Most of the literature that focuses on European experiences confirms this trend. But it is important to point out that this is a statistical observation. There will be exceptions. For example, the biker gangs in Northern Europe and North America retain the hierarchical, ethnicity based, business organizational frameworks.

which is a different notion of nexus.[116] Chen concludes that the primarily explanatory factor for the increase in organized crime is political corruption (2005:82).

The China focus here is an important dimension in understanding the more sophisticated uses of the cyber infrastructures by non-traditional TOC in the region. This is not to say that the problem of TOC is an exclusively Chinese one; but rather that because of China's unique social, economic and political trajectory, organized crime of all types is flourishing.[117] Additionally, non-traditional TOC in Hong Kong SAR and mainland China provides many of the transnational 'bridges' in East Asia for other criminal entities in the Philippines and Indonesia.

Chen notes important domestic evolutionary trends among active organized crime citing cases from Zhengzhou, Henan, Chengdu and Sichuan. Chen breaks organized crime in mainland China down into three types: a) criminal means to legal businesses; b) purely illegal markets; and c) mobs or gangs of hooligans (2005:82). According to Chen's findings, organized crime leaders in the more sophisticated type-A group, in general, have taken earnings from illicit activities and actively invested in legitimate businesses.[118] This is certainly not a new tactic, but as Chen argues:

> their organizations do not necessarily quit crime [after transitioning to legitimate enterprises], but rather undergo 'upgrading' in the structural arrangement, membership, and patterns of criminal conduct. They typically evolve from loosely structured gangs into more formal organizations with a rigid pyramidal hierarchy and discipline. While continuing to recruit among marginal social groups, they also approach people with political offices or social status of membership (Chen 2005:86).

---

[116] Chen notes that criminologists in China point out that most of the crime is collective but not organized crime. Chinese researchers make the distinction using levels of planning and coordination to separate real 'organized crime' (Chen, 2005:83-84).

[117] For more on how changing social forces and circumstances – especially capitalism and democratic versus patriarchal leadership - are altering transnational patterns of crime in the Asia Pacific region more generally see Shaw (2003).

[118] Chen identifies several 'secret societies' as the closest type of sophisticated organized crime that resemble organizations in the West and closely parallel very traditional Chinese secret societies like the Green-Red Gang (2005:84). The notion of a 'secret society' has made a kind of come-back in China since a series of reforms in the 1990s designed to "stream-line" government operations. These reforms, in part, devolved administrative power and responsibilities for managing sub-regional economic growth and development to lower paid local officials (2005:85).

These hierarchical evolutions increase trust levels among the organizations members and thereby insulate leaders from prosecution through a strategy of compartmentalization.[119] What Chen does not account for in the type a) group is the extent to which transnational links are made and how they are sustained – or if they exist at all. This is an especially important gap in the literature on TOC in East Asia but given that Chen's results show clearly that government officials are increasingly joining the type a) organizations in Shanxi, Hunan, and Guangxi Provinces and in some cases even "assuming political offices personally" (2005:105) it is safe to assume that the domestic-international interfaces are many and grow increasingly complex. Interestingly, in response to this evolution of domestic organized crime, the communist party in Beijing amended several domestic laws in 1997 which strongly suggest "that the regime no longer treats criminal secret societies as purely criminal cases but as the problems of a political nature" (Chen, 2005:106) indicating both a nascent internal-domestic securitization process and that the more traditional, locally entrenched groups are not necessarily the *a*political actors implied in the more general definitions of organized crime.[120]

There are two important considerations to keep in mind. First, the Triads are not synonymous with Chinese criminal syndicates. Not all syndicate members or criminals are automatically triad members. But all triad members are criminals, if only because membership alone is considered a criminal offense under Hong Kong's 1994 Organized

---

[119] Evolution implies smooth upward progression. My interviews in the region lead me to believe that punctuated equilibrium is the more appropriate descriptive term.

[120] The evolutionary trend is horizontal as well as vertical. For example Wong found that in counterfeit medicine markets, traditional organized crime waited to enter into this underground business and when it did it began it connections with mostly informal gangs. From Wong's field interview of a mid-level criminal member: "If you are in the business of selling and trafficking in illegal drugs, the police are always after you, but counterfeit drugs, very little" (2004:167-169). Wong also discovered connections between illicit markets, TOC groups and the PRC military, whom are still involved with running illegal businesses even though the central government, through a series of policy measures, has restricted the Army from owning companies (2004:170-171).

Serious Crimes Ordinance as well under legislation in the PRC.[121] Second, critical to understanding TOC in East Asia – especially the more sophisticated criminal activity - is the practice of "guanxi" or personnel relationships and connections (Hart, 1999). The activities of both traditional and non-traditional criminal groups are based on evolving ties between sets of individuals, associations, and legitimate organizations. The extent of transnational organized crime in the region is generally uncovered through an examination of the financial and personal ties, however remote, among participating individuals.[122]

When Hong Kong reverted from British to Chinese rule in 1997 there were concerns in the policy communities of East Asia and North American that the Triads and other organized crime groups would leave the city in favor of 'greener' pastures.[123] The thinking at that time predicted that much of the 'organized' element of the Triads would constrict back into rudimentary criminal enterprises like extortion, gambling and drug trafficking in new locations. Litner observed that "in the 1980s, many outside observers and analysts thought the gangs that were based in the then British colony would leave once it reverted to Chinese rule in 1997. In the end, the reverse turned out to be the case. Not only did the Hong Kong Triads make arrangements with the territory's new overlords" but "both Triad-linked criminal groups and various syncretic sects, are also expanding at a breathtaking pace. An entirely new breed of entrepreneurs is emerging on

---

[121] Much of the new legal definition of 'organized crime' emerged out of Beijing's 1996 Strike Hard Campaign (pīnyīn = yān dā).

[122] For more on the role of guanxi see Chen (2005:93-94) and Pye (1981:139-141). During my interviews in Hong Kong I noticed that, from the perspective of the individuals interviewed, the role of personal ties and connections are very important for both traditional and non-traditional criminal organizations in East Asia. Guanxi, however, played less of a role in the non-traditional groups which appear to rely on more corporate ties and relationships along professional lines.

[123] This observation, in many respects, is difficult to empirically verify. In part, this is because there has been little scholarly attention to Asian organized crime in North America relative to other forms. An exception is the recent work of Zhang and Chin (2003). A key point here is that the victims of Asian organized crime in North America are often within the Asian North American communities themselves. As an example, see the study of Korean gangs in the United States by Ahn (2004).

the fringes of China. The businesslike and well-connected, pinstriped suit-wearing managers of the Sun Yee On Triad have shown where the future lies" (Lintner, 2004:84; Chu, 2005:5).

The post-1997 Hong Kong transition opened up both legal and illegal markets inside China. There, a period of accelerating economic growth and development in provinces such as Guangdong and more specifically in the Pearl River Delta region was generating enormous wealth but also putting extraordinary pressure on state institutional capacity.[124] In addition to the northward focus of the Hong Kong SAR based groups Chu identifies three important trends in East Asia TOC between 1997 and 2004. By using the Sun Yee On, Wo Shing Wo, and 14K groups as case studies Chu concluded that "First, triad members from various societies group together to run profitable criminal projects. Second, they team up with legitimate entrepreneurs to monopolize a newly developed market. Lastly, triad members increasingly invest in legitimate businesses (Chu, 2005:5).[125]

It was not just the Hong Kong based groups that were looking for new opportunities in mainland China during the 1990s. Taiwanese organized crime was also moving into the mainland in search of vulnerable, more conducive environments. But it is important to point out that there are considerable differences with their counterparts in Hong Kong. Taiwanese organized crime, while structured, is not as 'sophisticated' as the Hong Kong Triads and the mainland Tongs. A research report published by the National Central

---

[124] The Independent Commission Against Corruption (ICAC) set up in Hong Kong in 1974 was designed to kick-off a quiet revolution against perceptions and patterns of corruption in Hong Kong government and society - specifically the role that the Community Relations Department of the ICAC played. To counter the possibility of a return of corruption post-1997, the ICAC began a new push similar to the 1970s to ensure that pre-ICAC days did not return. It is important to point out that much of the post-1997 ICAC effort was designed to calm the Hong Kong population and, likely the markets as well (Lai 2000:79-80, 83, 85). Singapore has also had similar programs and offices designed to boost institutional capacity and raise awareness and education among the business and general population.

[125] Shenzhen and Shanghai are two important cities for the Hong Kong to China trend pattern.

Police University[126] in Taipei found that the most active and organized groups in Taiwan rely primarily on 'brute force' crimes along with some involvement in the construction industry. According to the report, in the Bamboo United group "the level of professionalism within the gang is not as high as the public has imagined" (Anonymous Authors, 2005:16). These findings seem to suggest that there is little evidence of the rapid evolutionary patterns in Taiwanese TOC that are found in other groups in East Asia and southern China. The report also observed that in "the Bamboo United, decisions about what criminal markets to enter are primarily based on (1) the kinds of businesses existing within a branch's territory and (2) the kinds of businesses with which branch leaders are familiar" (2005:14). This is the stick to what you know stratagem.

If the cases of Hong Kong SAR, China and Taiwan are representative of environments with long lineages of both traditional and non-tradition transnational and national organized criminal groups, the Philippines is one of the few exceptions in the region. The Filipino based TOC groups are a relatively new phenomenon. These groups have developed the sophistication in the strategies and tactics of both national and transnational criminal activities found elsewhere in the region, but they have yet to adopt the more rigid and pronounced organizational hierarchies or the flattened, sophisticated social networks found in the non-traditional and traditional groups in Hong Kong, China and Japan. The more innovative groups in the Philippines are usually broken down into specialized cells that perform specific tasks. There is evidence that approximately 5% of these groups are using the cyber infrastructure both as force multiplier and as a method to steal digital goods (Interviews in Manila, Philippines 2003). Increasingly, Filipino organized crime is being used and is forming relationships with East Asian Triads and the

[126] The report was published in the journal *Trends in Organized Crime* but the authors remain anonymous. Please see reference list. In text citation as 'Anonymous multiple authors'.

Tongs in Southern China primarily to take advantage of the country's unique geography and low institutional capacity - the military's inability to secure borders and law enforcements scarce resources being diverted to terrorism and internal security matters (Confidential Interviews, Manila and Caticlan, Philippines 2003).

There are, of course, other states in Asia with similar and dissimilar struggles with both traditional and non-traditional forms of transnational organized crime. A general pattern does seem to be apparent. States with growing TOC levels are generally those with low institutional capacity i.e. low levels of the rule of law – similar in measure to the independent variable used in Part One of this dissertation, and have high economic growth rates with rapidly diffusing technologies and infrastructures. This lop-sided development is a perfect environment for the attachment of organized crime onto weak institutions and fertile for the operational mechanisms of non-traditional transnational criminal activities.[127]

External international system factors have also played large role in East Asia. One of the conclusions of the United Nations Centre for International Crime Prevention (UNCICO) survey published in 2000 was that "the available evidence suggests that new technologies and other developments related to globalization have lowered the barriers to entry in respect of some criminal activities, and have as a result diversified the nature and types of activities that criminal groups are involved in" (UNCICO 2000:49-50). This

[127] The political-institutional 'variable' is also a factor in other Asian states even though they have high levels of institutional capacity. The case of the Yakuza in Japan and gambling is instructive. In Japan there are very complex of regulatory controls on gambling which are administered as leisure activities. The pachinko gaming industry generates hundreds of billions of dollars (US) and has close ties the traditional forms of organized crime. The industry itself is administered by the National Police Agency who must enforce laws governing this industry that were written in 1907 and are very difficult to understand, let alone enforce. This is a small example of pre-War laws carrying over into modern Japan. Furthermore, up until the early 1990s organized crime in Japan could operate, to a certain extent, in the 'open' because membership in these groups was not illegal. There were no statutes in Japan comparable to the US Racketeer Influenced and Corrupt Organizations Act of 1970 (RICO). To rectify this, the Japanese Diet passed the Boryokudan Countermeasures Law in 1991.

would, in part, explain the high variance in the type of transnational organized groups (traditional and non-traditional) found operating in East Asia and the explosive growth in some criminal enterprises in the region.

Cognizant of the growing complexity of criminal enterprises and the high cross-group variance of characteristics and features of and between domestic traditional and non-traditional transnational organized crime, the UNCICO survey argued that "the collection of information on transnational organized crime must focus on the lowest possible level, that of the criminal groups themselves. While criminal clusters may contain specific characteristics – indeed, these are presented at various points in the report – they do not on their own constitute valid research categories for the study of organized crime" (UNCICO, 2000:47).[128] The report continues by laying out a standardized system for examining trends in transnational organized crime which should consist of three components – that of "groups," "clusters" and "markets" (2000:52).

Both traditional and non-traditional forms of transnational organized crime thrive in particular types of states. In East Asia, the TOC groups, both traditional and non-traditional, succeed in states where there is rapid economic growth, readily available technology, weak institutional capacities and extreme variance in socio-economic conditions which provide a large pool of 'foot soldiers'.

The growth of both types of groups in the region has resulted in cooperation and functional linkages of convenience. The loose ad hoc ties between non-traditional TOC and traditional organized crime serve two purposes. First, it limits risk in both

[128] This is easier said then done. I have tried to stick to social scientists that follow this anthropological approach to the study of organized crime, see Chen (2005), Chu (2005), and Zhang and Chin (2003) for recent efforts in Asia. On the impact and use of cyber infrastructures and TOC see Nordstrom (2003) for her study of smuggler's use of information technology in southern Africa. Nordstrom's work is the only example that I could find in this vein. In terms of political science and international relations research (specifically security studies) Allan Castle argued that when trying to understand the impact of TOC on security, "these activities are best conceptualized from a policy viewpoint [and arguably from a conceptual viewpoint as well] in terms of their effects, rather than their predicate nature" (Castle 1997:28).

organizations by limiting each type of social network to sporadic, temporary connections. It is less likely that law enforcement would be able to see the entire chain or complete network by compromising only a handful of nodes. There is a multiplicative effect here. As one interviewee put it "the cooperation between new groups and old is being made more efficient by abstract and very real underground market forces" (Confidential Interview, Hong Kong SAR, 2002).

While the trend toward an increase in non-traditional types of TOC in Europe and North America has come with a relative decline of more traditional criminal 'cartels' and 'families' but because of unique state environments in East Asia the emergence of new non-traditional TOC groups has not slowed or diminished the evolutionary trajectories of the more traditional 'secret societies', Tongs, Triads and other more scale-free networks. It is important to note that non-traditional groups can and do act as facilitators of transnational activity for the more traditional organized criminal groups; they become specialists for hire, contractors that provide enhanced services. This littoral nature of the 'underworld' makes non-traditional TOC groups the most innovative in their use of technologies (Confidential Interviews, Hong Kong SAR and Tokyo, Japan 2003). It is not yet clear if states in the region will be able to keep pace with these changes.

Non-traditional security threats in East Asia

A security threat is both an existential or empirical reality and a social process which is intersubjectively constituted. Both of these components intermix through a complicated social dynamic that involves factors ranging from deep genetic predispositions in humans to socially constructed perceptions about the world. The ontological debate over the idea of security often hinges on the relative weight placed on the impact of material versus socio-cultural variables. A puzzle for students of

International Relations and security studies centered on explaining why some empirical threats become or are responded to as dangers to 'national security' and others do not make it as security issues. Existential security threats come from actors or processes with the combination of hostile intent and the capacity to carry it out. But by this definition alone there are a plethora of both potential and actually threats to security ranging from communicable diseases and environmental climate change to terrorism and rogue states.

The 'threat spectrum' is enormous. Complicating matters is the level of analysis problem. Existential threats can impact at the individual level, the level of the state and the international system (Castle, 1997). This crossing of the levels of analysis does not, however, immediately justify special measures that only the state can legitimately employ. Indeed, an analysis of a possible nexus between transnational organized crime and network intruders as a security issue rests rather precariously on two possible presuppositions: that TOC groups and syndicates are already security threats or that a potentially rapid technological innovation by TOC groups will take them from being non-security threats, or purely criminal matters, to having the potential to be articulated as a danger. Would a nexus really be a threat?

The Copenhagen School is a particularly appropriate theoretical framework in this case because it does not focus primarily on the material but rather on the social processes involved within and between the starting point of how a threat is identified to the point when a rhetorical justification of extraordinary response mechanism is articulated by the state. Thus, Buzan argues that military issues are just one area that posses an inherent capacity to induce fears over state and international security and thus all have the potential to become securitized (Buzan, 1995:205-208).

For Castle the link between TOC and security begins with an understanding of intent,

and as such:

> organized crime exists almost entirely for the purpose of making money outside the confines of legally acceptable behaviour. If this is the case then the primary risk for other actors is not to their physical security but rather to their economic well-being, as a consequence of the economic distortions resulting from activities such as extortion, fraud, and smuggling (Castle, 1997:2).

Castle establishes four criteria for determining if TOC groups can be seen as presenting a threat to state security based on two assumptions about the nature of security. First, security is a "commodity or condition over which violent dispute is a significant possibility" and that is important to understand that these "contents and commodities" change over time (1997:3). Second, if TOC is a grave threat to security it should 'threaten' one or more of the following contents or commodities: a) the maintenance of the core values of a society; b) the freedom of that society's population from grave or existential threats; c) the maintenance by constituted authorities of control over the legitimate use of force; and, d) the maintenance by constituted authorities of control over defined national territory (1997:6-7).

Where Castle parts ways with the soft constructivists of the Copenhagen School in understanding the link between non-traditional threats to security is in limiting its subjective nature; or more precisely, that security is purely what states make of it. He cautions that any "examination of transnational organized crime as a security issue, finessed by reference to security as a self-defined and evolving concept which eludes the boundaries of traditional concepts of state security, would be in serious danger of predetermining its own conclusion" (1997:4). Thus Castle opts for an examination of the alleged threat posed by TOC groups within the back-drop of more traditional understanding of the referent objects of security. This is important because an investigations' conclusion would be on the same terms as how state and non-state actors perceive the potential threat themselves – using the same criteria. Indeed, much, if not all

of the literature, on the link between TOC groups and security begin at this point.

The empirical criteria of what threat TOC groups pose can be whittled down further. For example, Dupont's study of the link between organized crime and security is anchored on the characteristics of illegal organization itself and its permanence in society. The illegal groups most likely to threaten security are not the groups that are "random and transient" but directed by groups with a recognizable structure, leadership and established modus operandi" (Dupont, 1999:435-436). Dupont sees four key links between sophisticated TOC groups and operating in the East Asia region. The first link is directly related to sovereignty in the sense that they have the "capacity to undermine the authority and legitimacy of governments" (1999:436). This capacity, Dupont argues, can and may interfere with both the states monopoly on violence and its principle source of revenue – taxation. The second link centers on the concept of economic security. Developing states are most at risk because of the culture shifting that takes place when individuals and businesses develop a pattern of working outside rule and norms of regulated economic activity (1999).

The third and fourth links between TOC and security are exogenous to the state. TOC groups if left "unchecked", Dupont argues, will "subvert the norms and institutions that underpin global order and the society of states" (1999:436). This increasing level of sophistication, capacity and international cooperation, according to Dupont, forces the state to begin to reach for the traditional tools of national security. It is this reaching into the "strategic domain" which can then blur the lines between military and law enforcement responses (1999:436). By studying narcotics trafficking in East Asia Dupont concluded that transnational organized crime is "arguably the most pressing and vexatious of an emerging set of transnational security issues, none of which can be

adequately addressed without substantial regional cooperation" (1999:455). For Dupont, the link between TOC groups and security in East Asia exists because criminal entities "violate the sanctity of the region's borders and weaken the authority of national governments" and are also "challenging East Asian states' traditional monopoly of power and taxation" (1999:454-455). Like Castle's more general conclusions (1997) Dupont argues that the illicit drug trade in the region involving a relatively high degree of variance in criminal organizations is "emerging as a significant long-term security issue" (1999:434). The temporal elements sketched by the phrases "most pressing" and "significant long-term" is never clearly nailed down; but at least there are some warning signs.

The importance of weak institutional capacity cannot be understated and is a theme that consistently surfaces in the literature. Castle concluded in 1997 that while "the threat to the nation state posed by criminal groups has been overstated in general terms, particularly with respect to short-term existential threats, the threat is very real for poorly institutionalized, non-democratic states. The threat which presents itself is a security threat in terms of the future democratic development and political stability of newly-democratizing areas" (Castle,1997:ii). This local nature of both traditional and non-traditional TOC groups is precisely why some scholars argue that civil society, especially in the form of strong bonds of trust between government and society, are crucial components of any response to transnational organized crime (Shelley, 1994; Chen, 2005:100-102).[129]

Other than outlier cases like Columbia and Georgia, TOC groups may indeed

[129] Although, there are cases where the trend has been halted, and in some cases shows signs of retreat of traditional forms of TOC. For example, the case of Macau and PRC initiated reforms in the SAR, see Lo (2005). It could also, however, be argued that in this case it was a relatively easy 'territory' to stabilize given that much of it was under the control of one triad leader with whom the government in Beijing "penalized" and then came to an understanding with.

undermine the integrity of certain types of states and in certain state contexts, but have yet to present a threat to the nation-state itself – i.e. mature, capable states (Shelly, 1995). On balance, TOC groups do not constitute a short-term threat to security. Over the long-run, however, the prognosis is less positive. TOC groups, if left to evolve, will pose a direct threat to the security of less developed countries with low levels or uneven levels of institutional capacity. States like Columbia and Georgia are thus warning signs. The interaction between organized crime and political institutions at the local and sub-regional levels in East Asia may act as important indicators.

Because the pressure that TOC groups are putting on security the responses must be multidimensional and multijurisdictional – hence responses at all levels of analysis. Institutional capacities at the national, regional and international levels are of paramount importance because not only do TOC groups "pose serious threats to both national and international security" but additionally they are "extremely resistant to efforts to contain, disrupt, or destroy them" (Williams, 1996:96). Given this resistance, Godson and Williams argue that responding to this "challenge requires a comprehensive strategy that combines law enforcement and regulatory responses, such as enhanced intelligence analysis and intelligence sharing, state-building, and trans-state cooperation, with non-regulatory approaches, such as the extension of the strategy to civil society and the private sector. The latter would include changing cultural attitudes towards organised crime and corruption" (1998:66).

Transnational organized crime and the cyber infrastructure

On October 11, 2001 in Singapore a joint communique was issued at the conclusion of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC). The statement noted "with particular concern the increase in cyber crime in this region and its

serious impact on the peace, security, prosperity." Indeed, a recent report has suggested that one in ten Internet transactions in East Asia is fraudulent (Brey, 2002). Cyber security issues have made it onto the agendas of regional security meetings and in national policy statements. This reflects a growing perception in the region that governments do not have a comfortable level of control over their cyber infrastructures at a period when their institutions and economies grow increasingly reliant on these technologies.[130] At a rhetorical level the link between 'cyber crime' and security is being made.

Empirical evidence or case studies on the relationship between TOC groups and systems intruders are rare. This is not surprising. Some observations, however, have been made in relation to the broader concept of cyber crime and its link to organized crime. Phil Williams argues that:

> organized crime and cyber-crime will never be synonymous – most organized crime will continue to operate in the real world rather than the cyber-world and most cyber-crime will continue to be the result of individuals rather than criminal organizations per se. Nevertheless, the degree of overlap between the two phenomena is likely to increase considerably in the next few years (Williams, 2002:1).

Williams goes further by suggesting that TOC groups do not necessarily need to develop in-house expertise about cyber space because it would be more efficient to contract systems intruders capable of performing needed tasks "ensuring through a mixture of rewards and threats that they carry out their assigned tasks effectively" (2002:2). Williams' description would mean that system intruders would just become part of TOC groups. This blunts, if not understates, the complexity of the phenomenon is East Asia. The evidence of more sophisticated uses of computing technologies in East Asia by either

[130] Cyber crime, which is often linked to organized crime, is invariably cited as an emerging non-traditional security issue of serious concern. See (2002) Joint Declaration of ASEAN and China on Cooperation in the Field of Non-Traditional Security Issues 6th ASEAN-China Summit Phnom Penh, 4 November; the (2004) Joint Communique of the Fourth ASEAN Ministerial Meeting on Transnational Crime (AMMTC) Bangkok, 8 January; and the (2004) Joint Communique of the First ASEAN Plus Three Ministerial Meeting on Transnational Crime (AMMTC+3) Bangkok, 10 January.

traditional or non-traditional TOC groups has been slow to accumulate. In one of the few examples Shelley and Picarelli, in their work on the possible convergences between TOC and terrorist groups, cite a report which "noted that Triads in Hong Kong were recruiting graduates of local technical colleges to serve as counterfeiters for the criminal gangs" (2002:310). Overall, however, solid evidence is paltry.

In theory, part of the potential power of using the cyber infrastructure for TOC groups is in the secure, relatively anonymous ability to both communicate and exchange data without physical interactions. This reduces the risks of detection. This is certainly the case in East Asia. But there are some notable exceptions. Technology can also be seen by traditional TOC groups as a threat as well as an opportunity (Confidential Interview, Tokyo 2003). For example, Internet technologies that send packets of data over unknown landscapes can be 'sniffed' by intelligence and law enforcement, and cell phones can be tapped and traced to a general geographical location.[131] This would explain Williams' theory that traditional organized crime's reliance on the 'contractors' to incorporate and effectively use technology will likely grow. In mainland China, for example, there is good reason to be suspicious of possible 'eaves droppers', even if it is extraordinarily difficult for state agencies (i.e. law enforcement and intelligence) to hone in on particular paths of criminality taking place within and from the cyber infrastructure (Confidential Interview, Hong Kong SAR 2003).

The ability to act at a distance through the cyber infrastructure where opportunities appear to outweigh such risks is key. There are always new physical, safer territories from which to place cyber operations, further lowering the risk:

[131] Using cloned cell phones would help to mitigate this problem as well as the use of proxy servers and judiciously employed encryption may provide necessary camouflage. However, the use of encryption can make traffic stand out enough to be identified for further interrogation.

> For criminals and terrorists, these divergences offer opportunities to launch attacks at minimal risk – even if the source of the attack is somehow discovered. This suggests that there might be a form of jurisdictional arbitrage with potential attackers seeking out low risk jurisdictions from which to launch their attacks. Over the longer term, of course, the opportunities for arbitrage of this kind can be diminished through more inclusive laws criminalizing this kind of activity, through the harmonization of laws among states, and through the extension of extradition treaties and mutual legal assistance treaties. As well as using jurisdictional arbitrage computer intruders also seek to cover their tracks by going through multiple jurisdictions. In some cases, this makes it impossible to track the activity back to source by complicating the digital trail. In others, it adds significant legal obstacles as some states are simply unwilling to cooperate in investigations There is also the potential for mischief with the possibility that skilful intruders might lay a false trail that lead to unwarranted but damaging accusations against innocent parties (whether individuals, groups or nations) (Shimeall, Dunlevy and Williams, 2001).

The availability of jurisdictional arbitrage, absence of harmonized laws, and uneven institutional capacities across states in East Asia would mean that acting at a distance through the cyber infrastructure to perpetrate crimes against firms or states could be done within the comfort zones of the local embeddeness of the traditional criminal organization.

In addition to the murky predicate nature of these activities, measuring state responses through policy and legal responses is difficult at best. Cyber crime legislation in East Asia is just emerging from early stages of development still exhibiting wide variation across criminal justice systems. This variation is not surprising given the different historical, social and political contexts within which these laws have evolved, and the differing levels of technological development within the region. This dynamic between the cyber infrastructure and TOC groups makes the task of both law enforcement and research and information collection activities more difficult (Williams, 2001b). Organized network intruders that have organically evolved will be more likely to engage in "hands-off" or distanced cybercrime because of the role of moral disengagement and differential association This may, in part, explains the "keep the nerds at a distance" behavior that I found in many of my field interviews in East Asia.

There does not appear to be an immediate, short-run threat to the security of states in

East Asia. This conclusion is tempered by the overwhelming consensus in the literature that both traditional and non-traditional TOC groups pose a long term threat, especially to certain types of states in certain contexts; like weak or failed states. But the growth of traditional and non-traditional organized crime can be associated with states in East Asia that do not fall into the standard definition of what would constitute a weak state. The link then between security and TOC groups in the region presents something of a puzzle or at the very least a trend that diverges somewhat from experiences in other parts of the world.

Chapter Eight: Organized Crime and Compromised Nodes

Introduction

Is transnational organized crime a threat to state security in the digital age? In order to address this question several over lapping themes will be developed. First, the chapter introduces that concept of nexus between two previously distinct, hidden social networks: system intruders and transnational organized crime (TOC). What emerges from this research on a possible nexus between the two groups is the implications for regional security. In other words, if there is a nexus between TOC groups and systems intruders that provide advanced innovation, how does this change the calculus between the link between security and TOC in East Asia? Does it change at all?

The second theme that will be developed is the concept of digital black markets. The market concept explores the mechanisms by which system intruders are sustained, outlines the various actors, the basic microeconomics, and integration trends. The third over lapping theme in this chapter is the role of state capacity in East Asia. This is, in part, why digital black market dynamics are specifically interesting and of immediate importance to East Asia and to regional security. In light of the rapid innovation and the state's perception of a loss of control in the cyber realm, are the institutional capacities levels high enough in the region to allow for adaptation to co-evolve with criminal innovation?

The chapter presents two case studies. The first is an examination of a bot-network operated out of Hong Kong SAR and Shenzhen, China. The case provides a technological starting point to a possible nexus between TOC groups and systems intruders. I argue that bot herders – the individuals or small groups that build and

maintain bot nets – have become new cyber infrastructure security actors. The second case examines instances of sophisticated network intrusions for the purpose of economic gain. The purpose of this second case study is to examine the possibility that a stable nexus has formed in the region between systems intruders and TOC. If there is a nexus, the formation of a stable illicit market would be a key indicator to the stability and longevity of links between TOC groups and 'hackers'.

The chapter will argue that while criminal innovation is taking place – which is producing an uneven adaptation space across the region between law enforcement and TOC groups – this does not necessarily change the short-run link between organized crime and security. There are, however, an emerging set of new security actors that have the potential to alter the links between security and TOC but these 'information markets' and actors that rely on the cyber infrastructure are not beyond the reach of the state. Due to the nature of the use of cyber infrastructure security actors by TOC in the short run, it is unlikely to change the trajectory of the relationship between TOC innovation and security in the region. Among these cyber security actors there is intense competition within groups of system intruders. An externality of these adaptations is that bot nets and those that operate them are becoming a kind of pseudo or meta cyber infrastructure for both traditional and non-traditional forms of organized crime in the region. The trafficking in illicit data, obtained by systems intruders, in East Asia is a growing problem and one that mirrors, in many ways, the growth of trafficking more generally. It draws on the problem of flatter, more nimble social networks, jurisdictional arbitrage, and the problem of state capacity.

The scope of the nexus between organized crime and cyber crime will be restricted for

both case studies. Terms such as computer crimes, computer-related crime, high-technology crime and cyber-crime are often used interchangeably even as they comprise separate and distinct crimes.[132] Fausto Pocar defines cyber-crime as "the criminal use of any computer network or system on the internet, which implies attacks on or abuse of the system network for criminal purposes" (Pocar, 2004:33). While Pocar's definition is quite broad, it has the advantage of seeing the computer as both a tool for the perpetration of a crime and as a target. I also use the phrase 'cyber-crime' here as short-hand for conventional crimes that are enabled by the infrastructure such as industrial espionage which is theft and bot networks which is misuse and criminal trespass. This implies that there is no *pure* computer or cyber based crimes. Computer enabled, and/or cyber crimes take place in new environments and utilize new tools but they do not constitute the invention of never-before-seen criminal activity. In short, these are old crimes with new tactics and strategies and the addition of new security actors.

Criminals connecting in cyberspace

Both traditional and non-traditional organized criminal groups innovate by using the cyber infrastructure to "communicate, to organise themselves better, to widen the spectrum of their businesses, to update their modus operandi and techniques, and to avoid law enforcement risk" (Savona and Mignone, 2004:4). Criminal innovation, however, does necessarily imply that a stable nexus exists between the computer 'underworld' and TOC groups in East Asia. A stable nexus between criminal organizations in East Asia would exist if there are continuing links and relationships between system intruders and

[132] See comparison between European Convention on Cyber Crime <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> and UN Resolutions 55-63, 56-121, and 57-239>.

TOC groups that affect both groups in a manner that would not have otherwise have taken place. This does not necessarily imply symbiosis or co-dependence, but rather that the linkages between the two groups are profitable enough and organizationally efficient enough to spark continued interaction.

The use of the phrase "nexus" to describe nebulous links in security is not new; a recent example on the subject of terrorism and piracy by Gal Luft and Anne Korin (2004). There are distinct pitfalls that must be carefully acknowledged and hurdled when making links between secretive actors and their impact on security in East Asia. Hamilton-Hart wrote a provocative argument which clearly outlines the dilemma for researchers (Hamilton-Hart, 2005:303-325). She points to several problems, but chief among them is that researchers cannot simply identify links or points of connection without making a statement on their importance and clearly identifying what a reader might infer from this.[133] The potential problems inherent in studying terrorist nexuses extend to the question of organized crime and systems intruders.[134]

A few examples from other research efforts on criminal innovation as a security threat are instructive. A recent study by Nordstrom (2003) based on field work in the southern Africa region looked at the relationship between parts of the cyber infrastructure and smuggling networks. Nordstrom found that smugglers were procuring customized software adapted to suit the needs of their operations. In one example, the nexus was based on familial ties wherein the smuggler paid his son - who happened to be studying at a leading university in the UK – to do the customizations and keep him up-to-date on the

[133] The academic study of terrorism in Southeast Asia has been the focal point of this debate, see Brown (2006).
[134] See also Brown (2006).

latest technology (Nordstrom, 2003:238).

A second example from Nordstrom's work shows that there are high-tech links between criminal organizations, not just between crime groups and 'civilians'. In that region, for example, smugglers often require the services of forgers who now have their own websites (2003:246). This is also the case in East Asia. For example, in the Philippines the "really good forgers that are worth their weight in gold" run web servers for criminal e-commerce but are obscured and kept hidden from both the casual web surfer and law enforcement.

Nordstrom also found that smugglers 'cracked' into systems with security work schedules of firms and other organizations (2003:247). This illustrates an important point: it is not necessarily the high security servers systems that contain the useful information. It is taking advantage of low priority or sub-systems where one can glean useful pieces of data that can then be connected to other information. But her study also found simpler uses of the cyber infrastructure.[135] For example, smugglers make extensive use of look-outs, individuals with a cell phone (2003:244). Again, this kind of counter-intelligence activity takes place in East Asia. In Shenzhen, TOC groups have installed networks of wireless cameras that send transmission over the Internet. These cameras watch for police movement and competitor organizations becoming a kind of counterintelligence node. The wireless cameras are cheap, discreet, nearly impossible to trace and can work longer hours than their human counter parts with cell phones. The

[135] Interestingly, Nordstrom documents a conversation with a smuggler in which she asks why smugglers (who are very wealthy) choose the cyber infrastructure over the creation of their own communications channels. The answer is that hiding in the noise of the cyber infrastructure is much more tactically beneficial than would the creation of their own 'channels' or vectors of communication (Nordstrom 2003:246-247).

wireless counter-intelligence nodes or networks were designed and installed by a small group of systems administrators that were worked on contract (Confidential Interview, Hong Kong SAR 2003).

These are certainly examples of cooperative business relationships but it is important to point out that the nexus can also be unstable. In Russia, for example, there are cases where the nexus is based on coercion and co-optation. This co-optation of systems intruders by TOC groups begin to look more like a draft by "traditional criminal organizations [that] have recruited ex-hackers and 'crackerz' to carry out computer crimes and attacks on their behalf" (Savona and Mignone, 2004:12). Examples of this complex interdependence in East Asia abound. In one case an engineer who faced a layoff after a Japanese corporation outsourced its legacy software development teams to South Asia and who was subsequently hired for a position with much lower pay, was blackmailed into providing system passwords to "local gangsters" which trapped the engineer into a "relationship that he just can't get out of" (Confidential Interview, Tokyo 2002).

Case one: bot-nets in Hong Kong SAR and Shenzhen, China

In the cyber infrastructure compromised machines (nodes) can be used to build "bot-networks" which are rented out for periods of time on a kind of black-market for network intruders or other malicious users.[136] The early motivation for creating bot nets lie in their ability to provide secret communications "resource sharing, and curiosity have historically been primary motivators for underground research and 'hacking'." As the cyber infrastructure evolved online attackers have shifted their focus from curiosity to

[136] The use of the term 'bot net' should not be confused with 'bot'. The later is shorthand for a robot

financial gain. In order to "accomplish this goal, they vigorously pursue access to information and capacity" (Ianelli and Hackworth, 2005:2).

Bot nets are built by breaking into other nodes in cyber space and taking them over without being noticed by the individual or organization that owns or operates the device. But before a compromised node is brought online and added to a bot net, it is searched for interesting files. For example, if it is a business machine, it is searched for the CD keys for software packages running on that machine. The keys are then sold to pirates. A bot net's collection of compromised nodes thus has intrinsic value for stolen information as well as through their more active use of providing difficult to trace platforms for more sophisticated attacks. Some compromised nodes are rented for phishing, other are leased to spammers. Thus the accumulation and "controlling a large group of these systems provides attackers and their collective associates (i.e., crews) enormous power" (2005:3). While adding to the bot net or "herd" of compromised nodes can be done manually, tools such as autorooters are now used to expand bot nets (2005: 8).[137] But the more intricate bot net expansions in East Asia are still often performed manually (Confidential Interview, Manila, Philippines 2003).

The 'herd' of compromised nodes is managed remotely via differing 'layers' of the cyber infrastructure. Bot nets can are managed and built using various architectures of command and control: peer-to-peer, web-based, the Internet Relay Chat infrastructure, and now even the DNS system can be used for command and control functions (although

---

without a body (software) which is often used on the Internet to do various tasks, see Hotlz (2005).

[137] For more on autorooters see Tanase (2002) available online from: <http://www.securityfocus.com/infocus/1619>. In brief, an autorooter adds efficiency and automation to get 'root' on a system.

it is a lot less efficient).[138] After the intrinsic value of a compromised node has been mined and the compromised node added to the larger bot net the nodes can be sold, leased or rented. Bot nets "are also one of the many things available for sale in the underground economy. The market for bot nets is competitive, and they will be sold to anyone willing to pay the asking price" (Ianelli and Hackworth 2005:3).[139] If existing bot net software or bot nets do not meet a client's particular needs, custom designed software and networks can be ordered for a premium.[140] The bot nets themselves can also be traded "for goods or services" thus the "possibilities are endless, but some of the items commonly bartered for bots include physical goods, such as computers and jewelry, batches of credit card information, shell accounts on servers, or even other botnets" (2005:6-7).[141]

---

[138] This, of course, raises the question of how to deal with bot nets. While any strategy must be multidimensional and exist in both real space and cyber space, one defense against a large bot net is to use the bot net against itself – compromise the network of compromised nodes. The idea here would be to allow an enforcement system (good guy) to be infected with the bot net; in other words join their network. Once inside the network, the traffic between bot net nodes could be 'sniffed' to find out what command and control system is being used and any security protocols that are necessary to control the bot net. Then upload a retro virus or other electronic pathogen into the bot net that would begin to quietly fix the infected system and remove the bot net binaries to turn the compromised node back into a tame or domicile node.

[139] The Ianelli and Hackworth study cites another study which claims that a compromised node can sell for US$0.04 to US$0.10 per typical compromised system (2005:7). From my last email exchange with an interviewee (originally conducted in Hong Kong 2003) the price range was between US$0.05 and US$0.25 (Confidential email exchange on February 3, 2005 PDT; Leyden, 2005). This begs the question: why? Perhaps it is the effectiveness of state and private sector counter actions since one would anticipate the price dropping in an 'expanding' bot net context. This could be the result of general inflation or that the more sophisticated use of bot nets is generating higher profits. My thanks to Brian Job for pointing this out.

[140] By custom designed illegal software or malware, Ianelli and Hackworth (2005) mean the addition of server-class services to money making dimensions of bot nets. They found that "[t]o facilitate the operation of bot nets, bot malware can include useful services like HTTP and FTP. These types of services allow bots to host
a) phishing sites b) web pages where infected systems can log their infection status c) malware download sites d) spyware data drop off sites and e) bot command and control sites" (2005:10).

[141] In Southeast Asia (esp. Hong Kong SAR and the Shenzhen region) bot herders are beginning to earn income by selling more basic services like privacy and anonymity online (Interview Hong Kong SAR, Manila, Philippines). This begs the question: why would opt for an expensive 'solution' provided by a bot herder when there are free web-based alternatives like Tor? Tor is a service that is part of the Onion Router which is sponsored by the Electronic Freedom Foundation. Tor helps anonymize WWW traffic by

In the Hong Kong-Shenzhen case, for example, bot nets are broken down into small-blocks and big-blocks of compromised nodes. Clients (renters) usually meet with administrators or builders of bot-nets in Internet Relay Chat (IRC) rooms. From that point payment is made using an online method or a barter arrangement is made whereby code for exploits is exchanged or some other type of information of value. The benefit for the renter is that he/she does not have to maintain or use a privately obtained chained-relay from which to send spam or launch attacks (Confidential Interviews, Hong Kong 2002). A market based system also means reducing the risk of being discovered by law enforcement by providing a quick and easy method of access to these types of relays which can then be 'recycled.'

Competition between bot nets that are controlled from East Asia is growing fierce. Bot nets must be defended from both other bot herders and hackers, and from endogenous repair by the legitimate user or administrator of the compromised node.[142] In general,

---

bouncing it between volunteer servers called onion routers. They mask the origins and make it easier to evade filters, such as those installed by firms, educational institutions, and governments. The draw-back of Tor and other free online services is that the data can be slower (much greater latency) due to the high frequency of 'hops' and the low number of volunteer onion routers. While Tor does come with a proxy server, it is a system that still 'leaks' data and thus is not perfectly anonymous. Bot nets can provide similar services but with none of the latency issues and, in general, bot herders can get closer to the provision of truly anonymous cyber infrastructure activity (though no technology can provide true anonymity). See <http://tor.eff.org/> for more information.

[142] For a detailed technical discussion of the tactics used to defend bot nets see Ianelli and Hackworth (2005:20-26), for a simplified, birds-eye-view please consult BBC (2005b). For information on research on bot net 'hunting', see Naraine (2005). Although it should be noted that bot net hunting research has been labeled vigilantism by critics. A variation of this strategy has been used by Microsoft Corporation to track down illegal spamming organizations. Microsoft researchers set up a system and allowed it to be infected with Trojans used by spammers. They then monitored the system for 20 days – watching it send out 118 million spam emails per day – in order to gather intelligence and evidence against the groups. The effort was done in cooperation with the US Federal Trade Commission, see Keizer (2005). Yet another program to try and curtail the growth a bot nets is due to begin early 2006. In a three-month pilot program, the Australian Communications and Media Authority will attempt to identify compromised nodes and ask their owners to clean them or risk being disconnected from their ISPs. This mirrors – albeit in a much less formal manner – recent efforts by the US Federal Trade Commission (FTC) which has begun to send reports to ISPs reporting the number of compromised nodes on their networks. The FTC has contacted hundreds of ISPs informally requesting that they block port 25 (email server), attach rate limits for relays

"[b]otnet command and control (C&C) communications tend to be unencrypted, and since it's not uncommon for multiple bot infections to be located on the same network or system, attackers commonly instruct their bots to sniff network traffic looking for competing botnet communications" (Ianelli and Hackworth, 2005:6). This has sparked cyber turf wars over compromised nodes which can be likened to the cattle rustling of 19th century North American west. In the Hong Kong-Shenzhen case, the potential for real world violence is growing. One interview wondered out load if the links between bot herders and organized crime would further intensify as traditional organized crime groups seek to utilize a back-to-the-future strategy of creating a protection racket.

The stakes are growing primarily because the value and financial rewards of effective, efficient bot nets is increasing. But it is not just the value of intrinsic mined data, large bot nets can be leased and sometimes managed for 'spamming'. Clients who are spammers provide bot herders with a lucrative, low risk source of revenue for lower valued parts of the 'herd' of compromised nodes. For example, "As the botnet grows, it becomes a lucrative asset to its owner" and "there is evidence that the compromised machines are being rented out for spam runs, distributed denial-of-service attacks linked to business blackmail" (Naraine, 2005). For spamming purposes, bot herders break their nets down into various categories and typologies: by machines that have high bandwidth-low latency, by legal jurisdictions (arbitrage), and by country (Interview Taipei, 2003).[143]

The jurisdictional arbitrage dimension is an important one because the "spam chain is

---

(open and closed), and if possible and where necessary, isolate compromised nodes until they can be 'patched'.

[143] There is no reliable data on bot nets by country.. The only way to reliably measure this would be to count the number of compromised nodes as shown in Part One of this study; but this would, at best, be a proxy measure.

complex" and "most [of the] people responsible for sending spam are based in the US, though a growing number are now organized criminals in Eastern Europe and Russia. China is the location of choice for the servers that host the spammers' websites and for buying and selling lists of spam zombies" (Galloway, 2004). Managing networks of compromised nodes in the absence of a strong legal environment means being able to sell, rent or lease jurisdictional arbitrage in cyber space. Galloway argues that:

> Another reason China has become the world's spam central has to do with the industry's growing sophistication. The days when most spam was dispatched from servers in the basement office of some unscrupulous American ex-con are waning. The modern spam industry now is spread across the globe and has become infested by technically advanced programmers from Russia and Eastern Europe, often in league with local organized crime syndicates (Galloway, 2004).

The choice of jurisdiction is key. Further investigative work by Galloway found that "China also dominates the market for buying and selling lists of zombie PCs, which are peddled by virus writers on Internet forums also found on Chinese servers. Lists can currently be had for about US$2,000-$3,000 per 20,000 compromised proxies" (Galloway, 2004).[144] The microeconomics of price levels for black market cyber goods fluctuates because supply and demand curves are highly elastic.

The demand for services provided by bot nets are not just related to data theft, intrinsic mining, or herd utilization. Bot herders can also provide complete software, web hosting and security solutions for phishing – the practice of relieving an unsuspecting web surfer of their personal data such as banking and credit card information. This too has spawned

---

[144] This works out to around US$0.15 per compromised node; within the range that Ianelli and Hackworth (2005) found and hovering around the mean discovered in my own field interviews. But these compromised nodes would be of lesser quality when compared to the rest of a bot herd. Eventually compromised nodes that are sold or leased to spammers will be blocked or become neutered; hence the lower price. For example, if a typical user in the Middle East wished to view a banned website through a proxy the "black market access to filtered pages in Saudi Arabia runs anywhere from $26 to $67 per Web site" (Palmer, 2005). But black market access to pirate servers (machines that store stolen digital goods) can run users up to US$1000.00 per month depending on the quality, type and scarcity of the data (Confidential Interview, Tokyo 2003). This is likely a response to scarcity and increased risk.

an underground economy (Abad, 2005). Fraud is also a common use of less sophisticated bot nets. In 2004 US law enforcement arrested an individual with a small 'herd' who "allegedly used automated software to infect Windows systems, advertised and sold access to the compromised PCs, and used the software to perpetrate click fraud, garnering tens of thousands of dollars in affiliate fees" (Lemos, 2005a).[145]

In the case of the Hong Kong-Shenzhen bot nets presented here, the individuals that operate and build them are keenly aware of law enforcement adaptation and the arrests in Europe and North America. To adapt, they now use anti-forensics techniques such as dead-man switches and increasingly rely on counter-intelligence on law enforcement activities. In Shenzhen this is provided by contacts and informal relationships with organized crime in southern China (Confidential Interviews Hong Kong and via email correspondence April 15, 2002 and November 10, 2004).

In Hong Kong and Shenzhen the interface between bot herders and TOC groups is two dimensional. First, the mined intrinsic data is sorted and then sent to a 'black' machine or secret server. From this point meta-data on the stolen files are sent to another server and stored in a database which is accessible to a select group of buyers. The buyers can sign up for regular emails listing results. Other hackers and select individuals monitor these lists and when something of interest appears the bot herder is contacted for more information and access is granted to the database containing the meta-data on the files

[145] For more on click fraud see Mann (2005). There have also been instances of law enforcement success in arresting operators of much larger more sophisticated bot nets. For example, "Dutch authorities arrested three men in the Netherlands who allegedly controlled a network of more than 1.5 million compromised computers. In August, the FBI and Microsoft helped authorities in Turkey and Morocco track down two men suspected of creating and spreading the Zotob worm--a program that consisted of bot software modified to exploit a flaw in Windows 2000" (Lemos, 2005b).

located on the black server.[146] When I asked about what would constitute a "select" individual the response was generally along the lines of someone who is known, can be trusted and has money.[147] The interviewees were quite clear that organized criminals that belonged to long established groups in the region did have 'accounts'. To my surprise, I was told that two accounts were set up for two separate individuals in the PRC military. I asked if they thought this was a bit of a security risk. The response I got back "no no, not a risk. They pay well and on time" (Confidential Interview, via email correspondence August 2, 2005).[148]

The role of traditional organized criminal groups in the operation and market surrounding bot nets is still unclear. Individuals belonging to more traditional TOC groups in the region do act as 'stand-in' brokers for cases when the intrinsic data found by bot net expansion is significantly more valuable than the norm. In these instances, the data is not sent out to the "lists" but is instead advertised to preferred clients and managed

---

[146] This is very similar to the findings of an extensive study done on phishing markets. The underground phishing economy "is often the end of the line for the phisher. At this point phishers are now providers of credential goods with a limited supply of customers. Consumers of financial institution credentials are known as Cashers. The Casher's main role is to take the phished credentials and obtain currency directly from the accounts attached to the credentials. Phishing and Cashing are distinct and often separate roles" (Abad, 2005). Furthermore, the "phishing marketplace is a loosely tied group of forums where participants can trade goods, services, and money. The key goods are credentials. Credentials are then valued according to the level of detail" (Abad, 2005). The source cited is from the online academic journal First Monday and consequently has no page numbers, see Abad (2005) and <http://www.firstmonday.org>.

[147] The role of trust varies across countries and regions. In a recent study, Cook *et al.* (2005) looked the role of risk taking in building trust relationships cross-nationally. Specifically, they performed experiments in Japan and the US in order to assess the independent effects of risk taking actions on the level and building of trust. What they found is that Americans do indeed take bigger risks with a higher degree of frequency than their Japanese counterparts. Their findings are important for understanding differences in the role that risk plays in building trust relationships because the results showed that even though the American sample engaged in more risks they were no better than the sample from Japan at improving cooperation. While risk taking is important in American trust relationships, the concept of assurance plays more of a role in the Japanese context (Cook *et al.,* 2005).

[148] The reader should be aware that it is difficult to infer anything substantive from this. The military accounts could simply be for soldiers looking for a way to earn additional income. Alternatively, however, it could indicate that the use of those accounts was sanctioned and used by the state as some sort of intelligence stream.

by the 'stand-in' broker (Confidential Interview via email correspondence August 2, 2005). There is a hierarchy here; at the bottom are information on individuals corporate information and finally, and at the top of the hierarchy, information from government networks. In general, autorooters skew compromised nodes toward the lower value end which are less protected. But occasionally, they manage to get into higher end systems or systems that are connected to higher value targets. Usually, cracking into high value systems needs to be done manually. But one-off flukes using autorooters happen. In the Hong Kong-Shenzhen case, bot herders immediately drop what they are doing and turn their attention to a one-off fluke produced by an autorooter (Confidential Interviews Hong Kong SAR, Kuala Lumpur, Tokyo, and Vancouver 2002-2004).

Does this constitute evidence of a stable nexus? Perhaps. Two interviewees claimed that up to 25% of bot net activity is now "owned" or in some way operated by more traditional TOC groups in the region (Confidential Interviews, Hong Kong SAR, Manila, Philippines 2002, 2003).[149] This is an interesting observation but one that cannot be verified. The concern here is that other 'data points' indicate that both traditional and non-traditional TOC groups in the region are, for the lack of a better word, taking a hands-off, wait and see approach. The only evidence to contrary that was found, regarding the percentage or extent of involvement with bot nets in East Asia was an interviewee responded by arguing that "the Triads are still unsure about the 'business' of bot nets. They are sure that they are useful but things are good right now for them so why get more involved" (Confidential Interview, Manila 2003).[150]

---

[149] To be clear, the control of "activity" refers to access to the spoils of bot net construction and usage.
[150] This is loosely connected to the field observations made by Natasha Wong (2004) in her study of traditional organized crime in southern China and its connection to the pharmaceutical industry. Wong

The risk versus reward analogy drawn from Wong's study of counterfeits is also useful for demonstrating the attractiveness of bot net production, even if the evolution of the bot net 'industry' is beginning to look more like industrial espionage than software piracy. For example, Wong quotes one interviewee as stating simply that "[i]f you're in the business of selling heroin or cocaine, the police are on your tail. If you are making fake meningitis medicine, they don't even know you're there" (Wong, 2004:168). Thus, clamping down on the building and selling the wares gained from bot nets in Shenzhen is unlikely, at least at this point, to be a priority for law enforcement. In Hong Kong, however, the picture is quite different. The 'head' of the bot net may be located somewhere in Kowloon, but bot herders are fully aware that the law enforcement in Hong Kong is much more sophisticated, better funded, and have made high-tech crime a priority, forcing much of the 'real life' activities between bot herders and organized crime into geographic spaces of convenience – out of Hong Kong and into China.[151]

Bot nets are becoming security proxy actors that provide a kind of emerging pseudo-infrastructure in cyber space. This pseudo-infrastructure has an enabling effect for both traditional and non-traditional TOC by providing sources of data through services, revenue streams, and operational needs such as secure, anonymous communications.[152] The links, however, between bot nets and TOC groups in the region appear to be more

---

notes, "[t]here are many facets to the reality here. United States pharmaceutical firms are learning that, excluding amateurs, not only are the counterfeiters from organized crime networks, local police, or the military, but they also may be their own suppliers. What's more, China's state owned enterprises (SOEs) have participated in the manufacture and export of counterfeit medicine as well" (2004:162). Like counterfeit pharmaceuticals, traditional organized crime in China is attracted to the illicit industry after it has shown profitability and the returns are worth the risk (Wong, 2004:167-168). This is, I think, an accurate analogy to describe the links between both traditional and non-traditional TOC groups and bot nets in Southeast Asia.

[151] This is explored in Chapter Ten.

[152] This enabling effect in addition to more the more mundane impact of technology on TOC groups that in

like that of a service provider than an intimate business relationship. There are points of collusion and cooperation which provide the necessary, but not sufficient, conditions for a stable nexus between the system intruders and traditional and non-traditional organized crime in the region. In short, the nexus appears to be forming. It is no longer at an embryonic stage nor does it appear to be fully developed.

Case two: digital black markets and security

Bot herders in East Asia provide cyber pseudo-infrastructure by proxy to the criminal world. But this is only one aspect of this study's investigation of an emergent infrastructural nexus. The Hong Kong-Shenzhen bot net case presented here is a clearer developed case. Case two of the black market for illicit data is linked in many ways to the growth of bot nets but is still distinct and as such is worth exploring. The trafficking in illicit data, obtained by systems intruders, in East Asia is a growing problem and one that mirrors, in many ways, the growth of trafficking more generally. It draws on the problem of flatter, more nimble social networks, jurisdictional arbitrage, and the problem of state capacity.

A recent book by Moisés Naím on the security implications of trafficking provides a reasonable starting point. Naím argues that traffickers are transforming economies and reshaping politics in many regions of the world. In his view the pursuit of illicit profits is a powerful driver of political upheaval and international instability and that black-market networks are subtly transforming international politics (Naím, 2005). In other words, transnational black markets are a threat to the security of states and are slowly whittling away at state autonomy and control. There are two driving factors: first, a

---

general maximizes their profits while minimizing their risks of detection and arrest (Savona and Mignone,

transformation of power caused by revolutions in technologies; and second, changes in politics during the 1990s that were triggered by the end of the Cold War (2005). But does this perspective underestimate the durability and resilience of the state in the face of illicit network threats.[153] The argument here is that it is the weak states which are the most vulnerable and less able to massage their 'sovereignty' enough to allow cooperation and international linkages necessary to combat these networks.

The central feature of a black market is its illegality, "be it in the good or service being traded, or the actors (organized crime groups and individuals) involved. Although the actor(s), good(s) or service(s) may not be criminal in nature, the transaction(s) are. Criminal markets often emerge whenever organized crime identifies and exploits loopholes (i.e. regulatory) in legal markets that then become profitable market niches for it" (CISC, 2005:17). In almost all black markets it is the 'middle men' that reap the profits rather than the suppliers or dealers. Those that can provide the infrastructure control black markets. In the past black markets used to be small, isolated and segregated from the legal economy. In weak states black markets become institutionally embedded in the legal economy. Not only because black market entrepreneurs are able to operate in a matrix of legitimate transactions in hopes of a durable commercial existence, but because legal businesses show a tendency to use increasingly sophisticated methods (Naylor 2002).

In another case that was discovered in 2005 "it was reported that over the past five years, Chinese hackers had successfully probed and penetrated a number of US

2004: 3).

[153] An opposing view, in reference to non-traditional network based security threats, would be Matthew Shambaugh (2005).

Department of Defense (DoD) networks. In at least one of the attacks, a Trojan horse computer programme was used to obtain data from a future Army command and control system" (Jones, 2005:6).[154] Some have speculated that because of both technical aspects and level of organization required to carry out these attacks from East Asia that, *a priori*, there had to be either state sanctioned or state sponsored.[155] I would argue that TOC groups in East Asia have both the resources and sophistication to perpetrate this level of activity alone and that one cannot deduce *a priori* that a government was behind the attacks. Yet, this evidence, in combination with what has been presented in this chapter indicates that as a nexus forms between systems intruders and TOC groups in the region there are also state actors exploring the uses of the cyber underworld in a more 'official' capacity.

While is often taken axiomatically that sophisticated 'hacking' activity has been stable across time, primarily because of the skill level involved, this may change as the rewards

---

[154] See also Tiboni (2005).

[155] I disagree with the conclusion that just because it was a sophisticated 'operation' that it had to be perpetrated by the government of China. While this is certainly possible, my field research has clearly shown that some TOC groups operating in East and Southeast Asia have a high level of technological and operational sophistication (not to mention resources) to accomplish Titan Rain. The Titan Rain perpetrators appeared to have used a variant of the Myfip worm (Brenner, 2005). The original Myfip only stole .pdf files; the Myfip-B and later variants generally steal date files with the following extensions (Brenner, 2005). The items in the list below are prefaced by an apteryx (*) which is a standard wild-card character indicating any file name:

*.pdf - Adobe Portable Document Format
*.doc - Microsoft Word Document
*.dwg - AutoCAD drawing
*.sch - CirCAD schematic
*.pcb - CirCAD circuit board layout
*.dwt - AutoCAD template
*.dwf - AutoCAD drawing
*.max - ORCAD layout
*.mdb - Microsoft Database

I would also add the *.xls for MS Excel files to Brenner's (2005) list. During my field work, interviewees claimed that once a system had been compromised, tailor made search algorithms would be executed (designed for that operating system) to search for files matching the list above (Confidential Interviews, Kuala Lumpur 2003, Hong Kong SAR 2002, Tokyo 2003, Vancouver 2002-2004, and Manila 2003). The

for digital goods become greater and law enforcement focuses on the more public forms of cyber crime (Hinde, 2004:13).[156] The nature of the arrangements between system intruders and both NTOC and TOC groups can, and are often, fleeting. It may be interesting to note that payment for bot-net usage and or information stolen from compromised nodes of corporations or government is sometimes made in Colombian emeralds. In East Asia "the irony is that sophisticated groups of organized crime have found ways to gather data from telecommunications companies in the region, the same telecoms that law enforcement uses for packet sniffing, the data has value, it can then be sold on an access-based, or used by an organization for counter-intelligence purposes. It's not just the CIA that can hire database engineers and data miners" (Confidential Interview, Kuala Lumpur, Malaysia 2003).

The dynamics of the cyber black market

The trend is evolving to include more than crimes of opportunity but to creating opportunities based on market demands. This indicates that the underground market for stolen proprietary data is shifting from a supply-side to a demand-side dynamic in the region (Confidential Interviews, Hong Kong 2003, Kula Lumpur 2003, Tokyo 2002,

---

operational dilemma is the speed of the search versus the amount of CPU resources taken.

[156] A third case from the region further illustrated the point. During sometime mid-2002 an individual programmer with expertise in databases and network security was approached by an acquaintance and a former college friend to participate in a group that was being put together for the purpose of building customized software. The group was located was Hong Kong SAR and surrounding area. The assembled group was co-managed by an experienced "cracker" and a member of an organized crime group (name not provided). The interviewee's task was to write software to provide covert access and retrieval to a database owned by a telecommunications company in western Canada. The database was a customer and accounting system. Two small-group meetings interviewee claimed that a member of the PLA China was in attendance. After working on the code, the project was aborted at some point late 2003. The interviewee was paid and handed over the work that had been done (author has not had contact with interviewee since January 2004). The interviewee noted that a bot herder was, at some point, going to be involved. He speculated that a small, secure bot net could be used to transit the data and possibly store it for later analysis and retrieval. But this, admitted the interviewee, was very speculative (Confidential Interview Hong Kong SAR 2003, email correspondence February 16, 2004).

Seattle 2004).The use of a microeconomic model is particularly fitting in light of the results from the field research. During the late 1990s the market in East Asia for illegally obtained data – everything from research results from labs in Singapore to proprietary production methods from plants in the Philippines – was a niche market dominated by supply-side movement. In other words, TOC groups or independent network intruders would steal data, largely as crimes of opportunity, and then attempt to find a buyer.

If a buyer of the data approached a group or individual to steal the information it was usually considered a rare event or what can be formally called a niche market. The supply curve was highly elastic; meaning that successful attempts were relatively low and inconsistent. Now the underground market in East Asia has begun to swing to a demand side dynamic. Potential buyers of the data approach known actors in the Shenzhen, usually individuals with formal ties to TOC groups in the region. They then organize the transaction and employ stables of network intruders to accomplish the request. The demand side is relatively elastic but information gained through interviews indicates that this elasticity is decreasing. This means that a reasonably stable market, with known pricing levels is emerging. There are mixed forms of transnational organized crime using the expertise of each other to create an infrastructure that allows them to do what they need to do. These markets may challenge traditional notions of security as they internationalize and growth and expansion through international demand and supply. Indeed, the market for stolen data is rapidly shifting from a primarily supply driven to driven by both supply and demand side dynamics.

Conclusion: What is the Nexus?

Internet and computing technologies that are adopted, in any organizational structure,

impact in a vertical and horizontal manner. Vertical integration into both types of TOC groups in East Asia is a result of the integration of a younger, often more formally educated, generation. In general, it is this 'layer' that has become the innovation vectors pushing older and younger, less educated, members of Triads and other groups to use certain technologies. The uses range from secure, encrypted communications to untraceable cellular telephones. In one example, participants in a triad based in Hong Kong were involved in a smuggling ring targeting high-tech components for robotic manufacturing lines. Because this required the participation of individuals from three countries, a network intruder was hired to design a website that would operate hidden on the public Internet. The website had shifted IP addresses at regular intervals and used several layers of authentication. Once triad members "logged-on" they were able to view logistical information as well as messages from participants in other countries (Confidential Interview, Hong Kong 2003).

Vertical integration of Internet technologies allows the more sophisticated groups to streamline and secure communications, produce and distribute timely information, as well as control the level of access to this information. Maps can be distributed, photos, instructions and so on, all at a minimal risk. Face to face communication is still the most secure form of information transmission, but the use of software designed especially for them by a stable of network intruders or "hackers" means that specialized customizations can be quickly added and constantly maintained.[157] Vertical integration of Internet technologies allows operations to be streamlined in only the top-tier of TOC groups

[157] In one particular example, a series of webcams were setup outside of a target facility in the outskirts of Hong Kong weeks before the crime was committed. All of this 'intelligence data' could be stored and analyzed on a server by a select group of individuals with the correct privileges (Confidential Interview,

operating in East Asia.

Horizontal integration allows TOC groups to accomplish two critical tasks: bring in new "hacker" talent and use the technology to gain access to critical information. First, elements of TOC are now playing the role of an agent to negotiate deals between network intruders and clients. Corrupt government officials, other organized criminal elements, individuals, and increasingly, firms in both East Asia. This is a more recent development which may explain concerns in some policy circles that terrorist groups are contracting out certain computing "services" through TOC agents that have been developing "stables" of talent. It must be pointed out, however, that these links are at best theoretical and only scant anecdotal evidence was found.

Second, the horizontal integration of Internet technology allows for the theft of data. There are cases where stables of network intruders working under the supervision of several triad members to steal proprietary information from corporate and public laboratories in Singapore, to high-tech manufacturing plants in Taiwan, Japan and Southern China (Confidential Interviews, Hong Kong SAR, Manila, Tokyo, Kula Lumpur, 2003). This is a particularly attractive horizontal strategy because the rewards are high but the risk is very low. In most of the instances that I came across, the techniques often employed a combination of remote network intrusion from a distance with various types of social engineering strategies.

In the very near future, machines will overtake humans to become the biggest users of the Internet as the cyber infrastructure adds electronic sensors, smart homes, and RFID tags that track objects in physical space (ITU, 2005). With more machine than human

---

Hong Kong 2003).

activity in the cyber infrastructure, the number of compromised nodes will grow. My conclusion here is that the increasingly organized and sophisticated use of elaborate cyber infrastructure strategies and tactics in East Asia has connections to the more traditional and non-traditional forms of TOC but participation by these actors is far from systemic and persistent. The digital divide within traditional triad organizations means that their respective leadership or hierarchies are rarely aware of the use of high-tech tactics and strategies. These conclusions parallel changes in transnational organized criminal activity in the region observed by Zhang and Chin (2003) and discussed in Chapter Seven. Small, nimble, highly skilled networks or ad hoc groups are not necessarily replacing more traditional forms of TOC in the region. Because, from an operational perspective, these crimes are highly technical and strategically sophisticated, traditional organized crime groups in the region are becoming market consumers of the raw illicit data, rather than producers.

It should be pointed out that this is not true in all cases. There were a few claims made by interviewees that bot herders were forming more stable relationships or partnerships with the traditional crime groups but it is far from clear what this looks like or how it will evolve. It is, therefore, still unclear as to the extent of the activity, relative extent in East Asia, of both bot net growth and the cyber black markets that support them.

The key conclusion here is that the trafficking in illicit data, obtained by systems intruders, in East Asia is a growing problem and one that mirrors, in many ways, the growth of trafficking more generally. It draws on the problem of flatter, more nimble social networks, jurisdictional arbitrage, and the problem of state capacity. Intrinsic data mined from compromised nodes from around the world, stored on servers in Shenzhen

and Hong Kong, customized software services developed for both the cyber and organized criminal underworlds – all adaptations in the face of both changes in black markets and law enforcement. Can the state adapt in the face of a nascent nexus between systems intruders, TOC groups, and possibly other state actors? Do cyber enabled organized crime groups in the region constitute of threat to security? These are the subjects to which the following chapters now turn.

Chapter Nine: Bot Nets and Back Channels, The Return of the State

Introduction

In the previous chapters, a link has been established between both traditional and non-traditional forms of organized crime groups in East Asia and system intruders operating in the 'cyber underworld.' That link has been characterized and tentative claims made about what these links might mean for security in the region. The process of state responses to threats from the cyber infrastructure has been introduced as a series of coevolutionary competitive processes. This cat-and-mouse adaptive game is influenced not only by the actors and payoffs but also by the national environments in which they take place. As will be shown below, adaptive competitive processes do not take place in a vacuum. This final substantive chapter turns now to the remaining conceptual and substantive questions. First, if there is an adaptation space between state responses to cyber security threats, is it increasing or decreasing? Second, what conclusions can be drawn regarding state capacity to respond to cyber security threats in the region?

Chapter eight concluded that while criminal innovation does not, in the short run, constitute a threat to security, this does not mean that states will 'see' it that way. There have been fairly consistent efforts in the region to securitize the cyber infrastructure. This is driven by two critical tensions in both the behaviour of state actors and in policy discourse. The first tension is driven by a loss of control narrative regarding cyber space. Here states see a 'space' that is not 'in control' and can thus be a threat to security. The second tension is enveloped by a tendency to see the cyber infrastructure in territorial terms as anarchical and subject to power projection in order to maximize the national interest. This emerging virtual realism accurately characterizes and explains state behavior in East Asia toward the cyber infrastructure both in the realm of security and in

international politics more generally.

This chapter will begin with a discussion of the loss-of-control narrative and situate it within the context of an emerging virtual realism. The following section discusses the coevolutionary gap between law enforcement agencies and criminal innovators within the context of three brief cases: Singapore, Hong Kong SAR, and China. It will be important to situate state responses in the region against international models and, in principle, make tentative distinctions among global models used in the United Kingdom (UK) and the United States (US). This section illustrates the problem of accurately describing the competitive processes by using a predator-prey model. This will only be a very initial examination within the context of an explicit coevolutionary competitive model. It is initial, or tentative, because of the number and complexity of the actors involved: a) state – law enforcement and intelligence; b) cyber actors – systems intruders and bot nets; and c) TOC and NTOC groups. Despite the problems associated with accurately characterizing the gap, it is clear that the widening has been arrested in some countries, but continues to widening in others.

The chapter concludes with a discussion of East Asian states in a cyber world characterized by virtual realism. There are several important issues regarding states in East Asia. First, the problem of jurisdictional arbitrage has only recently been addressed in the region. This has exposed, not surprisingly, a host of interconnected issues such as state capacity, victim silence, and particular norms and culture. These issues stand in tension with an emerging realism in the region, especially in light of the evidence found in Part One of this study linking the level of the rule of law and the number of compromised nodes in East Asia.

Virtual realism and a loss of control

A number of scholars have noted the growing gap between cyber infrastructure threat perception and reality. One research effort is particularly relevant for this work. Peter Shields studied the response of the US government to the migration of money laundering to the cyber infrastructure, for example, through the cyber payment system. Shields argues that in general there are growing distortions between the evolution and growth of the cyber infrastructure and threats to security from organized crime. His main thesis is that "the 'loss-of-control' narrative obscures the fact that much of the money-laundering problem has been fueled not by technology developments per se, but by the dynamics interaction between these technological developments and ongoing developments in criminal justice policy and associated changes in the US state" (Shields, 2005:485). Shields is careful not to underestimate the very real pressure or gap between law enforcement and criminal innovation but he is interested in teasing out a more nuanced understanding of the growing gap. This is important because, as Kenneth Minihan discovered in a sweeping study of the US military's cyber infrastructure conducted in 1996, "[o]ur [US] ability to network has far out paced our ability to protect networks" (Minihan, 1996:14).

While Shields analysis is methodologically problematic (relying on narrative analysis alone) he does have a point: "it would be a mistake to view the 'information revolution' as the sole or primary driver of these phenomena" (Shields, 2005:495). Shield argues that the loss-of-control narrative, which has become "dominant", and that a "central element of this storyline is that the 'information revolution' has plunged law enforcement into crisis" (2005:495). More specifically that the cyber infrastructure is "portrayed as undermining law enforcement's 'follow-the-money' approach to combating organized

crime" (2005:495). The loss-of-control narrative, according to Shields, characterizes the state as "purely reactive" and "greatly understates the degree to which the US state has actually helped to create the conditions that have generated and exacerbated the money-laundering problem" (2005:497).

Shields analysis does, however, lead to an important point: the sense of a loss-of-control effects international security relations because the US has begun in earnest "the export of surveillance-intensive money laundering countermeasures to unwilling countries" which can be "justified in a similar way" as the crisis generated by a loss-of-control (2005: 502). A very similar brand of export from the US to East Asian countries is evident. An example is the use of the US model for detecting emerging problems which borrows from epidemiology and the use of "syndromic surveillance" (Stoto, 2005). The idea here is that in addition to state policies aimed at retaking the cyber infrastructure – a device-by-device security strategy – law enforcement agencies have begun to implement broad syndromic surveillance programs designed to act like early warning systems used by disease outbreak and control programs. The strategy involves the use of passive and active monitors that rely on disclosure and reporting of Internet security 'outbreaks' using an infection control analogy from epidemiology (Milito, 2006). As Casman *et al* (2005) note, there is a tradeoff between sensitivity and specificity in syndromic security strategies. This means that it is highly unlikely that syndromic surveillance systems can detect the first or even sixth case of a newly emerging threat. Syndromic surveillance capacities provide the state a kind of 'population-wide' monitoring framework within a social, political and temporal milieu that would otherwise make overt intrusions by the state into the cyber infrastructure untenable in most cases.

Moved to an international level of analysis, Shields work provides a theoretical

starting position in understanding how criminalization and securitization of the cyber infrastructure by states in East Asia is occurring simultaneously. Most countries in the international system now make commitments to rolling out information infrastructure. It is viewed as a tool of both economic and military empowerment. But it also ushers in a host of non-traditional vulnerabilities and insecurities that are difficult to for states to understand and respond to.

Adaptation space

A coevolutionary competitive process means that when an adversary is faced with a quickly evolving predator the tendency is to reach for the tools that are known best to both predator and prey. Framed within the context of state institutional capacity this usually means more police and more laws and, possibly even framing the problem as a threat to 'national security' which then provides a rhetorical foundation for the use of extraordinary measures to confront the threat.[158] The state is in a unique position in the predator prey analogy because it is both prey when the target of attacks and predator responding to or attacking. But as has been argued in Chapter Seven, state actors too are feeling their way around the nexus as predator, not just as prey. Responding to quickly evolving criminal networks has only in recent years begun to stimulate a more focused response from the law enforcement communities in the region. This shift appears to be evolving from a universal approach to the cyber infrastructure to a more concerted device-by-device strategy. But as we have seen in previous chapters, there is a certain

[158] There is a growing array of international and national laws to deal with 'cyber crimes'. A full survey of these legal apparatuses is well beyond the scope of this study. However, I do note that the importance of understanding cyber crime is most certainly linked to knowledge of cyber crime legislation and privacy laws. For a detailed look at the international legal instruments developed to combat 'cyber-crime' see Pocar (2004) and Urbas (2001). Pocar argues that despite a very long list of international legal tools that have been developed to address the impact of technology and criminal innovation especially the use of the cyber infrastructure, other than specific European conventions, few of the international legal instruments have come into force (2004:31). The bulk of the heavy lifting is done by national legislation. The exception is the EU Convention on Cybercrime which is the standard to which other efforts are often compared.

cyber security viscosity at work – i.e. the degree to which the illicit data in the cyber underground resists flow under an applied force stemming from state laws and regulation.

There are a number of models of coevolutionary competitive processes that can describe asymmetrical arms races: the Tron Game, the aggressor-defender model, and the more familiar predator-prey model. The Tron game has been used in studies setting humans against web robots (software based artificial intelligence) in the cyber infrastructure. The Tron game is a type of "live and let live" model inspired by the 1980s science fiction movie *Tron*. According to Funes *et al* "two robot players make tightest [sic] spirals in order to stay as far from the opponent as possible. This form of collusion is a frequent suboptimal equilibrium that prevents learning robot strategies by self-play in a coevolutionary arms race" (1997:6). While the eventual goal is to approach and cut-off the opposing player – thereby destroying it – this does not fit the competitive processes in cyber infrastructure security because the strategy used in the beginning of the game is to stay as 'far away' as possible. It is only after the "structure" of the game forces competitors into tighter confines, does the "race" begin.

Another possibility is the aggressor-defender used by Anderson (2004). Using an abstract geometric approach, Anderson argues that in "multiagent systems, small changes in individual-level rules may lead to very large changes at the group-level. This phenomenon is striking in the aggressor-defender game, a simple participative game in which each participant randomly selects two others from the group A and B. In the aggressor game, everyone tries to position themselves so that A is always between themselves and B" (2004:175). In a very abstract manner, the aggressor-defender game does incorporate the "positioning" of the actors involved in this analysis: the state, nodes in the cyber infrastructure, and criminal innovation. But it does not accurately describe

the "chase" that ensues, nor does it apply to the types of information exchanges and equilibrium dynamics seen in cyber incidents, as discussed in Chapter Three.

The final framework is a predator-prey model. This model is generally used to describe the dynamics of biological and ecological systems in which two species interact, one is a predator and one is its prey. This model holds for the action-reaction between attacks, defence, and then subsequent iterations which lead to new strategies. But the predator-prey model describes the ebb and flow of population dynamics (Volterra, 1931). So, while an explicit Lotka-Volterra model of predator-prey interaction is not useful for this study, as an analogy it may work. But there are limitations to the predator-prey analogy. For example, Robert Jervis (1997) who wrote about international system change and the state, argues for a more nuanced view of coevolution in the sense that actors not only compete with one another in their environments, they change it (1997:48). This interaction or feedback is the point at which complexity theory, according to Jervis, can help explain the unintended consequences of international processes. Be that as it may, the adaptive understanding of the state and the cyber infrastructure in this study stops at the point where Jervis and others take off. A much 'simpler' objective is to restrict the analysis to the adaptation space in a coevolutionary environment and not account for interactions feeding back into that same environment.

In methodological terms, coevolutionary competitive processes, while conceptually useful, are very difficult to 'test'. This is the trade-off when using these frameworks; they are easy to conceptualize but very difficult to generate testable hypotheses. This holds true in Biology and is also a factor in this study. In International Relations, for example, Cederman (1997) defines complex adaptive systems within the context of International Relations as an "adaptive network exhibiting aggregate properties that

emerge from the local interaction among many agents mutually constituting their own environment" (1997:50). But Cederman's definition is used to distinguish complex adaptive systems as an alternative modeling methodology to more traditional agent-based and game theory computer simulations. Coevolutionary competitive processes are a more abstract idea when compared to the strategic adaptation inherent in Cederman's complex adaptive systems model. While analytic 'solutions' are certainly possible, they are rarely tested against empirical data obtained outside simulations. The questions, however, that are central to the use of coevolutionary frameworks to study adaptive competitive processes are never-the-less relevant here: what is it, exactly, that adapts (Price, 1997:245-247)? Is it the state? The institutions? Or the individuals that make the institutions work?

The Red Queen effect (discussed in Chapter Two) is another good example of the inherent limitations. Recall that the effect, for the purpose of this study, makes two claims: first, that it takes all the 'running' an actor can do just to maintain its position. Thus, the ability, or likelihood, of survival does not increase over time. Second, as Fici and Pollack (1998) argue in their analysis of the application of genetic algorithms to game theory, the "desired arms race does not simply involve competition, but also enculturation towards convention" (1998:9-10). Abstract, yes, but important in understanding that the competitive process itself produces a culture which feeds back into the process. This is very difficult to observe empirically, and limits the extent of the substantive conclusions.

Coevolutionary patterns in cyber infrastructure security are rooted in what Savona and Mignone identify as a paradox. The paradox, they argue, is that

> law enforcement agencies exploit technologies in their crusade against crime, which – as explained – is also highly dependent on new technologies. From this standpoint, new technologies are a threat and a piece of good fortune for both criminals and law enforcement authorities. In fact, criminals enhance their activities by means of ICT, which make them vulnerable to the risks of being intercepted by the technological solutions used by the police (2004:18).

But the goal of an optimal state response is to disrupt or dissolve networks rather than try to destroy them – at least, in theory. Mathematical modeling, for instance, does show that this is the most efficient way to handle social networks in which the links or connections are not entirely known (Levine, 2004:7). This appears simple in theory, but in practice closing the gap between criminal innovation and state responses become much more complicated. Police agencies have very low levels of trust not only between countries but also within – and it is trust, even in the cyber infrastructure, that makes things happen.

In addition to trust, politics also plays an especially important role (Kluver, Randolph, Indrajit, Banerjee, 2005). This is due to "many nations … rising to this challenge [cyber crime], individually and collectively, but the web of international cooperation does have its holes and those nations that lag behind the leaders risk becoming havens for cybercriminals of the future" (Grabosky 2004:1). Other scholars have more explicit advice for law enforcement when faced with nimble social networks.[159] Phil Williams argued that the "approach has to be strategic, with clear and realistic objectives (containing and weakening rather than eradicating organized crime), coordination of efforts to pursue these objectives, explicit measures of effectiveness, and efforts to think through the implications of success (how the criminals might adapt and how to ensure that the threat they pose is less rather than more severe after their adaptation)" (2004:4).

[159] Interesting endnote on how technology and crime is impacting Criminology as a discipline: "in the fast moving world of the future it is likely that criminology will have to sacrifice some scholarly rigor in favour of timeliness and relevance" (Clarke, 2004:60).

On the one hand, the cyber infrastructure was designed to route around obstacles, but both TOC and NTOC groups must effectively neutralize efforts at social control in cyber space in order to be successful innovators of these technologies.[160] In an environment in which these dualities increasingly matter, does narrowing or widening the adaptation space simply boil down to resources? Possible, but unlikely. A study by Kenny (2003) that looked at how flatter networks are changing the illicit drug trade concluded that while "non-state criminal enterprises cannot match the technological sophistication of drug enforcement and intelligence agencies, they possess important advantages over their state adversaries, including the clandestine nature of narcotics trafficking, flatter decision making hierarchies, and fewer bureaucratic restraints to action" (2003:133). In East Asia, they can and do, match the state – but only certain states. The prescription, it would seem, would be to fight networks with networks. But simply throwing networks at other networks does not address jurisdictional arbitrage, weak states with low institutional capacities, victim silence, and differing norms and cultures across countries – especially in East Asia.

The UK model is often held as an example by both practitioners and scholars of an effective institutional and organizational response to high-tech crime. The National High-Tec Crime Unit (NHTCU), headquartered in London, was created in April of 2001. Originally tasked with fighting cyber crime like fraud and phishing it has rapidly

[160] McMullan and Perrier (2003) have a great discussion of early works in criminology and sociology. Specifically, the impact of what Haggarty (2005) calls the "the accelerated embrace of new crime-fighting technologies" (2005:492) and the subsequent "unanticipated consequences of technologies" (2005: 495). McMullan and Perrier also found that technological payoffs do not often emerge as expected. For example, the "system of mobile communication fostered the development of 'response time' as a measure of police success, although we now recognize that the speed of response bears little relationship to police effectiveness" (2005:495). The authors have also studied the technologies which have been used by organized crime against gambling-related computer systems in Nova Scotia, Canada. Sophisticated organized crime that employs advanced technologies in either method or organization do so not as a tool to accomplish the job (i.e. steal the data) but must also consider it to blunt, manipulate, circumvent or 'hack' state control.

expanded to deal with organised crime and individual hackers and set up the first formal links with industry to increase the effectiveness of cyber crime prevention and reporting. The model is being replicated in Australia and South Africa. The NHTCU from the beginning appeared to make a conscious choice not to field experts in all areas of the cyber infrastructure. Instead they chose to focus on two dimensions: 1) forensic computing; and 2) network investigation.

To help manage the problem of firms staying quiet after serious system breaches the NHTCU created and launched the Confidentiality Charter for businesses (NHTCU, 2005). The Charter has shown promising results in allaying the concerns of firms when reporting breaches, but it is still voluntary. To date, however, there is only one jurisdiction in the world that requires, by law, that firms report system intrusions – California. California has also devised a new type of model to respond to cyber infrastructure crimes. The Northern California Model operates on a regional basis rather than a national one. The US Department of Justice has set up ten regional units across the US staffed by technical experts as well as lawyers. What is also different from the UK model is the focus on intellectual property rights rather than the crimes. What is unique about the California initiatives is that they place considerable emphasis on providing the 'right tools' for both the lawyers and investigators.

Briefly, there are two capabilities that cyber crime investigative agencies should possess. First, each organization should have the ability to investigate crimes occurring on computer networks. Second, an organization should have the forensic capability to analyze seized electronic evidence. Self-evident, perhaps, but states such as the Philippines use a single unit to exercise both functions, while others such as Hong Kong separate these functions into different units. It unclear which models work best (holding

other factors constant) but innovation appears to be key in East Asia.[161] Huey argues that it is not just a lack of resources and training, it is that police agencies often treat cyber enhance crime and the technologies involved as a kind of black-box primarily because of the territorial nature of policing itself. Huey argues that this "is because historically the nature of policing in society has been intricately tied to spatial arrangements. The public police meet their prescribed mandate through techniques involving the oversight of very carefully defined territories" (Huey 2002:244). Measured by basic capabilities alone, the Philippines, China, and Indonesia all appear to be lacking in one facet or another.

In addition to basic capabilities, there are law enforcement tactics which can include monitoring and infiltrating clandestine cyber social networks like bulletin groups and IRC channels, developing computer programs to information and incident data, and making connections – both formal and informal - with security personnel working for private sector firms and state security agencies. Increasingly, these links are being made across borders in order to address the problem of jurisdictional arbitrage and the digital divides that exist between information rich police forces versus information poor agencies in East Asia.

In this regional context, cyber security issues were in the past been linked to economics. This stands in stark contrast to state response patterns in the US. In the US case, a much more subtle, hegemonic strategic approach has evolved rather than the 'surveillance' focused approaches in East Asia. Both approaches often involve the private sector. But in the US case, the cooperation is built on strategic footings.

---

[161] As an example, one of the more basic measures is the Police innovation curve. There are few openly available studies on this subject. However, one particular research effort of police adaptation at the micro level stands out. The authors looked at municipal forces in North American and found that "[a]doption and extent of utilization proved to be largely independent processes. Involvement in cosmopolitan networks, experience with using databases for law enforcement, and the human capital capacities of the organizations influenced the adoption decision, while organizational resources and experience in using the system drove the level of actual use" (Skogan and Hartnett, 2005). The finding is rather stark.

Lichtblau and Risen, writing in the New York Times found that one "outside expert on communications privacy who previously worked at the N.S.A. said that to exploit its technological capabilities, the American government had in the last few years been quietly encouraging the telecommunications industry to increase the amount of international traffic that is routed through American-based switches" (2005). In effect, this extends the information territory of the US, at the loss of others – especially in East Asia. These two approaches point to a key difference in managing the growth of the cyber infrastructure. What is important is that states in East Asia are now mirroring or responding to the US approach in an attempt to 'secure' and maintain the integrity of their infrastructures.

Similar cooperation strategies are employed in East Asia. For example, the governments of South Korea, Japan, Singapore and Hong Kong, for example, require Internet service providers to keep information on users and to help law enforcement agencies track their online activities. In Japan, the Communications Interception Law was passed in August 1999, allowing law enforcement officials access to private e-mail accounts if they were investigating certain types of crime (Williams, 2000). The Communications Authority of Thailand (CAT) by law has minimum 32 per cent share in all privately-owned ISPs. In addition the National Information Technology Committee (NITC) has ordered ISPs to retain connection data about their customers for at least three months. The goal is to enable prosecutors to take action against those who surf to 'undesirable' websites and to facilitate government authorities to block such sites. (Reporters Without Borders, 2002).

Moving to the case studies will demonstrate not just the adaptive responses in East Asia to criminal innovation as a security problem but also situate this process within a

strategic cyber awakening in the region. Three cases will be presented: Singapore, Hong Kong SAR and China. The complex two-level game that states in the region must play within cyber space continues to evolve and change. The cases show that while the idea of security in the cyber infrastructure is changing in the region, there does not appear to be a threat to the infrastructure itself. But rather, the threats are effects of contending social and political forces.

Singapore

National information infrastructure strategies and policies in Singapore have been cornerstones to economic growth (Kraemer and Dedrick, 1996). Growth, jobs, and the ability to compete in region by attracting MNCs and reinforcing the city-state's role as a regional hub. Singapore's vision is of an intelligent island; one that can achieve balance between economic openness and a kind of communitarian ideology. Political and religious websites must register with the government's Media Development Authority (RWB, 2003:100). There is good reason for the government in Singapore to worry. The country has made science and technological development the foundation of its economic plan. The fours pillars of growth: biomedicine, electronics, chemicals and engineering have seen massive investments from both public and private monies since 2000. The key to the *four pillars* is the idea of taking an initial idea through the research and development stage all the way to commercialization, all accomplished within the city state (Young 2004:48-51).

Singapore's policy toward the cyber infrastructure began in the 1990s with a strong government controls which have gradually been reduced as a culture of self-regulation has embedded in society (Lee 2005:79). This is a unique model in East Asia. The practicability of self-regulation relies on the application of 'auto-regulation', where

cryptic and arbitrary policies and legal codes as governmental technologies are employed by regulatory authorities to "shape, normalize and instrumentalize the conduct, thought, decisions and aspirations of others" (Miller and Rose, 1990:82). With the holistic application of 'auto-regulation', the otherwise complex and arduous task of Internet policing in Singapore is made less onerous, aided and empowered or 'coregulated' by laws, policy codes, statements and generalised techniques and technologies of surveillance designed to shape the conduct of individuals and groups within society.

While the auto or self regulation model now dominates the more public dimensions of cyber security, very little is known regarding Singapore's response to the emerging nexus between systems intruders and law enforcement.[162] In November 1998, the local Straits Times reported that a section of the Singapore Police Force has been set up to "patrol the alleys of cyberspace" (Chong, 1998). While their official role is to keep hackers and cyber-crime at bay, the very existence of a 'cyber-police' branch in the late 1990s served to reinforce the widespread belief that Internet surveillance is conducted in Singapore (Lee and Birch, 2000:159). In April 1999 some anecdotal evidence surfaced that SingNet was conducting secret scanning of its subscribers' web accounts, supposedly for vulnerabilities to virus attacks (Chong, 1999b:1). No further information on this 'cyber-police' has been available since.[163] It is probable that this branch has been subsumed under the Technology Crimes Division of the Criminal Investigations Department (CID) of the Singapore Police Force (SPF).[164] It has also formed close ties with local universities for forensics, security research and support (Straights Times, 2001).

Singapore's strategy is not limited to strictly law enforcement and intelligence

---

[162] In many ways the Singapore model has been a 'beacon' for other states in East Asia, especially China.
[163] For a history of Internet regulation in Singapore see Rodriguez (2000).
[164] I have not had a chance to do extensive field work in Singapore; much of what is openly known about the case is often rumor or anecdotal evidence and the few quasi-academic articles that have been written.

institutional capacity building. There has also been a concerted effort to engage the 'hacker' community. Government and industry have in the past organized a contests to find the city state's best computer hacker. Six teams competed in hacker challenges organized by the government-funded National Infocomm Competency Center. Singapore has not made cyber infrastructure security an entirely separate pillar but has that required law enforcement, legal, and intelligence personnel take courses on computer use and misuse. Singapore was one of the first countries in East Asia to routinely jail 'hackers'. System intruders, or anyone using the Internet for anything "untoward", were routinely jailed for up to three years or fined up to US$5,800 under the state's Computer Misuse Act.

What is key in the minds of policy makers in Singapore is the how valuable information becomes as it goes from concept or idea through to potential commercialization, traveling all the while from hard drive to hard drive. This new information economy is being 'mapped-out' by both traditional and non-traditional TOC groups in East Asia; targeted because of both the sheer volume and value that much of the data produced in areas like biomedicine to nanotechnology (Confidential Interview, Hong Kong 2003). The Singapore economic development initiatives mean that the value of the data sitting on hard drives in labs and administrative offices cannot be understated. Despite Singapore's technological prowess and the relatively small number of users and content it must regulate, the government has not pursued a China-type firewall strategy. Instead, the Singaporean government has openly recognized that absolute control is not possible (Rodriguez 2000:24). From what is known Singapore appears to possess a kind of cyber siege stance in its policy toward the infrastructure. This makes sense historically when looking at other dimensions of the city state's security. Singapore's foreign and

defence policy has been rooted in a kind of siege and insecurity, and has shown a remarkable ability to cope and mitigate innate vulnerabilities. In Singaporean security policy "nothing is taken for granted and nothing is guaranteed" (Leifer, 2000:162).

Two laws in Singapore shape law enforcement's response to cyber threats: the Singapore Computer Misuse Act and the Electronic Transaction Act. Both laws are similar to other pieces of legislation in the region except on two points.[165] First, recent changes to the Computer Misuse Act allow security agencies to take whatever pre-emptive measures necessary to counter or prevent threats against the infrastructure. Second, Singapore has modified both Acts to require any user to hand over encryption keys to law enforcement. As of 2003, only Singapore and Malaysia have enacted laws that would require users to disclose their keys or face criminal penalties. In both of those countries, police have the power to fine and imprison users who do not provide the keys or plain text version of any encrypted file. This includes an extra-territoriality dimension which requires users to render assistance to law enforcement even if the files are located in another jurisdiction.[166]

Much of the evolution in the legal environment and the growth in cyber security awareness in law enforcement and intelligence agencies is guided by Singapore's "Infocomm Security Master Plan." The Master Plan articulates what Singapore sees as the threats from cyber terrorists, cyber criminals and "irresponsible" hackers (Choudhury, 2005). Little, however, is known about the effectiveness of its cyber security

---

[165] Singapore and India are the only two states in Asia where interception warrants are issued by executive authorities alone (Wong, 2005:65). Places where interception warrants are issued by courts: Canada, New Zealand, the Philippines. Other countries where interception warrants are issued by executive authorities or courts, for example, Thailand. For a good comparison of Hong Kong SAR, Australia, the UK and the US interception laws and regulations see Wong (2005).

[166] I should point out that there are additional data retention and storage regulations forthcoming in Singapore. In general, data retention regulations make it 'easier' for law enforcement to monitor the infrastructure and gather traffic data. This, as opposed to content data, for which no retention laws or regulations exist. For example, in Canada, law enforcement face a much lower threshold for obtaining warrants for traffic data. The threshold to obtain warrants for content data are considerably higher.

infrastructure in closing the adaptation space with innovation in TOC groups outside Singapore's borders. The key is management of the cyber infrastructure and the coevolutionary adaptive processes within its territory but this has the paradoxical effect of 'pushing' the problem to other jurisdictions without the capacity to respond. This process highlights one imperative of jurisdictional arbitrage in a coevolutionary adaptive environment where there are extremes in cross-national institutional capacity. While the 'inside' of a states information territory may be 'secure', it will only be as secure as the weakest state.

The problem here is that, in the long run, this does not change the likelihood of infrastructure instability – it simply transfers it. This is the essence of the Red Queen effect. In the Singapore case – the paradox underscores a result of the Red Queen effect, even though adaptation has been in one sense more successful than other countries in the region, the probability or chance that there will be serious infrastructural instabilities remains constant. Recall the underlying process of the Red Queen effect is that it takes all the running you can do just to remain in one spot. What is unique is that it is 'easier' for states to securitize an external threat to the cyber infrastructure.

Hong Kong SAR

Second only to Singapore in their response to criminal innovation, the Hong Kong Police have also begun aggressively adapt to criminal high-tech innovation. A Computer Crime Section was set up in 1993 to investigate complaints of serious computer crime. This was followed the provision of resources for preventing computer crime and increasing the capability of handling computer crime at the local detachment level. The capability was strengthened with the upgrade of the Computer Crime Section to the

Technology Crime Division in 2001.[167] The Division is designed to enhance police expertise in computer crime investigation, established a computer forensics laboratory to support investigations and conduct research and development.[168]

The adaptation space in both the Singaporean and Hong Kong responses to criminal innovation is slowly closing. But the adaptation is uneven in addressing jurisdictional arbitrage – especially southern China. Law enforcement heads from Hong Kong, Guangdong, Macau regularly meet for Tri-partite sessions for the promotion of intelligence sharing and co-operation on investigations. The tripartite meeting is a bi-annual event.

While Singapore and Hong Kong national information infrastructure strategies and policies grew out of a purely economic dimension, such evolutionary trajectories are not entirely uniform across East Asia (Kraemer and Dedrick, 1996). In Japan, for example, the cyber infrastructure development was to support new economic growth and jobs, deal with US threat in high-tech business, then catch-up with US lead in PCs, software and networking. Singapore's 'intelligence island' and Hong Kong 'information hub' all have a regional market competition influence that sees the integrity of their cyber spaces as key to maintaining an image. In other words, the perception and reality of a clean, safe cyber infrastructure is a paramount goal. But this is not consistent across the region. In Japan, for example, it is a vision and image of a 'multimedia information society' which

---

[167] There is extensive capacity building in other law enforcement agencies in Hong Kong. For example, the Anti-Internet Piracy Team in the Customs and Excise Department is responsible for investigating copyright piracy on the Internet which set up its own computer forensic laboratory in 2000. It is responsible for providing computer forensic technical support for examining electronic evidence contained in seized computer systems.

[168] Another example which sets Hong Kong SAR law enforcement apart from regional counterparts is the advanced computer forensics tools that they have devoted resources to -- tools that in the past were the purview intelligence agencies. The Commercial Crime Bureau "Technology Crime Division" (TCD) has, in co-operation with the Hong Kong University of Science and Technology, developed a high-powered system to crack password-protected files. The system, known as a 'password cracking cluster', consists of 25 high-powered computers. An adaptation to the increasing use of strong encryption in the conduct of crime.

often informs cyber infrastructure policies. The Japanese government has, however, followed the lead of many other countries by aggressively and quietly taking back cyber space. For example, the Diet voted in March 2001 to spend slightly above US$1 million to create email monitoring software called "Kari-no-mail." It was ready by the end of that year and is reportedly being installed on the country's ISPs (RWB, 2003:70). If the reporting is correct, both the relative low cost and ease of implementation is notable.

China

State responses to criminal innovation in China are complex and as rooted in existing social and political contexts as other East Asian states discussed above. Inefficiencies and inconsistencies toward the infrastructure appear to originate within the central government where a number of different government agencies claim authority over 'IT' and thus, the infrastructure itself. In 1998, the government planned to create a single body called the Ministry of Information Industry (MII) for telecommunications, but because of bureaucratic competition between agencies and ministries ended up as a kind of 'home land security department' for cyber space – complete with the problems and complications that accompany the creation of extremely large, heterogeneous government bodies.

The political super systems in China, called the *xitongs*, which organize the line ministries have created a large amount of dissonance. The clash of motivations between central and local level bureaucracies as well as the Chinese government's often unique internal logic (Mertha, 2005) are key to understanding cyber security in China. In other words, there is significant bureaucratic vulnerability to corruption and technical incapacity. This, not surprisingly, leads to problems in hiring and personnel retention in both law enforcement and intelligence agencies in China. Hong Kong SAR and China

often choose to hire cyber crime investigators only from within the police force and then provide them with training in computer technology. Others, such as the United States, have at times gone outside organizations to hire individuals who already have computer security expertise and then provide them with training in various aspects of law enforcement.

PRC Police forces face broader capacity problems in a unique social political context. In China responses criminal innovation are also hampered by exogenous variables like the slow pace of law enforcement reform and what one scholar calls the the crisis of legitimacy crisis. "Police law reform legislation, such as the Police Law, is making an impact in revolutionizing modernising, and institutionalising the police of the PRC" which has resulted in an uncertain result that has been impossible to measure (Kam, 2005:11-12). This, in addition, to poor funding and high levels of corruption have left many law enforcement efforts in mainland China blunted. The focus for the government in Beijing remains political control over cyber space, rather than law enforcement. The government is also pushing for an internationalization of cyberspace which is designed to buttress rather than supplant its controls "at the borders" (Neill, 2005:18). The 'internationalization' here is more akin to the making of state centric enforcement and regulatory regimes. This tandem approach to cyber infrastructure security is perhaps the best example of the tensions between internationalization and the desire to stem the ill-effects of globalization.

CCP leadership and Chinese academics warned about the ways in which Internet technologies can challenge state sovereignty by magnifying so called sources of post-Cold War instability (Hughes, 2003:140).[169] The Internet enhances not only traditional

[169] A recent by Villeneuve (2006) on WWW content filtering noted that states are "seeking to assert information sovereignty over their cyber–territory" (2006). China is the prototypical case.

state-based threats to security but also non-traditional threats like those from digitizing organized criminal groups in the region. MII and CCP see these threats within the context of broader notions of global power (2003:141). What has emerged then is a virtual realism designed to consolidate and expand its information territory and preserve the integrity of its information borders (2003:142). This goal appears to hold across states but it is in strategies where the differences are to be found.

Singapore and Hong Kong SAR, which have taken an economic centric approach, are holding the adaptation space constant, and in a few dimensions reducing the gap with criminal innovators. This is not the case in China. Here the gap is widening. The securitization of the cyber infrastructure by Beijing has put the focus on threats to the state itself and rotates on a kind of elliptical public policy orbit centered on cyber territorial integrity. This, viewed from an outside perspective, often gives it an appearance of contradiction and confusion.

East Asian region

While there are emerging, robust mechanisms to deal with cyber crimes and transnational organized through increasingly elaborate policy frameworks akin to regional frameworks for combating terrorism, real progress to date has been slow. Consequently, cyber security cooperation across the Asia Pacific tends to take the form of a network of overlapping frameworks between member countries, dialogue partners and other nations from across the globe. This network relies on the tapestry of interlocking associations, agreements and arrangements that emphasize collaboration and cooperation in combating a transnational threat such as terrorism.

In East Asia, much of the relevant organized crime initiatives have been subsumed under 'terrorism' in a post-9-11 world. Action has been taken in the region to enhance

bilateral and multilateral cooperation to combat terrorism through the Association of South East Asian Nations (ASEAN), the ASEAN Regional Forum (ARF), and the Asia Pacific Economic Cooperation (APEC). The frameworks provided by these organizations are based on the global instruments for terrorism and transnational crime together with regional specific instruments.[170] The effectiveness and progress thus far has been minimal. East Asian states are being pushed to adopt Council of Europe's convention on Cybercrime and it is possible that points will be adopted into national legislation, but progress has been slow (Urbas, 2001; APEC-TEL, 2002).

Other examples of cyber security networking include a conference on strengthening international law enforcement cooperation to deal with cyber crime, held in July 2003 by the Asia-Pacific Economic Cooperation (APEC) e-Security Task Group. By 2004 ASEAN will set up a framework to share information in order to respond to incidents like fast spreading viruses or other forms of "cyber crime". Each member country will set up a "Computer Emergency Response Team" (CERT) to coordinate the cooperation. through online exchange of information on cyber crime activities via the ASEAN Secretariat as well as the sharing and analysis of critical intelligence information. A related APEC initiative is the 'Cybersecurity tool kit' which is to be developed jointly with several business organisations including Microsoft. To date, few, if any, of these initiatives have born fruit, suggesting that it will bilateral modalities, rather than regional coordination, in the fight against criminal innovation.

The role of the US in the region should not be discounted. There are two reasons for

[170] Partial list of notable regional frameworks includes: 1) ASEAN Declaration on Transnational Crime 1997 2) ASEAN Ministerial Meeting on Transnational Crime (AMMTC) 3) ASEAN Chiefs of National Police ASEANAPOL) 4) Senior Officers Meeting on Transnational Crime (SOMTC) 5) ASEAN Plan of Action to Combat Transnational Crime 6) APEC Shanghai Summit 7) ASEAN Regional Forum statement on Cooperative and Counter-Terrorist Action on Border Security, June 2003 8) APEC forum meeting, Bangkok, 2003 agreement on measures for terrorism and transnational crime.

this. First, the US case is useful not necessarily as a benchmark of optimal adaptation but as a comparative tool using the 'biggest' case of cyber security responses. Second, the adaptive process in the East Asian cases does not take place in a vacuum. The US itself is engaged in its own unique coevolutionary process against criminal innovation using the cyber infrastructure. The extra regional influence on the strategies and tactics being adopted in many regional cases cannot be discounted. The US has exported much of its own security concerns to other states and along with it a set of norms as to the conduct of both law enforcement and intelligence toward the cyber infrastructure. One example was the early cooperation between the US Federal Bureau of Investigation (FBI) and the Indian Central Bureau of Investigation (CBI) in 2000 to fight cyber crime in India. After FBI experts trained Indian policeman to handle computer crimes, the Indian CBI then went on to set up its own Cyber crime unit. (BBC News, 2000b) In February 2004, the CBI announced that they will soon begin networking with nine other Asian countries through a 'Cyber Crime Technology Information Network System' (CTINS) which was initiated by the National Police Agency of Japan (newindpress.com, 2004).

The US has offered bilateral assistance arrangements to train law enforcement and policy makers in Philippines, for example, but most were seen as free trips to California and as such the Philippine government frequently uses such training programs offered by the US as a reward system – sidelining most of individuals working in line agencies (Confidential Interview, Manila 2003). Most of the externally funded strategies in the Philippines have failed primarily because of graft and mismanagement. This is troubling because the Philippines is the weak link East Asian cyber security. Here the role of low levels of state capacity become clear.

Most of the patterns of bi-lateral engagement by the US in East Asia on cyber

infrastructure security matters originate in the Clinton administration. The 1994 Communications Assistance for Law Enforcement Act (CALEA) which made mandatory the installation of remote access to digital switches so that cyber infrastructure traffic would be available for law enforcement. As opposed to the UK NHTCU which has a confidentiality charter, US opted for what is often perceived as heavy handed legislation.[171] The California Database Breach Notification Security Act or California Senate Bill 1386, which requires the organizations to notify California residents when they believe personal data has been compromised. These domestic policy initiatives were watched carefully by East Asian states as possible models for domestic control of their own cyber territories, but also because much of Asia's Internet traffic gets routed through the US, creating concerns about security.

East Asia in an international context

There are two approaches that emerged for international legal frameworks and cyber-crime. Pocar notes that:

> On the one hand, they provide for the duty of contracting states to implement internationally agreed norms within their own borders, with a view to bringing the legal system of contracting states closer both as to the substance and the practice of criminal law. On the other hand, these rules establish procedures for relevant international relations, aimed at providing such forms of cooperation between national judicial authorities as may interact with each other both swiftly and efficiently (Pocar, 2004: 31).

There are three central problems that states must overcome in order to halt the growth of the gap between TOC innovation and responses by law enforcement: 1) procedural challenges; 2) assimilating different jurisprudential systems; and 3) ensuring offenses in one country are actually offences in another. The central problem in East Asia that exasperates or diminishes national policies and strategies is the growing digital divide between states in the region. Digitally rich states with high institutional capacity are now

[171] Although it is important to point out that this currently a proposal in the UK to revive the idea of key escrow systems for encryption keys - an idea was roundly rejected in the US.

faced with low digital capacity neighbors. One successful international effort designed, in part, with this in mind is the Financial Action Task Force (FATF). The FATF is a good example of the state and legitimate non-state actors, for example, banks and other financial intuitions, marshaled together in a network to fight nimble money laundering networks that frequently use jurisdictional arbitrage as a cornerstone in both their tactics and strategies.

A critical component of the response to cyber threats must be the development of effective intelligence analysis by responding to what is different about intelligence gathering and analysis in cyber-space and what sets it apart from more traditional intelligence pursuits (Williams, Shimeall and Dunlevy, 2002). The mixing of both intelligence based and law enforcement based strategies comes with its own set of liberal democratic dilemmas. As one scholar noted "there exist examples in US history of a danger implicit in the pursuit of RMA-type information- and intelligence-gathering systems, namely the expansion of government power at the expense of civil liberties and libertarian values" (Morgan, 2003). As the nexus between high technology criminal innovators becomes more securitized these dilemmas will be more salient within national contexts.

Can the state in East Asia marshal its own networks of cooperation? Or will it rely on traditional state-based legal institutional frameworks to combat illicit networks?[172] East Asian governments have begun to report incidents and share information with other governments and are now part of international teams that are members of a global

[172] As mentioned above, the issue of money laundering, security, and the cyber infrastructure falls beyond the scope of this study. It is, however, a critical case in understanding the full extent of the nexus between TOC and cyber infrastructure based actors, and their impact on security. As for the potential for states to marshal networks to fight networks, the picture and potential is unclear. The strategy may make sense for certain problems but there are so few cases (of either success or failure) that a full assessment is not possible.

affiliation known as the Forum of Incident Response and Security Teams (FIRST). But other than Australia, Singapore, Hong Kong SAR and Japan, few states have managed to narrow the widening gap. Not surprisingly, East Asian states with pre-existing low levels of capacity are most susceptible to jurisdictional arbitrage and will likely remain compromised cyber spaces for the foreseeable future.

Uneven adaptation spaces

The coevolutionary gap between criminal innovators and state responses mechanisms in East Asia is profoundly uneven – in one dimension, the growth of the gap is nominal and in others, it is widening. Ultimately, the threat posed by these processes to security depends on how security is defined. At the individual level there is empirical evidence to suggest that the threat emanates from both criminal elements and the state itself. What is interesting is that there does not appear to be a threat to the cyber infrastructure itself. This is important because both TOC and NTOC groups require the infrastructure to thrive, as much as the state does.

Recall DK Matai's theory linking socio-political instabilities in the international system to cyber infrastructure incidents. Part One of this dissertation found that there is some evidence in support of a connection – especially the level of the rule of law in East Asia. The conclusions in Part Two regarding state capacity, the problem of jurisdictional arbitrage and the profoundly uneven adaptation space between criminal innovators and state responses bring the discussion full circle. The role of jurisdictional arbitrage and the idea of threats coming from 'inside' and 'outside' a state from both traditional and non-traditional organized criminal groups produces a paradox. That is, the act of closing the adaptive gap in one state pushes the problem to weaker states creating an increasing threat from 'outside' a state's cyber territory. It is unlikely that the gap between criminal

innovators and systems intruders in the region will fundamentally alter their capacity to threaten the security of states in the region in short run. However, the adaptive competitive process is strongly influenced and, in part, driven and constrained by existing security pressures, capacity, and unique security cultures.

Conclusion: Bowing to Quirinus

Introduction

The relationship between technology and power changes rapidly. In many ways the cyber infrastructure has ushered in an age of electronic uncertainty as states in East Asia navigate their way through multiple security modes and modalities. This is not without historical precedent. For example, during the late 1800s, in the post-Crimean War period, the British Navy, and indeed all navies, faced rapid technological change. Naval power leading up to this period had changed little - relying on wooden ships and cannon. The introduction of metal plating and steam power kicked off a coevolutionary competitive process between armor thickness and firepower between navies; a competitive process into which tactics and strategy were also drawn. Some states were able to initiate rapid adaptation processes, but this was a trajectory that left many naval powers with rag-tag collections of ships that reflected the fits and starts produced by the rapid change in technology. Like the major navies of the late 1800s, cyber warfare and infrastructure security is a patchwork of various tactics, strategies and technologies with seemingly little symmetry of purpose or trajectory. This age of uncertainty in the infrastructure has produced a patch-work collection of technical and cultural adaptations.

In light of results on cyber infrastructure security issues, it seems that the more complicated a perceived vulnerability or threat is the more likely that there will be disconnects in the securitization process. Gaps begin to grow between threat perception and reality. The Internet has gone through or is currently going through a unique period of securitization – in different ways in different societies – but the process remains incomplete, and in some cases it is desecuritizing. It is true that threats from the Internet

and to the Internet are no longer associated with the stateless geography of the "hacker" but from real, often geopolitical, geographies. The result is the territorialization of the Internet and how state actors understand it. To state this in more blunt terms: a new virtual realism is emerging. Yet, the linkages between the existential threats and the performative acts are becoming too difficult to understand and articulate outside of technically minded epistemic communities. How this links to the finding that institutional capacity is positively related to the state's capacity to fully protect the cyber infrastructure from a growing number of compromised nodes is unclear.

The Internet and its constituent components and applications have increased the importance of non-state actors in matters of national and international security. The assumption here is that these actors become both challengers and new providers of security, usually because they have adapted to the new network environment faster than state institutions and organizations. It is unclear, however, if scholars and observers of international politics are truly cognizant of the changes taking place. One of the first explicit treatments of the subject of information technologies and its impact on international politics observed that politics would pay little attention to IT unless it has the potential for weapons development or for "explicit means of extending one nation's power and influence over others" (Murphy 1986: ii). It is important to emphasize that the perspectives on the impact of the Internet and security since the early 1980s have not necessarily predicted the whittling away of state autonomy. But they do suggest that change brought about by technologies like the Internet require a re-thinking of the strict state-centric models of security.

Compromised Nodes, Stability and Security

The central question for part one of this study was: across an upper stratum of countries, what factors best explain the variation in compromise nodes? The 'foil' for Part One was DK Matai's theory that cyber infrastructure instabilities could be associated with geopolitical instabilities. Taking into account both the size of economy and the level of Internet technology diffusion only, the level of the rule of law mattered above and beyond the level of cyber infrastructure diffusion. In East Asia, the role of the rule of law had a greater impact on the number of compromised nodes. This goes a long way to explaining why countries in that region such as South Korea and Singapore which have similar levels of diffusion have such dissimilar numbers of compromised Internet devices. There is no evidence, however, of a difference between democracies and non-democracies and their ability to control the number of compromised nodes. Cross-nationally, the level of democracy did not appear to be a factor. Nor did this help explain inter-regional variation between East Asia and the rest of the world. A key implication of this result is that non-democratic regimes do not necessarily have an "authoritarian advantage" in controlling the number of compromised nodes or, inversely, are any more susceptible to instabilities in the cyber infrastructure. Regime type does not matter.

The role of political institutional factors in explaining country differences in regression slopes was of particular interest. At a fundamental level, states are responsible for creating and maintaining the laws, policies and practices toward the security and integrity of the Internet. Unlike the level of democracy, rule of law does appear to be linked to the dependent variable. The measure of the rule of law used in this study, from an institutional perspective, is broad. Future research should be done in order to explore what particular features of a states legal norms and traditions influence the integrity of the

Internet in national contexts. It appears, then, that DK Matai was half right. The rule of law, as a broad proxy measure for stability and institutional capacity can be linked to cyber infrastructure instabilities as measured by the number of compromised nodes – but only in East Asia. Ralf Bendrath's (2003) gap between cyber threat perception and reality is now a little narrower.

Conflating traditional and non-traditional concepts about what constitutes security in an era of rapid diffusion of information technologies is part of the appeal of a node based level of analysis. Whether the issue is cyber warfare between states, critical infrastructure protection or criminal innovation, at the root of each security dilemma that emerges from each dimension is the problem of the compromised node. Understanding this requires framing technologies such as the Internet not just as a mode of communications but also as an environment that provides the ability to act at a distance.

The use of a node based framework, as opposed to a network level of analysis, proved to be useful in one sense, but like frameworks based on the structural idea of networks, it has its limits. From a 'technical' point of view of cyber infrastructure security it is the compromised node that is one of the central problems in a digitizing world both in physical and theoretical terms. Other approaches used in International Relations to study security and the information revolution commonly employ more traditional frameworks built around the international system or the state and more recently the "network" level of analysis (Deibert 2002). Using a node-based level of analysis allows for a contribution to the 'broadening of security' project that has occupied much of the International Relations literature recently and at the same time grounds the research in the technical realities that are often overlooked or misunderstood. Deibert's (2002) idea of a network security

image also allows for this, as do his concept of "collective images" of cyber infrastructure security: state, national, private and network. The network image, as Deibert articulates it, is an intersubjective frame and is thus another referent open for empirical study (2002, 2003). Like the compromised node level, the network security image is not a theory, but a way of structuring empirical research using data derived from the infrastructure itself.[173]

This study's use of a large-N data set presents results that are suggestive but far from conclusive. The next step in the quantitative cross-national research is clear. The cross-sectional design used for this study is limited in its explanatory power. The use of longitudinal or time-series based statistical research would greatly increase the confidence of the results presented here. This next step in the research would see the DShield data for the period of 1999-2005 gathered and processed in order confirm the findings presented in Part One. A time-series design based on all data from 1999-2004 would increase both the validity and reliability of these findings and at the same time allow for more precision in the noise reduction techniques – especially the 'on-off' behavioral patterns found in both this study and the Yegneswaran *et al* research.[174]

The nexus and coevolutionary adaptation

The choice to focus on East Asia for this study was timely. The region provides a diversity of actors. There is no other region in the world where there are extremely deep Internet diffusion patterns and where there are both non-democratic and democratic

[173] There are few examples of this type of research design in International Relations and security studies. The OpenNet Initiative (http://opennet.net) is one of the exceptions.

[174] For more on noise reduction techniques in general and within the context of intrusion detection systems see Barford, Jha and Yegneswaran (2004). The reader should also be aware of Internet background radiation or cyber background noise. In Pang *et al.* (2004) researchers showed that monitoring any portion of the cyber infrastructure will reveal "incessant" activity. This background radiation is made up of "fundamentally nonproductive traffic, either malicious (flooding backscatter, scans for vulnerabilities, worms) or benign (misconfigurations)" (2004).

regimes. Indeed, East Asia has now surpassed other regions in use of technology. Along side state actors in the region, and often at odds with them, are a host of non-state actors that are taking advantage of rapid Internet diffusion. This relationship between the state and sophisticated organized crime gives the rest of the world a look into one possible future; a future where those that possess the technological upper hand, and are willing to use it, can circumvent state responses almost at will.

From Part Two of the dissertation, a number of conceptual conclusions can be drawn. First, the co-evolutionary competitive processes spurned on by traditional and non-traditional organized criminal innovation has produced an uneven adaptation space in East Asia. There are points where the gap is narrowing, points where the gap has seen very little change, and points where it is widening. The key driver of this uneven adaptation space is the problem of jurisdictional arbitrage. The key difference between TOC and NTOC groups is there ability or desire to use the cyber infrastructure to perform a jurisdictional "jump." TOC groups in East Asia that had some connection to systems intruders in the nexus are less likely to use the cyber infrastructure to escape unfavorable jurisdictions primarily because "cyberspace" does not fundamentally change the very 'local' environment in which they operate. While NTOC groups appear to make the most use of bot nets and the services that they provide to obscure possible communications eavesdropping by the state and so on.

This coevolutionary competitive process is made somewhat more complicated by state actors that behave as both 'competitors' against criminal innovation using the cyber infrastructure and as passive supporters of the intrinsic data mined by the growth of bot networks. The loss-of-control thesis presented earlier, which paints a rather stark picture

of the state as being driven by purely territorial control interests, is now not so clear or uniform across countries. In the East Asian context, it may be less about recovering some sense of a loss of autonomy in the cyber infrastructure and more about power gains and traditional notions of security. This result moves beyond Shields' (2005) analysis which situated the state as a bounded international actor reacting to a perceived loss of control.

Further complicating and frustrating state responses to the nexus between organized crime groups and network intruders is the emergence of relatively stable black markets for stolen data, especially in the cases presented here which are driven by the growth of bot nets.. The relationship between bot nets, black markets and both traditional and non-traditional organized crime is supported by an emerging pseudo cyber infrastructure that can provide an array of services and capabilities to various non-state actors. Again, the key to this alternate or pseudo infrastructure is jurisdictional arbitrage. Even though the regional diffusion of the cyber infrastructure has enabled regional states, it has also exposed them to a new array of threats. These threats are from within and across national boundaries making it difficult for governments to unilaterally securitize emergent threats from the cyber infrastructure. As a result, it is becoming increasingly necessary for East Asian governments to protect their interests by working together. To do so effectively will require the implementation of policies and processes used to encourage regional integration in other sectors of cooperation and transfer them into the realm of the cyber infrastructure.

From both Part One and Part Two, a number of substantive conclusions can be drawn. First, the nexus between network intruders and the two broad types of organized crime groups operating in the region does pose a threat to security in the short run. The long

run, however, is much more difficult to offer prognosis on. If the nexus between the two groups begins to spurn increasingly higher levels of sophistication in organized crime, then states in East Asia may find it difficult to coevolve the capacity to respond. This is of particular concern in countries like China. China is especially important and unique here, primarily because of the distinctiveness of its current economic and political development trajectory and that the countries plays host to a growing array of both traditional and non-traditional organized criminal groups. The nexus does not appear to constitute an immediate threat to state security in the short run; it does not change the fundament goals of TOC – financial gain, not power. What is different is the participation of state actors in both the bot net and illicit data market is troubling for a region already struggling with states that have low institutional capacity.

The nexus between TOC and NTOC does not alter previous studies on the relationship between these types of non-state actors and security. Recall the discussion and contrast between the way the Copenhagen School and the more "realistic" assessments of what makes a threat a threat in the region? Does a rapid coevolutionary process with an uneven adaptive gap change the original calculus of either the Copenhagen School or the "realistic" assessments of Castle (1997), Emmers (2003), or Dupont (2003)? On both counts, in the short term, the answer is no. Law enforcement response and adaptation has been robust – in some cases the gap has narrowed slightly. The adaptation space is widening primarily because of digital divides between countries response capacities in the region. The result is a kind of 'net loss' or overall widening. This is driven, of course, because of the transnational nature of the infrastructure. There is nascent international cooperation in the region, but it is strong only on a sub-regional basis often

involving bilateral modes of cooperation. In more theoretical terms, however, analyses of organized crime as a threat to security in the region that are based upon more constructivist perspectives have an edge in their prescriptions: the criminalization rather than securitization of this perceived security threat may help to narrow the gaps.

Conclusion

There are additional substantive issues that revolve around the East Asia factor in a more "systemic context." Differing state responses to cyber security issues in the region are rooted in institutional capacity and in individual state strategic culture and history. But the regional context here is also important. It is likely that the critical tension between the processes of internationalization and globalization are intimately reflected into the cyber infrastructure. This study has shown that while the state is still the only actor with the resources, authority and legitimacy to provide security, the Internet will continue to evolve and thus still has the potential to produce a relative reduction in state autonomy. At this point, the Herrera's (2002) notion of indeterminancy in, and of, the infrastructure is more clear. The current coevolutionary adaptive trend between non-traditional security threat in cyber space, while uneven and often producing paradoxical security outcomes, signals the return of state sovereignty in the cyber infrastructure. This is in part due to a new virtual realism that is emerging as a dominant framework for state policies toward the infrastructure in East Asia.

References

Abad, Christopher. (2005) The economy of phishing: A survey of the operations of a phishing market. *First Monday* 10. <http://firstmonday.org/issues/issue10_9/abad/#a3>

Ahn, Daniel. (2004) Profiling Culture: An Examination of Korean American Gangbangers in Southern California. *Asian Law Journal* 1: 57-98.

Albert, Réka and Barabasi, Albert-László. (2001) Statistical Mechanics of Complex Networks. *Review of Modern Physics* 74: 432-455.

Anderson, Carl (2004) Linking Micro- to Macro-level Behavior in the Aggressor–Defender–Stalker Game. *Adaptive Behavior* 12: 175-185.

Anonymous. (2005) Organized Crime Gangs in Taiwan. *Trends in Organized Crime* 8: 13-23.

APEC-TEL (2002) *Recommendation by the APEC Telecommunications and Information Working Group [TEL] to APEC Senior Officials [SOM] for An Cyber Security Strategy.* Singapore: Asia Pacific Economic Cooperation

Aronson, Jonathan. (2002) "Global Networks and Their Impact." In *Information Technologies and Global Politics*, edited by J. N. Rosenau and J.P. Singh, pp. 39-64. Albany, NY: State University of New York Press.

Arquilla, John. (2003) Thinking about new security paradigms. *Contemporary Security Policy* 24: 209-225.

Arquilla, John and David Ronfeldt (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy.* San Francisco, CA: RAND.

Arthur, Charles. July 31, 2004. Hackers will settle your scores online (prices start at £50). The Independent.

Australasian Centre for Policing Research (2000) *The Virtual Horizon: Meeting the Law Enforcement Challenges*. Scoping Paper. Adelaide: Australasian Centre for Policing Research.

Baer, Walter. S. (2003) Rewarding IT security in the marketplace. *Contemporary Security Policy* 24: 190-208.

Bajwa, Deepinder S., Lewis, L. Floyd, Pervan, Graham and Lai, Vincent. S. (2005) The adoption and use of collaboration information technologies: international comparisons. *Journal of Information Technology* 20:130-140.

Bakos, George. 2002. *SQLsnake code analysis.*

<http://www.incidents.org/diary/diary.php?_id/157>

Ballard, James David, Hornik, Joseph G. and Douglas McKenzie. (2002) Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues. *American Behavioral Scientist* 45:989-1016.

Barford, Paul; Jha, Somesh; Yegneswaran, Vinod (2004) *Fusion and Filtering in Distributed Intrusion Detection Systems*. Proceedings of the 42nd Annual Allerton Conference on Communication, Control and Computing. <http://www.cs.wisc.edu/~pb/fnf_final.pdf>

Bauer, John. May 20, 1998. Testimony to the Subcommittee on Technology, Terrorism and Government Information. Committee on the Judiciary, United States Senate. Washington. <http://www.securitymanagement.com/library/bauer.html>

BBC. July 22, 2005a. Google site 'used by drug gang'. BBC News. <http://news.bbc.co.uk/2/hi/technology/4706489.stm>

BBC. March 17, 2005b. Have hackers recruited your PC? BBC News. <http://news.bbc.co.uk/2/hi/technology/4354109.stm>

Beare, Margaret. E. (2000) *Structures, Strategies, and Tactics of Transnational Criminal Organizations: Critical Issues for Enforcement*. A paper presented at the Australian Institute of Criminology, Australian Customs Service, and Australian Federal Police Transnational Organized Crime Conference. Canberra, March 9-10.

Becker, Ted. and Slaton, Christa. D. (2000) *The Future of Teledemocracy*. New York, NY: Praeger Publishers.

Belcher, Tom, Yoran, Ramesh, Higgins, Mark., Dunphy, Brian, and Odom, Jeff. (2002) *Riptech Internet Security Threat Report: Attack Trends for Q3 and Q4 2001*. Alexandria, VA: Riptech Inc.

Bell, Daniel. (1973) *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York, NY: Basic Books.

Bellamy, Christine, and Taylor, John. A. (1998) *Governing in the Information Age*. Buckingham: Open University Press.

Bendrath, Ralf. (2003) "Cyber-Angst and the Real World – Any Link?" In *Bombs and bandwidth: the emerging relationship between technology and security*, edited by R. Latham, pp. 49-73. New York, NY: The New Press.

Beniger, James. (1989) "The Evolution of Control." In *Computers in the Human Context*, edited by T. Forester, pp. 316-334. Cambridge, MA: MIT Press.

Berkowitz, Bruce, and Hahn, Robert. W. (2003) Cybersecurity: Who's Watching the Store? *Issues in Science & Technology* 19: 55-64.

Bethencourt, John, Franklin, Jason and Mary Vernon (2005) *Mapping Internet Sensors With Probe Response Attacks*. USENIX Security '05. <http://www.usenix.org/events/sec05/tech/bethencourt/bethencourt_html/index.html>

Bertsekas, Dimitri and Robert Gallager (1991) *Data Networks*, 2nd Edition. Prentice Hall: New York, NY.

Biever, Celeste. December 17, 2005. Busted! The gold standard in digital security lies in tatters. New Scientist, 44-45.

Borland, John. November 19, 2003. Spyware steps out of the shadows. CNET.

Branigan, Steven (2004) *High-Tech Crimes Revealed: Cyberwar Stories from the Digital Front*. New York: Addison-Wesley.

Braumoeller, Bear. F. (2004) Hypothesis Testing and Multiplicative Interaction Terms. *International Organization* 58: 807-820.

Brenner, Bill. August 31, 2005. Myfip's Titan Rain connection. SearchSecurity.com.

Brey, Marianne. March 20, 2002. Fraud hits one in ten Internet deals. CNN.

Brown, Graham. (2006) The Perils of Terrorism: Chinese Whispers, Kevin Bacon and Al Qaeda in Southeast Asia – A Review Essay. *Intelligence and National Security* 21: 150–162.

Bryen, Stephen (2002) *A collective security approach to protecting the critical network infrastructure*. ITU new initiatives workshop: creating trust in critical network infrastructures. Republic of Korea, May 20 to 22.

Burroughs, Daniel J., Wilson, Linda F., and Cubenko, George. V. (2002) *Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods*. Dartmouth College: Institute of Security and Technology Studies. <http://www.ists.dartmouth.edu/IRIA/projects/ipccc.final.pdf>

Business Software Alliance (2003) *The Eight Annual BSA Global Software Piracy Study: Trends in Software Piracy 1994-2002*. Washington, DC: BSA. <http://www.caast.org/resources/2003_global_study.pdf >

Buzan, Barry (1998) *Security: A New Framework for Analysis*. London: Lynne Rienner.

Caelli, Francesco and Coleman, Wilbur. J. (2001) *Cross-country Technology Diffusion: The Case of Computers*. NBER Working Paper No. 8130. Cambridge, MA: NBER.

Calvani, Sandro (2002) Drug criminals are using high tech as a new weapon. A speech given at the launch of the INCB Annual Report, United Nations Drug Control Programme, February 26. Manila: Philippines.

Canadian Scandal Made in Hong Kong. October 2, 2003. The Asian Pacific Post.

Casman, Elizabeth, and Cooper, Duncan. June 22, 2005. Syndromic surveillance. Issues in Science and Technology. <http://www.keepmedia.com/pubs/IssuesinScienceandTechnology/2005/06/22/>

Castells, Manuel (2001) *The Internet Galaxy*. Oxford: Oxford University Press.

--------. (1998) *The Information Age: Economy, Society and Culture. Volume III. End of Millenium*. Oxford: Blackwell Press.

Castle, Allan (1997) *Transnational Organized Crime and International Security*. Working Paper No. 19. Vancouver, BC: Centre of International Relations, University of British Columbia.

Cavazos, Edward and Gavino Morin (2005) *Cyberspace and the Law: Your Rights and Duties in the On-Line World*. MIT Press: Boston, MA.

Cavusoglu, Huseyin, Birendra Mishra and Srinivasan Raghunathan (2002) *The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers*. Unpublished paper. <http://www.utdallas.edu/~huseyin/breach.pdf>

Cederman, Lars-Erik (1997) *Emergent Actors in World Politics: How States and Nations Develop and Dissolve*. Princeton, NJ: Princeton University Press.

Cerf, Vinton and Kahn, Robert (1974) A Protocol for Packet Network Interconnection. *IEEE Transactions on Communications* 22: 637-648.

Chan, Anita (2003) Coding Free Software, Coding Free States: Free Software Legislation and the Politics of Code in Peru. *Anthropological Quarterly* 77: 531-545.

Cheung, Anthony B. L. (2000) Globalization Versus Asian Values: Alternative Paradigms in Understanding Governance and Administration. *Asian Journal of Political Science* 8: 1-15.

Chin, Ko-lin, Sheldon Zhang, and Kelly, Robert (1998) Transnational Chinese Organized Crime Activities. *Transnational Organized Crime* 4: 127-154.

Chin, Ko-lin (1996) *Chinatown Gangs*. Oxford: Oxford University Press.

Choudhury, Amit Roy. February 17, 2005. $38m infocomm security masterplan unveiled. Business Times. <http://it.asia1.com.sg/newsdaily/news001_20050224.html>

Chu, Yiu Kong (2005) Hong Kong Triads After 1997. *Trends in Organized Crime* 8: 5-12.

CISC (2005) *The 2005 Annual Report on Organized Crime in Canada.* Ottawa, ON: Criminal Intelligence Service Canada. <http://www.cisc.gc.ca/webpage/index_b_e.htm>

Clark, David (1988) Design Philosophy of the DARPA Internet Protocol. *Proceedings of ACM SIGCOMM* August:106-114.

Clarke, Richard (2004) Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research* 10: 55-63.

Cohen, Saul. B. (1973) Geography *and Politics in a Divided World*, 2nd ed. New York, NY: Oxford University Press.

Conway, Maura (2002) Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. *First Monday* 7. <http://www.firstmonday.org>

Cook Arthur B. (1904) The European Sky-God. *Folklore* 15: 264-315

Cook, Karen, Toshio Yamagishi, Coye Cheshire, Robin Cooper, Masafumi Matsuda, and Rie Mashima (2005) Trust Building via Risk Taking: A Cross-Societal Experiment. *Social Psychology Quarterly* 68: 121-142.

Council of Europe Octopus Programme (2005) Summary of the Organized Crime Situation report 2004: Focus on the Threat of Cybercrime. *Trends in Organized Crime* 8: 41-50.

Council of Europe (2001) Convention on Cybercrime. European Treaty Series No 185, Strasbourg: Council of Europe. <http://conventions.coe.int/treaty/EN/projets/projets.htm>
Cole, Eric and Ring, Sandra (2005) *Insider Threat.* New York, NY: Syngress.

Cowie, James, Ogielski, Andy T., Premore, Brian J., and Yuan, Yougu (2002). *Global Routing Instabilities Triggered by CodeRed II and Nimda Worm Attacks.* <http://www.renesys.com/projects/bgpinstability>

David, Paul and Julie Ann Bunn (1988) The Economics of Gateway Technologies and Network Evolution. *Information Economics* 3: 165-202.

Dawkins, Richard and Krebs, John R. (1979) Arms Races Within and Between Species. *Proceedings of the Royal Society of London* B 205: 489-511.

de Sola, Ithiel (1977) *The Social Impact of the Telephone.* Cambridge, MA: MIT Press.

Deibert, Ronald J., and Stein, Janice G. (2003) "Social and Electronic Networks in the War on Terror." In *Bombs and Bandwidth: the emerging relationship between technology and security*, edited by R. Latham, pp. 157-174. New York, NY: The New Press.

Deibert, Ronald J. (2002) "Circuits of Power: Security in the Internet Environment." In *Information Technologies and Global Politics*, edited by J. N. Rosenau and J.P. Singh, pp. 115-142. Albany, NY: State University of New York Press.

--------. (2003) Black Code: Censorship, Surveillance, and Militarization of Cyberspace. *Millennium: Journal of International Studies* 32:501-530.

Deloitte Touche Tohmatsu (2004) *2004 Global Security Survey*. New York, NY: Deloitte Touche Tohmatsu.

Denning, Dorothy (2003) "Cyber-security as an Emergent Infrastructure." In *Bombs and Bandwidth: the emerging relationship between technology and security*, edited by R. Latham, pp. 25-48. New York, NY: The New Press.

--------. (2001) *Is Cyber Terror Next?* New York: U.S. Social Science Research Council. <http://www.ssrc.org/sept11/essays/denning.htm>

--------. May 23, 2000a Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism. U.S. House of Representatives, Committee on Armed Services. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>

--------. (2000b) "Cyberterrorism," Global Dialogue. Autumn. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc>

--------. (1999) *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Washington DC: Nautilus Institute. <http://www.nautilus.org/infopolicy/workshop/papers/denning.html>

Der Derian, James (2000) Virtuous War / virtual theory. *International Affairs* 76: 771-788.

Deutsch, Karl W. (1966) *Nationalism and Social Communication: An Inquiry into the Foundations of Nationality*. New York: Wiley.

--------. (1963) *The Nerves of Government: Models of Political Control and Communication*. New York, NY: The Free Press.

--------. (1959) The Impact of Science and Technology on International Politics. *Daedalus* 88: 669-685.

--------. (1957) Mass Communications and the Loss of Freedom in National Decision-

Making: A Possible Research Approach to Interstate Conflicts. *Journal of Conflict Resolution* 1: 200-211.

Desouza, Kevin C. and Hensberg, Tobin (2003) Semiotic emergent framework to address the reality of cyberterrorism. *Technological Forecasting & Social Change* 70: 385-396.

Dodd, Annabel, *The Essential Guide to Telecommunications*, 3rd ed.

Dulchinos, Donald P. (2005) *Neurosphere: The Convergence of Evolution, Group Mind, and the Internet.* York Beach, ME: Weiser Books.

Dutton, William. H. (1999) *Society on the Line: Information Politics in the Digital Age.* Oxford: Oxford University Press.

Duk-kun, Byun. November 19, 2003. Largest Internet hacking ring uncovered in Korea. Sydney Morning Herald.

Dunn, M. (2002) *Information Age Conflicts.* Zurich: Swiss Federal Institute of Technology.

Edwards, Paul N. (1994) "From 'Impact' to Social Process: Computers in Society and Culture" In *Handbook of Science and Technology Studies*, edited by S. Jasanoff, pp. 23-41. Beverly Hills, CA: Sage Publications.

Embar-Seddon, Ayn (2002) Cyberterrorism: Are we Under Siege? *American Behavioral Scientist* 45: 1033-1043.

Emmers, Ralph (2003) ASEAN and the Securitization of Transnational Crime in Southeast Asia. *The Pacific Review* 16: 421-440.

Erickson, Jon (2003) *Hacking: The Art of Exploitation.* No Starch Press: New York. NY.

--------. (2001a) "Securitizing IT." In *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, edited by J. Eriksson, pp. 1-16. Aldershot: Ashgate Publishing.

--------. (2001b) Cyberplagues, IT and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management* 9: 211-22.

Evans, Paul and Wurster, Timothy S. (2000) *Blown to Bits: How the New Economics of Information Transforms Strategy.* Cambridge: Harvard Business School Press.

Ferguson, Niels and Schneier, Bruce (2003) *Practical Cryptography.* New York, NY: John Wiley & Sons.

Ficici, Sevan G., and Pollack, Jordan B. (1998) "Challenges in Coevolutionary Learning: Arms-Race Dynamics, Open-Endedness, and Mediocre Stable States." In *Proceedings of*

the Sixth International Conference on Artificial Life, edited by A. Belew and K. Talor. Cambridge, MA: MIT Press. <http://www.demo.cs.brandeis.edu/papers/Challenges.pdf>

Fidler, Daniel. P. (1998) The Internet and the Sovereign State: The Role and Impact of Cyberspace on National and Global Governance. *Indiana Journal of Global Legal Studies*. 5: <http://ijgls.indiana.edu/archive/05/02/fidler2.shtml>

Fighting growing onslaught of spam. April 6, 2005. China Daily. <http://english.people.com.cn/200504/06/eng20050406_179661.html>

Finckenauer, James O. (2005) Problems of Definition: What is Organized Crime? *Trends in Organized Crime* 8: 63-83.

--------. (2002) "Chinese Transnational Organized Crime: The Fuk Ching," *Participating in the U.N.'s crime prevention program*. New York, NY: National Institute of Justice International. <http://www.ojp.usdoj.gov/nij/international/chinese.html>

Flachaire, Emmanuel (2005) More Efficient Tests Robust to Heteroskedasticity of Unknown Form. *Econometric Reviews* 24: 219-241.

Fountain, Jane. E. (2001) *Building the Virtual State: Information Technology and Institutional Change*. Washington, DC: Brookings Institution.

Fox, John (2003). Effect Displays in R for Generalised Linear Models. *Journal of Statistical Software* 8: 1-18.

--------. (2002) *An R and S-Plus Companion to Applied Regression*. London: Sage Publications.

Frederick, Howard. H. (1993) *Global Communication & International Relations*. Belmont, CA: Wadsworth Publishing Company.

Freeman, Chritopher (1996) "The Two-Edged Nature of Technical Change," in Dutton (1996): 19-36.

Freeman, Edward H. (2006) Disclosure of Information Theft: The ChoicePoint Security Breach. *Information Systems Security* 14: 11-15

Friedman, Thomas L. (2000) *The Lexus and the Olive Tree: Understanding Globalization*. New York, NY: Anchor Books.

Fukuyama, Francis. (1999) "Information and Biological Revolutions: Global Governance Challenges." In *Summary of a Study Group*, edited by C. S. Wagner. MR-1139-DARPA. RAND.

Funes, Pablo, Sklar, Elizabeth, Juillé, Hugues and Pollack, Jordan (1997) *The Internet*

as a Virtual Ecology: Coevolutionary Arms Races Between Human and Artificial Populations. Brandeis University Computer Science Technical Report CS-97-197. <http://demo.cs.brandeis.edu/papers/cs-97-197.pdf>

Galloway, Collin. December 14, 2004. Spammers hide behind the Great Wall. Asia Times.

Gerring, John (2004) What is a Case Study and What Is It Good for?" *American Political Science Review* 98: 341-354.

Ghosh, Pallab. February 13, 2004. Net system monitors plane health. *BBC News*. <http://news.bbc.co.uk/go/pr/fr/-/2/hi/science/nature/3484619.stm>

Ghosh, Ajoy, Phillip Hourigan, Rowan Price, Stephen Ford, and Gary Gaskell (2003) *The 2003 Australian Computer Crime and Security Survey*. AusCERT, Australia.

Giacomelloa, Giampiero and Lucio Picci (2003) My scale or your meter? Evaluating methods of measuring the Internet. *Information Economics and Policy* 15: 363–383.

Giddens, Anthony (2000) *Runaway World: How Globalization is Reshaping our Lives*. London: Routledge.

Gilpin, Robert. (1981) *War & Change in World Politics*. Cambridge: Cambridge University Press.

Godson, Robert and Phil Williams (1998) Strengthening cooperation against transnational crime. *Survival* 40: 66-88.

Goldstone, Jack A., Robert H. Bates, Ted Robert Gurr, Michael Lustik, Monty G. Marshall, Jay Ulfelder, and Mark Woodward (2005) *A Global Forecasting Model of Political Instability*. Paper prepared for the annual meeting of the American Political Science Association, Washington, D.C.

Goodman, S., P. Hassebroek, D. King, A. Ozment (2003) International Coordination to Increase the Security of Critical Network Infrastructures. *Journal of Information Warfare* 2: 72-87.

Gordon, Robert M. (2000) Criminal business organizations, street gangs and 'wanna-be' groups: A Vancouver perspective. *Canadian Journal of Criminology* January: 39-60.

Gorman, Sean P. (2002) *The Network Advantage of Regions: The Case of the USA, Europe, and China*. Unpublished paper.

Grabosky, Peter (2004) The Global Dimension of Cybercrime. *Global Crime* 6: 145-157.

--------. (2000) *Cybercrime and Information Warfare*, Paper presented at the Transnational Crime Conference convened by the Australian Institute of Criminology, Canberra, Australia. March 9-10.

Graham, S. (2002) "Communications Grids: Cities and Infrastructure." In *Global Networks: Linked Cities*, edited by S. Sassen, pp. 71-92. New York, NY: Cambridge Press.

Graham-Rowe, Duncan. July 12, 2001. Chameleon code gives hackers advantage. New Scientist.

Gray, Chris Hables. (2003) "Perpetual Revolution in Military Affairs, International Security, and Information." In *Bombs and Bandwidth: the emerging relationship between technology and security*, edited by R. Latham, pp. 199-214. New York, NY: The New Press.

Gray, Colin S. (1996a) The Continued Primacy of Geography. *Orbis* Spring: 247-259.

--------. (1996b) A Rejoinder. *Orbis*. Spring: 274-276.

Grove, G., Goodman, S. and S. Lukasik (2000) Cyber-attacks and international law. *Survival* 42: 89-104.

Gurr, Ted R., Woodward, Mark and Marshall, Monty G. (2005) *Forecasting Instability: Are Ethnic Wars and Muslim Countries Different?* Paper present for the annual meeting of the American Political Science Association, Washington, D.C., September 1-4. <http://globalpolicy.gmu.edu/pitf/PITFethnicmuslim.pdf>

Hafner, Katie and Markoff, John (1991) *Cyberpunk: Outlaws and hackers on the computer frontier*. New York, NY: Simon and Schuster

Haggerty, Kevin D. (2004) Technology and crime policy. *Theoretical Criminology* 8: 491-497.

Hall, Eldon C. (2000) From the Farm to Pioneering with Digital Control Computers: An Autobiography. *IEEE Annals of the History of Computing* 22: 22-31.

Hansen, Mark, Stuart Madnick, and Michael Siegel (2002) *Process Aggregation Using Web Services*. MIT Sloan School of Management Working Paper. February 28: 1-15.

Hargittai, Eszter (1999) Weaving the Western Web: Explaining Differences in Internet Connectivity Among OECD Countries. *Telecommunications Policy* 23:701-718

Hart, Cordell M. (1999) *Money and 'Guanxi': Keys to Understanding Crime By Asians*. International Information Programs. Washington, D.C.: U.S. Department of State. <http://usinfo.state.gov/regional/ea/chinaaliens/guanxi.htm>

Heim, Michael (1998) *Virtual Realism*. London: Oxford University Press

Herrera, Geoffrey L. (2006) *Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space*. A paper prepared for the 47th Annual International Studies Association Convention. March 22-25, San Diego, CA

--------. (2004) *New Media for a New World? Information Technology and Threats to national Security*. A paper prepared for the 2004 meeting of the International Studies Association. March 17-21, Montreal, Quebec

--------. (2002) The Politics of Bandwidth: International Political Implications of a Global Digital Information Network. *Review of International Studies* 28: 93-122.

Hinde, Stephen (2004) Hacking gains momentum. *Computer Fraud & Security* 11: 13-15.

Holloway, Darren (2005) The digital divide in Sydney. *Information, Communication & Society* 8:168-193.

Holtz, Thorsten (2005) A short visit to the bot zoo. *IEEE Security & Privacy* 3: 76-79.

HoneyNet Project (2002) *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community*. Boston, MA: Addison Wesley.

Hughes, Christopher R. (2003) "Fghting the smokeless war: ICTs and international security." In *China and the Internet: The Politics of the Digital Leap Forward*, edited by C. R. Hughes and G. Wacker, pp. 139-161. New York: RoutledgeCurzon.

Huey, Laura and Rosenberg, Richard S. (2004) Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention. *Canadian Journal of Criminology and Criminal Justice*. October: 597-606.

Huey, Laura J. (2002) Policing the abstract: Some observations on policing cyberspace. *Canadian Journal of Criminology*. July: 243-254.

Hughes, Thomas (1983) *Networks of Power: Electrification in Western Society, 1880-1930*. Baltimore, MY: Johns Hopkins University Press.

Hutchinson, William and Matt Warren (2001) Principles of Information Warfare. *Journal of Information Warfare* 1: 7-15.

Ianelli, Nicholas and Aaron Hackworth (2005) *Botnets as a Vehicle for Online Crime*. Pittsburgh, PA: CERT Coordination Center and Carnegie Mellon University. <http://www.cert.org/archive/pdf/Botnets.pdf>

Isenberg, David. (2000) "An Electronic Pearl Harbor? Not Likely." In *The Information Revolution and National Security*, edited by T. Copeland, pp. 92-102. Carlisle Barracks: US Army War College, Strategic Studies Institute.

Ishikawa, Katsumi (2001) The Japanese intelligence culture. *Competitive Intelligence Review* 12: 51-56.

International Telecommunications Union (2005) *ITU Internet Reports 2005: The Internet of Things*. New York, NY: International Telecommunications Union.

--------. (2004). *The Digital Access Index*. New York, NY: ITU. <http://www.itu.int/ITU-D/ict/dai/index.html>

Japan arrests 2 more people over data leak at Softbank's Yahoo affiliate. May 31, 2004. The Canadian Press.

Jervis, Robert (1997) *System Effects: Complexity in Political and Social Life*. Princeton, NJ: Princeton University Press.

Jin, Dal (2005) Socioeconomic implications of broadband services. *Information, Communication & Society* 8: 503-523.

Joint Communique of the Third ASEAN Ministerial Meeting on Transnational Crime (AMMTC). October 11, 2001. Singapore: ASEAN.

Joint Communique of the Fourth ASEAN Ministerial Meeting on Transnational Crime (AMMTC). January 8, 2004. Bangkok: ASEAN.

Joint Communique of the First ASEAN Plus Three Ministerial Meeting on Transnational Crime (AMMTC+3). January 10, 2004. Bangkok: ASEAN.

Joint Declaration of ASEAN and China on Cooperation in the Field of Non-Traditional Security Issues 6th ASEAN-China Summit. November 4, 2002. Phnom Penh: ASEAN.

Jones, Andy (2005) Information Warfare – what has been happening? *Computer Fraud & Security* 11: 4-7.

Jones, David S. (1999) Changes in Surveillance of Regulatory Enforcement Programmes in Singapore. *Asian Journal of Political Science* 7: 105-125.

Kalathil, Shanthi. and Boas, Taylor (2003) *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Regimes*. Washington, DC: Carnegie Endowment for International Peace.

Karam, Souhail. November 28, 2005. Cybercrime yields more cash than drugs: expert. Yahoo News (Reuters).

<http://labs.news.yahoo.com/s/nm/20051128/wr_nm/cybercrime_dc>

Katzenstein, Peter J. (2005) *A World of Regions: Asia and Europe in the American Imperium*. Ithaca, NY: Cornell University Press.

Keizer, Gregg. October 27, 2005. Microsoft Hunts For Zombie Spammers. Information Week.
<http://www.informationweek.com/story/showArticle.jhtml;jsessionid=0HJBRZJ2FG3A0QSNDBECKHSCJUMEKJVN?articleID=172901083&pgno=1>

Kenny, Michael C. (2003) Intelligence Games: Comparing the Intelligence Capabilities of Law Enforcement Agencies and Drug Trafficking Enterprises. *International Journal of Intelligence and CounterIntelligence* 16: 212-243.

Keohane, Robert O., and Nye, Joseph. S. (1998) Power and Interdependence in the Information Age. *Foreign Affairs* 77: 1-10.

Kiiski, Sandra and Pohjola, Matti. (2001) *Cross Country Diffusion of the Internet*. World Institute for Development Economics Research, discussion paper 2001/11: United Nations University.

King, Gary (1988) Statistical Models for Political Science Event Counts: Bias in Conventional Procedures and Evidence for the Exponential Poisson Regression Model. *American Journal of Political Science* 32: 838-863.

Kling, Rob (1994) Reading 'All About' Computerization: How Genre Conventions Shape Non-Fiction Social Analysis. *The Information Society* 10: 147-172.

Kluver, Randolph and Indrajit Banerjee (2005) The Internet in nine Asian nations. *Information, Communication & Society* 8: 30-46.

Korzyk, Alexander D., and J.G. VanDyke (1998) *A Forecasting Model for Internet Security Attacks*. Working paper.
<http://csrc.nist.gov/nissc/1998/proceedings/paperD5.pdf>

Kovacich, Gerald L., and Jones, Andy (2002) What Infosec Professionals Should Know About Information Warfare Tactics by Terrorists. *Computers and Security* 21: 113-119.

Kramer, Hilary. August 14, 2004. Cyber fears on fed's web plan. New York Post: Online Edition. <http://www.nypost.com/business/18671.htm>

Kraemer, Kenneth L., and Dedrick, Jason (1996) National Information Infrastructure: A Cross-Country Comparison. *Information Infrastructure & Policy* 5: 81-94.

Krahmann, Elke (2005) American Hegemony or Global Governance? Competing Visions of International Security. *International Studies Review* 7: 531-545.

Krebs, Brian. January 11, 2006. A Time to Patch. Washington Post. <http://blogs.washingtonpost.com/securityfix/2006/01/a_timeline_of_m.html>

Krim, Jonathan. April 12, 2004. A need for greater cybersecurity. Washington Post,

Krutskikh, Andrei (1999) Information Challenges to Security. *International Affairs* 45: 29-37.

Lai, Alan (2000) A Quiet Revolution: The Hong Kong Experience. *Trends in Organized Crime* 5: 79-87.

Langlois, Jean-Pierre P., and Langlois, Catherine C. (2005) Fully Informed and on the Road to Ruin: The Perfect Failure of Asymmetric Deterrence. *International Studies Quarterly* 49: 502-527.

Latham, Robert (2005) "Networks, Information, and the Rise of the Global Internet." In *Digital Formations: IT and New Architectures in the Global Realm*, edited by R. Latham and S. Sassen, pp. 146-177. Princeton, NJ: Princeton University Press.

--------. (2003) Information technology and Social Transformation. *International Studies Review* 4: 101-115.

Laudon, Ken. C. (1977) *Communications Technology and Democratic Participation.* NewYork, NY: Praeger.

LeBeuf, Marcel-Eugène (2001) *Organized Crime and Cybercrime Criminal Investigations and Intelligence on the Cutting Edge.* Technical Report – Information Technology Series. Ottawa, ON: Canadian Police College.

Lee, Terence (2005) Internet Control and Auto-regulation in Singapore. *Surveillance & Society* 3: 74-95.

Lee, Zedn. June 24, 2004. Chnese hackers behind cyber attacks in Taiwan? CNETAsia.

Lemos, Robert. March 11, 2005. Suspected bot master busted. SecurityFocus.

Leiffer, Michael (2000) *Singapore's Foreign Policy: Coping with Vulnerability.* London, UK: Routledge.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff (2003) *A Brief History of the Internet.* Reston, VA: Internet Society. <http://www.isoc.org/internet/history/brief.shtml>

Lemos, Robert. October 12, 2005a. Arrests unlikely to impact bot net threat, say experts.

Security Focus. <*http*://www.securityfocus.com/news/11344>

--------. December, 29 2005b. Data security moves front and center in 2005. Security Focus. <http://www.securityfocus.com>

Levine, Joel H. (2004) *The p-Normal Distribution: On the Prediction and Destruction of Networks*. Working paper, NAACSOS. Dartmouth College.

Lewis, James A. (2002) *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington, DC: Center for Strategic and International Studies.

Leyden, John. June 3, 2005. Hackers plot to create massive botnet. The Register Online. <http://www.theregister.co.uk/2005/06/03/malware_blitz/>

Libicki, Michael (1995) *What Is Information Warfare*? ACIS Paper #3. Washington, DC: National Defense University.

Lichtblau, Eric and Risen, James. December 24, 2005. Spy Agency Mined Vast Data Trove, Officials Report. New York Times. <http://www.nytimes.com/2005/12/24/politics/24spy.html?hp&ex=1135486800&en=7e76956223502390&ei=5094&partner=homepage>

Lilley, Peter (2003) *Dirty Dealing: The Untold Truth about Global Money Laundering, International Crime, and Terrorism*. New York: Kogan Page.

Lintner, Bertil (2004) Chinese Organized Crime. *Global Crime* 6: 84-96.

Lippmann, Richard David J. Fried, Isaac Graf, Joshua W. Haines, Kristopher R. Kendall, David McClung, Dan Weber, Seth E. Webster, Dan Wyschogrod, Robert K. Cunningham, and Marc A. Zissman (1998) Evaluating Intrusion Detection systems: 1998 DARPA Off-line Intrusion Detection Evaluation. *Proceedings of IEEE Security Symposium*.

Loree, Don (2002) Organized Crime: Changing Concepts and Realities for Police. *Trends in Organized Crime* 7: 73-78.

Lo, Shui Hing (2005) Casino Politics, Organized Crime and the Post-Colonial State in Macau. *Journal of Contemporary China* 14: 207-224.

--------. (1999) Cross-Border Organized Crime in Greater South China. *Transnational Organized Crime* 5: 176-194.

Lowman, John and Palys, Ted (2001a) Limited Confidentiality, academic freedom, and matters of conscience: Where does the CPA stand? *Canadian Journal of Criminology* October: 497-508.

--------. (2001b) Social research with eyes wide shut: The limited confidentiality dilemma. *Canadian Journal of Criminology* April: 255-267.

Luft, Gal and Korin, Anne (2004) Terrorism Goes to Sea. *Foreign Affairs*. November/December.

Mahoney, Michael S. (1988) The History of Computing in the History of Technology. *IEEE Annals of the History of Computing* 10: 113-125.

Mann, Charles C. January, 2006. How Click Fraud Could Swallow the Internet. Wired Magazine. <http://www.wired.com/wired/archive/14.01/fraud.html>

Marsden, Peter V. (2003) Interviewer effects in measuring network size using a single name generator. *Social Networks* 25: 1-16.

Marshall, Monty G., and Gurr, Ted R. (2005) *Peace and Conflict 2005: A Global Survey of Armed Conflicts, Self-Determination Movements, and Democracy*. College Park, MA: Center for International Development and Conflict Management, University of Maryland.

Matai, DK (2005) *Cyberland Security: Organised Crime, Terrorism and the Internet.* Transcript of a speech given at the Oxford Internet Institute. Oxford: University of Oxford. <http://www.oii.ox.ac.uk/>

Matthew, Richard, and George Shambaugh. (1998) Sex, Drugs and Heavy Metal: Transnational Threats and National Vulnerabilities. *Security Dialogue* 29: 163–176.

-----. (2005) The Limits of Terrorism: A Network Perspective. *International Studies Review* 7: 617-627.

Mathews, John T. (1997) Power Shift. *Foreign Affairs* 76: ???-???

Mesthene, E. (1969) "The Role of Technology in Society." Reprinted (2000) in *Technology and the Future*, edited by A.H. Teich, 8th Edition. Boston, MA: St. Martin's.

McCormick, John and Gage, Deborah. March 16, 2005. Shadow Crew: Web Mobs. Baseline. <http://www.baselinemag.com/article2/0,1397,1774393,00.asp>

McMullan, John L., and Perrier, David C. (2003) Technologies of Crime: The Cyber-Attacks on Electronic Gambling Machines. *Canadian Journal of Criminology and Criminal Justice*. April: 159-186.

McWalters, Ian (1999) *The Link Between Organized Crime and Corruption – A Hong Kong Perspective*. A paper presented at the 9th International Anti-Corruption Conference. Durban, South Africa. October 10-15.

Meet the Hackers. May 29, 2006. Business Week Online.

<http://www.businessweek.com/magazine/content/06_22/b3986093.htm?campaign_id=bier_tcm>

Mercene, Recto. July 20, 2004 Govt agents bust cyber crime gang. Today.

Mertha, Andrew C. (2005) *The Politics of Piracy: Intellectual Property in Contemporary China*. New York, NY: Cornell University Press.

Moore, David (2002) *Network Telescopes: Observing Small or Distant Security Events*. Cooperative Association of Internet Data Analysis. <http://www.caida.org/_outreach/presentations/2002/usenixsec/>

Morgan, Patrick M. (2003) Information warfare and domestic threats to American security. *Contemporary Security Policy* 24:161-189.

Miles, I. (1996) "The Information Society," in Dutton (ed.): 37-52.

Milito, Rodolfo A. (2006) The Inside-Out Approach to Infection Control. *Information Systems Security* 14: 33-37.

Minihan, Kenneth A. (1996) Intelligence and Information Systems Security: Partners in Defense Information Warfare. *Defense Intelligence Journal* 5: 13-23

Mueller, Milton L. (2002) *Ruling the Root: Internet governance and the taming of cyberspace*. Boston, MA: Massachusetts Institute of Technology.

Mumford, Lewis (1934) *Technics and Civilization*. New York, NY: Harcourt Brace Jovanovich.

Murphy, Brian M. (1986) *The International Politics of New Information Technology*. London: Croom Helm.

Naím, Moisés (2005) *Illicit: How Smugglers, Traffickers and Copycats are Hijacking the Global Economy*. New York, NY: Doubleday Press.

Naraine, Ryan. June 17, 2005. Botnet Hunters Search for 'Command and Control' Servers. eWeek.com. <http://www.eweek.com/article2/0,1759,1829347,00.asp>

National Hi-Tech Crime Unit (2005) *Confidentiality Charter*. London, UK: NHTCU. <http://www.nhtcu.org/media/documents/publications/CON_05.pdf>

Naylor, Robert T. (2002) *Wages of Crime: Black Markets, Illegal Finance, and the Underworld*. Ithaca, NY: Cornell University Press.

National Academy of Sciences (1998) *Internet Counts: Measuring the Impacts of the Internet*, National Academy Press.

<http:// www.bsos.umd.edu/cidcm/wilson/xnasrep2.htm>

Neill, Donald A. (2005) *China versus the Internet*. Directorate of Strategic Analysis Background Paper. Ottawa, ON: Department of National Defence, Government of Canada

Nielsen, Suzanne C. and Donald Welch (2003) Teaching Strategy and Security in Cyberspace: An Interdisciplinary Approach. *International Studies Perspectives* 4: 133-144.

Nordstrom, Carolyn (2003) "ICT and the World of Smuggling." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by R. Latham, pp. 235-250. New York, NY: The New Press.

NTU, police team up to fight cyber crime. December 19, 2001. Straits Times. <http://it.asia1.com.sg/newsarchive/12/news003_20011219.html>

Nunberg, Barbara (2002) Civil Service Quality After the Crisis: A view of Five Asian Cases. *Asian Journal of Political Science* 10: 1-20.

Nuttall, Chris. November 11, 2003. Crime gangs extort money with hacking threat. Financial Times.

Nykodym, Nick, Taylor, Robert and Vilela, Julia (2005) Criminal profiling and insider cyber crime. *Computer Law & Security Report* 21: 408-414.

Ortis, Cameron J., and Evans, Paul M. (2003) The Internet and Asia-Pacific security: old conflicts and new behaviour. *Pacific Review* 16: 549-572.

Palmer, Kate. March 15, 2005. Contrabandwidth. Foreign Policy Magazine. <http://www.foreignpolicy.com/story/cms.php?story_id=2787>

Pang, Ruoming, Yegneswaran, Vinod, Barford, Paul, Paxson, Vern and Larry Peterson (2004) *Characteristics of Internet Background Radiation*, Proceedings of ACM SIGCOMM/USENIX Internet Measurement Conference. <http://www.cs.wisc.edu/~vinod/radiation-paper.pdf>

Paxson, Vern (1998). *BRO: A System for Detecting Network Intruders in Real Time*. Proceedings of the 7th USENIX Security Symposium. <http://www.icir.org/vern/papers.html>

Pei, Minxin. January 15, 2005. Dangerous Denials. Foreign Policy Magazine. <http://www.foreignpolicy.com/story/cms.php?story_id=2753>

Pescapè, Antonio and Giorgio Ventre (2005) Experimental analysis of attacks against intradomain routing protocols. *Journal of Computer Security* 13: 877-903.

Piore, Adam. December 22, 2003. Hacking for dollars. Newsweek International.

Pocar, Fausto (2004) New Challenges for International Rules Against Cyber-Crime. *European Journal on Criminal Policy and Research* 10: 27-37.

Pollins, Brian M. (1996) Global Political Order, Economic Change and Armed Conflict: Co-evolving Systems and the Use of Force. *American Political Science Review* 90: 103-117.

Pool, Ithiel de Sola (1990) *Technologies Without Boundaries: On Telecommunications in a Global Age*. Cambridge: Harvard University Press.

Porter, Michael E. March 15, 2001. Strategy and the Internet. Harvard Business Review, 63-78.

Poulsen, Kevin. Feb 17, 2005. Feds square off with organized cyber crime. SecurityFocus. <http://www.securityfocus.com/news/10525>

--------. August 18, 2004. South Pole 'cyberterrorist' hack wasn't the first. Security Focus. <http://www.securityfocus.com/news/9356>

--------. June 30, 2001. Cyber Terror in the Air. SecurityFocus.com. <http://www.securityfocus.com/columnists/6>

Press, Larry (1998) An Internet Diffusion Framework. *Communications of the ACM* 41: 1112-1130.

Protecting the family jewels/ July 24, 2004. The Economist.

Prowse, Catherine Elaine (1993) *A network analysis of Vietnamese criminal organizations*. Thesis (M.A.) University of Calgary, AB.

Pye, Lucian (1981) *The Dynamics of Chinese Politics*. Cambridge, MA: Gunn & Hain.

Quirinus. (2006). In Encyclopædia Britannica. Retrieved May 27, 2006, from Britannica Concise Encyclopedia. <http://concise.britannica.com/ebc/article-9376325/Quirinus>

Raab et al., (1999) "The Information Polity." In *Society on the Line: Information Politics in the Digital Age*, edited by W. Dutton, pp. 283-299. Oxford: Oxford University Press.

Radcliff, Deborah. July 13, 2004. Companies adapt to a zero-day world. SecurityFocus.

Ratcliffe, Jerry (2005) The Effectiveness of Police Intelligence Management: A New Zealand Case Study. *Police Practice & Research* 6: 435-451.

Reporters Without Borders (2003) *Obstacles to the Free Flow of Information Online: The Internet Under Surveillance*. Paris, France: Reporters Without Borders.

Ripsman, Norrin M. and Paul, Tom V. (2005) Globalization and the National Security State: A Framework for Analysis. *International Studies Review* 7: 199-227

Roberts, Paul and Lemon, Summer. May 27, 2004. International police nab virus suspects. IDG New Service.

Roché, Sebastian (2005) Prevention and Security: A New Governance Model for France through a Contract-Based Territorial Approach. *Canadian Journal of Criminology & Criminal Justice* 47: 407-426.

Rockstrom, Anders, and Zdebel, Bengt (1998) A Network Strategy for Survival. *IEEE Communications Magazine* 36: 36-40.

Rodriguez, Joseph (2000) A Comparative Study of Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn. *Asian-Pacific Law & Policy Journal* 1: 1-47.

Rosecrance, Richard. (1996) The Rise of the Virtual State. *Foreign Affairs* 75: 45-61.

Rosenau, Jame. (2002) "Information Technologies and the Skills, Networks, and Structures that Sustain World Affairs." In *Information Technologies and Global Politics*, edited by J. N. Rosenau and J.P. Singh, pp. 275-288. Albany, NY: State University of New York Press.

--------. (1998) "Global Affairs in an Epochal Transformation." In *Information Revolution and International Security*, edited by H. C. Ryan and E. C. Peartree, pp. 33-57. Washington, DC: Center for Strategic and International Studies Press.

Ross, Jeanne (1995) *Johnson & Johnson: Building an Infrastructure to Support Global Operations*. MIT Center for Information Systems Research. Working Paper 283, September: 1-10.

Rothkopf, David. J. (1998) Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs* 51: 325-360.

Roughgarden, Tim (2003) The Price of Anarchy is Independent of the Network Topology. *Journal of Computer and System Sciences* 67:341-364.

Royal Canadian Mounted Police (RCMP) (2002) *Hackers: a Canadian police perspective Part II*. Prepared by the Criminal Analysis Branch, Criminal Intelligence Directorate Royal Canadian Mounted Police. March 14.

Russell, Ryan, Tim Mullen (Thor), FX, Dan "Effugas" Kaminsky, Joe Grand, Ken Pfeil,

Ido Dubrawsky, Mark Burnett, and Craig, Paul. (2003) *Stealing the Network: How to Own the Box*. Syngress Publishing Inc: Rockland, MA.

Safire, William. February 2, 2004. The farewell dossier. The New York Times.

Savona, Ernesto U., and Mignone, Mara (2004) The Fox and the Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research* 10: 3-26.

Savvas, Antony. November 8, 2005. Australian government recruits ISP zombie hunters. CompuerWeekly.com. <http://www.computerweekly.com/Articles/2005/11/08/212867/AustraliangovernmentrecruitsISPzombiehunters.htm>

Schuck, Amie M. (2005) American Crime Prevention: Trends and New Frontiers. *Canadian Journal of Criminology & Criminal Justice* 47: 447-462.

Seetharaman, Krishnan (1998) The CORBA Connection. *Communications of the ACM* 41: 34-36.

Segal, Ben (1995) *A Short History of Internet Protocols at CERN*. CERN IT: Geneva, Switzerland. <http://ben.home.cern.ch/ben/TCPHIST.html>

Shapiro, Andrew L. (2000) *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*. New York: Public Affairs.

--------. July 12, 1999. Think Again: The Internet. Foreign Policy Magazine, 14-27.

Shaw, Victor N. (2003) Within and Without National Borders: Crimes and Deviance in Asia and the Pacific. *International Journal of Comparative Criminology* 3: 119-148.

Shelley, Louise I., and Picarelli, John T. (2002) Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism. *Police Practice and Research* 3: 305-318.

--------. (1998) Crime and Corruption in the Digital Age. *Journal of International Affairs* 51: 607-620.

--------. (1995) Transnational Organized Crime: An Imminent Threat to the Nation-State? *Journal of International Affairs* 48: 488-489.

Shields, Peter (2005) When the 'information revolution' and the US security state collide. *New Media & Society* 7: 483-512.

Shiels, Maggie. March 1, 2002. Cyber security given new emphasis. BBC News UK

Edition.

Shimeall, Timothy J., Casey J. Dunlevy and Williams, Phil (2001) *Intelligence Analysis for Internet Security: Ideas, Barriers and Possibilities*. CERT Analysis Center, Software Engineering Institute, Carnegie Mellon University. <http://www.cert.org/archive/html/spie.html>

Short, James, and N. Venkatramen (1992) Beyond Business Process Redesign: Redefining Baxter's Business Network. *Sloan Management Review* Fall: 7-21.

Shu-ling, Ko. July 16, 2004. Beijing wages cyberwar against DPP headquarters. Taipei Times. <http://www.taipeitimes.com/News/front/archives/2004/06/16/2003175231>

--------. September, 4 2003. Cabinet says computers under attack. Taipei Times.

Sidak, Gregory J., and Singer, Hal J. (2001) Cable Modems and DSL: Broadband Internet Access for Residential Customers. *American Economic Review* 91: 245-267.

Singh, J.P. (2002) "Information Technologies and the Changing Scope of Global Power and Governance." In *Information Technologies and Global Politics*, edited by J. N. Rosenau and J.P. Singh, pp. 1-38. Albany, NY: State University of New York Press.

Skogan, Wesley G., and Hartnett, Susan M (2005) The Diffusion of Information Technology in Policing. *Police Practice & Research* 6: 401-417

Slatalla, Michelle and Quittner, Joshua (1995) *Masters of deception: The gang that ruled cyberspace.*: New York, NY: HarperCollins Publishers

Snoeren, Alex, Craig Partridge, Luis Sanchez, Christine Jones, Fabrice Tchakountio, and Kent, Stephen (2001) Hash Based IP Traceback. *Proceedings of ACM SIGCOMM.*

Somawaji, Anil (2004) How to Win an Evolutionary Arms Race. *IEEE Security and Privacy*. November-December: 70-72.

Sophos (2004) *Virus writing on the increase - Sasser worm the major irritant of 2004, but Netsky worms dominate reports*. London, UK: Sophos Inc. Available online: http://www.sophos.com/pressoffice/pressrel/uk/20040728topten.html

Stallings, William (1993) "The OSI Reference Model." In *Networking Standards: A Guide to OSI, LAN, and MAN Standards*, edited by W. Stallins, pp. 17-56. New York, NY: Addison-Wesley.

Staniford, Stuart, James Hoagland, and McAlerney, Joseph (2002) Practical Automated Detection of Stealthy Portscans. *Journal of Computer Security* 10: 105-136.

Stanton, John J. (2002) Terror in Cyberspace: Terrorists Will Exploit and Widen the Gap

Between Governing Structures and the Public. *American Behavioral Scientist* 45: 1017-1032.

Sterling, Bruce. August, 8 2004. The Other War on Terror. Wired. <http://www.wired.com/wired/archive/12.08/view.html?pg=4>

--------. (1992) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York, NY: Bantam Books. <http://www.farcaster.com/sterling/contents.htm>

Stinson, Douglas (1995) *Cryptography Theory and Practice.* London: CRS Press Inc.

Swaine, Michael D. (2005) "Chinese Crisis Management: Framework for Analysis, Tentative Observations, and Questions for the Future." In *Chinese National Security Decision Making Under Stress*, edited by A. Scobell and L. M. Wortzel, pp. 5-54. Carlisle, PA: Strategic Studies Institute, U.S. Army War College. <http://stinet.dtic.mil/cgibin/GetTRDoc?AD=A438913&Location=U2&doc=GetTRDoc.pdf>

Tan, Siong Thye (2002) Money laundering and E-commerce. *Journal of Financial Crime* 9: 277-286.

Taylor et al (1999) "Innovation in Public Service Delivery." In *Society on the Line: Information Politics in the Digital Age*, edited by W. Dutton, pp. 265-282Oxford: Oxford University Press.

Telang, Rahul and Sunil Wattal (2005) *Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical Investigation.* A paper presented at the Fourth Workshop on the Economics of Information Security, Kennedy School of Government Harvard University, 2-3 June. <http://infosecon.net/workshop/pdf/telang_wattal.pdf>

The Knightmare (1994) *Secrets of a Super Hacker.* New York, NY: Loopmanics Unlimited.

The Worldwide Web and Internet Technology. June 1, 1998. Harvard Business Review, No. 9-198-020, 1-11.

Tiboni, Frank. August 22, 2005. The new Trojan war: Defense Department finds its networks under attack from China. FCW.com.

Trim, Peter R. J. (2003) Public and Private Sector Cooperation in Counteracting Cyberterrorism. *International Journal of Intelligence and Counter Intelligence* 16: 594-608.

Tsagarousianou, Roza, Tambini, Damian D., and Bryan, Cathy (1998) *Cyberdemocracy: Technology, Cities, and Civic Networks.* London: Routledge.

United Nations Centre for International Crime Prevention - UNCICP (2000) Assessing Transnational Organized Crime: Results of a Pilot Survey of 40 Selected Organized Criminal Groups in 16 Countries. *Trends in Organized Crime* 6: 44-92.

Urbas, Gregor (2001) *Cybercrime Legislation in the Asia-Pacific Region*. Background paper. Canberra, Australia: Australian Institute of Criminology.

van Dartel, Michel, Sprinkhuizen-Kuyper, Ida, Postma, Eric, and Jaap van den Herik (2005) Reactive Agents and Perceptual Ambiguity. *Adaptive Behavior* 13: 227-242.

van Valen, L. (1973) A New Evolutionary Law. *Evolutionary Theory* 1: 1-30.

Vargo, John, and Ray Hunt (1996) "Local Area Networks - Principles and Components." In *Telecommunications in Business: Strategy and Application*, edited by R. Irwin, pp. 167-223. New York, NY: McGraw-Hill.

Vaughan-Nichols, Steven J. February 12, 2002. Web Services: Beyond the Hype. Computer, 18-21.

Venkatraman, N. (1994) IT-Enabled Business Transformation. *MIT Sloan Management Review* Winter: 73-87.

Verton, Dan. August 30, 2004. Organized Crime Invades Cyberspace. ComputerWorld.

--------. February 13, 2003. Criminals using high-tech methods for old-style crimes. ComputerWorld.

Villeneuve, Nart (2006) The filtering matrix: Integrated Mechanisms of information control and the demarcation of borders in cyberspace. *First Monday* 11: <http://firstmonday.org/issues/issue11_1/villeneuve/index.html>

Vlahos, Michael (1998) Entering the Infosphere. *Journal of International Affairs* 2: 497-525.

Waever, Ole. (1995) "Securitization and Desecuritization." In *On Security*, edited by R. D. Lipshutz, pp. 46-86. New York, NY: Columbia University Press.

Waldrop, M. Mitchell. May 13, 2002. Grid Computing. Technology Review, 37.

Wall, David S. (2001) *Crime and the Internet*. London: Routledge.

Ward, Andrew. July 17, 2004. Beijing blamed for wave of cyber attacks. Fnancial Times.

Wearden, Graeme. November, 21 2005. Government sees silver lining in botnet cloud. ZDNet UK. <http://news.zdnet.co.uk/internet/security/0,39020375,39237406,00.htm>

Weber, Stephen (2005) "The Political Economy of Open Source Software and Why it Matters." In *Digital Formations: IT and New Architectures in the Global Realm*, edited by R. Latham and S. Sassen, Princeton, pp. 178-211. NJ: Princeton University Press.

Wenger, Andreas. (2001) The Internet and the Changing Face of International Relations and Security. *Information and Security* 7: 1-15. http://infosec.procon.bg/contents/vol_7.htm

Wescott, Clay G. (2001) E-Government in the Asia Pacific Region. *Asian Journal of Political Science* 9: 1-24.

Williams, Michael. C. (2003) Words, images, enemies: Securitization and international politics. *International Studies Quarterly* 47:511-531.

Williams, Phil (2004) *Threats from Nonstate Actors / Criminal Networks*. The United Nations Secretary General's High-Level Panel on Terrorism and Non-state Actors. New York: United Nations. <http://www.un-globalsecurity.org/pdf/Williams_paper_nonstate_actors_crime.pdf>

--------. (2002) *Organized Crime and Cyber-Crime: Implications for Business*. Pittsburgh, PA: CERT Coordination Center, Carnegie Mellon University. <http://www.cert.org/archive/pdf/cybercrime-business.pdf>

--------. (1999) "Getting rich and getting even: Transnational threats in the twenty-first century." In *Organized Crime: Uncertainties and Dilemmas*, edited by S. Einstein and M. Amir, pp. 29-55. Chicago, IL: University of Illinois Press,.

--------. (1995) Transnational Criminal Organizations. *Washington Quarterly* 18: 57-71.

--------. (1994) Transnational Criminal Organizations and International Security. *Survival* 36: 109-128.

Williams, Phil, Shimeall, Timothy and Dunlevy, Casey (2002) Intelligence Analysis for Internet Security. *Contemporary Security Policy* 23: 1-38.

Wilson, Ernest J. (2004) *The Information Revolution and Developing Countries*. Cambridge, MA: MIT Press.

Wooldridge, Jeffrey M. (2003) *Introductory Econometrics: A Modern Approach*. 2nd edition. Mason, OH: Thomson South-Western.

Wong, Kam C. (2004) The police legitimacy crisis and police law reform in China: Part II. *International Journal of Police Science & Management* 7: 1-14.

Wong, Natasha (2004) Counterfeit Medicine: Is it Curing China? *Asian-Pacific Law &*

Policy Journal 5: 155-187.

Wong, Poh-kam (2003) Global and National Factors Affecting E-Commerce Diffusion in Singapore. *The Information Society* 19: 19-32.

--------. (2002) ICT production and diffusion in Asia Digital dividends or digital divide. *Information Economics and Policy* 14: 167–187.
Wong, Thomas. February 2, 2005. Regulation of Interception of Communications in Selected Jurisdictions. Research and Library Services Division of the Legislative Council Secretariat. Hong Kong SAR: Legislative Council Secretariat.

Wright, Quincy (1965) *A Study of War*. Chicago, IL: University of Chicago Press.

Xin, Xiaohui and Rudel, Thomas K. (2004) The Context for Political Corruption: A Cross-National Analysis. *Social Science Quarterly* 85: 294-309.

Yegneswaran, Vinod, Barford Paul and Johannes Ullrich (2003) "Internet Intrusions: Global Characteristics and Prevalence," SIGMETRICS, ACM.

Young, Emma (2004) The game is on. *New Scientist* 183: 48-51.

Yum, Young-ok and Hara, Kazuya (2005) Computer-Mediated Relationship Development: A Cross-Cultural Comparison. *Journal of Computer-Mediated Communication* 11: <http://jcmc.indiana.edu/vol11/issue1/yum.html>

Zacher, Mark (2002) "Capitalism, Technology, and Liberalization." In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, edited by J. N. Rosenau and J.P. Singh, pp.189-200. Albany, NY: State University of New York Press.

Zacher, Mark and Sutton, Brent A. (1996) *Governing Global Networks: International Regimes for Transportation and Communications*. Cambridge: Cambridge University Press.

Zhang S. and Chin, Ko-lin (2003) The declining significance of triad societies in transnational illegal activities. *British Journal of Criminology* 43: 463-482.

Zhang, Yin and Paxson, Vern (2000) Detecting Stepping Stones. *Proceedings of the 9th USENIX Security Symposium*. <http://www.icir.org/vern/papers/stepping/index.html>

Zinger, Ivan, Wichmann, Cherami and Gendreau, Paul (2001) Legal and ethical obligations in social research: The limited confidentiality requirement. *Canadian Journal of Criminology* April: 269-274.

Zipf, GK (1949) *Human Behavior and the Principle of Least-Effort*. Cambridge, MA: Addison-Wesley.

Zook, Michael (2000) Internet metrics: using host and domain counts to map the Internet. *Telecommunications Policy* 24: 613-620. <http://www.tpeditor.com/contents/2000/24-6+7.htm>

Interviews

Confidential Interview Tokyo, Japan 2001

Confidential Interview Tokyo, Japan 2002

Confidential Interview Tokyo, Japan 2002

Confidential Interview Hong Kong SAR 2002

Confidential Interview Hong Kong SAR 2003

Confidential Interview Hong Kong SAR 2003

Confidential Interview Kuala Lumpur, Malaysia 2002

Confidential Interview Kuala Lumpur, Malaysia 2002

Confidential Interview Manila, Philippines 2003

Confidential Interview Manila, Philippines 2003

Confidential Interview Seoul, Republic of Korea 2003

Confidential Interview Seattle, Washington 2002

Confidential Interview Seattle, Washington 2003

Confidential Interview Seattle, Washington 2004

Confidential Interview Toronto, Ontario 2004

Confidential Interview Vancouver, British Columbia 2001

Confidential Interview Vancouver, British Columbia 2002

Confidential Interview Vancouver, British Columbia 2003

Confidential Interview Vancouver, British Columbia 2005

Confidential Interview via email correspondence April 15, 2002

Confidential Interview via email correspondence February 16, 2004

Confidential Interview via email correspondence November 10, 2004

Confidential Interview via email correspondence August 2, 2005

Appendix A

Dependent variable:

Table A.1 – Internet diffusion and study dependent variables

Variable	Description	Measurement	Period	Source
TSOURCE	Source port data, the number of compromised nodes	Scale	2000-2002	DShield dataset

Independent variables:

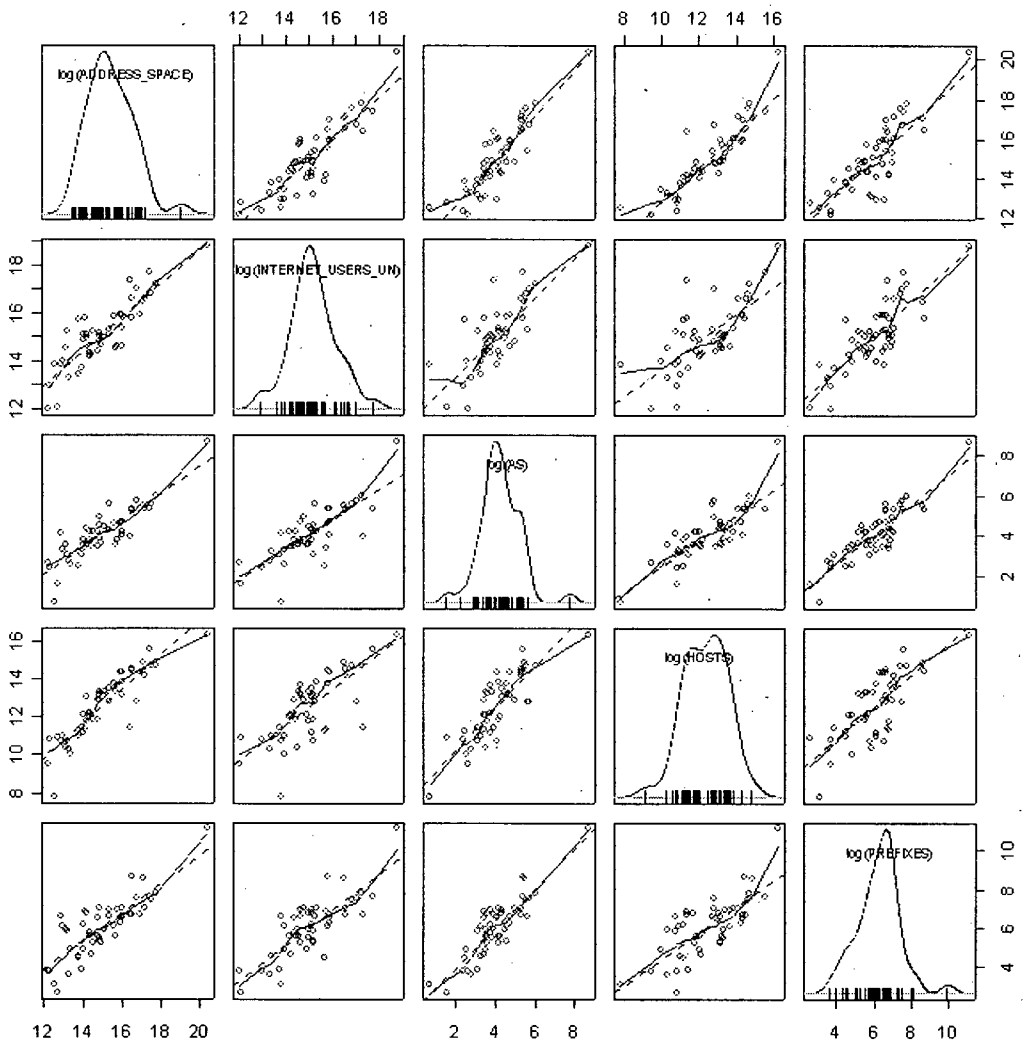
Table A.2 – Internet diffusion and study independent variables

Variable	Description	Measurement	Period	Source
Teledensity	Composite of land and cellular	Interval	1990-2001	OECD Communications 2001; Annual Yearbook on World Electronics Data by Elsevier.
Gini coefficient	Coefficient for income inequality	Interval	2000-2001	CIFP dataset
Education	Enrollment ratios across all levels	Percentage	2000-2001	UNDP Human Development Report
GDP	Gross domestic Product	Interval	2000-2001	OECD, Economist
Corruption index	CPI	Interval	2000-2001	Transparency International
E-economy	A collection of composites that measure the level of e-commerce	Interval	2000-2001	Economist intelligence unit
Encryption regime	Key escrow or private key system	Dummy (nominal)	2000-2001	Observation
Regime	Type of regime, democratic or non-democratic	Interval	2000-2001	POLITY IV Project
Region	East Asia, North America, Europe	Dummy (nominal)	2000-2001	
Population	Total state population	Interval	2000-2001	UN
PD	Political development (as constructed on freedom of the press).	Ordinal	2000-2001	Freedom House
Prefixes	Address prefixes	Interval	2000-2001	routing tables acquired from major Internet backbones (CAIDA)
Addresses	Announced addresses	Interval	2000-2001	
AS	Autonomous System	Count	2000-2001	Cooperative Association of Internet Data Analysis, Broadboard, CIRA, Oregon Routing Project

Sec_ser	Secure servers	Count	2000-2001	IMD (2000); Elsevier; WTO (2000); ITU; Netcraft
PC	Number of machines	Count	2000-2001	IMD (2000); Elsevier; WTO (2000); ITU; Netcraft
Traffic bandwidth	Packets through pipes (Gigabits per second)	Scale	2000-2001	CIRA
Rule of Law	Level of the rule of law in country	Interval	2000-2001	World Bank Governance Project
Democracy	Level of democracy	Interval	2000-2001	Polity IV Dataset

Chapter Four Diagnostics:

Figure 4.2 – Scatterplot matrix of address space, Internet users, hosts, ASs, prefixes by country.

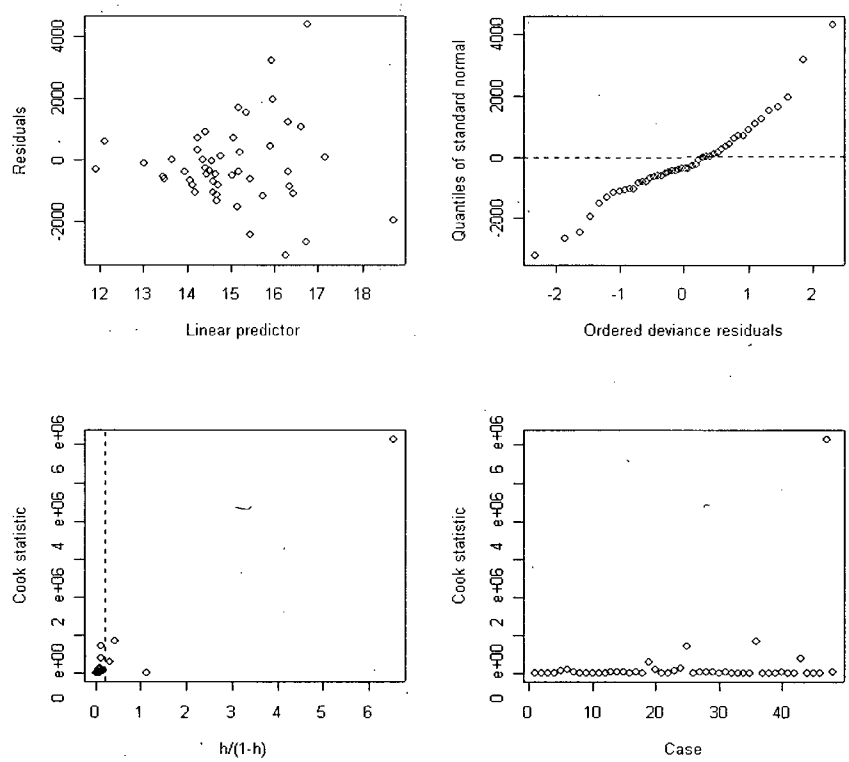


Chapter Five Diagnostics:

Figures 5.3 and 5.4 below display results for four basic diagnostic tests for the rule of law and democracy models with the US case included. The box in the top left is a plot of the jackknife deviance residuals against the fitted values. This serves as a visual check

for heteroskedasticity. The plot on the top right is a normal QQ plot of the standardized deviance residuals. QQ plots are usually presented with reference to a distribution in order to check for heavy tails or other anomalous patterns. The dotted line is the expected line if the standardized residuals are normally distributed (the line where $\alpha <= 0$ and $\beta <= 1$).

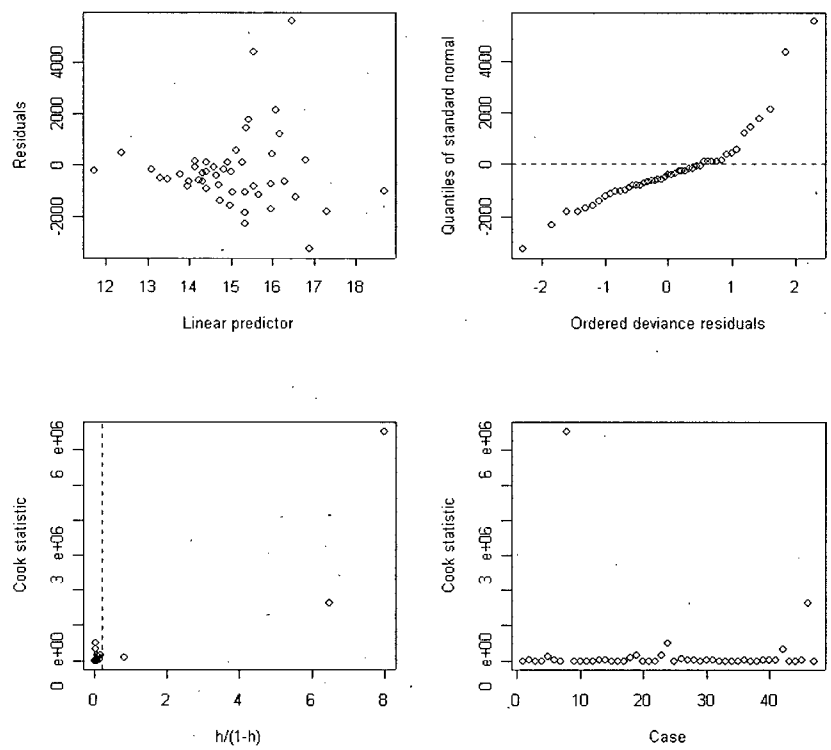
Figure 5.3 – Diagnostics for Model 1, Rule of Law



The bottom two panels are plots of the Cook statistics. On the left is a plot of the Cook statistics against the leverages. In general there will be two dotted lines on this plot. The horizontal line is at 8/(n-2p) where n is the number of observations and p is the number of parameters estimated. Points above this line may be points with high

influence on the model. The vertical line is at 2p/(n-2p) and points to the right of this line have high leverage compared to the variance of the raw residual at that point. If all points are below the horizontal line or to the left of the vertical line then the line is not shown. The lower right hand corner plot shows the Cook's D this time plotted against case number - the higher points are observations that are influential.

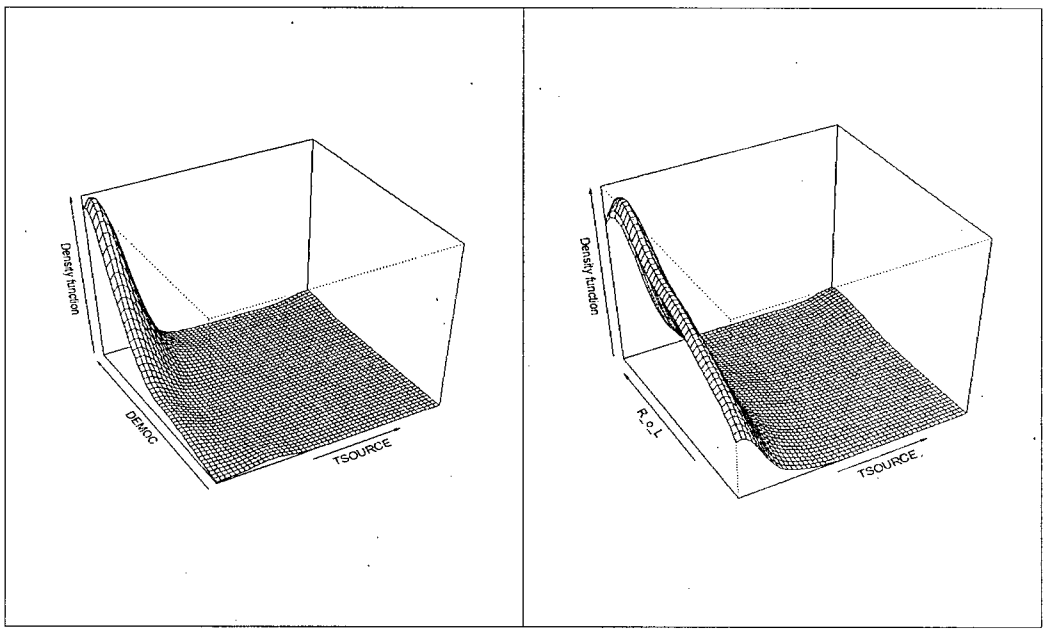
Figure 5.4 – Diagnostics for Model 2, Democracy



The contour plots in Figure 5.5 below depict the level of clustering between source, democracy and rule of law graphically. The rule of law variable preformed slightly better than the *democ* measure. Contour plots display the probabilities as volumes under the

curve where the total area equals one. Other potential replacements or proxies for these measures did not perform much better. An ideal distribution would appear like an even 'mountain' centered in the middle of the plot box.

Figure 5.5 – Bivariate density estimates for democracy and rule of law



Methodological notes:

Cross-sectional data: Undertaking a cross-national research projects using cross-sectional data in International Relations, or more generally in the social sciences, is fraught with methodological difficulties under even the best conditions. This is because they are essentially snap-shots in time of very complex behavioral processes analyzed in the aggregate. One of the advantages of quantitative research is that assumptions can be more clearly laid out. At the same time, however, one of the disadvantages of quantitative research is the sensitivity to the conclusions drawn to those same assumptions. Careful description of the methodological problems is especially important when the data are

nonstandard or have not been extensively used in other studies. This section covers the methodological and theoretical caveats that need to be kept in mind when reviewing this research.

Noise reduction in DShield data: Returning briefly to the noise reduction issues in h_*, it is important to keep in mind that not everything that is reported to Dshield.org is an actual attack. It is possible that as much as an eighth of the observations are not incidents from compromised nodes. This is because the LCD format is global or in other words a large N means accepting more noise in the data across countries. For example, it is possible that some number of source IPs simply should not be included in the data. The source IP could be traced back to a primary DNS. The report about the DNS server could be due to a firewall that blocked some of the return packets from a lookup. In this case the observation is not a result of an attack; but it could have been an incident of some sort which in the end cannot be properly distinguished. Furthermore, each IP address may represent multiple systems if a network address translation (NAT) gateway is used. It is also possible that there has been a double-counting of counting compromised nodes if the source network uses a dynamic IP address assignment and reboots. These are just some of the factors that contribute to measurement error in the dependent variable.

This section of the study also needed to give full consideration to port scans from spoofed sources. Normally there is little benefit to an performing an individual spoofed port scan simply because the source does not get a response back. The primary reason for using spoofing port scans is to create spurious background noise to hide the real sources. The Yegneswaran *et al* study addressed this concern by correlating reports from multiple sources. They found that the effect of the spoofed sources are marginalized and real

sources rise to the top. In theory the spoofed port scans form only a small fraction of all recorded port scans (Yegneswaran *et al.,* 2003).