ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

CYBER INFRASTRUCTURE PROTECTION - VOL 1 - PART 2 OF 3

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-144
Course Content:	56 pgs
PDH/CE Hours:	4

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-145 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. The Routine activities theory (RAT) is made up of three distinctive elements: 1. A suitable target is available, 2. There is a lack of a suitable guardian, and 3. There is a motivated offender.
   a. True
   b. False
2. According to the reference material, computer attacks are also costly, as unauthorized access of computer systems cost U.S. businesses $__ million dollars in 2006 alone.
   a. 15
   b. 20
   c. 25
   d. 30
3. GhostNet cyber espionage study and analysis report of the Information Warfare Monitor on distributed malware attacks originating out of China. This attack led to the Compromise of at least 1,295 computers in 103 countries, of which nearly __ percent might be high-value targets
   a. 10
   b. 20
   c. 25
   d. 30
4. According to The Council of Europe's Convention on Cyber-crime one of the 5 keys areas for substantive crimes where each state must adopt criminal laws is the misuse of devices
   a. True
   b. False

5. According to the reference material, in 2006 cellular telephones were recovered in investigations in a majority of violent crimes and in over 95 percent of drug crimes.
    a. True
    b. False
6. According to the reference material, other countries have laws designed to regulate various types of misconduct with computing devices. Which of the following countries implemented the Information Technology Act of 2000?
    a. Canada
    b. United Kingdom
    c. India
    d. Germany
7. The Council of Europe's Convention on Cyber-crime is a primary component of such an evolving regime. This treaty emerged after lengthy negotiations between members of the Council of Europe and nonmember states. Which of the following countries was NOT mentioned in the reference material?
    a. China
    b. Canada
    c. Japan
    d. Dominican Republic
8. According to the reference material, 18 U.S.C. § 1029 is the federal criminal statute that deals with Fraud and Related Activity in Connection with Computers
    a. True
    b. False
9. Using Figure 6.4, and the corresponding reference material, what percentage of police executive offers reported the inability to use evidence from cell phones due to lack of training or access to forensic specialists?
    a. 15
    b. 30
    c. 50
    d. 60
10. According to the reference material, 18 U.S.C. § 3121 is the federal criminal statute that deals with Recording of Dialing, Routing, Addressing, and Signaling Information.
    a. True
    b. False

CONTENTS

PREFACE

The Internet, as well as other telecommunication networks and information systems, have become an integrated part of our daily lives, and our dependency upon their underlying infrastructure is ever-increasing. Unfortunately, as our dependency has grown, so have hostile attacks on the cyber infrastructure by network predators. The lack of security as a core element in the initial design of these information systems has made common desktop software, infrastructure services, and information networks increasingly vulnerable to continuous and innovative breakers of security. Worms, viruses, and spam are examples of attacks that cost the global economy billions of dollars in lost productivity. Sophisticated distributed denial of service (DDoS) attacks that use thousands of web robots (bots) on the Internet and telecommunications networks are on the rise. The ramifications of these attacks are clear: the potential for a devastating large-scale network failure, service interruption, or the total unavailability of service.

Yet many security programs are based solely on reactive measures, such as the patching of software or the detection of attacks that have already occurred, instead of proactive measures that prevent attacks in the first place. Most of the network security configurations are performed manually and require experts to monitor, tune security devices, and recover from attacks. On the other hand, attacks are getting more sophisticated and highly automated, which gives the attackers an advantage in this technology race.

A key contribution of this book is that it provides an integrated view and a comprehensive framework of the various issues relating to cyber infrastructure protection. It covers not only strategy and policy issues, but it also covers social, legal, and technical aspects of cyber security as well.

We strongly recommend this book for policymakers and researchers so that they may stay abreast of the latest research and develop a greater understanding of cyber security issues.

PART II:

SOCIAL AND LEGAL ASPECTS

CHAPTER 6

THE INFORMATION POLITY: SOCIAL AND LEGAL FRAMEWORKS FOR CRITICAL CYBER INFRASTRUCTURE PROTECTION

INTRODUCTION

This chapter examines how public policy may evolve to adequately address cybercrime. Traditional legal protections against criminal activity were developed in a world wherein any criminal violation was coupled with physical proximity. Global information networks have created criminal opportunities in which criminal violation and physical proximity are decoupled.

We argue that cyberspace public policy has not adequately incentivized and supported protective behaviors in the cyber community. We examine the roles that user-level/consumer-level conduct, social engagement, and administrative policy play in pro-tecting information infrastructure. We suggest proac-tive work with laws and administrative/citizen-level engagement to reform the cyberspace community. To that end, we examine applicable legal and transna-tional regimes that impact such a strategy and options for expanding administrative and citizen engagement in the cyber security enterprise.

The cyber infrastructures of the United States and Europe offer inviting targets for attack, whether for profit, malice, or state objectives. The enmeshing natures of computer networks have changed the calculus for both delineating and protecting critical cyber infrastructure. The boundaries between such infrastructure and external systems using the infrastructure have become so intertwined that it may be impossible to separate them. Those external systems may become threat vectors themselves.

This enmeshing has blurred the identity between physical and "logical" frontiers for purposes of state boundaries, jurisdiction, and sovereignty. Cyber security issues move quickly past the national level to that of provinces, states, localities, businesses, and citizens.

Carolyn Pumphrey discussed in detail how local law enforcement strategies might effectively be blended with military/homeland security efforts to protect cyber systems. She noted that transnational threats, including those of cyber security, straddle "domestic and foreign spheres" that present "profound constitutional and security challenges" for the United States.[1]

Public security is a function of several factors, including law and effective law enforcement, social norms, and technical protections. Effective security in cyberspace requires a similar configuration. A neighborhood where neighbors watch out for each other and discourage criminality; timely response by police and the courts; and where residents lock their windows and doors will be much more secure. Together, the community's norms, habits, and formal institutions serve protective functions.

The conceit we call cyberspace can equally benefit from an equivalent set of protective elements. Yet efforts to incentivize such protective elements have not been sufficiently developed. Of particular concern are the capabilities of local law enforcement, business, and individuals to play their part in cyber security as a necessary component of protection of all cyber infrastructures.

Law, norms, and technology impact these capabilities. At the same time, they may raise issues relating to the preservation of rights and liberties of liberal Western countries seeking to respond to external threats.

Review of laws and administrative systems can avoid misunderstandings as to proper conduct in investigating the misuse of computers and networks. It can also aid in protecting researchers from legal problems in their work, especially for research done outside of government.

The significance of the threat is seen in the March 29, 2009, GhostNet cyber espionage study and analysis report of the Information Warfare Monitor on distributed malware attacks originating out of China.[2] These attacks use a combination of Trojan malware-Gh0st RAT (Remote Access Tool) and social engineering via e-mail to infect vulnerable machines. The key findings were:

- Compromise of at least 1,295 computers in 103 countries, of which nearly 30 percent might be high-value targets,
- GhostNet penetration of sensitive computer systems of the Dalai Lama and other Tibetan targets, and
- GhostNet is a covert, difficult-to-detect system capable of taking full control of affected systems.[3]

Compromised systems included government offices of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, Bhutan, and embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany, and Pakistan.

This report comes on the heels of U.S. Government reports that computing systems at power utility companies where compromised by overseas attacks.[4]

The GhostNet report further suggests that cyber security outside of classified government operations is woefully inadequate, whether in commercial or civic organizations.

We suggest a proactive strategy that blends law enforcement, military, and citizen engagement for the protection of the cyber infrastructure and enhancement of cyber security. To that end, we examine applicable legal and transnational regimes that impact such a strategy and options for expanding administrative and citizen engagement in the cyber security enterprise. These options may offer a vital complementary element to the cyber security of the United States as well as other countries.

JURISDICTION AMONG DISTRIBUTED SOVEREIGNS

The exclusive power and jurisdiction to regulate is a jealously guarded prerogative of sovereign nations. Jurisdiction may refer to a particular entity asserting a right to regulate conduct, such as a nation or a province, and in addition to the right of that entity to regulate conduct, but also to punish conduct. The right to regulate is usually bounded by a grant of rights itself limited by physical boundaries, such as the boundaries of a nation, state, province, or locality. It encompasses regulation through substantive criminal law that defines wrongful conduct, procedural criminal law that defines how the law is enforced, and laws for resolving problems between jurisdictions, e.g., extradition and transfer of an offender found in one jurisdiction to another jurisdiction for offenses committed in that latter state.

A state may also assert the right to act against conduct outside of its boundaries that has an impact inside those boundaries. It may assert jurisdiction over acts of its citizens that occur abroad. It may assert jurisdiction based on treaties, maritime law, or international law.

In the distributed, transnational environment of cyberspace, the assertion of a right to regulate must still address the practical problems of enforcement in foreign jurisdictions. If the domestic cyber infrastructure is attacked by someone operating in another jurisdiction, cooperation by the authorities in that foreign jurisdiction may be needed. If investigative data on an attack are to be found in a foreign jurisdiction, even if the attacker is in yet another jurisdiction, speedy local cooperation is needed. Obtaining this cooperation may be difficult.

For example, in the Gorshkov/Ivanov cases, the defendants broke into various U.S. corporate computer systems from their home base in Russia; they then offered their computer security expertise for hire.[5] To simplify the jurisdictional problems, the U.S. Federal Bureau of Investigation (FBI) convinced them to demonstrate these skills in a meeting in the United States that was videotaped and keylogged. After logging in to his home machine to download his toolkit, Ivanov was arrested. The agents then took the keylogger data, logged into Ivanov's home machine in Russia, and downloaded files evidencing his illegal access to machines in the United States. Both were convicted and sentenced to prison. However, Russian authorities were not happy with the actions of the U.S. authorities and initiated criminal proceedings against the two FBI agents involved in the remote (but unauthorized) access to Ivanov's machine in Russia.

The complexity of transnational actions increases with other issues of data and computing regulation in each country. The most effective tool to remedy this is cooperation, which may be manifested in treaty law promoting mutual benefit. This may not be possible with any country that expressly or implicitly condones cyber attacks against foreign targets. But it can still be effective in rallying countries to work together and set a foundation for diplomatic solutions. First, we provide a general discussion of local law in this area and then proceed to the use of treaty law to create a more effective transnational regime.

LOCAL SUBSTANTIVE CRIMINAL LAW AND THE EXERCISE OF SOVEREIGNTY

Criminal and delictual law adapt to injuries and misconduct with new technologies, particularly where those technologies threaten rights in new and unforeseen ways. The legal regime for computer misuse addresses the core function of these machines; their ability to store, manipulate, and transmit information.

A traditional crime may be committed with a new computer tool, such as murder by entering false information in a medical database.[6] Crimes previously the province of technical specialists, such as criminal copyright infringement, may now easily be committed by laypersons. Some crimes require new, *sui generis* statutes to control misconduct unseen before the rise of computing technologies.

Review of computer misuse must consider several issues:

- Misuse may fit traditional criminal law elements. For example, a computer can be used to store or transmit information on terrorist activity or other criminal dealings, like a notebook.
- Computer misuse may only partially correspond to traditional criminal law elements, requiring legal revisions to correspond to technical facts of computers and networks. For example, a computer may be used to copy and transmit information in violation of intellectual rights and for industrial espionage, violations that in the past required significant time and resources.
- Or that misuse may not fit within the elements of standard crimes, requiring use of new criminal statutes to address the danger. For example, a computer can be used to transmit information that, while harmful, does not fit the elements of traditional crimes requiring proximity of the offender to the target or financial motive. The Filipino computer student who wrote the "I Love You" computer virus was not prosecuted because the Philippines had no law at the time criminalizing such conduct.[7]

The intersection of the old and the new with cybercrime make for an evolving area of practice. Review of incidents of computer misuse will require a combination of both traditional and innovative case analysis in law enforcement, especially where the computer crime itself shares elements of old and new types of offenses, as seen in Figure 6.1.

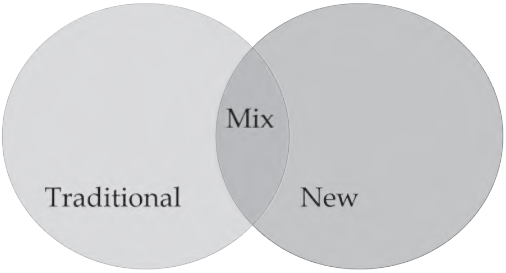

Figure 6.1. Evolving Law Enforcement Practice.

Examples of Local Substantive Criminal Laws.

The issue of jurisdiction and sovereignty plays a major role in the promulgation of laws as each sovereign may choose to create its own set of criminal laws relating to computer misconduct. They may do so with little regard for what any other jurisdictions may choose to regulate.

The general categories of regulation in this area are exemplified by the Council of Europe's Convention on Cybercrime, discussed further below. Those categories are:

- Unauthorized access to computer, (this includes exceeding authorized access to a computer),
- Unauthorized interception of data,
- Unauthorized interference with data,
- Unauthorized interference with a system,
- Misuse of devices.

Different jurisdictions may adopt criminal laws in each of these areas or only some of them; the particular provisions may vary from one jurisdiction to another.

Some primary U.S. federal criminal statutes related to computer intrusions that reflect these categories are:

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C. § 2510 et seq. Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Records Access
- 18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information.

Each of the American states has its own computer crime laws that may reflect some or all of these issues. For example, Kentucky statutes focus on unlawful access to a computer:

- KRS 434.845 Unlawful access to a computer in the first degree (fraud).
- KRS 434.850 Unlawful access to a computer in the second degree (damage).
- KRS 434.851 Unlawful access in the third degree (damage).
- KRS 434.852 Unlawful access in the fourth degree (access).
- KRS 434.855 Misuse of computer information.
- KRS 150.363 Computer-assisted remote hunting unlawful—Citizens with disabilities.

While its primary focus is on unlawful access, Kentucky's prohibition on computer-assisted remote hunting is a good example of how special local concerns may lead to unique laws on computing.

Similarly, other countries have laws designed to regulate various types of misconduct with computing devices, such as:

- Canada
  - Unauthorized use of computer interception of communications
- United Kingdom
  - Computer Misuse Act 1990, as amended
  - Data Protection Act 1998
- India
  - Information Technology Act 2000
- Germany
  - Unauthorized acquisition of data
  - Unauthorized circumvetion of system security

This structure for substantive criminal laws that define prohibited conduct is also matched by systems of procedural laws by which the substantive law is enforced. These laws may vary between jurisdictions.

Procedural Criminal Laws.

Enforcement of substantive criminal law is guided by rules of procedure that seek to assure reliability and fairness in the administration of justice. They may also reflect national interests in the protection of certain rights of citizens. As with substantive criminal law, criminal procedure may vary between jurisdictions.

One area of procedure deals with the proper use of evidence. Electronic evidence alone or matched with other evidence may indicate a crime and additional evidence of that crime. That additional evidence, once obtained, can correlate the electronic record with other actions. This correlation and development role is particularly important for remote data collected over networks; correlation to other evidence is a key function of electronic evidence in prosecuting a digital crime.

Another area addresses the protection of privacy rights of citizens from government intrusion. For example, absent special circumstances, the search or seizure of a person or his effects without consent is illegal in the United States unless an application under oath is made before a neutral magistrate that sets out facts to establish “probable cause” to believe a crime has been committed and evidence of that crime will be found in the place searched and things seized. Probable cause itself means a fair probability under a commonsense analysis that evidence is to be found at the place to be searched. This and other rules define procedural law for law enforcement and prosecution in the United States.

For example, Figure 6.2 shows a diagram of the process by which computational forensic data may be used within the criminal justice process in the United States.

Meeting the procedural requirements of each jurisdiction may slow computer crime investigation across multiple jurisdictions. It may, in fact, render an investigation impossible. To counter investigative obstacles, a transnational legal regime is developing through bilateral and multilateral treaties to harmonize substantive and procedural criminal law between countries and to create a system for mutual assistance and cooperation in cybercrime investigation and prosecution. That developing regime is seen in cooperation between nations as outlined by the Convention on Cybercrime of the Council of Europe.

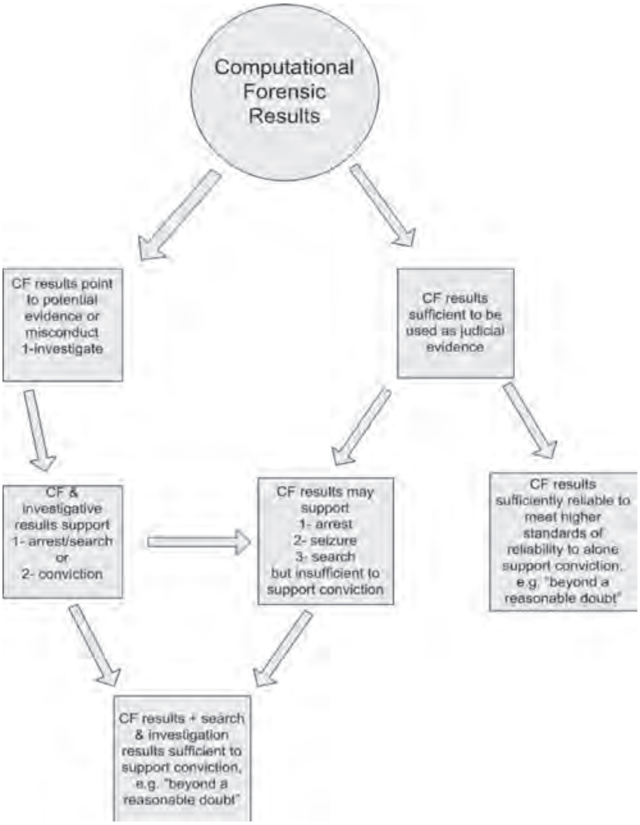
Computational Forensic Results
CF results point to potential evidence or misconduct 1-investigate
CF results sufficient to be used as judicial evidence
CF & investigative results support 1- arrest/search or 2- conviction
CF results may support 1- arrest 2- seizure 3- search but insufficient to support conviction
CF results sufficiently reliable to meet higher standards of reliability to alone support conviction, e.g. "beyond a reasonable doubt"
CF results + search & investigation results sufficient to support conviction, e.g. "beyond a reasonable doubt"

Figure 6.2. The Use Path for Computational Forensic (CF) Results.[8]

A TRANSNATIONAL LEGAL REGIME AND COOPERATION ACROSS FRONTIERS—THE CONVENTION ON CYBERCRIME

Miles Townes and others argue that an international regime to protect our interconnected information infrastructure is needed.[9] Nicholas Seitz, Townes, and Lorenzo Valeri all support the premise that an international regime of information assurance is essential; Valeri calls for "specific international 'clusters of rules or conventions,' the content of which cannot be just independently devised by states or international businesses."[10]

The Council of Europe's Convention on Cybercrime[11] is a primary component of such an evolving regime. This treaty emerged after lengthy negotiations between members of the Council of Europe and nonmember states; Canada, Costa Rica, Dominican Republic, Japan, Mexico, Philippines, South Africa, and the United States.

The Convention is structured to address the issues of substantive criminal law, procedural criminal law, and interjurisdiction relations. By harmonizing these three areas, the Convention promotes greater uniformity between national laws and facilitates cooperation between states, vital for the preservation of time-sensitive, evanescent electronic evidence. It does this by requiring each country joining the Convention to:

- adopt criminal laws that define crimes in five fundamental areas of computer and network misuse, creating a common base of substantive criminal law;
- adopt and implement procedures for investigation, evidence collection, evidence preservation, and prosecution of digital crime and use of electronic evidence, building a common base of procedural criminal law across countries; and,
- Building on the common foundation in both substantive and procedural criminal law, states must then adopt measures to assure international cooperation and mutual assistance in

investigations involving multiple jurisdictions, addressing particularly difficult problems of the preservation and disclosure of data and the extradition of citizens to foreign jurisdictions.

The five key areas for substantive crimes where each state must adopt criminal laws are:

1. Unauthorized access to computer, (this includes exceeding authorized access to a computer),
2. Unauthorized interception of data,
3. Unauthorized interference with data,
4. Unauthorized interference with a system, and
5. Misuse of devices.

The Convention looks at intentional conduct "without right."

The Convention permits variations between nations. In our earlier list of U.S. laws, these five areas are addressed by those statutes; 18 U.S.C. § 1030. "Fraud and Related Activity in Connection with Computers," in particular, addresses unauthorized access and interference with data and systems.

The common procedural criminal law for law enforcement investigative and prosecutorial activities include the preservation, acquisition, and use of electronic evidence. The most sensitive of the three areas relates to requirements for international cooperation and mutual legal assistance. Cross-jurisdictional law enforcement efforts entail risks that range from different procedures to different communications protocols to challenges to national sovereignty. The Convention seeks to minimize these problems by first harmonizing criminal laws and then having states adopt procedures and practices for cooperation and mutual assistance between countries on cybercrime matters.

These procedures should address assistance and cooperation in data preservation and disclosure and the extradition of suspects.

The Convention creates a foundation for cooperation between countries in investigating cybercrime between countries, including activities impacting criminal cyber infrastructure. But this foundation must be supplemented by other human participant elements within the cyber community. The enmeshed nature of our cyber-information world has made the home front the frontier of cyber conflict. Local matters of law enforcement and public security are intertwined with those of national cyber security.

We discuss possible ways to incentivize protective behaviors in the following section.

SOCIAL NORMS AND CRIMINOLOGICAL THEORY

Law enforcement is not the sole factor in assuring public security. The values and actions of a community contribute to its security. As Stanley Cohen argues, the strength of social control depends on formal and informal social control.[12] Laws and law enforcement represent formal social control, whereas the attitudes and actions of individuals represent informal social control. Both spheres can impede unlawful activities, but states with strong overall levels of social control will have high degrees of both formal and informal social control.

The opportunity theory perspective provides a useful way of conceptualizing the potential effect of informal social control on cyber security. Routine activities theory (RAT) is made up of three distinctive elements:

1. A suitable target is available,
2. There is a lack of a suitable guardian, and
3. There is a motivated offender.[13]

Where all of these elements are present, the risk of criminal conduct increases. Conversely, the absence of one of these elements reduces the risk of misconduct.

In the context of cyber security, there is an abundance of suitable targets and a lack of suitable guardians. However, changes in attitudes, present in the informal sphere of social control, can increase rates of suitable guardianship.

Attitudes have been used to explain a wide range of behaviors, including racism, prejudice, voting, and attraction. There is no universal definition of attitude, and the concept itself has been measured in hundreds of ways. As M. Fishbein and I. Azjen write, "[A] definition of attitude appears to be a minimal prerequisite for the development of valid measurement procedures."[14] J. M. Olson and M. P. Zanna define an attitude as favorable or unfavorable evaluative reactions toward an object which may be manifested through beliefs, feelings, or inclinations toward action.[15]

Social psychological research in value diffusion[16] and norms[17] suggest that attitudes can be manipulated via intervention. Boyd and Richerson argue that values can differentially spread in a population based on biasing factors. When an individual is exposed to different values, an individual's decision to adopt one of the values and not the other may be biased from randomness by properties of the social context which render the selected value more appealing. Preferential value diffusion has been borne out in economics and diffusion of innovations research.[18]

A norm favoring a particular value may cause that value to become ubiquitous in a population. There is no universally agreed upon definition of "norm": the Merriam-Webster Dictionary defines a norm as "a principle of right action binding upon the members of a group and serving to guide, control, or regulate proper and acceptable behavior." A norm has two primary subtypes, social and legal. A social norm, unlike a legal norm, is informal and appears to arise and be enforced[19] without deliberate planning, writing, or enforcement.[20]

In the externality model of norm development, norms emerge when the actions of individuals produce either costs or benefits to others.[21] When individual X does an act that individual Y does not like or perceives as harmful, Y may respond negatively, often reasoning that "you shouldn't do that." An individual's being harmed is not enough to generate a norm; however, if enough similarly situated individuals perceive the same harm, this response will become a norm and have a constraining effect on behavior. As long as the benefit/harm is easily identified (such as death, theft, or pollution), the externality model accounts for why certain deviant behaviors are punished (they are viewed as harmful rather than harmless) and punished to varying degrees (certain behaviors are viewed as extremely harmful or intolerable); in many cases, however, the benefit/harm is often culturally defined and subject to debate.

Using the externality model puts an onus on information because an externality is socially constructed: Individuals need to decide what is harmful, and definitions thereof may vary depending on social and contextual factors. For example, the linking of complex issues such as cyber security and individual autonomy may be hotly debated. For example, some individuals may argue that individuals are responsible for others but bear no responsibility for others' cyber security (referred to hereinafter as isolationist norm). By contrast, others may argue that such an orientation is too myopic and is subject to the freeloader fallacy. While such an approach would be effective for a security-minded individual if everyone else was like-minded, such an approach is suboptimal if others fail to consider cyber security. In that case, the community's cyber security vulnerabilities will create widespread opportunities for network-based attacks, which ultimately may compromise the isolationist individual's cyber security.

Based on this externality model, we argue for cyber security policy changes to foster information that supports an integrationist norm, wherein individuals recognize that their failure to be proactive in pursuing cyber security is morally irresponsible and exposes them and others to harm. Successful informational campaigns have changed public norms. For example, public awareness of harms created by littering and second-hand smoking have largely emerged over the last 40 years as a result of commercials, scientific studies, and laws. National awareness of littering was heightened by commercials featuring a weeping Native American surveying a litter-strewn American landscape. Such commercials transformed littering from a local problem to a collective problem. The act of littering acquired a moral dimension and was reconceptualized as harmful and disrespectful to others. Littering itself may be punished informally by others via informal sanctions, such as rude responses. Current informal norms disfavor littering in many contexts, and many children are taught not to litter from early ages.

In cyber security contexts, information campaigns could foster integrationist norms by presenting cyber security as a moral obligation of personal responsibility, wherein the failures of the few may lead to great harm for others. Recent cyber attacks have utilized cyber security flaws on un-updated computers to create drones of attack computers. Educating the public about operating such computers would harden targets by presenting such actions as not only foolish and shortsighted but leading to the harm to others.

Ultimately, optimal public policy changes social values relating to personal responsibility. Information campaigns could be reconceptualized as moral imperatives. In so doing, motivated individuals will harden cyber targets by proactively pursuing cyber security.

ADMINISTRATIVE ENGAGEMENT—MARSHALLING AND ENABLING EXISTING LAW ENFORCEMENT

Enabling local law enforcement to address cybercrime matters can increase the presence of "suitable guardians" and reduce the motivations of some offenders. U.S. law enforcement at the local level expects growth in the use of electronic evidence as proof of system misuse. Lawyers and judges have also expressed the desire for better training in this area. This reflects the vast expansion of consumer computing devices in society.

It also reflects a dangerous skills gap in law enforcement relating to consumer computing and telecommunications devices. For example, in 2006 cellular telephones were recovered in investigations in a majority of violent crimes and in over 80 percent of drug crimes.[22] See Figure 6.3.

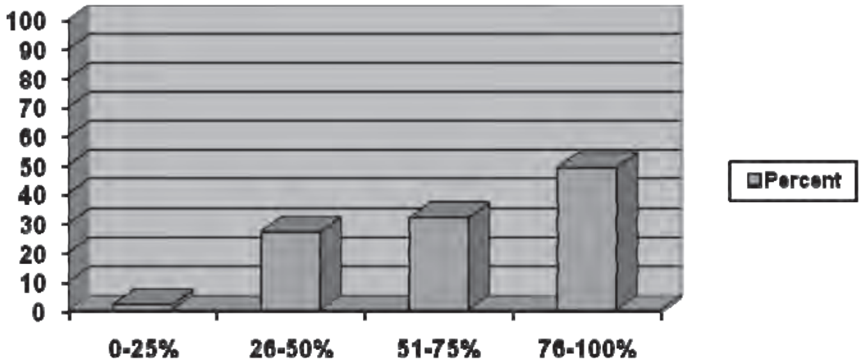

Figure 6.3. Involvement of Cell Phones In Violent Crimes.[23]

Yet a majority of police executive officers also reported an inability to use evidence from those systems due to lack of training or access to forensic specialists. See Figure 6.4.

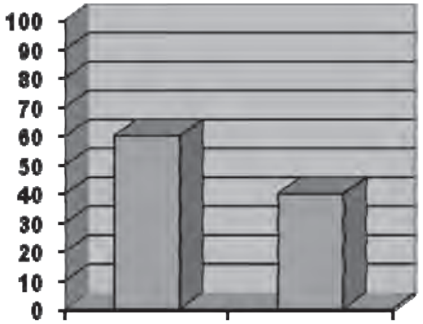

Figure 6.4. Inability to Search for Cell Phone Evidence Due to Timely Access to Forensic Examiners and Lack of Forensic Skills.[24]

Similar surveys relating to general electronic evidence and systems produced indications of expectations of increased use and desire for training in this area among judges, attorneys, and even corrections officers.[25]

If the resources to address cybercrime at all levels are to be marshaled at all levels, we must enable local law enforcement to address these threats.

Expanded Law Enforcement Engagement.

Expanded law enforcement engagement may be achieved through cross-disciplinary training for necessary skills and for the support of their use via local capacity-building. This engages law enforcement, public defenders, prosecutors, corrections, and the judiciary in the training and support services.

Training would focus on:

- Law enforcement training. Computer forensic examination training on how and where to manually locate data on digital media storage devices, use of automated computer forensic tools locate, identify, and report information of evidentiary value, including specific information in formats such as hexadecimal or binary within data sets, carve information from the data set in a forensically sound manner, and articulate the findings.
- Law enforcement training. Digital evidence collection training to provide a measurable proficiency in digital evidence recognition, seizure, packaging, transportation, and storage.[26]
- Law enforcement administrative officer training. Training for administrative officers on managing and supervising their people on the

use and analysis, collection and preservation of digital evidence, particularly from cell phones and other portable electronic devices.

- Defender training. Support for training public defenders in the effective assistance of counsel in cases involving digital evidence.
- Prosecutorial training. The prosecutorial use of computer forensic data in the courtroom.
- Judicial training. Judicial practice relating to the use of computer forensic data in the courtroom.

Support services should include statewide networks of resources, such as self-service digital forensic workbenches available to local law enforcement that may not be able to afford their own forensic systems but continue to collect digital evidence repositories. Where evidentiary issues may require higher-level analysis, this workbench system would support chain-of-custody valid transmittal to regional computer forensic laboratories and other forensic analysts capable of such high-level analysis.

This distributed local investigative capacity would expand the protective capabilities needed to protect systems from cyber attack. Feeding local investigative results into the system of transnational cooperation envisioned by the Convention on Cybercrime would speed response while effectively leveraging all resources in what is already an asymmetric risk environment.

Given the cross-jurisdictional issues noted earlier, such a system could use national and state-level organizations to mobilize collaboration. Law enforcement, prosecutors, and judges all have national organizations to help implementation at the state level. Similarly, these groups have statewide organizations that can carry implementation to local jurisdictions.

Many states have resources within the computer science, computer engineering, and computer information systems departments of state universities to further support this effort with their expertise. The expertise and experience developed within these departments is a significant resource that will decrease the cost of training development and delivery, and resource development.

Sustainability and expansion will depend on the selection of state and local law enforcement, prosecutors, and judicial professionals who themselves will serve as resources and future trainers to maintain and further the skills relating to computer forensics, cell phone forensics, and digital evidence.

CITIZEN ENGAGEMENT

The home front is the frontier in this conflict. The citizen computer user must be engaged in this process. Risk can evolve when home/business systems ". . . are being increasingly subverted by malicious actors to attack critical systems."[27] Community awareness and training on basic cyber security are needed for home and small business users; the threat mandates such action.[28] The strategy emphasizes the role of public-private engagement.[29]

This framework encompasses all who use computer systems. The National Institute of Standards and Technology (NIST) has outlined standards on technical security and security training and awareness for nontechnical users of computer systems.[30] NIST's Computer Security Resource Center (CSRC), the Small Business Administration (SBA), and the

National Infrastructure Protection Center (Infragard) have together advocated computer security trainings for small businesses.[31] Educause, the association for IT in education, advocates starting cyber security education in kindergarten.[32] The Awareness and Outreach Task Force of the National Cyber Security Partnership, an industry association, recommends the development and distribution of cyber security guidebooks and toolkits for small business and home computer users.[33]

Collaboration between government, business, schools, and consumers improves security by mitigating the exploitation of home and small business systems for computer security attacks. It prevents the use of compromised home computers to help storm the security bastions of any other computer on the Internet in a coordinated, multitiered, and destructive attack. It limits risks of compromise to critical systems, such as medical and mechanical systems, that are real, mortal threats.

Direct Engagement—A Training Response.

There must be direct engagement of school, home, and small businesses in securing computers and broadband connections from attack and compromise. This engagement requires the training of users for their own protection and the protection of others.

Three barriers hinder that engagement. As a matter of cost, home and small business users may not be able to hire expertise for computer security. As a matter of training, the generally low-level of computing literacy makes it difficult for home and small business users to implement secure practices themselves. As a matter of culture, school, home, and small business users may defer to others in reference to their systems' operations.

These are overcome by basic computer security training for consumers and by ongoing efforts of business and government to provide security tools for the home and small business computer user. A cost-effective model of such training was proposed by the University of Louisville student chapter of the Association for Computing Machinery (ACM). [34]

First, training identifies the threats to home and small business systems. Often, even with news coverage of virus and worm outbreaks, consumers are unaware of the level of threat associated with Internet and broadband usage. Second, training looks to "best practices" with the use of; (a) protective technology, and (b) safe user practices. System maintenance practices, though inconvenient, offer better security for systems. Safe personal computer use practices secure the users themselves, especially children.[35]

The Benefits of Engagement.

Citizen engagement has the dual benefit of hardening the vast distributed set of available targets and developing new guardians in the form of the computer users themselves. Securing home and small business computers can only happen with the engagement of citizens in the security enterprise. By the very nature of the Internet, individuals must be active participants in the security of their own systems. Civil engagement highlights the need for all Americans, in their homes and businesses, schools and churches, to be part of the security solution. Personal responsibility in this effort is essential for success.

This requires the computer security community to educate the public about personal security efforts.

Information technology is not a profession and is not bound by proactive professional ethical mandates,[36] even though proactive attention to safety and security may be expected.[37]

This training solution promotes safety, security, and social responsibility by advancing the understanding of computing in the critical area of security.[38]

CONCLUSION

Cyber infrastructure needs security that can only happen via collaboration between citizens/system users, businesses, law enforcement agencies, and civil institutions that provide the knowledge and improved technologies needed for secure computing. Should such collaboration fail to develop, computing in our country, and its benefits, will suffer.

As a collaborative effort, cyber security requires personal responsibility from citizens and institutions. Protective factors in cyber security are minimized when participants blindly delegate all responsibility to others and continue to deploy and use networked systems.

Optimally, public policy will foster both law enforcement and citizen engagement in information security. Failure to engage these resources will continue to leave gaps in protection and create opportunities for harm to our people and our country.

ENDNOTES - CHAPTER 6

1. Carolyn Pumphrey, "Introduction," in Carolyn Pumphrey, ed., *Transnational Threats: Blending Law Enforcement and Military Strategies*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2000, pp. 1-17, available from *www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=224*.

2. Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, March 29, 2009, available from *www.infowar-monitor.net/ghostnet*.

3. *Ibid.*, p. 6.

4. Justin Blum, "Hackers Target U.S. Power Grid: Government Quietly Warns Utilities To Beef Up Their Computer Security," *Washington Post*, March 11, 2005, p. E01.

5. Art Jahnke, "Alexey Ivanov, and Vasiliy Gorshkov: Russian Hacker Roulette," CSO Online, January 1, 2005, available from *www.csoonline.com/article/219964/Alexey_Ivanov_and_Vasiliy_Gorshkov_Russian_Hacker_Roulette*.

6. Susan Brenner, "Cybercrime Metrics: Old Wine, New Bottles?" *Virginia Journal of Law and Technology*, Vol. 9, No. 13, Fall 2004.

7. Wayne Arnold, "TECHNOLOGY; Philippines to Drop Charges on E-Mail Virus," *New York Times*, August 22, 2000, available from *www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html*.

8. C-T Li, *Handbook of Research on Computational Forensics, Digital Crime and Investigation: Methods and Solutions*, Hershey, PA: IGI Global, 2010.

9. Miles Townes, "International Regimes and Information Infrastructure," *Stanford Journal of International Relations*, Vol. 1, No. 2, Spring 1999.

10. *Ibid*.; Nicholas Sietz, "Transborder Search: A New Perspective on Law Enforcement?" *International Journal of Common Law and Policy*, Vol. 9, No. 2, Fall 2004; Lorenzo Valeri, "Securing Internet Society: Toward an International Regime for Information Assurance," *Studies in Conflict & Terrorism*, Vol. 23, Iss. 2, January 2000, pp. 129-146, particularly p. 141.

11. Council of Europe CETS No. 185 Convention on Cybercrime, opened for signature November 23, 2001, available from *conventions.coe.int/Treaty/en/Treaties/Html/185.htm*, signed and ratified by 27 states.

12. Stanley Cohen, *Visions of Social Control: Crime, Punishment, and Classification*, Cambridge, UK: Polity Press, 1985.

13. M. Ouimet, "Internet Crime and Trends," in F. Schmallager and M. Pittaro, eds., *Crimes of the Internet*, Upper Saddle River, NJ: Pearson Education Inc., 2009, pp. 408-416.

14. M. Fishbein and I. Azjen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975.

15. J. M. Olson and M. P. Zanna, "Attitudes and Attitude Change," *Annual Review of Psychology*, Vol. 86, 1993, pp. 852-875.

16. Robert Boyd and Peter J. Richerson, *The Origin and Evolution of Cultures*, Oxford, UK: Oxford University Press, 2005.

17. Christine Horne, "Sociological Perspectives," in Michael Hechter and Karl-Dieter Opp, eds., *Social Norms*, New York: Russell Sage, 2001, pp. 3-34.

18. Everett Rogers, *The Diffusion of Innovations*, New York: Free Press, 1983.

19. Robert C. Ellickson, "The Evolution of Social Norms: A Perspective from the Legal Academy," in Michael Hechter and Karl-Dieter Opp, eds., *Social Norms*, New York: Russell Sage, 2001, pp. 35-75.

20. Michael Hechter and Karl-Dieter Opp, "Introduction," in Michael Hechter and Karl-Dieter Opp eds., *Social Norms*, New York: Russell Sage, pp. xi-xx.

21. Harold Demsetz, "Toward a Theory of Property Rights," *American Economic Review*, Vol. 57, No. 2, 1967, pp. 347-359.

22. Michael Losavio, Deborah Wilson, and Adel Elmaghraby, "Prevalence, Use and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small Scale Digital Devices," *Journal of Digital Forensic Practice*, Vol. 1, December 2006, pp. 291-296.

23. *Ibid*.

24. *Ibid*.

25. Michael Losavio, Julia Adams, Marc Rogers, "Gap Analysis: Judicial Experience and Perception of Electronic Evidence," *Journal of Digital Forensic Practice*, Vol. 1, March 2006, pp. 13-18; Michael Losavio, Deborah Wilson, Adel Elmaghraby, "Implications of Attorney Experiences with Digital Forensics and Electronic Evidence in the United States," Third International Workshop on Systematic Approaches to Digital Forensic Engineering, Institute of Electrical and Electronic Engineers (IEEE), May 22, 2008, Berkeley, CA; Survey of digital forensics session attendees of the Kentucky Council on Crime and Delinquency, September 2008 (unpublished); Survey of attendees at federal defender training, New Orleans, LA, February 2008 (unpublished).

26. See Technical Working Group for Electronic Crime Scene Investigation, *Electronic Crime Scene Investigation: A Guide for First Responders*, Washington, DC: National Institute of Justice, July 2001.

27. Michael Losavio *et al*., *The Key Asset Protection Partnership: Computer Security, Homeland Security and Community Engagement,* The American Community Preparedness Conference, Louisville, KY, May 12, 2004, p. 38.

28. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information*

and Information Systems, Gaithersburg, MD: National Institute of Standards and Technology, February 2004, as applied to the collateral impact of home system compromise on infrastructure.

29. *Ibid*., p. ix.

30. M. Wilson, and J. Hash, *NIST Special Publication 800-50, Building An Information Technology Security Awareness and Training Program,* Gaithersburg, MD: National Institute of Standards and Technology, October 2003.

31. Available from *csrc.nist.gov/securebiz/index.html*; presentation of Dr. Alicia Clay of NIST to the Department of Computer Engineering and Computer Science, Speed School of Engineering, University of Louisville, March 2004.

32. R. Peterson, *Protecting Our Nation's Cyber Space: Educational Awareness for the Cyber Citizen*, Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, United States House of Representatives, 2004, available from *www.educause.edu/ir/library/pdf/SEC0407.pdf*. In his remarks, Peterson notes that training is not sufficient; secure technology must be an objective of all software development.

33.· Awareness and Outreach Task Force of the National Cyber Security Partnership, *2004 Task Force Report*, 2004, available from *www.educause.edu/ir/library/pdf/SEC0403.pdf*.

34. *CyberBlockWatch*, available from *www.speedacm.org/dhs*.

35. Available from *www.staysafeonline.info/*.

36. J. L. Linderman and W. T. Schiano, "Information Ethics in a Responsibility Vacuum," *The DATA BASE for Advances in Information Systems*, Vol. 32, No. 1, 2001, pp. 70-74.

37. P. J. Denning, "Who Are We?" *Communications of the ACM*, Vol. 44, No. 2, 2001, pp. 15-19.

38. M. Losavio, "Cybersecurity and Homeland Security," *Kentucky Bench and Bar*, Vol. 67, No. 6, 2003, pp. 36-38.

CHAPTER 7

THE ATTACK DYNAMICS OF POLITICAL AND RELIGIOUSLY MOTIVATED HACKERS

Thomas J. Holt

INTRODUCTION

There is a significant body of research focused on mitigating cyber attacks through technical solutions. Though these studies are critical to decrease the impact of various vulnerabilities and hacks, researchers still pay generally little attention to the affect that motivations play in the frequency, type, and severity of hacker activity. Economic gain and social status have been identified as critical drivers of computer hacker behavior in the past, but few have considered how nationalism and religious beliefs influence the activities of some hacker communities. Such attacks are, however, gaining prominence and pose a risk to critical infrastructure and web based resources. For example, a number of Turkish hackers engaged in high profile web defacements against Danish websites featuring a cartoon of the prophet Muhammad in 2005. In order to expand our understanding of religious and nationalist cyber attacks, this chapter will explore the active and emerging hacker community in the Muslim majority nation of Turkey. Using multiple qualitative data sets, including interviews with active hackers and posts from multiple web forums, the findings explore the nature of attacks, target selection, the role of peers in facilitating attacks, and justifications through the lens of religious and national pride. The results can benefit information security professionals, law enforcement, and the intelligence community by providing unique insights on the social dynamics driving hacker activity.

The growth and penetration of computer technology has dramatically shifted the ways that individuals communicate and do business around the world. The beneficial changes that have come from these technologies have also led to a host of threats posed by computer criminals generally, and hackers specifically. In fact, the number of computer security incidents reported to the U.S. Computer Emergency Response Team (CERT) has grown in tandem with the number of individuals connected to the Internet.[1] Data from CERTs around the world suggest that the number of computer attacks have increased significantly since 2001.[2] Computer attacks are also costly, as unauthorized access of computer systems cost U.S. businesses $20 million dollars in 2006 alone.[3]

Research from the social sciences has explored computer attackers and malware writers in an attempt to understand their reasons for engaging in malicious activity. Criminological examinations of hacker subculture found that computer hackers value profound and deep connections to technology, and judge others based on their capacity to utilize computers in unique and innovative ways.[4] Similar research on virus writers suggests they may share hackers' interests in technology, though they are driven by more malicious interests.[5]

A small body of research has also considered the motives that drive the hacker community.[6] The Honeynet Project argues that there are six key motivations in the hacker community: money, entertainment, ego, cause, entrance to a social group, and status. A number of studies have identified the significant financial gain that can be made by hacking databases to steal credit cards and financial information.[7] Additionally, a burgeoning market has developed around the sale of malicious software and stolen data, particularly in Eastern Europe and Russia.[8] Additionally, research on the enculturation process of hacker subculture has found that peer recognition is vital to gain status and recognition.[9]

Research on cause-based hacking has, however, increased in recent years as more countries become connected to the Internet. Mainstream and alternative political and social movements have grown to depend on the Internet to broadcast their ideologies across the world. Groups have employed a range of tactics depending on the severity of the perceived injustice or wrong that has been performed.[10] For example, the native peoples, called Zapatistas, in Chiapas, Mexico, used the Internet to post information and mobilize supporters to their cause against governmental repression.[11] Chinese hackers frequently engage in cyber attacks against government resources in the United States and other nations to obtain sensitive information and map network structures.[12] Finally, a massive online conflict developed between Russian and Estonian factions in April 2006 when the Estonian government removed a Russian war monument from a memorial garden.[13] This conflict became so large in scope that hackers were able to shut down critical components of Estonia's financial and government networks, causing significant economic harm to citizens and industry alike.[14]

Though there is a growing body of research considering hacking as a means to a political or patriotic end, few have considered the ways that religion affects hacker behavior. This is a particularly salient issue when considering the growing number of Muslim nations connecting to the Internet. The penetration of high speed Internet connectivity and computer technology in Muslim-majority nations is changing the landscape of the Internet, enabling political and religious expression and global exposure to various perspectives.

These benefits are, however, offset by the growth of hacker communities that are motivated by religious beliefs. For example, a Danish newspaper published a cartoon featuring the prophet Muhammad with a bomb in his turban in 2005.[15] This image was deemed offensive by the Muslim community, and the newspaper's website was defaced repeatedly, along with any other site that featured the cartoon.[16] Thousands of websites were hacked or defaced by Turkish hackers, who in turn received a great deal of attention by the press for their efforts.[17] As a consequence, Turkish hacker groups have become active participants in a range of attacks against various targets across the globe.[18]

In light of the potential threats and the under-examined nature of this problem, this chapter explores the ways that the specific motives of religion and nationalism affect hacker attitudes and activities. Using multiple qualitative data sets collected from active Turkish hackers, the findings consider how political and religious ideologies shape perceptions and justifications of hackers within this community.

DATA AND METHOD

The data for this chapter consists of two unique resources: a series of 10 in-depth interviews conducted via e-mail or instant messaging with prominent hackers in the Turkish community, and explorations of six websites operated by and for Turkish hackers.

The first data set consists of interviews that probe individuals' experiences and impressions of the Turkish hacker community on and offline. They were asked to describe their experiences with hacking, interactions with others in on and offline environments, and their direct opinions on the presence of a hacker subculture in Turkey.

Interviewees were identified and contacted through the use of two fieldworkers with significant status among Turkish hackers. Individuals who responded to the solicitation were sent a copy of the survey protocol, allowing the respondent to complete the instrument at their leisure. In addition, individuals were given the option to complete the instrument in either Turkish or English. Interviews completed in Turkish were transcribed from Turkish to English by a certified translator to ensure accurate and reliable data.

To gain more insight into the Turkish hacker community, ethnographic observations were conducted in six Turkish hacker web forums where the interviewees claimed to visit or post content on a regular basis. Participants in these forums interact with one another by posting on "threads" within the forum. Threads are textual conversations that are organized chronologically within the forum.[19] These posts are cultural artifacts that are amenable to analysis as they resemble a running conversation between participants.[20] These sites were also publicly accessible, in that anyone could access the forum content without the need to register with the site. This sort of publicly accessible web forum is common in online ethnographic research, as individuals who are unfamiliar with a certain form of behavior may be most likely to access a public forum first.[21] Specific web addresses and names of these sites are not provided to protect the anonymity of the users. The content of these sites were translated using machine translation programs to ensure accurate translation.

Both data sets were printed and analyzed by hand using the three-stage inductive analysis methodology derived from grounded theory.[22] This coding and analysis scheme is particularly useful as it permits the researcher to develop a thorough, well-integrated examination of any social phenomena. Any concepts found within the data must be identified multiple times through comparisons to identify any similarities.[23] In this way, findings are validated by their repeated appearances or absences in the data, ensuring they are derived and grounded in the data.

For this analysis, the techniques of hacking and significance of religion and national values were inductively derived from the repeated appearance of specific actions, rules, or ideas in the data. The value of these concepts is generated from positive or negative comments of the respondents. In turn, theoretical links between these concepts are derived from the data to highlight the value of nationalism, Islam, or other interests that structures the behavior of hackers. The findings are discussed using direct quotes from both data sets where appropriate.

FINDINGS

Knowledge Among Turkish Hackers.

To understand the Turkish hacker community, it is necessary to first consider how individuals relate to computer technology, and their peers. To that end, Turkish hackers suggested that their ability to target and engage in attacks depended on their knowledge of computers and networked systems. Those with a deeper understanding were able to engage in more successful and novel attacks than others.[24] Hackers across the data sets gained knowledge on computer systems in two ways: personal experience and through peer mentoring. The interviewees argued that learning through practice and trial and error are essential to increase knowledge of computer systems, in keeping with research on hacker communities around the globe.[25] For example, "Agd_Scorp" stated that he learned computer systems and hacking through "trial and error, and some documents on the Internet. But trial and error is the best method."[26] Similarly, "The Bekir" described gaining access to information online, but needed to expand his knowledge through firsthand experience: "In the beginning I looked at illustrated explanations on the web and acted accordingly, but they were not sufficient for me. I wanted to learn how this was done, how these were provided and I fiddled about with them a lot until they broke down."[27]

Several of the individuals interviewed also stated that they gained practical knowledge through direct and indirect assistance from others in the hacker community. Individuals could gain indirect assistance from their peers by accessing videos or documents posted in a number of outlets online. These materials provide detailed information on system processes, as well as step-by-step instructions on methods of hacking. For example, "Iscorpitx" made video tutorials on web defacements in order to help the community. He succinctly explained his reasons, stating: "In general, I like sharing the things I do after a while. A lot of videos I recorded while defacing online were very useful for a lot of people who are on the security side of this business. Of course, you can't be skilled and informed in every subject. Everybody needs help."[28] Similarly, "Axe" stated that his hacking activities began in earnest when he felt "it was the time to apply what I saw in the videos I watched."[29]

Forums are also an important resource for information since they act as repositories for information on computers and hacking. All of the forums in this sample had sections devoted to computer security, networking, and hacking, with distinct subsections centered on specific operating systems, programming languages, and tools. Thus, visiting a forum enabled an individual to learn on his own by reading the various materials posted. Forums also provide individuals with indirect assistance through tutorials written by skilled hackers that provide direct information on the process of engaging in attacks. For example, two of the forums in this sample had how-to guides on structured query language (SQL) injection and the process of defacing websites. Three others had detailed tutorials on how to perform cross-site scripting attacks against a variety of sites. These resources are written so as to inform other hackers, and provide clear advice to the larger population of hackers. Thus, myriad resources are available to facilitate indirect social learning in the Turkish community.

Direct interactions with others online are also important to the development of Turkish hackers. Only three interviewees suggested that they were directly taught how to hack by their peers, suggesting this is an infrequent practice among Turkish hackers. For example, "Blue Crown" described his introduction to hacking through a unique interaction:

> I had some interest in hacking but I wasn't planning to get involved in this business. One day, an interview with a hacking group on television caught my attention. . . I turned on my computer and immediately started to browse. I met a hacker with a code name SheKkoLik in Ayyildiz Tim. I owe him/her a lot. . . I thought I couldn't do anything but s/he helped me and taught me a few things. I learned quickly thanks to the interest I had.[30]

Online discussions with other hackers were, however, very common and critical to provide useful information on technology and hacking. In fact, the majority of respondents suggested that they visited either forums or chatted with others using Microsoft (MSN) Instant Messaging. Forums enable individuals to connect with and ask questions of other hackers. When an individual asked a question, forum users would give web links that would help answer the question. These links provided specific information about an issue or topic discussed in the string without repetition or wasted time for the other posters. This would also encourage self-discovery as the user would have to actively open the link and read to find their answer. Some users would also provide brief instructions that would help to address the issue, though this could often encourage debate over the accuracy of the answer. In fact, "The Bekir" espoused the value of forums, stating: "There was a web forum, which was created by a very close friend of mine. I was in that forum for 2-3 years and it was quite nice . . . I learned a lot of things at that site and helped them to learn a lot of things as well."[31] This suggests knowledge is vital to facilitate attacks and develop skills within the Turkish hacker community.

Knowledge and Attack Methods.

The process of acquiring knowledge of computers and hacking has a critical impact on the types of attacks individuals perform. Those with greater skill could complete more sophisticated attacks. "Iscorpitx" succinctly described this issue, stating:

> If a hacker wants to harm a site where s/he has an obsession, s/he will. If s/he can't, s/he can get help. If s/he can't do anything, s/he can stop the publication of the website using a DDoS attack. But if s/he wants, s/he can cause harm. The ones who have enough knowledge and information can manage this; otherwise it is very difficult. The ones who don't have enough knowledge can't get help as well.[32]

This statement emphasizes the range of attacks that hackers can engage in. In fact, "Amon" was a very skilled hacker who indicated he could complete hacks related to "ASP, SQL union, update, Linux root, etc. It is easy to use if you know what you are doing. Of course, I generally use my own tools."[33]

The types of tools used also depend on the target and end goal of the hack. For example, "Crazy King" suggested that he and his colleagues:

> use a key logger and trojan in personal and special/private attacks. We use bots to overstrain the server and put it out of operation in transcendent systems . . . They are the sources that we develop ourselves and belong to us.[34]

"Blue Crown" made a similar point, suggesting:

> When I'm going to perform a personal hack, I need an undetected keylogger or trojan. Some trojans

> are subject to payment and some of them are free of charge. The only difference between these two trojan types is that trojans subject to payment are undetectable (they can't be caught). I can make a free of charge trojan "undetectable" by using some Crypt programs. Friends who develop the Crypter work for this. They usually use well-known and existing weak points/holes. If Turkish hackers find a hole/weak point, they share this after exploiting it.[35]

The notion that Turkish hackers use existing flaws and weaknesses is an important point due to the fact that the forums also provided access to a variety of resources and attack tools. Individuals could quickly and efficiently download a variety of malware, such as Turkojan. This tool is an efficient Turkish made trojan that is designed to "steal passwords, act as a remote viewing tool, and efficiently alter system processes."[36] Multiple versions of this tool were available, as were a variety of other programs, such as password sniffers, rats, virus code, and rootkits made by hackers in other countries. Thus, access to web forums coupled with a strong knowledge of computer technology enable Turkish hackers to engage in a variety of attacks against global targets.

Religion, Politics, and Hacking.

Turkish hackers across the data sets placed significant emphasis on using their knowledge to support "the mission." In this case, the mission referred to attacks against a variety of targets based on religious and national beliefs. The importance of a mission was evident across interviewees, and reflected these beliefs. For example, "Amon" suggested that "everything is for the mission. . . . Which other nation is as patriotic as Turks."[37] "Ghost 61" also described how the mission makes Turkish hackers unique relative to other communities: "everyone does this [hacking] for money and financial benefits, but Turkish hackers do it for the flag, for the homeland."[38] "Iscorpitx" also reflected on the range of interests and missions evident in the Turkish hacker community:

> Among Turkish hacker groups, we can count Islamic groups, revolutionist groups, groups with ideas supporting Ataturk, nationalist groups, etc. There are very talented and skilled young people. . . But these talents are very rare. They have much respect for their national and moral values.[39]

The forums also supported the notion of a military-style mission, as individuals regularly evoked nationalistic and religious symbols as part of their avatar, or personal image. Forum users across the sites used images of the Turkish flag as part of their avatar background, or featured pictures of the national soccer team players because of their pride in the team. Others' avatars used military images, such as soldiers carrying rifles, bombs, or missiles. Some used pictures of masked militants holding rifles or making threatening gestures with swords or knives.

The mission within the Turkish hacker community affects the nations targeted in their attacks. Several of the individuals interviewed argued that they target resources in countries that are perceived as threats to or enemies of Muslim nations. For example, "Ghost 61" stated "I determine it [targets] according to the agenda; usually they are countries like the USA, Israel, Russia, in other words, enemies of Muslims."[40] "Agd_Scorp" echoed this sentiment stating that he targeted those countries that "deliberately attacks Muslims . . . America is the country which killed the most Muslims in the world. And United Nations also killed many Muslims and innocent people."[41] In fact, "Blue Crown" noted that Danish websites were a particularly large target due to their portrayal of the prophet Mohammed in a disparaging cartoon. He indicated that "nearly HALF of the sites with the .dk extension were hacked by Turkish hackers in order to protest the disgusting and dreadful cartoons by Denmark."[42]

The types of sites Turkish hackers targeted were also impacted by the mission. Individuals actively attacked websites and resources that are perceived as either against Islamic religious precepts or actively harmed Turkish interests. For instance, "The Bekir" wrote that: "I determine my targets in terms of hits. I was working on hacking websites that were involved in terrorism; if the hacked website is big then it makes a greater splash, I'm usually working on hacking terrorism sites, etc."[43] "Blue Crown" suggested that he and his peers "hack PKK and pornographic sites."[44]

One of the most important and common forms of attacks used to support the mission are web defacements. This involves using an exploit or vulnerability to replace or remove a web page with a new image of the hackers' choosing.[45] Defacements enable hackers to post messages and images that indicate their perspectives and beliefs, as well as gain status by listing their name and group affiliation. To that end, the interviewee "Iscorpitx" held a world record for mass defacements and used this type of attack as a means to support his religious agenda. He actively selected sites that act in opposition to Islamic tenets, particularly "gambling sites, child pornography and disgusting pornography were always my targets. . . I think there's no other defacer who harmed sites in these sectors as much."[46]

The forums also had teams that operate in support of web defacements. One such forum had an "operations" section dedicated to discussions and listings of all the sites that the group's members have defaced. The titles of threads within this subforum clearly indicate the diverse range of targets defaced by Turkish hackers, and to a lesser extent, their connection to Islam:

- Threat to French Site
- Korean Yahoo Sites – "I have defaced a famous Korean site."
- The group has defaced 1,000 sites!
- Join our site and help deface
- Our martyrs have defaced many sites
- Deface Announcements
- We will eliminate the world (world wide web)
- Web sites hacked
- 20 web site templates hacked
- Adina Hotel hacked
- 20 Video Sites Hacked
- English Receiving Site Hacked
- USA Enterprises Hacked
- Buddhism and Satanism Sites Hacked.[47]

The importance of "the mission" also affects social organization practices among Turkish hackers. Though many individuals stated they hacked by themselves, they would work with others depending on the size and scope of the target. "Amon" emphasized this point, writing:

> They [Turkish hackers] form groups. It doesn't take long, it is done quickly. They do not team-up for a single website. Then somebody comes up and announces that he broke into a site...You check it and it is really broken... But then it becomes a team job, although a single person discovers it usually.[48]

"Crazy King" also elaborated on this point, writing:

> If popular events (like war) are the case, they come together as a team in order to harm the systems with country extensions. Individually they target large systems and work individually in order to leave protesting messages. They do this by telling their common actions to each other or with the documents they write in the forums or videos or texts. If there is a very important event involving the world and people, they can immediately come together.[49]

The forums also provided some important insights into organizational hierarchies. For example, one site established its leadership and attack command structure based on individual performance in a hacking challenge set up through their website. Individuals must progress through 13 missions, and their performance establishes how they will participate in the larger group. The missions include the following activities:

1. HTML code
2. SQL Injection
3. RC4 Encryption
4. Zip Crack
5. Page Redirect
6. PWL Crack
7. Secret Question
8. VB Script Encode
9. JS Password
10. Serv-U FTP
11. ICQ Dat Crack
12. Front Page
13. Carefully

All of the forums also provide a detailed command structure for their forums, composed of administrators who supervise and control the sites that house the forums, co-administrators who handle certain aspects of the site and forums, super-moderators who manage the entire web forum, and forum moderators who deal with content-specific subforums. This structure ensures easy operation and management, and establishes clear levels of respect and status that must be afforded to the management structure. One site even provided a flow chart to specify forum operations and dictate how complaints and suggestions move through the chain of command. Thus, religion and national pride clearly affect the actions, targets, and practices of Turkish hackers.

DISCUSSION AND CONCLUSION

This chapter sought to explore the impact of religious and political motives on the activities of the Turkish hacker community. The findings indicate that they place significant value on understanding computer technology because their level of knowledge impacts their ability to hack. Hackers could increase their understanding of computer systems by working with various technologies on their own, or by reading tutorials and watching videos posted online. Interacting with other hackers in forums is also important as these relationships can foster an individual's development as a hacker. In this way, the Turkish hacker community reflects the critical role of technology in structuring hacker and virus writer behavior across the globe.[50]

The interviewees and forum users also indicated that they were heavily influenced by their religious and national affiliations. In fact, the importance of Islam for the Turkish community cannot be understated as it provided a "mission" that must be completed. The types of attacks that Turkish hackers engaged in also appeared to encompass the entire spectrum of the global hacker community. Individuals used malware, SQL injection attacks, and web defacements in order to attack various resources. The scope of their attacks were, however, heavily focused on websites and resources in countries that are perceived to either slight the Muslim community, or Turkey specifically.

As a result, it may be that cause-driven hackers are apt to attack high value or visibility targets, rather than large populations of computer users and general resources. This is quite different from the practices of financially motivated hackers, such as in Russia and Romania.[51] As such, further comparative research is needed with a sample of hackers from a variety of Muslim-majority nations to understand the significance of political and religious ideology on hacker activity.

In addition, there may be some distinctive attack signatures that can be developed based on cause-driven attacks. The consistent recognition of "the mission" across the data sets, and the organizational hierarchies present in the forums and interviewee experiences suggest that the tactics employed by religious or politically motivated hackers may differ from those driven by other agendas. Thus, there may be value in developing baseline predictive models of attacker behavior using log files from actual incidents. Future research analyzing multiple real world attacks may be useful in developing technical solutions to mitigate attacks against critical infrastructure and computer resources. Yet there is a strong likelihood that the form and shape of hacker activity varies across countries and political ideologies. Thus, it is essential that researchers begin to focus on computer attackers in a global context to better understand the individuals that attempt to compromise computer systems.

ENDNOTES - CHAPTER 7

1. T. A. Longstaff, J. T. Ellis, S. V. Hernan, H. F. Lipson, R. D. McMillian, L. Hutz Pesante *et al.*, "Security of the Internet," in M. Dekker, ed., *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 15, 1997, pp. 231-255.

2. 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.

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

4. T. J. Holt, "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures," *Deviant Behavior*, Vol. 28, pp. 171-198, 2007; T. Jordan and P. Taylor, "A Sociology of Hackers," *The Sociological Review*, Vol. 40, pp. 757-80, 1998; P. A. Taylor, *Hackers: Crime in the Digital Sublime*, New York: Routledge, 1999; D. Thomas, *Hacker Culture,* Minneapolis: University of Minnesota Press, 2002.

5. A. Bissett and G. Shipton, "Some human dimensions of computer virus creation and infection," *International Journal of Human – Computer Studies*, Vol. 52, 2000, pp. 899-913; S. Gordon, "Virus Writers: The End of the Innocence?" 2000, available from *www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf*; S. Gordon and Q. Ma, *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Cupertine, CA: Symantec, 2003.

6. A. Bissett and G. Shipton, "Some human dimensions of computer virus creation and infection"; Gordon, "Virus Writers"; The Honeynet Project, *Know Your Enemy: Learning About Security Threats*, 2nd Ed., Boston, MA: Addison-Wesley, 2004.

7. S. Furnell, *Cybercrime: Vandalizing the Information Society,* Boston, MA: Addison-Wesley, 2002; G. Newman and R. Clarke, *Superhighway robbery: Preventing e-commerce crime.* Cullompton, UK: Willan Press, 2003; L. James, *Phishing Exposed*, Rockland, MA: Syngress, 2005.

8. James, *Phishing Exposed*; Honeynet Research Alliance, "Profile: Automated Credit Card Fraud," *Know Your Enemy Paper* series, 2003; R. Thomas and J. Martin, "The underground economy: Priceless"; *login,* Vol. 31, pp. 7-16, 2006; T. J. Holt and E. Lampke, "Exploring stolen data markets online: Products and market forces," Criminal Justice Studies, Forthcoming.

9. Holt, "Subcultural evolution"; Jordan and Taylor, "A Sociology of Hackers"; Taylor, *Hackers;* Thomas, "Hacker Culture."

10. D. E. Denning, "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy," in J. Arquilla and D. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica, CA: RAND, 2001, pp. 239-288; T. Jordan and P. Taylor, *Hacktivism and Cyberwars: Rebels With a Cause,* New York: Routledge, 2004.

11. Denning, "Activism, hacktivism, and cyberterrorism"; R. Cere, "Digital counter-cultures and the nature of electronic social and political movements," Y. Jewkes, in *Dot.cons: Crime, deviance and identity on the Internet,* Portland, OR: Willan Publishing, 2003, pp. 147-163.

12. Denning, "Activism, hacktivism, and cyberterrorism"; S. W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State,* New York: Oxford University Press, 2008.

13. Brenner, *Cyberthreats;* G. Jaffe, "Gates Urges NATO Ministers To Defend Against Cyber Attacks," *The Wall Street Journal On-line,* June 15, 2006, available from *online.wsj.com/article/SB118190166163536578.html?mod=googlenews_wsj;* M. Landler and J. Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 24, 2007, available from *www.nytimes.com/2007/05/29/technology/29estonia.html*.

14. Brenner, *Cyberthreats;* Landler and Markoff "Digital Fears Emerge After Data Siege in Estonia."

15. M. Ward, "Anti-cartoon protests go online," *BBC News*, February 8, 2006, available from *news.bbc.co.uk/2/hi/technology/4692518.stm*.

16. *Ibid.*

17. *Ibid;* D. Danchev, "Hundreds of Dutch web sites hacked by Islamic hackers," *ZDNet,* available from *blogs.zdnet.com/security/?p=1788*.

18. Danchev, "Hundreds of Dutch web sites hacked by Islamic hackers."

19. D. Mann and M. Sutton, "Netcrime: More Change in the Organization of Thieving," *British Journal of Criminology*, Vol. 38, pp. 201-29, 1998.

20. *Ibid.*; Holt, "Subcultural evolution."

21. Holt, "Subcultural evolution."

22. J. Corbin and A. Strauss, "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria," *Qualitative Sociology*, Vol. 13, 1990, pp. 3-21.

23. *Ibid*.

24. Holt, "Subcultural evolution"; Jordan and Taylor, "A Sociology of Hackers"; Taylor, *Hackers: Crime in the Digital Sublime;* Thomas, *Hacker Culture.*

25. *Ibid*.

26. Agd-Scorp, Interview, personal email, August 8, 2008.

27. The Bekir, Interview, personal email, July 29, 2008.

28. Iscorpitx, Interview, personal email, July 30, 2008.

29. Axe, Interview, personal email, August 1, 2008.

30. Blue Crown, Interview, personal email, July 30, 2008.

31. The Bekir, Interview.

32. Iscorpitx, Interview.

33. Amon, Interview, personal email, August 10, 2008.

34. Crazy King, Interview, personal email, August 10, 2008.

35. Blue Crown, Interview.

36. Forum, address withheld.

37. Amon, Interview.

38. Ghost GI, Interview, personal emails, August 9, 2008.

39. Iscorpitx, Interview.

40. Ghost GI, Interview.

41. Agd-Scorp, Interview.

42. Blue Crown, Interview.

43. The Bekir, Interview.

44. Blue Crown, Interview.

45. James, *Phishing Exposed*; Brenner, *Cyberthreats*.

46. Iscorpitx, Interview.

47. Forum, address withheld.

48. Amon, Interview.

49 . Crazy King, Interview.

50. Holt, “Subcultural evolution”; Jordan and Taylor, “A Sociology of Hackers”; Taylor, *Hackers: Crime in the Digital Sublime;* Thomas, *Hacker Culture;* Gordon, “Virus Writers”; Gordon and Ma, *Convergence of Virus Writers and Hackers.*

51. James, *Phishing Exposed*; Honeynet, “Profile”; Thomas and Martin, “The underground economy”; Brenner, *Cyberthreats.*