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 is-

sue 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 hack-

ers 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 fo-

rum 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 Mus-

lims . . . 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.*