ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

CYBER INFRASTRUCTURE PROTECTION - VOL 2 - PART 1 OF 3

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-147
Course Content:	83 pgs
PDH/CE Hours:	6

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

ELE-147 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. According to the reference material, cause is the second motivation for malicious online actors. Cause is defined as the use of technical expertise or skill in the pursuit of political, social, cultural, ideological, religious, or nationalistic goals.
    a. True
    b. False
2. Using Table 2-2 Malware and Related Services Offered in Hacker Forums, which of the following types of malwares had the highest minimum price?
    a. Traffic
    b. FTP Resources
    c. Bots
    d. Trojan Horses
3. Using Table 3-2. Physical Attack Frequencies on Foreign Country (Bagaria), what percentage of respondents would Participate in a protest at an anti-Bagaria rally?
    a. 20.0 %
    b. 53.6 %
    c. 56.6 %
    d. 23.8 %
4. According to the reference material, in the hypothetical cyber-attack frequencies on foreign country, over 75 percent of the respondents felt that posting a comment criticizing the Bagarian government was an appropriate response.
    a. True
    b. False

5. Using Table 3-6. Foreign Versus Homeland Target, which of the following responses had the highest mean severity?
    a. Cyber Homeland
    b. Physical Homeland
    c. Cyber Foreign
    d. Physical Foreign
6. A diverse range of products enabling individuals to engage in a variety of cybercrimes was also available in the market, including Distributed Denial of Service (DDoS) attacks, spam, attacks, and hosting malicious content online. The primary service offered in these forums related to the distribution of spam (32.4 percent), or unwanted messages to email accounts, ICQ numbers, and mobile phones.
    a. True
    b. False
7. Using Table 2-1. Descriptive Data on Forums Used, what was the longest duration a forum was used to obtain information about the availability of selling/buying hacking services?
    a. 20.00 months
    b. 29.50 months
    c. 36 months
    d. 36.25 months
8. According to the reference material, 85 percent of all iFrame ads involved hackers leasing access to their active iFrame infra-structure on compromised servers through "traffic streams."
    a. True
    b. False
9. According to the reference material, MEECES—describes six motivations for malicious online actors. Which of the following motivators was NOT cited in the reference material?
    a. Ego
    b. Cause
    c. Emotion
    d. Entrance to social group
10. Using Table 2-2 Malware and Related Services Offered in Hacker Forums, which of the following types of malwares contributed the least to the number of average posts?
    a. Bugs
    b. FTP Resources
    c. Cryptors
    d. Traffic

CONTENTS

PREFACE

This book is a follow-on to our earlier book published in 2011 and represents a detailed look at various aspects of cyber security. The chapters in this book are the result of invited presentations in a 2-day conference on cyber security held at the City University of New York, City College, June 8-9, 2011.

Our increased reliance on the Internet, information, and networked systems has also raised the risks of cyber attacks that could harm our nation's cyber infrastructure. The cyber infrastructure encompasses a number of sectors including the nation's mass transit and other transportation systems, railroads, airlines, the banking and financial systems, factories, energy systems and the electric power grid, and telecommunications, which increasingly rely on a complex array of computer networks. Many of these infrastructures' networks also connect to the public Internet. Unfortunately, many information systems, computer systems, and networks were not built and designed with security in mind. As a consequence, our cyber infrastructure contains many holes, risks, and vulnerabilities that potentially may enable an attacker to cause damage or disrupt the operations of this cyber infrastructure. Threats to the safety and security of the cyber infrastructure come from many directions: hackers, terrorists, criminal groups, and sophisticated organized crime groups; even nation-states and foreign intelligence services conduct cyber warfare. Costs to the economy from these threats are huge and increasing. Cyber infrastructure protection refers to the defense against attacks on such infrastructure and is a major concern of both the government and the private sector.

A key contribution of this book is that it provides an integrated framework and a comprehensive view of the various forms of cyber infrastructure protection. We, the editors, strongly recommend this book for policymakers and researchers.

CHAPTER 1

INTRODUCTION

Tarek Saadawi
Louis H. Jordan, Jr.
Vincent Boudreau

In recent years, the analysis of cyber security has moved into what one might call a series of second-generation conversations. The first generation, dominated by engineers and computer programmers, regarded the issue as primarily a technical matter, and sought responses from cyber threats mainly in the development of protective software and hardware design. In its early phases, cyber threats were primarily regarded as politically neutral, and without a great deal of economic motivation. Hence, how these threats were generated, and what social or political actors or systems directed these attacks, mattered little. Up-to-date anti-virus software and other protective technology were judged sufficient to protect both personal and public cyber assets against attack.

Several things have changed since those early conversations. First, and most obviously, technology has grown more complex and more networked. As our society demanded more interactive cyber systems, the danger of contamination across these systems has grown. Second, cyber attacks have become less economically or politically neutral than in previous generations. Evidence is mounting that both governments and insurgent groups are using cyber platforms as a way of mounting attacks. Threats to cyber security from economically motivated groups, and especially, increasingly well-organized criminal syndicates, are

more advanced. Third, innovations in cyber technology each year make increasingly sophisticated cyber weapons more widespread. Moreover, as the market in malware evolves, the technology can be rented, making the threat more and more affordable. Finally, trends in technology development suggest that, generally, efforts to defend against cyber attacks will always be more expensive than efforts to develop new forms of attack. Over time, therefore, the possibility of developing purely technical solutions to the threats against cyber security seems dauntingly uneconomical, even if entirely technologically feasible.

There is a relentless struggle taking place in the cyber sphere as government and business spend billions attempting to secure sophisticated network and computer systems. Cyber attackers are able to introduce new viruses and worms capable of defeating many of our efforts. The military depends more on technological solutions than ever before. A cyber attack on military operations could be more devastating than the effects of traditional weaponry. Additionally, these attacks will come from an unseen adversary who will likely be unreachable for a counterattack or countermeasure. In this "Fifth" generation of warfare, the battlefield is everywhere, and everyone potentially becomes a combatant, which causes grave new questions in the areas of the law of war as well as national sovereignty. The U.S. military must work closer than ever before with the various agencies of government, business, and academia to understand the threat and develop various modes of fighting cyber attacks.

Where, then, has the discussion of cyber security turned? Some answers lie in reversing trends toward greater integration and increasing technological sophistication. As cyber threats diffuse across increas-

ingly connected networks, some have sought to counter them by developing lower-technology systems unintegrated with the larger cyber infrastructure, simply by having their own isolated cyber islands disconnected from the larger cyber systems. Others continue—as they must—to fight the war on a technological front, developing faster and more sophisticated ways of countering cyber threats. But for many, the evolution of cyber security requires a new and deeper understanding of the social, economic, and political dynamics that animate cyber terrorism and cybercrime. As with conventional security analysis, or efforts to decrease or frustrate criminal behavior more generally, we have begun to consider how the social forces that motivate and govern the generation of cyber threats can influence cyber security. By understanding how the market in criminal malware operates, or figuring out the dynamics that hold organized crime together, cyber security specialists can more effectively develop methods of staving off those threats. While the last several decades have perhaps encouraged us to think of cyber threats as programs, viruses, worms, spyware, and botnets, current conversation recalls that people—connected to one another in organizations or through networks, motivated by political or criminal concerns, living in societies and subject to laws—deploy these threats.

The tools of foreign policy, conventional security studies, criminology, sociology, and economic theory are all relevant to the analysis of these threats. Deterrence theory, for example, focuses on how to prevent people with capacity from acting to inflict harm. Game theory explores how different political objectives and modes of interaction—reassurance, recognition, security, and prestige—influence exchanges of threat or

attack. But if useful, these analytic tools need now to navigate an entirely new landscape. How, for instance, can one deter an entity that thrives on the secrecy of an Internet identity? Are there ways of deterring cyber warriors who thrive on the prestige of making a bold cyber strike? Can we translate strategies designed to influence the behavior of nation-states (who must balance a range of goals that include their power, the stability of their regimes, and the well-being of their populations) to use against smaller networks, with neither citizens nor legal standing to worry about? In important and obvious ways, we cannot simply turn to the established works of social scientists for answers.

The problem, of course, is compounded by the technological side of things, and the fact that social scientists, computer scientists, engineers, and technicians have an uneven track record of working together to solve these problems (though in the current environment, work together they must). Does current technology allow us to deter a cyber attack credibly? If political strategy suggests a move from the existing, more defensive posture, to one that favors a proactive attack on insurgent or criminal organizations, what might such a weapon look like, and what are the broader implications of using offensive cyber weapons? As such questions illustrate, the solution to many of today's most pressing cyber threats (as well as those we can imagine emerging in the near and distant future) rests not in the realm of the social sciences, but in efforts to integrate lessons derived from those sciences into the design of technological work; the march of cyber technology needs to merge around politically informed strategies for the deployment of that technology. Hence, while cyber security once functioned mainly as a shield to deflect attacks, wherever they

came from and however they were directed, contemporary technological design must figure out both how to protect cyber assets, and how to identify, interdict, disrupt, and frustrate the organizations that mount attacks against them.

This book is designed as a way of entering this conversation. The chapters in this book were mainly presented as papers at the Cyber Infrastructure Protection 2011 conference at the City College of New York, in early-June 2011. At this conference, presenters were asked to think about the relationship between the technical and human elements of the threats to cyber security. The discussion was wide ranging, including experts in law, criminal behavior, international dynamics, and, of course, technical elements of cyber security. This book includes many of those papers, as well as several additional contributions. By presenting this work, more research and development of strategy toward a more integrated approach to cyber security, which borrows both from the fields of technology and engineering and from broader social scientific approaches, may take place.

OUTLINE OF THE BOOK

The book is divided into three main parts. Part I discusses the economic and social aspects of cyber security, covering the economics of malicious software and stolen data markets as well as the emergence of the civilian cyber warrior. Part II deals with laws and cybercrime, covering social and justice models for enhanced cyber security, and provides an institutional and developmental analysis of the data breach disclosure laws. Part II also provides solutions for the critical infrastructure that protect civil liberties and

enhanced security, and explores the utility of open source data. Part III presents the technical aspects of the cyber infrastructure and presents monitoring for Internet service provider (ISP) grade threats as well as the challenges associated with cyber issues.

ECONOMICS AND SOCIAL ASPECTS OF CYBER SECURITY

The first two chapters in this book provide a framework for the economic and social aspects of cyber security. In Chapter 2, Thomas Holt explains how hackers utilize data from a sample of active, publicly accessible web forums that traffic in malware and personal information to consider the supply and demand for various types of malicious software and related cybercrime services which have a prospective economic impact on cybercrime campaigns against civilian and business targets. In order to explore and expand our understanding of the economics of cybercrime in general, this chapter utilizes a qualitative analysis of a series of threads from publicly accessible Russian web forums that facilitate the creation, sale, and exchange of malware and cybercrime services. The findings explore the resources available within this marketplace and the costs related to different services and tools. Using these economic data, coupled with loss metrics from various studies, this analysis considers the prospective economic impact of cybercrime campaigns against civilian and business targets. The findings provide insights into the market dynamics of cybercrime and the utility of various malware and attack services in the hacker community. In summary, this chapter explores the market for malicious software and cybercrime services in order to understand the

price and availability of resources, as well as the relationship between the price paid for services and the cost experienced by victims of these crimes.

In Chapter 3, Max Kilger focuses on the civilian cyber warrior—who poses perhaps the most significant emerging threat to domestic and foreign critical infrastructures. Chapter 3 starts by providing some basic background for a schema that outlines six motivational factors that encourage malicious online behaviors.

The key concept is that perhaps for the first time in history, an everyday ordinary civilian can effectively attack a nation-state—in this case, through a cyber attack on some component of that nation-state's critical infrastructure. "Effectively" here means that the attack can cause significant widespread damage and has a reasonably high probability of success and a low probability of the perpetrator being apprehended. One of the first things that one might want to investigate in the chain of actions for a terrorist act is the initial starting point, where individuals begin thinking about and rehearsing in their minds the nature, method, and target for the terrorist attack. A key point for historical and social significance of the emergence of a civilian cyber warrior is the psychological significance of the event. The reassessment of the usual assumptions of the inequalities of the levels of power between nation-states and citizens establishes new relationships between institutions of society, government, and individuals.

An initial examination of the severity of physical attacks and cyber attacks that respondents feel are appropriate to launch against a foreign country bring both good news and bad news to the table. On the one hand, the vast majority of respondents select only responses that have minor or no consequences to the

targeted foreign country. On the other hand, there are a nontrivial number of respondents who personally advocate the use of physical and cyber attacks against a foreign country that have some moderate to very serious consequences. While there is some comfort in the fact that expressing intentions to commit terrorist acts is only the first link in the behavioral chain from ideation to the execution of an attack, and bearing in mind that this is a scenario-based situation, even a small incidence of individuals who would consider some of the most serious acts is troubling. This suggests that the emergence of the civilian cyber warrior (and perhaps the physical attack counterpart) is an event to take into account when developing policies and distributing resources across national priorities to protect national critical infrastructures. Knowing the enemy can be a key element in gaining a comprehensive perspective on attacks against online targets.

LAW AND CYBERCRIME

Legal and cybercrime are explored in Part II of this book. In Chapter 4, Michael M. Losavio, J. Eagle Shutt, and Deborah Wilson Keeling argue that to change the game in cyber security, we should consider criminal justice and social education models to secure the highly distributed elements of the information network, extend the effective administration of justice to cybercrime, and embed security awareness and competence in engineering and common computer practice. Safety and security require more than technical protections and police response. They need a critical blend of these elements with individual practice and social norms. Social norms matched with formal institutions enhance public safety, including in the

cyber realm. Informal and formal modes of controlling and limiting deviant behavior are essential for effective security.

Chapter 4 suggests that routine activity theory, opportunity theory, and displacement theory—frameworks for analyzing crime in communities—are ways to conceptualize and pattern the benefits of informal social control on cyber security. Routing Activity Theory (RAT) presents that, for cyber security, the analysis should equally consider the availability of suitable targets, a presence or lack of suitable guardians, and an increase or decrease in the number of motivated offenders—particularly those seeking financial gain or state advantage. Online social networks themselves suggest opportunities for the examination of RAT-based security promotion. Facebook, MySpace, and LiveJournal are online social networks that can promote cyber security within and without their domains. RAT can also be applied to criminal activity involving computing systems. Criminological principles to cyber security also relate to the use of criminal profiling and behavioral analysis. The reactive use of these techniques, much like the use of technical digital forensics in network settings, serves to focus an investigation and response in particular areas and on particular individuals. The proactive use of profiling can deter or prevent crime, such as drug courier profiling.

In Chapter 5, Melissa Dark considers the state data breach disclosure laws recently enacted in most states of the United States. Three reasons make the state data breach disclosure laws of interest: (1) the rapid policy growth; (2) the first instance of an informational regulation for information security; and, (3) the importance of these laws to prevent identity theft and to protect privacy. Technological advancements are changing the information security and privacy landscape con-

siderably. Yet, these policies are blunt instruments not suited to careful excision of these ills. Some advocates of modifying existing laws assert that the outcome of data breach disclosure should be to motivate large-scale reporting so that data breaches and trends can be aggregated, which allows a more purposeful and defensive use of incident data.

In Chapter 6, Joshua Gruenspecht identifies some problems of identity determination that raise some of the most complicated unresolved issues in cyber security. Industry and government are pursuing a number of approaches to better identify communicants in order to secure information and other assets. As part of this process, some policymakers have suggested that fundamental changes to the way in which the Internet transmits identity information may be necessary. Authentication is "the process of establishing an understood level of confidence that an identifier refers to a particular individual or identity." Authentication often involves an exchange of information before some other transaction in order to ensure, to the extent necessary for the transaction at hand, that the sender of a stream of traffic is who he or she claims to be or otherwise has the attributes required to engage in the given transaction. Attribution is the analysis of information associated with a transaction or series of transactions to try to determine the identity of a sender of a stream of traffic. Information collection and analysis is the focus of attribution. This chapter focuses on authentication and attribution; two other issues closely relate to identity and are critical elements of any secure system: authorization and auditing. This chapter considers these problems and concludes that authentication-oriented solutions are more likely to provide significant security benefits and less likely to produce undesirable economic and civil liberties consequences.

In Chapter 7, George W. Burruss, Thomas J. Holt, and Adam M. Bossler focus on the value of open reporting for malware creation and distribution. The authors consider how this information combines with other measures to explore the country-level economic, technological, and social forces that affect the likelihood of malware creation. The chapter proposes that online repositories containing data on malicious software can be valuable to study the macro-level correlations of malware creation. The data for the dependent variable used for this study (MALWARE) came from an open source malware repository where individuals could post information obtained on malicious software. The data for the independent variables derive from the *CIA World FactBook* and from Freedom House, a nongovernmental agency that collects annual data on political freedom around the globe. The chapter concludes that the diverse and sophisticated threats posed by hackers and malicious software writers require significant investigation by both the technical and social sciences to understand the various forces that affect participation in these activities. The chapter suggests that there is a strong need for greater qualitative and quantitative examinations of hacker communities around the world. Research on hacker subcultures in the United States, China, and Russia suggests that there are norms, justifications, and beliefs that drive individual action.

CYBER INFRASTRUCTURE

In Chapter 8, Abhrajit Ghosh presents a comprehensive view of network security from several years of research conducted at Telcordia; in particular, the problem of monitoring large-scale networks for malicious activity. The goal of the developed system is to detect various types of network traffic anomalies that could be caused by Distributed Denial of Service (DDoS), spamming, Internet protocol (IP) address spoofing, and botnet activities. Currently, three types of anomaly detectors are provided to collect data and generate alerts: (a) Volume Anomaly Detectors; (b) Source Anomaly Detectors; and, (c) Profile Anomaly Detectors. The goal of the source anomaly detectors is to identify instances of source IP address spoofing in observed flows. Here data for the monitored ISP is acquired via NetFlow/sFlow data feeds from three flow agents. The profile anomaly detectors can detect any behavioral anomalies pertaining to hosts within the monitored network.

One profile anomaly detector that is currently part of the system can identify potential spammers using flow data and spammer blacklists. The Telcordia system incorporates an efficient real-time volume anomaly detector designed to give early warning of observed volume anomalies. The volume anomaly detector operates by considering a near-term moving window of flow records when computing traffic travels to a destination address. The system incorporates a correlation engine that correlates alerts generated by the different types of anomaly detectors. A significant issue with many anomaly detection-based approaches is their potentially high false-positive rate. The correlation engine component is designed to reduce the

possibility of generating false-positives. Finally, the use of an alert correlation component is valuable to a network operator who would be very interested in lowering false-positive rates.

The goal of Chapter 9, written by Stuart Starr, is to explore the state-of-the-art in our ability to assess cyber issues. To illuminate this issue, the author presents a manageable subset of the problem. Using that decomposition, he identifies candidate cyber policy issues that warrant further analysis and identifies and illustrates candidate Measures of Merit (MoMs). Subsequently, Starr characterizes some of the more promising existing cyber assessment capabilities that the community is employing. That discussion is followed by an identification of several cyber assessment capabilities that are necessary to support future cyber policy assessments. The chapter concludes with a brief identification of high priority cyber assessment efforts to pursue.

PART I:

ECONOMICS AND SOCIAL ASPECTS OF CYBER SECURITY

CHAPTER 2

EXPLORING THE ECONOMICS OF THE MALICIOUS SOFTWARE MARKET

Thomas J. Holt

This research was sponsored by the National Institute of Justice, Award No. 2007-IJ-CX-0018 (August 2007-November 2009). The points of view within this document are those of the author and do not necessarily represent the official position of the U.S. Department of Justice.

INTRODUCTION

The growth and function of malicious software markets have caused a shift in the way that hackers use and access malware with varying degrees of skill. Specifically, web forums allow individuals to purchase access to sophisticated malicious software to victimize vulnerable systems and individuals and to sell the data they illegally obtain for a profit. Those with limited technical capabilities can utilize products sold in these markets to engage in attacks, while individuals with greater skill can generate a profit by providing access to their infrastructure and resources. While researchers are constantly exploring these markets to identify emerging threats, few have considered the actual economic conditions that affect the market, including the costs and benefits for offenders, and the losses incurred by affected victim computers. This qualitative study utilizes data from a sample of active publicly accessible web forums that traffic in malware and personal information to determine: the supply

and demand for various types of malicious software and related cybercrime services; the offenders' costs associated with multiple forms of attacks; and the prospective economic impact of cybercrime campaigns against civilian and business targets. The findings will benefit computer security practitioners, law enforcement, and the intelligence community by exploring the market dynamics and scope of the underground economy for cybercrime.

OVERVIEW

As technology increasingly permeates all facets of modern life, the risks posed by cyber attacks have increased dramatically.[1] Hackers target all manner of systems around the world in order to steal information, compromise sensitive networks, and establish launch points for future attacks.[2] In fact, evidence suggests that the number of computer security incidents has increased as more countries connect to the Internet.[3] Many of these attacks stem from computer hackers living in China, Russia, and Eastern Europe.[4] A sizeable proportion of these actors utilize malicious software, or malware, to automate various aspects of an attack.[5]

Malicious software, including viruses, Trojan horse programs, and various other tools, simplify or automate portions of a compromise, making it possible to engage in more sophisticated or complex intrusions beyond the true skills of the attacker.[6] In addition, the emergence of botnet malware, which combines multiple aspects of existing malware into a single program, enables hackers to establish stable networks of infected computers around the world.[7] These botnets can engage in attacks ranging from the distribution

of spam, denial of service attacks, and network scanning. The growth of botnet malware in the computer underground has revolutionized malware, leading individuals to lease out their infrastructure to the larger population of semi-skilled hackers to engage in attacks.[8]

The evolution of malware has led to the formation of an online marketplace for the sale and distribution of malicious software, stolen data, and hacking tools.[9] These markets largely operate in forums and Internet Relay Chat (IRC) channels in Russia and Eastern Europe and enable hackers to buy or sell various tools and services to facilitate attacks against all manner of targets. Few studies have, however, considered the impact of these markets on the economics of cybercrime for both victims and offenders. For instance, the ability to purchase sophisticated malware may reduce the time an individual must invest in an attack, and diminish the requisite knowledge needed to hack.[10] In addition, limited research has considered the supply and demand for different services within the malware market, calling into question the perceived value of certain tools and attacks relative to other offenses. Finally, the lack of concrete loss metrics on the impact of cybercrime in both the public and private sector make it difficult to understand the profits a cybercriminal may acquire.

In order to explore these issues and expand our understanding of the economics of cybercrime in general, this chapter utilizes a qualitative analysis of a series of threads from publicly accessible Russian web forums that facilitate the creation, sale, and exchange of malware and cybercrime services. The findings explore the resources available within this marketplace and the costs related to different services and tools.

Using this economic data coupled with loss metrics from various studies, this analysis considers the prospective economic impact of cybercrime campaigns against civilian and business targets. The findings provide insights into the market dynamics of cybercrime and the utility of various malware and attack services in the hacker community.

HACKING, MALWARE MARKETS, AND THE ECONOMIC IMPACT OF CYBERCRIME

In order to examine malicious software markets, it is critical to first understand the general dynamics of the hacker community, whose members create and utilize malware. Hackers operate within a subculture that values profound and deep connections to technology.[11] This subculture is also a meritocracy, in which participants judge one another based on their capacity to utilize computer hardware and software in innovative ways.[12] Those who can devise unique tools and identify new vulnerabilities garner respect from their peers and develop a reputation for skill and ability within the subculture.

There are, however, a limited number of individuals with the knowledge or skill necessary to engage in truly sophisticated hacks and attacks.[13] A larger proportion of the hacker community has some demonstrable skill and can understand both the theory and mechanics behind an attack, but may not be able to create all the tools necessary to complete an attack on their own. Thus, they may seek out resources from those with greater skill in order to improve their capabilities. Similarly, a portion of the hacker community simply seeks to engage in attacks or applications of hacking without developing the requisite

knowledge necessary to complete the act.[14] These actors are referred to as "script kiddies," because they try to acquire malicious software and use these programs without understanding the full functionality or processes affected.

The variation in skill and ability within the hacker community, coupled with a strong desire for the free flow of information, led hackers to trade and distribute tools and information on and offline regularly.[15] In the 1980s and 1990s, individuals would often barter for new resources, whether through trading stolen information or credentials, bulletin board system (BBS) access, or other valuable resources.[16] The creation of electronic payment systems and changes in the popularity of technology and information sharing, however, has engendered the growth of online markets where hackers can sell tools and data.[17]

Examinations of these marketplaces indicate that hackers can now buy and sell resources to facilitate attacks or information acquired after a compromise. Hackers regularly sell credit card and bank accounts, pin numbers, and supporting customer information obtained from victims around the world in lots of tens or hundreds of accounts.[18] Individuals also offer cash-out services to obtain funds from electronic accounts or automated teller machine systems (ATMs) offline, as well as checking services, to validate whether an account is active, as well as any available balances. Spam- and phishing-related services are also available in Internet relay chat (IRC) channels, including bulk email lists to use for spamming and email injection services to facilitate responses from victims.[19] Some sellers also offer Distributed Denial of Service (DDoS) services and web hosting on compromised servers.[20]

These studies clearly demonstrate the burgeoning marketplace for hacking tools and stolen data, and some insights into the costs of goods and services. Few, however, have considered how the fee structures and pricing for malware and data services may affect offender decisionmaking. For instance, it is unclear how much an individual may earn from a spam, denial of service, or malware infection campaign relative to his or her initial investment. This is due to the substantial difficulty in obtaining information about the losses to individual and corporate victims of cybercrime.[21] Intrusions and attacks are often unreported to law enforcement, particularly in corporate settings, because businesses may not recognize, or may cover up, the problem to minimize customer concerns.[22] Similar issues arise in estimating the losses individual citizens experience due to cybercrime. Many home users may not recognize that their computer has been compromised or perceive that the incident may not be investigated or taken seriously by law enforcement.[23]

As a consequence, there are few official statistics available on the prevalence of cybercrimes reported to law enforcement agencies.[24] For instance, this information is not provided in the Federal Bureau of Investigation's (FBI) annual Uniform Crime Reports, and few industrialized nations report cybercrime through a central government outlet.[25] There are also a limited number of outlets that report the economic impact of computer intrusions and cyber attacks. This is due to the difficulty in accurately estimating the costs related to clean and mitigate an infection or patch all affected systems.[26] The variation in the impact of an attack also makes it difficult to determine appropriate loss metrics. For example, it is unclear whether the estimated financial harm of a DDoS attack is based on the pro-

spective loss of revenue from prospective customers or losses to employee productivity.

As a consequence, data on the costs of cybercrime are largely generated by small samples of corporations willing to provide information based on attacks within their environments.[27] Similarly, the Internet Crime Complaint Center is one of the few outlets that provides consistent statistics on the economic impact of certain forms of cybercrime victimization in the general population.[28] The reported estimates use only self-reported victimization as the basis for examination. Thus, it is unknown how common these offenses are in the general population or how the variation in losses affect individual behavior while online.

In light of the significant gap in our knowledge of the economics of cybercrime for both offenders and victims, this chapter will explore this issue using a qualitative analysis of 909 threads from 10 active web forums in Russia and Eastern Europe that are involved in the creation, sale, and distribution of malicious software. This chapter will explore the products and services available in the market, as well as the supply, demand, and price for these resources. In turn, this information will be used to develop estimates for profit margins based on costs and loss metrics for cybercrime campaigns against civilian and business targets.

Data and Methods.

The data for this study came from a sample of 10 publicly accessible web forums; six of these forums trade in bots and other malicious code, while four provide information on programming, malware, and hacking.[29] These data were collected as part of a larger project examining botnets using a snowball sampling

procedure in Fall 2007 and Spring 2008.[30] Specifically, two English language forums were identified through *google.com*, using the search term "bot virus carder forum dump." This is a standard technique used by social scientists to collect qualitative data online to obtain a wide sample of prospective sites.[31] After exploring the content of publicly accessible threads from these two sites, six other Russian language forums were identified via web links provided by forum users. In fact, most participants in forums involved in the sale and trade of malware communicate using the Russian language.[32] Thus, a sample of threads from each of these forums was examined by a native-speaking Russian research assistant to ensure the content focused on the sale and exchange of malware. Four additional Russian language forums were identified through links provided in these sites to create this sample of ten forums. Six of these forums focus exclusively on either open sales or requests for malicious software, hacking tools, cybercrime services, and stolen data. The remaining four forums provide a mix of sales, information sharing, and resources to facilitate hacking and malware creation. The names of each forum have been removed to maintain some confidentiality for the participants and forum operators.

Within these 10 forums, all of the available publicly accessible threads were downloaded and saved as web pages. There was a significant volume of information obtained, though the first 50 threads from each forum were translated from Russian to English to assemble a convenient sample of threads. A certified professional translator translated the first 50 threads from eight of the 10 forums. Additionally, 25 threads from Forum 06 and 21 threads from Forum 05 were translated. Due to limited translator availability and duplicate transla-

tions in some of the forums, a native Russian graduate student translated additional content.[33] This student translated an additional 150 threads from Forums 03 and 04, and an additional 138 threads from Forum 05. These three forums were selected for further analysis, since they were very active and provided greater detail on the activities and practices of actors within malware markets. Duplicate threads were translated to determine translator reliability, which appeared high across the two translators.

A total of 909 threads derived from this convenient, yet purposeful sample of 10 forums. The threads consisted of 4,049 posts, which provided a copious amount of data to analyze (see Table 2-1 for forum information). Moreover, the forums had a range of user populations, from only 35 to 315 users. These threads span a 4-year period, from 2003 to 2007, though the majority of threads were from 2007.

The translated threads were then printed and analyzed by hand to consider both the prevalence and cost of products and services bought and sold in these forums. A content analysis was conducted to identify products, resources, and materials either sold or sought out in these markets. Advertisement content was coded based on the details provided. A post was coded as a sale if an individual stated that he or she was "selling," "offering," or otherwise providing a service. Requests for products were coded based on the language used, such as "need," "buying," or "seeking." Each item either requested or sold was coded individually, such that an advertisement selling both a piece of malware and a spam database were coded as a single spam database and malware. Thus, the number of advertisements is larger than the overall number of threads where the advertisements appeared.

Forum	Total Number of Strings	Total Number of Posts	User Population	Timeframe Covered
01	50	183	88	6.00 months
02	50	164	50	20.00 months
03	200	1,203	315	10.75 months
04	200	812	273	12.50 months
05	159	369	153	6.75 months
06	50	251	82	36.25 months
07	50	379	116	29.50 months
08	50	291	95	36.00 months
09	50	172	35	10.50 months
10	50	225	95	1.50 months
Total	909	4,049	1,302	

Table 2-1. Descriptive Data on Forums Used.

The threads were also analyzed to determine the services either being sold or requested. Services were coded into categories based on the content of the ad. Specifically, any ad that provided a service, such as the delivery of spam, web hosting, and hacking was coded as "cybercrime services." Ads related to malicious software, including bots, Trojan horses, and iFrame tools, were coded as "malware." Individuals buying or selling credit card account information, records from keystroke logs on compromised machines, or other resources were placed into the category

"stolen data." The tag "ICQ numbers" were used for ads selling or requesting ICQ numbers for their personal use. Any advertisement that appeared to be for legitimate products such as computer hardware or software, video game resources, legitimate security or programming services, or other products were placed under the tag "Other Services." Information on stolen data, ICQ numbers, and other services are excluded from this analysis, since they comprise only 36 percent of all threads observed, and are ancillary to malicious software production and services to facilitate cybercrime.[34] Thus, removing these threads enables this analysis to focus on malicious software and cybercrime services in depth.

In order to examine the economics of cybercrime, simple equations and statistics will use data generated from two well known and highly regarded sources: the Computer Security Institute's (CSI) *Annual Computer Crime and Security Survey* and the Internet Crime Complaint Center's (IC3) *Annual Internet Crime Report*. The CSI report is developed in conjunction with the FBI and provides one of the few available resources for statistics on the economic impact of cybercrime in corporate settings. This survey is distributed to 5,000 businesses and organizations across the United States via physical and electronic mail.[35] Two follow-up solicitations are made, and the response rate is usually between 5 and 10 percent of all total recipients. As a result, the figures presented are most likely biased samples that may not accurately reflect the true costs of various attacks across businesses and institutions.

A similar bias is evident in the statistics provided by the Internet Crime Complaint Center. The agency is a joint operation of the FBI and National White Collar Crime Center, which takes reports from individuals

who self-identify as victims of certain types of online fraud.[36] Individuals must report any incident via an online form hosted on the IC3 website. Anyone who is not aware of this resource may not report his or her experiences, reducing the generalizability of the data. Additionally, since victims must estimate the loss they have experienced, the reported statistics may not accurately reflect the true costs of victimization.

Despite the validity and generalizability of the statistics produced by these agencies, there are few other consistently reported and widely cited resources on the economic harm caused by cybercrime. Thus, the data produced by these agencies preclude strong conclusions and limit the generalizability of the analysis. The significant lack of research in this area, however, demands that some exploratory investigation be conducted to provide initial estimates for both corporate or individual losses and the general return on investment for cybercrime. The statistics presented are based on the 2008 reports provided by each agency, since they reflect all reported incidents for the 2007 calendar year. This creates a consistent data point between the forum content and the economic harm reported by victims of cybercrime. Since the CSI received a very low response rate in 2008 and did not publish all economic loss estimates, data from the 2007 CSI report[37] will also be used to provide cost measures for certain offenses.

Finally, all the economic data estimated in this analysis do not include labor costs. It is unknown how many man-hours may be required to complete a successful attack due to variations in the actors' skill and technical expertise.[38] Similarly, the time spent to generate new infections or maintain an existing compromise may differ by attacker, based on the sophisti-

cation and ease with which they can manage the tools at their disposal.[39] Certain attacks may also require no investment on the part of the offender when paying for a service like a DDoS attack. Thus, time and labor costs will not be included in these economic estimates due to the difficulty in computing these figures.

FINDINGS

Before discussing the products available, it is necessary to consider the structure of the market as a whole. These forums comprise an interconnected marketplace composed of unique threads that act as an advertising space. Individuals created threads by posting their products or services to the rest of the forum. Alternatively, posters could describe in detail what they wanted in buying or acquiring on the open market. Both buyers and sellers provided as thorough a description of their products or tools as possible, including contact information, pricing information, and payment methods. Actors within these markets communicated primarily through the instant messaging protocol ICQ or email, which they can encrypt to protect both participants during the sales process. Some also used the private message (PM) feature built into each forum. PMs ensure quick contact and act as an internal messaging system for each site, though they may not be as secure.

Prices were in either U.S. dollars or Russian rubles, along with the desired method of payment through a web-based electronic payment system. Most participants used WebMoney [WM] or Yandex, since they enable the near-immediate transmission of funds between participants, with no need for face-to-face interactions. In addition, four of the forums identified

offered guarantor payment services, in which individuals act as middlemen to hold money on behalf of a buyer until the seller delivers the products or services ordered.[40] Guarantor services ensure a higher likelihood of successful transactions, because both the buyer and seller are aware they can withdraw that payment depending on delivery of an order. Thus, access to a guarantor service is an important way to ensure that transactions are successfully completed in a timely fashion.

There were, however, no actual public transactions of services observed in these forums. Instead, buyers and sellers gave some indication of how the process operated. An interested individual would contact the advertiser via ICQ or email and negotiate the cost for services rendered. The prospective buyer then pays for the product and awaits delivery from the seller. Many sellers indicated that they must receive payment in advance of services rendered. This process introduces the potential for buyers to lose money should a good or service fail to be provided, and facilitates buyers being cheated by untrustworthy operatives. As a result, the sales process appears to favor sellers rather than buyers.

Malware.

The most common resource available in malicious software markets were Trojan horse programs (see Table 2-2 for breakdown).[41] There were 78 ads related to Trojan horse programs, comprising 31.7 percent of all malware for sale. The cost of these programs varied significantly, from $2 to $5,000, depending on the quality and sophistication of the resource. A variety of Trojan horses were sold, ranging from well-known

resources like Pinch, which can steal information from over 30 well-known programs, to keylogging Trojan horses designed to steal funds from WebMoney accounts. There was a relative balance between sale ads (51.6 percent) and custom request ads (49.4 percent) seeking Trojan horse programs. Thus, there is still a significant demand for novel or unique Trojan horses with special qualities that may not otherwise sell on the open market.

The second most common malware were iFrame tools that enable the distribution and infection by unique malicious code through web browsers (30.5 percent). The concept and design of iFrames originate with .html programming to seamlessly push multiple .html files to a browser in a single page of content without the need for user interaction.[42] Hackers subverted this design function, however, to surreptitiously send malware to unsuspecting users. In fact, individuals sold iFrame "exploits" and "packs" one could place on a server to infect the personal computers of individuals who visit web pages hosted there. This type of attack exponentially increases the infection vector for malicious software, and the risk of identity theft, data loss, and computer misuse.[43] There were 14 ads (66 percent) selling access to iFrame scripts and infection packs, indicating there is a healthy supply of these tools on the market. The proportion of requests for these resources (34 percent) also suggests there is still a substantial demand for iFrame malware. The price for these products ranged from $2 to $450, depending on the quality and sophistication of the resource. This is somewhat lower than the prices for Trojan horses, potentially because of the unique application of iFrame tools and the knowledge required to establish the infrastructure and support infections.

Resources Max.	Number of Average	Percent of		Buy	Percent of	Sell	Percent of		Min
	Posts	Total	Posts	Total	Posts	Total	Price	Price	Price
Bots	16	6.5	8	50	8	50	30	2,000	322.27
Bugs	3	1.2	3	100	0	0	40	40	40.00
Cryptors, Joiners, and Polymorphic Engines	47	19.1	13	27.6	34	72.4	0.20	49	13.03
FTP Resources	27	11.0	15	55.6	12	44.4	20	1,000	271.66
iFrames and Traffic Sales	75	30.5	26	34.7	49	65.3			
Tools	21	28.0	7	33.3	14	66.6	2	450	79.25
Traffic	54	72.0	19	35.2	35	64.8	1	500	110.84
Trojan horses	78	31.7	38	48.7	40	51.3	2	5,000	742.97
Total	246	100	103	41.9	143	58.1			

Table 2-2. Malware and Related Services Offered in Hacker Forums.

In addition, 72 percent of all iFrame ads involved hackers leasing access to their active iFrame infrastructure on compromised servers through "traffic streams." Selling traffic enabled individuals to make a profit by uploading someone else's malware to the server so that it could be used to infect individual users. There were a number of iFrame traffic sellers, and their ads comprised 64.8 percent of the traffic market, suggesting that there may be some saturation of this resource in the hacker community. Most traffic stream providers based their pricing on 1,000 infections, with an average cost of $110.84 per 1,000 systems. Sellers also explained that they could acquire infections in specific countries, and streams in the United States

tended to have the highest price overall. Mixed traffic from various countries around the world was sold at the lowest overall price.

The third most prevalent form of malware sold were programs designed to either conceal or encrypt malicious code so it could be sent and activated undetected by antivirus programs. These tools were largely referred to as cryptors, and comprised 19.1 percent of the total programs offered in the malware market. Most individuals sold cryptors (72.4 percent), suggesting that these tools are readily available across the market. The average price for a cryptor was $13.03, which is substantially lower than all other forms of malware. This may stem from the utility of cryptor software, since it is not necessary to facilitate an attack. Thus, individuals may be more likely to sell these programs at a lower price in order to attract prospective customers.

Hackers also offered compromised File Transfer Protocol (FTP) servers, which hold sensitive information including web page content, databases, email accounts, and other data. FTP resources comprised 11 percent of the overall malware market, and the price depended on the quality and quantity of data offered. The average cost of FTP resources was $271.66 per item, and there was a substantial demand for these services. In fact, 55 percent of the ads involved requests for specific servers or attacks. Thus, individuals could seek out someone to complete an attack on their behalf as a service, rather than take the time to complete this act on their own.

The final types of malware offered in the markets were bots, which constitute 6.5 percent of all malware bought and sold. Eight individuals offered either unique executables of bot programs or leased their ex-

isting infrastructure for spam distribution or as an attack platform. There was an equal demand for custom builds of bot malware, suggesting there was a strong demand to create and establish individual botnets. The average cost of bot services was also higher than that of iFrame resources at $322.27, but lower than the price of a Trojan horse. The generally small proportion of ads related to bot malware may stem from the sizeable proportion of botnet-driven services available in the market.

Cybercrime Services.

A diverse range of products enabling individuals to engage in a variety of cybercrimes was also available in the market, including Distributed Denial of Service (DDoS) attacks, spam, attacks, and hosting malicious content online (Table 2-3). The primary service offered in these forums related to the distribution of spam (32.4 percent), or unwanted messages to email accounts, ICQ numbers, and mobile phones. The largest subcategory related to spam involved email databases that could be used to create distribution lists for spam delivery. Database sales and requests comprised 46.5 percent of the overall spam threads. Twenty-four individuals across five of the sites sold databases for spam, with variable costs based on the number of emails and the country location for each address. The majority of these ads involved sales of existing databases (78.8 percent), suggesting that there is a substantial supply of email addresses in the marketplace.

Resources	Number Percent of Posts Total	Percent of Min. Total Price	Buy Max. Posts Price	Percent of Average Total Price	Sell post
DDoS*	29	13.01	0	0.0	29
	100.0	0.41	25	14.26	
Hacking Services 47.7	30	14.0	16	53.3	14
Compromise 45.5	11	36.7	6	54.5	5
Email/Passwords 47.4	19	63.3	10	52.6	9
Proxies and VPN 84.0	25	11.4	4	16.0	21
Proxy 80.0	20	80.0	4	20.0	16
VPN 100.0	5	20.0	0	0.0	5
Spam Services 80.3	71	32.4	14	19.7	57
Databases	33	46.5	7	21.2	26
78.80.50	100	45.43			
Services	23	32.4	3	13.0	20
87.00.50	700	50.91			
Tools	15	21.1	4	26.7	11
73.32.00	180	59.11			
Web Hosting and Services 90.6	64	29.2	6	9.4	58
Domains 91.7	24	37.5	2	8.3	22
Hosting	30	46.9	3	10.0	27
90.00.853.00	48.89				
Registration	10	15.6	1	10.0	9
90.09.00	150	50.17			
Total 82.2	219	100.0	39	17.8	180
* Due to variation in pricing, DDoS estimates are based on the stated hourly rate or an average hourly rate based on prices for 24-hour attack.					

Table 2-3: Cybercrime Services Offered in Hacker Forums.#

#Due to significant missing data, hacking services, domain sales, and VPN service pricing are not included here.

The second largest subcategory of spam involved ads related to the actual distribution of spam messages. The majority of these ads were sales-related (87 percent), suggesting that there was significant market saturation for this service. In addition, the price for spam distribution was generally low, with an average of $50.91. Sellers often described giving substantial discounts for sizeable deliveries, with the final cost for spam distribution at an average of less than .0001 cent per message. Thus, the distribution of spam is a relatively inexpensive service to acquire. Finally, there were 18 threads (21.1 percent) pertaining to scripts and mailing programs to facilitate the distribution of spam. The average price for spam tools was $59.11, which was the most expensive average price in this category. The proliferation of spam resources suggests that this is now a service-driven product for attackers, requiring minimal knowledge of computer systems and networks.

Individuals also offered services to support a variety of malicious web content. Hackers need resources to host malicious content, such as malware or cracked software; thus, web hosting and domain resources comprised 29.2 percent of the threads related to cybercrime services in these markets. There were 30 threads related to web hosting made by 22 different usernames in five forums. Additionally, there were only three requests (10 percent) for web hosting services, suggesting there is a substantial supply of providers available. Descriptions of the hosting services varied, depending on the amount of storage needed and their desired level of customer support. The price range for service was variable, ranging from 50 cents to $300, with an average of $48.89. Thus, hosting services could be obtained for a generally low price, depending on individual needs.

Sellers also indicated what content they would not host in their ads. In particular, child pornography and bestiality-related content were regularly viewed as unacceptable. Hosting this sort of content may pose too much risk for a provider, since many countries have legislation and law enforcement initiatives to combat child pornography.[44] By contrast, malware was often cited as acceptable demonstrating the key intersection between malware and cybercrime service providers.

There were also nine individuals offering domain name registration services in order to shield actor identities from law enforcement and domain registration authorities. Since 90 percent of these ads were sales-related, there is a clear supply of providers within the market. In addition, seven individuals sold web domains comprising 37.5 percent of these services. Thus, there appears to be a solid support infrastructure in place to aid hackers in developing, hosting, and maintaining malicious web content.

Hacking services comprised 14 percent of all service-related posts, and offered two primary forms of attack. The first was account-related, including obtaining passwords from email accounts, website log-in screens, and forums in a surreptitious fashion. Eleven ads appeared in this sample of threads, suggesting that there is a relatively high demand (45.5 percent) for assistance with hacking. The second form involved compromising or attacking a specific target. There were 19 requests for compromise assistance with a similar distribution of buyers (52.6 percent) to sellers (47.4 percent). Specifically, 10 individuals requested assistance in obtaining access to different systems, ranging from hacking FTP servers to acquiring spam databases from specific websites. Nine users also advertised hacking services to order, including attacking Google Page Ranking systems or acquir-

ing passwords for email accounts. These ads did not provide any substantive information on pricing, making it difficult to determine price metrics. At the same time, the prevalence of requests and available service providers demonstrates that these forums engender individuals to engage in forms of cybercrime that may exceed their technical capabilities.

A proportion of sellers also offered DDoS attack services for a fee. These services comprised 13 percent of the overall posts related to cybercrime services in these forums including 29 ads across four of the forums (see Table 2-3 for detail). Sellers offered to flood a web server with requests, rendering them unable to complete the information exchange necessary to fulfill user requests for content.[45] As a result, individuals are unable to access resources hosted on the server for the duration of the attack. DDoS providers regularly mentioned that their services were supported by botnets, as in an ad from one provider who noted "Large quantity of BOTS online, quantity grows every day. BOTs are located in different time belts [zones], which allows the DDoS to work 24 hours a day." All of the ads in this sample were sales-related, indicating that these providers have completely saturated the market and are readily accessible to interested parties. The average cost for DDoS services was $14.26 per hour, indicating that this service is also relatively inexpensive.

The final service identified in these forums offered access to proxy services and Virtual Private Networks (VPN). These resources conceal an individual's IP address and location, reducing the likelihood of detection while one is engaging in attacks or malicious activity online by routing packet traffic from the user's system through IP addresses on a server.[46] The majority of ads for both proxy and VPN services were sales-

related (84 percent), suggesting there is a significant supply of these services within the malware market. The pricing for proxy services were often tiered based on the total number of proxies purchased, though the average cost of proxy services was $42.52. There was, however, too much missing data to calculate the cost of VPN services. Nevertheless, these findings suggest that tools to conceal an actor's location were readily accessible through these forums.

Examining the Economics of Cybercrime.

The cost metrics derived from these forums makes it possible to consider the economic gains individuals may generate from the use of malware and cybercrime services. For instance, the significant number of Trojan horses advertised calls into question the costs and benefits of obtaining malware for attack purposes. Using the average costs for tools, it is possible that an attacker may spend $755.80 to acquire a Trojan horse ($742.77) and encryption software ($13.03) to increase the likelihood of infection. If the attacker were to attempt to target victims randomly in order to establish an infection, he or she may distribute infected files via spam email.[47] If a proportion of unsuspecting recipients open the file, this may immediately create a series of infections with minimal effort. The average cost to obtain an email address from an existing database or send a message is .0001 cents. Thus, it would cost approximately .0002 cents to obtain and send a message to a single email address using the providers identified in these forums. At this rate, an individual would spend $20 to send out 100,000 spam messages. Adding this figure to the software costs increases the overall offender investment for a malware campaign to $775.80.

Comparing this figure against the loss to business and industry indicates that there is a significant difference in the harm that a hacker can cause. The CSI report indicates that the cost of remediating a virus or worm infection is $40,141 per respondent.[48] Thus, the cost to a victimized business can be up to 53 times greater than the initial investment made by the offender. Simple destruction or infections do not, however, generate revenue for an attacker. Instead, they must obtain sensitive data through key-loggers or mass intrusions into database information. These losses can be exponentially worse, as the average cost for the theft of proprietary data was $241,000 per respondent, and $268,000 for stolen customer or employee data.[49] Thus, the profit margin for malware acquisition can be substantial, depending on the quality and quantity of data acquired.

Examining the cost of botnet establishment and mitigation reveals a similarly high profit margin. For example, if an individual pays the average cost of $322.27 to acquire botnet software, and an additional $200 to send out a million spam messages, his or her total investment is $522.27. Within corporate environments, the average cost to mitigate and remove a botnet infection was $345,600 per respondent.[50] Using this metric, if a bot herder were able to establish 10 nodes across five companies, it is feasible that this might cause over $1.7 million dollars in damages. In addition, he or she could regain the initial investment costs by leasing their bot infrastructure to engage in a single 37-hour DDoS attack if he or she charged the average rate of $14.26 per hour. Alternatively, the bot herder would need to send out at least 5.2 million spam messages through his or her infrastructure at .0001 cents per message to earn back the investment.

A similar rate of return can be found with iFrame campaigns. If an offender wanted to establish his or her own iFrame service over a 6-month period, the offender may have to acquire three resources. First, the offender may spend up to $450 to purchase the most expensive iFrame kit available in the market. Second, if the offender does not have the capacity to compromise and install the kit on a server, he or she may identify a third-party web-hosting service for the kit. In this scenario, the offender would pay an average of $48.89 to host the malware each month for a total of $293.34. In addition, a weekly spam campaign may prove useful in order to drive prospective victims to the website. In this scenario, the individual would have to spend $4,800 to send out one million spam messages each week at $200 over a 24-week period. In total, an offender using each of these services, including paying the maximum for an iFrame kit, would spend $5,543.34 over a 6-month period.

If the attacker is successful and generating traffic, he or she may choose to lease out the infrastructure to generate a profit. Using the average cost metric for traffic sales at $110.84 per 1,000 infections, the offender would need to generate consistent traffic and infect at least 50,000 systems from mixed traffic to regain his or her initial investment. It is unclear from the posts and comments from sellers how long it takes to generate such traffic, though the sheer number of traffic resellers suggests that it is possible to establish and maintain such an infrastructure over time. Thus, there appears to be some substantial return on investment for iFrame operators who are willing to make operational expenditures in their infrastructure over time.

Since malware requires time, money, and some skill to use properly, some offenders may opt to lease

services from providers in the market. For instance, the availability of DDoS services in the forum suggests that individuals may be interested in paying for an attack rather than creating and maintaining their own botnet. Since the average cost of DDoS services in these forums was $14.26 per hour, a botmaster may generate an estimated $342.24 per day for a 24-hour attack. It is also clear that lengthy attacks decrease productivity and increase financial harm for the target. Thus, an offender may spend $1,026.72 for a 3-day attack based on a 72-hour rate at $14.26 per hour. This is most likely an overestimate, as DDoS providers offered discounted prices based on the length of an attack. Regardless, victims lost an average of $14,889.69 from DDoS attacks in 2006.[51] This is a substantial impact that well exceeds the initial cost paid by the offender.

A successful DDoS attack does not, however, generate any observable economic gain for the individual who ordered the attack. As a consequence, it is necessary to consider how an individual may use a DDoS provider to generate a substantial profit. To that end, a number of hackers blackmail businesses by threatening to take their systems offline using DDoS attacks. Prospective targets often pay ransoms to avoid a loss of service or embarrassment over a prospective attack.[52] In fact, CSI respondents paid an average of $824.74 to avoid or stop attacks in 2006.[53] To that end, a botmaster or his or her prospective client could readily generate a profit by simply threatening to attack a company. It is unclear how long an attack would need to take place to ensure payment of a ransom, though if an offender had to pay for a 24- to 48-hour attack, he or she could still generate a profit of approximately $150 or more based on the average business cost. The

profit margin increases substantially if an attack ends within a matter of hours. Thus, blackmail may be an extremely useful way to utilize DDoS services.

The same profit margins are evident in the use of spam providers. Since an individual attacker may spend approximately .0002 cents to obtain and send a message to a single email address, his initial investment is quite small. The likelihood of successful responses is equally low, since there are myriad security tools designed to filter or block spam messages from reaching the end user.[54] Depending on the scheme employed, however, an attacker need only affect a small number of users in order to make a profit. For instance, advance fee fraud ("419 scams") is one of the most economically rewarding spam schemes.[55] In these frauds, the sender poses as a banker, barrister, or wealthy heiress seeking assistance to move a large sum of money out of the country. The senders say they need the assistance of a trustworthy foreigner to help them complete this transaction due to various legal or familial issues. All that the victim needs to do is provide his or her name, address, and banking information, and in return that person can retain a portion of the total dollar amount described.[56]

Though it is unknown how many individuals who receive these messages actually respond to the fraudulent solicitation, estimates state that between 1 and 3 percent of all recipients are victims.[57] In addition, data from the Internet Crime Complaint Center suggest that victims lose an average of $1,922.99 when participating in the scheme.[58] With this in mind, if an offender spends $200 to send out one million advance fee fraud messages, he may receive an overly conservative response rate of .00005, or 50 recipients. Using the IC3 average dollar loss for this sort of scam, a cy-

bercriminal could earn $96,149.50 from these 50 respondents, which is 480 times their initial investment. Though these scams require a significant degree of human interaction with the victim and labor in order to be successful, the profit margin is still exceedingly high. Thus, spam distribution services are a key resource in the larger marketplace for cybercrime, and its low price may reflect the difficulty in effectively targeting and ensuring a high rate of return from an investment.

DISCUSSION AND CONCLUSIONS

This monograph sought to explore the market for malicious software and cybercrime services in order to understand the price and availability of resources, as well as the relationship between the price paid for services and the cost experienced by victims of these crimes. The findings suggest that myriad tools and services are available and sold for profit in an open market environment that encourages and supports cybercrime.[59] Individuals could procure spam, DDoS attack services, Trojan horses, iFrame exploit infections, web hosting, and various other resources at relatively low prices from the forums in this sample. Several of these services also depend on botnets for functionality, demonstrating the prominence of this malware in cybercrime.

The pricing structure and observed supply and demand for different resources suggest that these markets have made it easier for individuals to engage in computer intrusions and attacks. Participants in these forums no longer need to cultivate high levels of skill and technological sophistication, since they could readily request assistance to compromise email

accounts or servers, and lease existing infrastructure created by more skilled actors.[60] In fact, botmasters appear to recognize the value of their infrastructure and offer services enabled by their infrastructure to generate a profit. In turn, the marketplace appears to operate largely as a service economy in which individuals can select from multiple providers based on price and customer service in order to complete an attack that may well exceed their overall level of knowledge.

Examining the return on investment for engaging in various cybercrime schemes also suggests that attackers can generate a substantial profit or cause damage that far exceeds their initial investment. In fact, some of the least expensive products, such as spam distribution, may provide a massive gain for the individual attacker and a slight profit for the service provider. In addition, individuals who own and operate bot and iFrame infrastructure may generate a substantial profit over time by leasing their services. Those who lease or pay fees for service may, however, have a reduced risk of detection from law enforcement because they do not actually compromise systems or have a significant relationship to the affected systems. In addition, their profit margins may be slightly higher due to minimal labor and maintenance costs. Their limited skill set may diminish their overall earning lifetime capacity, since they may never cultivate the necessary skills to create and complete their own intrusions and attacks.

The findings of this exploratory analysis must be interpreted with caution due to the inherent limitations of the data. Specifically, the victimization statistics used in this analysis have extremely limited generalizability and are most likely biased samples representing small proportions of the total population. In addition, the CSI reports indicate that less than a

third of all incidents that occur are reported to law enforcement.[61] Thus, there is a critical need for increased reporting of cybercrime and improved measures for corporate and individual losses. The paucity of data in this area makes it difficult to understand or estimate the efficacy of cyber attacks and the overall economic gains made by offenders. Increased clarity in reporting is vital to move criminological and information security research beyond speculation, and to move case studies into quantifiable areas of loss calculation. In turn, one can better understand the economics of both attack and defense.

Additionally, the data used for the forum analyses derive from publicly accessible forums that are over 3 years old. The content of the data may be radically different from the resources available in private forums, which require registration and membership vetting in order to access posts.[62] In addition, the rapid changes in technology make it difficult to extrapolate these findings to the current resources that may be available in the malware marketplace. Finally, this analysis used a small proportion of threads from multiple forums, which may limit the amount of malware and services observed. Thus, there is a need for greater research to understand the practices and content of malware markets over time. Longitudinal research can provide insights into the shifts in available resources, and identify any declines or spikes in the price for a good or service. Such research can also identify new trends in malware and attack vectors, improving the response capabilities of law enforcement and security professionals. Future research should also develop comparative samples of threads from open and closed forums to consider variations in the products that can be acquired by those with greater penetration into

and status in the hacker community. In turn, this can substantially improve our understanding of the skill and ability present in the hacker community and its operational capabilities.

ENDNOTES - CHAPTER 2

1. S. Furnell, *Cybercrime: Vandalizing the Information Society,* Boston, MA: Addison-Wesley, 2002; Y. Jewkes and K. Sharp, "Crime, Deviance and the Disembodied Self: Transcending the Dangers of Corporeality" in Y. Jewkes, ed., *Dot.cons: Crime, Deviance and Identity on the Internet,* Portland, OR: Willan Publishing, 2003, pp. 1-14; D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age,* Cambridge, UK: Polity Press, 2007.

2. S. W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State,* New York: Oxford University Press, 2008; D. E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," J. Arquilla and D. F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica, CA: Rand, 2001; T. J. Holt and E. Lampke, "Exploring Stolen Data Markets On-Line: Products and Market Forces," *Criminal Justice Studies,* Vol. 23, 2010, pp. 33-50; The Honeynet Project, *Know Your Enemy: Learning About Security Threats,* Boston, MA: Addison-Wesley, 2001.

3. T. J. Holt, "Examining a Transnational Problem: An Analysis of Computer Crime Victimization in Eight Countries from 1999 to 2001," *International Journal of Comparative and Applied Criminal Justice,* Vol. 27, 2003, pp. 199-220.

4. Brenner, *Cyberthreats;* Denning, "Activism, Hactivism, and Cyberterrorism"; T. J. Holt, J. B. Soles, and L. Leslie, "Characterizing Malware Writers and Computer Attackers in Their Own Words," paper presented at the International Conference on Information Warfare and Security, Peter Kiewit Institute, University of Nebraska Omaha, NE, 2008.

5. *Ibid.*

6. Brenner, Cyberthreats; Denning, "Activism, Hactivism, and Cyberterrorism"; E. V. Kapersky, *The Classification of Computer Viruses,* Bern, Switzerland: Metropolitan Network BBS Inc., 2003, available from *www.avp.ch/avpve/classes/classes.stm*; P. Szor, *The Art of Computer Virus Research and Defense,* Upper Saddle River, NJ: Addison-Wesley, 2005; R. W. Taylor, E. J. Fritsch, J. Liederbach, and T. J. Holt, *Digital Crime and Digital Terrorism,* 2nd Ed., Upper Saddle River, NJ: Pearson Prentice Hall, 2010.

7. Taylor *et al*., *Digital Crime and Digital Terrorism.*

8. B. Chu, T. J. Holt, and G. J Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line,"* Washington, DC, National Institute of Justice, 2010, available from *www.ncjrs.gov./pdffiles1/nij/grants/230112.pdf*; J. Franklin, V. Paxson, A Perrig, and S. Savage, "An Inquiry Into the Nature and Cause of the Wealth of Internet Miscreants,"paper presented at CCS07, October 29-November 2007; T. J. Holt and E. Lampke, "Exploring Stolen Data Markets On-Line: Products and Market Forces," *Criminal Justice Studies,* Vol. 23, 2010, pp. 33-50; Honeynet Research Alliance, *Profile: Automated Credit Card Fraud,* 2003, available from *www.honeynet.org/papers/profiles/cc-fraud.pdf*; R. Thomas and J. Martin. 2006. "The Underground Economy: Priceless," *:login* Vol. 31, 2003, pp. 7-16.

9. *Ibid.*

10. T. J. Holt and M. Kilger, "Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers," *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing,* 2008, pp. 67-78

11. Furnell, *Cybercrime;* T. J. Holt, "Subcultural Evolution? Examining the Influences of On- and Off-Line Experiences on Deviant Subcultures," *Deviant Behavior,* Vol. 28, 2007, pp. 171-198; Holt *et al*., "Characterizing Malware Writers"; T. Jordan and P. A. Taylor, "A Sociology of Hackers," *The Sociological Review,* Vol. 46, 1998, pp. 757-780; P. A. Taylor, *Hackers: Crime in the Digital Sublime,* New York: Routledge, 1999.

12. *Ibid.*

13. Holt, "Subcultural Evolution?"; Holt and Kilger, "Techcrafters and Makecrafters"; The Honeynet Project, *Know Your Enemy;* Jordan and Taylor, "A Sociology of Hackers."

14. *Ibid.*

15. Holt, "Subcultural Evolution?"; T. J. Holt and M. Kilger, "Techcrafters and Makecrafters"; Holt *et al*., "Characterizing Malware Writers"; The Honeynet Project, *Know Your Enemy;* Jordan and Taylor, "A Sociology of Hackers."

16. The Honeynet Project, *Know Your Enemy*; G. R. Meyer, *The Social Organization of the Computer Underground,* Unpublished Masters Thesis, 1989, available from *www.csrc.nist.gov/secpubs/hacker.txt*; Taylor, *Hackers.*

17. Franklin *et al*., "An Inquiry Into the Nature and Cause of the Wealth of Internet Miscreants"; Holt and Lampke, "Exploring Stolen Data Markets On-Line"; Honeynet Research Alliance, *Profile: Automated Credit Card Fraud,* 2003; Thomas and Martin, "The Underground Economy: Priceless."

18. *Ibid.*

19. *Ibid.*

20. Chu *et al*., *Examining the Creation, Distribution, and Function of Malware On-line* ; Franklin *et al*., "An Inquiry Into the Nature and Cause of the Wealth of Internet Miscreants"; Honeynet Research Alliance, *Profile: Automated Credit Card Fraud,* 2003; Thomas and Martin, "The Underground Economy: Priceless."

21. Brenner, *Cyberthreats;* Furnell, *Cybercrime*; Holt, "Examining at Transnational Problem"; H. Stambaugh, D. S. Beaupre, D. J. Icove, R. Baker, W. Cassady, and W. P. Williams, *Electronic Crime Needs Assessment for State and Local Law Enforcement,* Washington, DC: National Institute of Justice; Taylor *et al*., *Digital Crime and Digital Terrorism.Wall, Cybercrime*.

22. *Ibid.*

23. Taylor *et al*., *Digital Crime and Digital Terrorism.*

24. Holt, "Examining at Transnational Problem"; Taylor *et al*., *Digital Crime and Digital Terrorism.*

25. *Ibid.*

26. Computer Security Institute, *Computer Crime and Security Survey,* 2008, available from *www.cybercrime.gov/FBI2008.pdf.*

27. *Ibid.*

28. Internet Crime Complaint Center, *IC3 2008 Internet Crime Report*, available from *www.ic3.gov/media/annualreport/2008_IC3Report.pdf*.

29. See Chu *et al*., *Examining the Creation, Distribution, and Function of Malware On-line* for additional detail.

30. *Ibid.*

31. C. Hine, ed., *Virtual Methods: Issues in Social Research on the Internet,* Oxford, UK: Berg, 2005; T. J. Holt, "Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using On-Line Data," *Journal of Criminal Justice Education,* Vol. 21, 2010, pp. 466-487.

32. Thomas and Martin, "The Underground Economy: Priceless."

33. The graduate translator provided translations from seven forums: six threads from forum 02; 150 from forums 03 and 04; 138 from forum 05; 25 from forum 06; one from forum 07; and one from forum 09.

34. See Chu *et al*., *Examining the Creation, Distribution, and Function of Malware On-line* for additional detail.

35. Computer Security Institute, *Computer Crime and Security Survey,* 2008.

36. Internet Crime Complaint Center, *IC3 2008 Internet Crime Report.*

37. Computer Security Institute, *Computer Crime and Security Survey,* 2007, available from *www.cybercrime.gov/FBI2007.pdf*.

38. S. Gordon, *Virus and Vulnerability Classification Schemes: Standards and Integration,* Symantec Security Response, 2003, available from *enterprisesecurity.symantec.com/content/knowledgelibrary.cfm?EID=0*; Holt *et al*., "Characterizing Malware Writers"; The Honeynet Project, *Know Your Enemy;* Jordan and Taylor, "A Sociology of Hackers."

39. *Ibid.*

40. *Ibid.*

41. It must be noted that two individuals sought out individuals who could identify zero-day vulnerabilities in systems so that they could be exploited for an attack. A third individual was selling information about a bug within the market. These posts, however, comprise only 1.2 percent of all malware-related posts, and are not discussed in detail in the larger text.

42. N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose, "All Your iFRAMEs Point to Us," *Proceedings of the 17th Conference on Security Symposium*, 2008, pp. 1-15.

43. Provos *et al*., "All Your iFRAMEs Point to Us."

44. Taylor *et al*., *Digital Crime and Digital Terrorism.*

45. Brenner, *Cyberthreats;* Taylor *et al*., *Digital Crime and Digital Terrorism;* Wall, *Cybercrime.*

46. *Ibid.*

47. *Ibid.*

48. Computer Security Institute, *Computer Crime and Security Survey,* 2008.

49. *Ibid.*

50. *Ibid.*

51. Since these data are not available in the 2008 report, this statistic is derived from the Computer Security Institute, *Computer Crime and Security Survey,* 2007.

52. Brenner, *Cyberthreats;* Taylor *et al*., *Digital Crime and Digital Terrorism.*

53. Computer Security Institute, *Computer Crime and Security Survey,* 2007.

54. T. J. Holt and D. C. Graves. "A Qualitative Analysis of Advanced Fee Fraud Schemes," *The International Journal of Cyber-Criminology* Vol. 1, 2007, pp. 137-154.

55. Holt and Graves, "A Qualitative Analysis"; Taylor *et al*., *Digital Crime and Digital Terrorism*.

56. *Ibid.*

57. *Ibid.*

58. Internet Crime Complaint Center. *IC3 2008 Internet Crime Report.*

59. Franklin *et al*., "An Inquiry Into the Nature and Cause of the Wealth of Internet Miscreants"; Holt and Lampke, "Exploring Stolen Data Markets On-Line"; Honeynet Research Alliance, *Profile: Automated Credit Card Fraud,* 2003; Thomas and Martin, "The Underground Economy: Priceless."

60. Holt and Kilger, "Techcrafters and Makecrafters"; Jordan and Taylor, "A Sociology of Hackers."

61. Computer Security Institute, *Computer Crime and Security Survey,* 2007.

62. Holt, "Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using On-line Data."

CHAPTER 3

THE EMERGENCE OF THE CIVILIAN CYBER WARRIOR

Max Kilger

Note: The information in the chapter derives from a current study by the author and other researchers.

INTRODUCTION

The advantages gained from making a concerted effort to develop an understanding of an adversary are difficult to overstate. Whether the analysis occurs through a psychological, social-psychological, anthropological, or strictly sociological perspective, the ability to "know your enemy" is a critical component of a comprehensive strategy to protect assets actively and proactively within critical infrastructures. While the deployment of defensive technical barriers, such as firewalls, intrusion detection systems, etc., are necessary actions to provide sufficient protection for digital networks that hold sensitive data or have supervisory control and data acquisition (SCADA) functions, the ability to develop a taxonomy of the perpetrators' motivations behind the vectors within the cyber-threat matrix can assist in making a more accurate assessment of the threat each type of actor presents to specific elements within specific infrastructures. In addition, developing a foundational understanding of the motivations of malicious online actors facilitates the ability to construct plausible future threat scenarios that may emerge in the near- to mid-term timeline.

This chapter will start by providing some basic background for a schema that outlines six hypothesized motivational factors to encourage malicious online behaviors. The focus of the discussion will then turn to one specific motivation and within that motivation, one specific archetype—the civilian cyber warrior—that poses perhaps the most significant emerging threat to domestic and foreign critical infrastructures. Finally, the chapter will conclude with an analysis of some preliminary data in an ongoing study that investigates some of the factors that may relate to this specific type of online malicious actor.

THEORETICAL BACKGROUND

Over the years, there have been a number of attempts to create taxonomies for malicious online actors. Many of these taxonomies rely partially upon the factor of skill and expertise possessed by the actor in various operating system platforms, networking protocols, digital hardware functionality, programming languages or shell scripting, or knowledge of specific system security strategies. These taxonomies also to some extent rely upon the type of target that the malicious actor specializes in. The Chiesa study utilized a combination of skill and target type as well as motivational attributes such as political reasons, escape from family situations, and conflict with authority as taxonomy criteria for classifying malicious online actors.[1] The Rogers study described two different dimensions—skill level and motivation—to build a multiclass taxonomy of hackers. His hacker class taxonomy includes classes of hackers such as petty thieves, old guard hackers, professional criminals and, more recently, political activists.[2] In *Cyber Adversary Charac-*

terization: Auditing the Hacker Mind, Tom Parker, Eric Shaw, Ed Stroz, Mathew Devost, and Marcus Sachs place emphasis not only on the properties of the attacker, but their model also examines in detail other factors such as the perceived probability of success of attack, perceived probability of detection and, other attack-associated metrics.[3]

The classification schema in this chapter is one developed by this author, Ofir Arkman, and Jeff Stutzman.[4] This schema—labeled MEECES[5]—describes six motivations for malicious online actors: Money, Ego, Entrance to social group, Cause, Entertainment, and Status. Money, of course, is the most obvious and self- explanatory motivation. The significant extent to which financial institutions have placed financial resources, such as checking, savings, credit lines, credit cards, and other components of the banking system online, has put tremendous amounts of financial capital at potential risk. The vast potential for wealth that has been exposed to the Internet has attracted a plethora of malicious actors from a number of different backgrounds. In addition to the malicious actors who were already motivated by financial gain, the magnitude of the financial resources available has likely also tempted other skilled individuals who might otherwise not have been spurred to action by this motivation.

Further, there are geo-economic factors at work here as well. Perhaps for the first time, individuals in countries where the standard of living is lower in comparison to first-world industrialized countries, the potential for finding gainful employment is uncertain, and, in some cases, the economic climate has forced highly educated individuals into underemployment, the allure of the possibility of gaining access to and

illegally acquiring significant sums of money is great. This has also led to the migration of more traditional organized crime members into the cyber environment. This infusion of sometimes technically unsophisticated criminals into cybercrime has also changed the dynamics of cybercrime gangs.

This was not always the case. During the early years of the hacking community, individuals who used their technical skills for personal monetary gain were shunned by the rest of the community. It was considered a violation of the code of ethics for hackers to deploy their skills to steal money or financial resources. This norm violation is still in place today in the hacking community, but it has been substantially weakened by the increasing number of skilled individuals who utilize their expertise for unlawful financial gain as well as the influx of a more traditional criminal element.

Ego is the second motivation in the schema.[6] Ego motivates individuals through the feelings of accomplishment that accompany overcoming a particularly difficult technical obstacle. Actions such as getting a hardware device to do something that was thought impossible, writing a complicated piece of code that intelligently adapts to situations, or bypassing a sophisticated security system such as a firewall or intrusion detection system are all examples of behaviors associated with the ego motivation. Note that the actions do not necessarily have to be malicious in nature—even difficult obstacles that are overcome in the course of lawful employment relate to this motivation.

The third motivation for malicious online acts is entrance to a social group. Hacking groups are more or less status-homogenous in terms of technical expertise.[7] While there is likely a leader of the hacking group

who possesses somewhat higher levels of skill and expertise, the majority of the individual group members have somewhat similar levels of technical proficiency, although it is likely that individuals are proficient in different areas, such as different operating systems or programming languages. This means that in order for an individual to join the group, that individual must possess levels of expertise similar to the members of the group he or she wishes to join. The key question is, how do prospective candidates demonstrate their level of expertise? It is almost certain that the members of the hacking group will not consider the word of the candidate at face value. One of the pathways in which the prospects can demonstrate their skills is writing an elegant piece of malicious code. Once written, the code goes to the hacking group, which in turn evaluates its function and programming aesthetic. If the group feels the code displays at least the minimum skill level necessary to belong to the group, it will admit the candidate. The code itself is often given to the members of the group as a sort of "initiation fee."

Cause is the fourth motivation for malicious online actors. Cause is defined as the use of technical expertise or skill in the pursuit of political, social, cultural, ideological, religious, or nationalistic goals.[8] Hacktivism is one of the more common types of malicious online behavior. The most common hacktivism events often take the form of website defacements. Examples of hacktivism include the long-running attack by the group Anonymous on the Church of Scientology starting in 2008,[9] attacks on Australian government websites by individuals upset by government plans to censor the Internet,[10] and the continuing saga of the Wikileaks exposure of hundreds of thousands of classified documents.[11] Cause may also take the form

of individuals launching a cyber attack against assets of a foreign country or even their own country in response to government actions that the individuals find objectionable. This specific instance of cyber attacks motivated by cause defines the actions of the civilian cyber warrior.

Entertainment is probably the least known and least common motivation for malicious online acts. Its origins probably emanate from the early beginnings of the hacker community. During these early days, humor often served a functional purpose in sharing common values by constructing humorous stories and tales that contained plays on technical terms and concepts. Humor also functioned as a mild form of social control—playing a humorous prank or joke on another hacker or system administrator often brought a bit of humility to the victim and returned a sense of balance to the social situation. Compromising a machine and leaving a humorous taunt directed at its system administrator for the lack of security controls at the compromised machine was a not-too-uncommon event.

Entertainment as a motivation for acts—malicious or not—appeared to decline for some time after the early years but has recently made a resurgence. This increase in incidences of the entertainment motivation may be due in part to the preponderance of potential victims—the influx of less technical individuals into the hacking community as well as the tidal wave of technically challenged people pouring onto the web has likely facilitated the popular return of this motivation.

The final motivation is that of status. The hacking community can be described as a strong meritocracy.[12] The position of individuals in the status hierarchy of their hacking group depends upon the level of techni-

cal skills and expertise they possess relative to other members of the group. The higher the level of expertise, the higher the status of the individual is in that hacking group. Note that this positive relationship is also salient when an individual in one hacking group is compared to another hacker in the larger hacking community. The person with the higher level of skills possesses the relatively higher status.

As was the case with the entrance to social group motivation, the validation of one's expertise and thus one's status within the hierarchy can be difficult to achieve. The difficulties in proving authorship of an elegant piece of code, especially to someone outside one's normal hacking group, make this avenue of validation more problematic. One avenue that does appear to work is the acquisition of status through contests of skill, which often occurs at hacker conventions. Typically these are some variation of "capture the flag" contests, in which the objective of the contest is to use your hacking skills and expertise to compromise computer systems in order to typically search out and find a catch phrase or encryption key—the possession of which provides evidence that the contestant possesses the requisite knowledge and skill to compromise the computer and acquire the flag.

A similar exercise involving employment of malicious online acts in the wild can also lead to status acquisition and validation. One example of this is the acquisition of secret documents as a means to gain status. In this situation, one assumes that the secret documents have such value that they are heavily protected by a number of sophisticated means often in some sort of defense in-depth configuration. In order to come into possession of electronic copies of these secret documents, the malicious actor must use a significant

amount of technical expertise and skill to break into the server without detection and exfiltrate copies of the secret documents.

One interesting consequence of obtaining status this way is that in the end, status exists within the possession of the secret documents. That is, these documents are status objects—they are items that in and of themselves impart status and have status. If the malicious actor publicizes or distributes the secret documents to his or her friends, then that actor in effect expends the status value that these documents have. Once they become collectively owned, they lose their status value and, consequently, the malicious actor loses status at the same time. This is one reason why, perhaps, in the case of Wikileaks, the principal actor in the incident—Julian Assange—was loathe to disclose all of the documents at once because he would have expended all of their status value and would have subsequently lost most of the status that was associated with their exclusive possession.

THE EMERGENCE OF THE CIVILIAN CYBER WARRIOR

The past few years have been witness to a significant focus on cyber-based threats. The realization of the vulnerability of the nation's critical infrastructures and the military to digitally based attacks has generated a flurry of interest and activity both by parties with substantial interests in the area—such as governmental entities carrying out national security directives—and within the military, where they deploy not only defensive strategies, but offensive strategies as well. The cyber arena has turned into the next battlefield.

The focus on the malicious actors targeting critical infrastructures in most of these scenarios has been directed at the elements of foreign nation-state intelligence organizations or military forces and previously identified foreign terrorist groups.[13] What has often been lost in the rush to protect critical infrastructures from digital attack is the idea that isolated individuals or small groups of individuals are, to a great extent, an unseen emerging threat vector to the nation's critical infrastructure.

What are the possible social dynamics behind this emerging threat? One central theme may be how technology is driving shifts in power relationships between nation-states and individuals. Foucault discusses at length the relationship between knowledge and power.[14] His argument might extend to the power-knowledge relationship within the possession of expert knowledge of technical aspects of integral digital control and communications systems embedded within national critical infrastructure. As Mathews observes, "information technologies disrupt hierarchies, spreading power among more people and groups."[15]

The key concept here is that perhaps for the first time in history, a regular civilian can effectively attack a nation-state—in this case through a cyber attack on some component of that nation-state's critical infrastructure. "Effective" in this sense means that the attack can cause significant widespread damage and has a reasonably high probability of success and a low probability of the perpetrator being apprehended. While some might argue that political assassination might already be an existing instance of this, the questions surrounding the probability of success and certainly around avoiding being apprehended make this less likely to be the case.

An example of how this shift in the balance of power between nation-state and individual may help the reader grasp the magnitude of the social-psychological shifts in thinking. Imagine that you are a citizen of country A and the government of country B is the direct causal agent for some significant actions that negatively affect your homeland and its people. Prior to the emergence of the Internet, an individual might write a letter to the President of country B and tell him or her why they object to Country B's actions. What is the likely result? Probably nothing happens that changes the actions or consequences of country B.

So this individual joins individuals who have similar feelings and meet at the embassy of country B to protest. What is the likely outcome of this action? The individual is likely to be arrested or injured by the crowd or police action without it having any real effect on country B. As the next step in the escalation, this individual cashes out his or her bank account and travels to country B, obtains some explosives and plots to damage a government building. Again, the outcome is likely not to be favorable. There is a reasonable chance that the individual will be detected by intelligence agents and/or law enforcement and arrested before he or she has the opportunity to carry out the plan. Another possible outcome is that the individual ends up blowing him or herself up while preparing the explosive device. Finally, even if the individual manages to execute the plot, he or she is likely to be arrested and, while the damage to the target might be significant, in an overall sense the nation-state and people of Country B are intact.

This example just reinforces the idea that a cyber attack on a national asset is a much more attractive path, because it likely has significantly more favorable

outcomes to the malicious actor. If this is the case, then why haven't widespread incidents involving isolated individuals launching serious cyber attacks against national critical infrastructures occurred more often? Rogers suggests that it is because criminals have been "reluctant to cross certain ethical boundaries" that perhaps terrorists are willing to cross.[16] A more likely reason is that this potential shift in the power relationship between individuals and the nation-state has just not reached cultural salience. As the salience of the shift in power balance diffuses into the more general population, in combination with the development and distribution adaptation of sophisticated cyber attack tools for less technical end users, the pool of potential malicious attackers who pose threats to online systems and critical infrastructures steadily grows.

Eventually one may begin to see the consequences of this sequence of events; hence, the importance of understanding more about the potential emerging threat from the civilian cyber warrior. One of the first things that one might want to investigate in the chain of actions for a terrorist act is the initial starting point where individuals begin thinking about and rehearsing in their minds the nature, method, and target for the terrorist attack. What does one know about the propensity of individuals in the more general population to contemplate a terrorist act? What would be the magnitude or severity of damage that someone might consider justified? There is a paucity of research focusing on this area, especially from a cyber attack perspective. The following analyses are some preliminary results from a recent, ongoing study of severity predictors of an attack on a foreign country's critical infrastructure, and the severity levels of an attack directed at one's own homeland.

METHODOLOGY

The following analyses use preliminary data collected from a study by Holt and Kilger.[17] The sample for this study comes from undergraduate and graduate students at a large Midwestern U.S. university. Students received an email inviting them to participate in the study; embedded within the email was a link to the online survey. A preliminary sample of 357 students completed the survey for the purposes of this analysis. The survey itself consisted of: measures for the level of technical expertise; hours spent online; questions about previous history of ethical conduct using computers; nationalism; country considered to be one's homeland; out-group antagonism measures; demographics; and other relevant measures.

The study design was a 2 x 2 factorial design. The first factor is type of attack—cyber or physical. One of the objectives of the study was to investigate the potential relationship between cyber and physical attacks on critical infrastructure. The second factor was the target country. The target country could be a nation-state that the respondent did not consider to be his or her country or homeland—that is, a foreign target. Alternatively, the target country could be a nation-state that the respondent stated was his or her homeland or own country—that is, a homeland target. The homeland target was felt to be especially relevant in gaining some understanding of which independent variables might be associated with an attack on one's own domestic critical infrastructure. The study design appears in Table 3-1.

	Target of Attack	
Type of Attack	**Foreign Country**	**Homeland**
Cyber	Cell 1	Cell 2
Physical	Cell 4	Cell 3

Table 3-1. Dependent Variable Design.

The dependent variable was the severity of the attack that the respondent felt was appropriate for the individual scenario outlined in each of the four study cells. The scenario for a physical attack on a foreign country had the following instructions to the respondent:

> Imagine that the country of Bagaria has recently promoted national policies and taken physical actions that have had negative consequences to the country that you most closely associate as your home country or homeland. These policies and actions have also resulted in significant hardships for the people in your home country. What actions do you think would be appropriate for you to take against Bagaria given their policies and physical actions against your home country? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

Following the instructions was a set of possible actions the respondent could take. These actions were ordered from lowest severity—doing nothing—to the highest severity response—in this case, travel to Bagaria and damage a government building with an explosive device. There were eight categories in all. Note that respondents were instructed to assume that

they had the abilities to carry out any of the responses. This was to ensure that they did not reject any category response because they felt they did not have the skills or logistics to carry out that action successfully. Also note that respondents were allowed to select more than one action. This conformed potential reactions to real-world situations in which multiple attacks might be contemplated as well as to provide for more layers of complexity within the dependent variable.

The cyber attack scenario had similar instructions but, of course, had a different set of category responses available for the respondent to select. Here are the instructions for the second part of the foreign target country scenario:

> Aside from physical activity, what online activities do you think would be appropriate for you to take against Bagaria given their policies and physical actions against your home country? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

There were nine possible response categories ordered by level of severity, ranging from doing nothing to compromising a nuclear power plant with the subsequent release of a small amount of radiation. Again, respondents could assume they had the skills necessary to carry out the attack. They also could—as was the case for physical attack responses—select multiple attacks with differing levels of severity.

The remaining two cells of the design involved retaliation against the respondent's home country infrastructure (e.g., domestic terrorist attack) for actions that his or her homeland or home country had taken

against its own people. Here are the scenario instructions for the physical homeland attack:

> Imagine that the country that you most closely associate as your home country or homeland has recently promoted national policies and taken physical actions that have had negative consequences to your home country. These policies and actions have resulted in significant hardships for the people in your home country. What actions do you think would be appropriate for you to take against your home country given their policies and physical actions? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

These instructions were followed by the same set of eight potential responses as found in the physical attack measure and ordered once again by severity from low to high. Similarly, the cyber attack scenario on the respondent's own homeland or home country had the following instructions:

> Aside from physical activity, what online activities do you think would be appropriate for you to take against your home country given their policies and physical actions? You may choose as many actions as you think the situation warrants. In this scenario, you may assume that you have the necessary skills to carry out any of the actions below.

Again, these scenario instructions had the same set of cyber attack responses as was the case for the cyber attack against Bagaria's critical infrastructure.

Because all of the respondents provided answers to each of the four scenarios, this study design facilitated the examination of a number of important variations in the nature of the attack of an individual

on a nation-state as well as the potential relationship between the severity of potential cyber attacks and physical attacks.

RESULTS AND DISCUSSION

The results presented in this chapter are preliminary, because of the fact that more data are being collected for the study. In addition, the authors of the study are still engaged in developing and testing a number of multivariate statistical models incorporating a number of independent predictor variables available in the data. However, because of the unique nature of this study, some initial descriptive results and simple univariate tests will be reported here.

First, an examination of the frequency distribution for the dependent variables for each of the four cells in the study is useful. The response frequencies for a physical attack on a foreign country appear in Table 3-2.

Action	Percent Response
Do nothing—let your country work it out on its own	37.8%
Write a letter to government of Bagaria protesting their actions	53.6%
Participate in a protest at an anti-Bagaria rally	56.6%
Travel to Bagaria and protest at their country's capitol building	23.8%
Travel to Bagaria and confront a Bagarian senior government official about their policies	20.0%
Travel to Bagaria and sneak into a military base to write slogans on buildings and vehicles	1.3%
Travel to Bagaria and physically damage an electrical power substation	2.6%
Travel to Bagaria and damage a government building with an explosive device	0.9%

Table 3-2. Physical Attack Frequencies on Foreign Country.

Fewer than 38 percent of respondents felt that doing nothing was an appropriate response to the scenario. The most popular responses appeared to be writing a letter (53.6 percent) or protesting at a rally against Bagaria (56.6 percent). Interestingly, a nontrivial percentage of respondents would consider traveling to Bagaria to participate in some sort of civil disobedience—either protesting in the capitol (23.8 percent) or confronting a senior government official (20.0 percent). Finally, a small but nonetheless troubling number of respondents would consider sneaking onto a military base (1.3 percent), damaging a power station (2.6 percent), or damaging a Bagarian government building with an explosive device (0.9 percent[18]). Now compare this to the responses that an individual respondent would make in conducting a cyber attack against a nation-state. Table 3-3 below reveals the frequency distribution for a cyber attack on a foreign country.

About 36 percent of the respondents indicated that doing nothing in terms of mounting a cyber attack against Bagaria was an acceptable response. Interestingly, over 75 percent of the respondents felt that posting a comment criticizing the Bagarian government was an appropriate response. This should not be surprising, given the involvement of a large proportion of the online population in social networks. It may also suggest that social networks may serve a functional purpose in providing a nondestructive way in which individuals can register their displeasure at a government or nation-state.

Action	Percent Response
Do nothing —let your country work it out on its own	36.2%
Post a comment on a social networking website like Facebook or Twitter that criticizes the Bagarian government	75.3%
Deface the personal website of an important Bagarian government official	11.2%
Deface an important official Bagarian government website	10.2%
Compromise the server of a Bagarian bank and withdraw money to give to the victims of their policies and actions	5.1%
Search Bagarian government servers for secret papers that you might be able to use to embarrass the Bagarian government	8.5%
Compromise one or more Bagarian military servers and make changes that might temporarily affect their military readiness	6.4%
Compromise one of Bagaria's regional power grids, which results in a temporary power blackout in parts of Bagaria	2.6%
Compromise a nuclear power plant system, which results in a small release of radioactivity in Bagaria	0.4%

Table 3-3. Cyber Attack Frequencies on Foreign Country.

Moving up the severity scale in Table 3-3, a nontrivial number of respondents would engage in some sort of website defacement—11.2 percent would deface the website of a specific government official, while 10.2 percent would deface a more general Bagarian government website. While website defacement generally is considered rather modest damage as far as cyber attacks go, it is still an illegal act and can cause significant embarrassment to the targeted government.

The remaining response categories in Table 3-3 are cyber attacks that are more serious in nature. A little over 5 percent of the respondents would attack a Bagarian financial institution and distribute the stolen funds to victims of the Bagarian government's actions.

In addition, about 8.5 percent of respondents would steal secret government documents to embarrass the Bagarian government à la the Wikileaks incident.

Now looking at attacks that were more directly focused upon a nation-state itself, about 6.4 percent of respondents would consider a cyber attack against a foreign country's military as an appropriate response to actions taken by that country. Finally, looking at cyber attacks that were more specifically focused on a country's critical infrastructure, 2.6 percent of respondents would consider an attack on another country's electrical grid as an appropriate response, while 0.4 percent of respondents would consider attacking a nuclear power plant in a foreign country as appropriate retaliation for acts committed by that foreign country.

An initial examination of the severity of physical attacks and cyber attacks that respondents feel were appropriate to launch against a foreign country brings both good news and bad news to the table. On the one hand, the vast majority of respondents select only responses that had minor or no consequences to the targeted foreign country. On the other hand, there are a nontrivial number of respondents who personally advocated the use of physical and cyber attacks against a foreign country that would have some moderate to very serious consequences. While there is some comfort to be had in the fact that expressing intentions to commit terrorist acts is only the first link in the behavioral chain from ideation to the execution of an attack, and bearing in mind that this is a scenario-based situation, even a small incidence of individuals who would consider some of the most serious acts is troubling. This suggests that the emergence of the civilian cyber warrior (and perhaps the physical attack coun-

terpart) is an event that should be taken into account when developing policies and distributing resources across national priorities to protect national critical infrastructure.

In contrast to the previous scenarios, in which feelings of nationalism may have played a substantial part in the motivation of individuals to react with more severe physical or cyber attack responses against a foreign nation-state, attacks against one's own country go against many of these nationalistic sensibilities. Nonetheless, domestic terrorism has in recent years gained significant national attention, both in the press as well as within federal law enforcement agencies.

The particular design of this study introduces an additional interesting but valuable complexity to this and future analyses. Approximately 10.4 percent of the respondents completing the survey identified themselves as having a homeland that was not the United States. Therefore, the homeland that they referred to in these next two scenarios was not the United States but rather a foreign country. This means that it is possible to make comparisons of attacks on the homeland when that homeland is the United States and when it is a foreign country. This may provide some additional perspective on cross-cultural differences in the civilian cyber warrior phenomenon.[19]

The first scenario is the one featuring a physical attack against one's own homeland. Table 3-4 displays the frequency distribution for the same response set that was used in the physical attack against a foreign country scenario discussed earlier.

Action	Percent Response
Do nothing—let your country work it out on its own	28.9%
Write a letter to government of Bagaria protesting their actions	68.9%
Participate in a protest at an anti-Bagaria rally	60.0%
Travel to Bagaria and protest at their country's capitol building	51.5%
Travel to Bagaria and confront a Bagarian senior government official about their policies	28.5%
Travel to Bagaria and sneak into a military base to write slogans on buildings and vehicles	2.1%
Travel to Bagaria and physically damage an electrical power substation	1.7%
Travel to Bagaria and damage a government building with an explosive device	0.9%
Compromise a nuclear power plant system, which results in a small release of radioactivity in Bagaria	0.4%

Table 3-4. Physical Attack Frequencies on Homeland.

Approximately 28.9 percent of respondents stated that doing nothing to their homeland was an appropriate response. Interestingly, this percentage was substantially smaller than that found in the foreign country example (37.8 percent). Perhaps one reason this is the case is because of the potency of negative feelings that an individual feels when one's own country commits acts against its own citizens.

Following that pattern, substantially more respondents selected writing a letter (68.9 percent) or attending a protest rally (60.0 percent) against their own country than was the case when the offending nation-state was a foreign country. Similarly, more people were willing to travel to their own capitol city and either protest (51.5 percent) or confront their own government official (28.5 percent) than in the foreign

country physical attack scenario. Vandalizing the military property belonging to one's own armed forces had an incidence of 2.1 percent, while attacking one's own national critical infrastructure had incidence rates of 1.7 percent for an attack on the power grid and 0.9 percent for an attack on a nuclear plant. A comparison of these last three attack responses between the foreign country as target and the homeland as target did not appear to reveal a consistent pattern, as was the case for other scenarios.

The final scenario involved cyber attacks against one's own country or homeland. The frequency distribution for this scenario appears in Table 3-5.

Almost 36 percent of respondents felt that doing nothing was an appropriate response when considering a cyber attack on their homeland. Again, about 75 percent of respondents would post a critical comment about their own country on a social network—very similar to the foreign country cyber attack scenario. Defacing the website of a specific government official in their own government received a 12.8 percent response, while defacing a more general government website was chosen by 11.5 percent of respondents as an appropriate response. Approximately 4.3 percent of respondents would extract funds from a bank based in their own country to distribute to the victims of aggressive action on the part of their own homeland.

Action	Percent Response
Do nothing—let your country work it out on its own	35.7%
Post a comment on a social networking website like Facebook or Twitter that criticizes your home country's government	75.3%
Deface the personal website of an important government official for your home country	12.8%
Deface an important official government website for your home country	11.5%
Compromise the server of a bank and withdraw money to give to the victims of the government's policies and actions	4.3%
Search your home country's government servers for secret papers that you might be able to use to embarrass the government	8.9%
Compromise one or more of your home country's military servers and make changes that might temporarily affect their military readiness	4.7%
Compromise one of your home country's regional power grids, which results in a temporary power blackout in parts of your home country	1.7%
Compromise a nuclear power plant system, which results in a small release of radioactivity in your home country	0.9%

Table 3-5. Cyber Attack Frequencies on Homeland.

A surprising 8.9 percent would consider actions akin to a Wikileaks event, in which they would attempt to exfiltrate copies of secret documents in order to embarrass their own government. Almost 5 percent would use a cyber attack to reduce the readiness of their own military forces. A little over 1.7 percent of respondents would attack their own national power grid, while just 0.9 percent suggested that attacking a nuclear power plant in their own country would be an appropriate response.

When one compares the homeland cyber attack distribution to the foreign country cyber attack scenario distribution, it seems that they are more

similar in shape than the two physical attack scenario distributions. It is unclear why this might be the case; perhaps it is due to the fact that the physical attacks require actual travel for some of the foreign country responses, and that may involve more risk than the cyber attacks in which it does not matter where the attacking individual is geographically located.

Now that we have an idea of the frequency distribution of the variables of interest, some simple, initial univariate analyses may prove useful here. One of the obvious questions concerns the hypothesis that there might be some difference between the severity levels of an attack based on whether the target was a foreign country or someone's own homeland. Controlling for the type of attack facilitates the analysis, because the response scales involved in the comparison are identical. For these and subsequent analyses, given the multiple response nature of the response variables, one should utilize the maximum severity response as the indicator of the severity of the response chosen by the respondent. That is, the study will use the most severe response of all the responses the respondent selects for a particular scenario. A simple parametric dependent sample paired t-test can be employed for these comparisons. Severity scores range from one to eight for physical attack responses and from one to nine for cyber attacks, with the highest value being the most severe response.

If you compare target countries—foreign country versus homeland—the first thing to notice in table 3-6 is that all the means have reasonably small values in comparison with the range of the scale. This is the result of most of the respondents selecting attack responses that were modest in their level of severity.

If there is some silver lining in this cloud, it is the fact that most of the respondents selected either no action or actions that had modest consequences. One would not want to live in a world where the results revealed variables near the top of the scale; however, in some less robust countries, this generalization might be false.

Comparison	Mean Severity	T	Df	Sig (2-tail)
Cyber Foreign	1.62	.57	356	.569
Cyber Homeland	1.60			
Physical Foreign	2.94	-7.80	356	<.001
Physical Homeland	3.46			

Table 3-6. Foreign Versus Homeland Target.

Interestingly, there is no evidence supporting a difference in mean attack severity between foreign and homeland targets for the cyber attack scenarios. If nationalistic factors were involved here, one would expect a more severe attack directed toward the foreign country. Perhaps the fact that one can launch this kind of attack without ever being physically close to the target may have some effect, which attenuated an individual's propensity to launch a more severe attack on one type of target than the other.

Examining the mean differences for the physical attack scenario, a statistically significant difference is detected—it appears that respondents selected a more severe level of attack for their own homeland than they would for a foreign country. Certainly, it is

not traditional nationalistic factors at work here. One possible reason for this might be the strong reaction from individuals to a government whose actions hurt their own people. One might think of this as a type of nationalism turned "inside out." One of the basic functions of government is to obtain and maintain the security and safety of its people. Governments violate a very strong cultural norm when they intentionally hurt the very individuals they should protect.

Finally, given that skill plays an important role in the strong meritocracy of the hacking community, this suggests that there might be a positive relationship between the severity of an attack on a nation-state's infrastructure and the skills of the individual selecting the type of attack. A principle components factor analysis was performed on eight measures of computer skills, such as installing an operating system or handling security issues, to produce a factor score-based variable that represents claimed technical skills by the respondent.

A quick look at Table 3.7 reveals that there are weak but statistically significant positive correlations between the skill factor variable and attack severity across all four attack scenarios. This suggests, as one might expect, a positive correlation between cyber attack severity and skill level for an individual. What is more surprising is that these correlations also exist between technical skills and physical attack severity. In addition, these weak but detectable correlations persist across both homeland and foreign country targets. Although caution must be taken because these are preliminary data, this finding may suggest that individuals with technical skills may pose multidimensional threats to critical infrastructure elements. It also suggests that there could be some crossover in the

mode of attack for individuals. This may be especially enlightening in the scenario in which individuals whose traditional mode of attack is cyber-based might transition to either a blend of cyber and physical attack or eventually migrate to a strictly physical attack.

Scenario	Pearsons r	Sig (1-tail)
Physical Foreign	0.096*	0.030
Physical Homeland	0.118*	0.013
Cyber Foreign	0.100*	0.030
Cyber Homeland	0.109*	0.020

Table 3-7. Correlations between Skill Factor and Attack Severity.

CONCLUSION

Hopefully, this discussion has addressed several objectives. First, it has given the reader a basic fundamental understanding of motivations associated with actors who perpetrate malicious online behaviors—knowing your enemy can be a key element in gaining a comprehensive perspective on attacks against online targets. A second objective of the study is to identify specific instances of the civilian cyber warrior as a potentially more serious threat to critical infrastructure. Finally, some simple and initial analyses on preliminary data from a recent study have provided some empirical data that can be useful in guiding further investigation.[20]

Future analyses involving multivariate analyses of the civilian cyber warrior used in this chapter are already underway, and very preliminary results suggest that some of the independent predictor variables

have statistically significant relationships to attack severity. Hopefully, this research will encourage others to pursue similar areas of investigation with the objective of better predicting the level of threat that the nation's critical infrastructure faces.

ENDNOTES - CHAPTER 3

1. Raoul Chiesa, Stefania Ducci, and Silvio Ciappi, *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, Boca Raton, FL: Auerbach Publishing, 2009.

2. Marc Rogers, *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach*, West Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University, 2005.

3. Tom Parker, Eric Shaw, Ed Stroz, Mathew Devost, and Marcus Sachs, *Cyber Adversary Characterization: Auditing the Hacker Mind*, Rockland, MA: Syngress, 2004.

4. Max Kilger, Ofir Arkman, and Jeff Stutzman, "Profiling," Honeynet Project, ed., *Know Your Enemy*, 2nd Ed., Boston, MA: Addison Wesley, 2004, pp. 505-556.

5. This was based upon the counterintelligence acronym MICE, which stood for the reasons someone would betray his or her country—Money, Ideology, Compromise, and Ego.

6. Kilger, Stutzman, and Arkin, "Profiling."

7. Max Kilger, "Social Dynamics and the Future of Technology-driven Crime," in Thomas Holt and Bernadette Schell, eds., *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications,* Hershey, PA: IGI-Global, pp. 205-227.

8. *Ibid.*

9. Ryan Singel, "War Breaks Out Between Hackers and Scientology—There Can Be Only One," *Wired Threat Level*, January 23, 2008, available from *www.wired.com/threatlevel/2008/01/anonymous-attac/*.

10. Michelle Starr, "Anonymous Attacks Australian Government Over Censorship," ChannelNews Australia, October 2, 2010, available from *www.channelnews.com.au/Content_And_Management/Industry/E4C6V5V6*.

11. Xeni Jardin, "Wikileaks Releases Classified Afghanistan War Logs: 'Largest Intelligence Leak in History'," *boingboing.net*, July 25, 2010, available from *boingboing.net/2010/07/25/wikileaks-releases-c.html*.

12. Kilger, "Social Dynamics and the Future of Technology-driven Crime."

13. Dorothy Denning, "A View of Cyberterrorism Five Years Later," Kenneth Himma, ed., *Internet Security: Hacking, Counterhacking and Society,* Sudbury, MA: Jones and Bartlettt, 2007, pp. 123-140.

14. Michael Foucault, *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, Brighton, UK: Harvester Press, 1980.

15. Jessica Mathews, "Power Shift," *Foreign Affairs*, 1997, Vol. 76, No. 1, pp. 50-66.

16. Marc Rogers, "The Psychology of Cyber Terrorism," Andrew Silke, ed., *Terrorist, Victims and Society: Psychological Perspectives on Terrorism and Its Consequences*, Chichester, UK: John Wiley & Sons, Inc., 12003, pp. 77-92.

17. Thomas Holt and Max Kilger, "Understanding the Behaviors of Cyberattackers Online and Offline," Presentation at the 10th Annual Honeynet Project Workshop, Paris, France, 2011.

18. Note that respondents are able to select more than one attack response, so the percentages will sum to more than 100 percent. One must be careful to observe that another result is that the percentages in the table are not strictly additive across response categories.

19. The authors of the study are currently engaged in negotiations with researchers in several other countries to deploy the study cross-nationally.

20. Holt and Kilger.