Insights into the Hacking Underground

Michael Bachmann & Jay Corzine

The Exigency of Cyber-Crime Research and Intervention

Estonia, April 26, 2007. In retaliation for the removal of a World War II-era statue of a Soviet soldier, pro-Russian hackers launched a month-long campaign that has become known as the first war in cyberspace. Using a technique known as distributed denial-of-service (DDoS) attack on a hitherto-unprecedented scale, the attackers managed to effectively shut down vital parts of Estonia's digital infrastructures. In a coordinated effort, an estimated one million remote-controlled computers from around the world were used to bombard the web sites of the President, the Prime Minister, Parliament and other government agencies, Estonia's biggest bank, and several national newspapers with requests. The attacks were so massive that NATO rushed a cyber-warfare team of international security experts to assist the Estonian government, and Jaak Aaviksoo, the country's defense minister, described the attack as a national security situation and requested that the European Union classify it as an act of terrorism (Landler & Markoff, 2007). In reference to the events in Estonia, Suleyman Anil, the head of NATO's incident response center, later warned attendees of the 2008 E-Crime Congress in London that "cyber defense is now mentioned at the highest level along with missile defense and energy security." According to Anil, "we have seen more of these attacks and we don't think this problem will disappear soon. Unless globally supported measures are taken, it can become a global problem" (Johnson, 2008, p. 1).

The above example is merely one incident of what have become a long series of high-profile hacking attacks (Aguila, 2008). Although warnings of the societal-level threat posed by cyber-attacks on critical network infrastructures have been heralded since the 1980s, it is only in recent years that the problem has made it onto the radar screens of governments. Partly due to the experience of Estonia, the U.S. and other countries around the globe are now reassessing the security situations of their key information systems. They are enacting new security measures to better protect their critical network infrastructures, and they are increasing their readiness to respond to large-scale computer incidents (NCIRC, 2008). In Britain, for example, Conservatives have recently proposed the creation of a new position for a cyber-security minister and a national hi-tech crimes police squad to better combat the "growing and serious threat to individuals, business and government […] that will continue to escalate as technology changes" (Johnston, 2008, p. 1).

The implementation of effective technological countermeasures against hacking attacks is facilitated by the knowledge that has already been accumulated through computer science research (cf. Chirillo, 2001; Curran et al., 2005; Erickson, 2008). Several studies conducted by computer scientists and computer engineers have closely examined the technical details of the various attack methods and have produced a significant body of information that can now be applied to help protect network infrastructures (Casey, 2004). Unfortunately, the guidance provided by these studies is limited to only the technical aspects of hacking attacks and, in contrast to the substantial amount of knowledge already gathered about how the attacks are performed, answers to the questions of who the attackers are and why they engage in hacking activities continue to remain largely speculative. Today, the persons committing the attacks remain mysterious for the most part, and information about them continues to be only fragmentary.

The current lack of information concerning the sociodemographic characteristics and the motives of cybercrime offenders can be attributed to a number of issues. One of the main reasons can be traced back to the unfortunate circumstance that, until recently, mainstream criminology has underestimated the potentially devastating societal impacts of cybercrimes and has diverted only limited attention to this relatively new type of criminal behavior (Jaishankar, 2007; Jewkes, 2006; Mann & Sutton, 1998). Cyber-criminology is only now beginning to evolve as a distinct field of criminological research, and it has yet to overcome many methodological and theoretical problems that other areas in criminology have already solved (Yar, 2005, 2006). Law enforcement responses have also been slow to develop and are hampered by several characteristics of cybercrimes, notably the frequent location of perpetrator and victim in different states or nations.

A particular challenge for researchers arises from the various methodological obstacles entailed in the sampling of cybercriminals. As a result of these difficulties, available data sources are scarce, and quantitative studies, such as the annual CIS/FBI Computer Crime and Security Survey, are limited to surveys of cybercrime victims. At this point, only a few qualitative case studies (eg. Mitnick & Simon, 2005; Schell, Dodge, & Moutsatsos, 2002; Taylor, 1999, 2000) and biographies (eg. Mitnick, Simon, & Wozniak, 2002; Nuwere & Chanoff, 2003) exist that examine individual hackers; their motivations, preferences, and hacking careers. While such studies are well suited to provide in-depth insights into the lives of a few individuals, they are unfit for providing generalizable information about the population of hackers at large. Yet, just “like in traditional crimes, it’s important to try to understand what motivates these people to get involved in computer crimes in the first place, how they choose their targets and what keeps them in this deviant behavior after the first initial thrill” (Bednarz, 2004, p. 1).

The aim of this paper which is excerpted from the first author’s dissertation research is to begin filling the wide gap in our knowledge about hackers and the hacking community by providing the first quantifiable insights into the hacking underground. Such insights are needed to create a more profound understanding of the nature of the threat and a more complete assessment of the problem and its solutions. The identification of the reasons and motives behind cyberattacks is not only beneficial for the effective direction of investigation and prosecution efforts and resources; it also helps to better identify the actors' behaviors, to develop better countermeasures, and to make IT systems safer.

Research Design

The goals of the study were to provide generalizable answers to the questions of who hackers are and why they hack. To achieve these goals, the research project was designed to produce quantifiable results that are more representative and can be generalized to a wider target population than those from previous qualitative case studies of hackers (Jordan & Taylor, 1998; Taylor, 1999). A survey was developed and used for data collection (Boudreau, Gefen, & Straub, 2001), because surveys are the data-collection method best suited to produce quantitative results that can be generalized to other members of the population of interest and oftentimes even to other similar populations (Newsted, Chin, Ngwenyama, & Lee, 1996). The survey consisted of a total of 72 items and gathered detailed information about the various phases of the respondents' hacking careers. It embodied items pertaining to the initiation of the hacking activity, its habituation, and the eventual desistance from hacking. It further assessed several other details of the respondent's hacking activity, including a variety of involved decisions and motivations.

The survey was fielded during the 2008 ShmooCon convention in Washington D.C. The ShmooCon convention was selected because its profile attracts a wide variety of hackers and security experts (Grecs, 2008), thus making it the ideal candidate to gather information about the larger population of hackers. Since its first convening in 2004, ShmooCon has developed into one of the largest annual conventions worldwide. Today, it is the largest hacker convention on the East Coast, and it is attended by both U.S. and international hackers and security experts. The 2008 convention was held over the weekend from Friday, February 15 to Sunday, February 17 in the Marriott Wardman Park Hotel in Washington D.C. It was attended by a total of 800 hackers and security experts. Of those, only hackers who had broken into computer systems, networks, or websites illegally, i.e. without an explicit permission from an authorized party, were selected for the study. This restriction systematically excluded about one-third of all attendees, who either claimed to hack only when legally contracted for testing purposes or attended the convention simply because they were interested in computer security issues but had never committed an actual hacking attack. The final sample consisted of 124 individuals, yielding a response rate of approximately 25 percent of the eligible attendees.

Findings

The study shows that the common stereotype of the hacker as a clever, but lonesome male adolescent whose computer proficiency compensates social shortcomings barely begins to tell the whole story of hackers' identities. That is not to say that this stereotypical portrayal of hackers is completely mistaken. Several aspects of the stereotype were indeed confirmed by the survey results as well as the researcher's personal observations during the conference. The participants in this study were indeed highly educated, intelligent persons who focused their intellectual interests on technological developments. Ninety percent of all respondents had at least some college education, and over one-fourth (27 percent) had attained either a Masters or a Ph.D. degree. Many of these technophiles appeared to be equally inventive, creative, and determined. These personality attributes emerged in several findings, including the predominant role of inquisitive motives for hacking activities, hackers' unusually high confidence in their general decision-making ability, and their typically extensive portfolio of various attack methods.

Consistent with the dominant stereotype, the convention attendees were also predominantly male (94 per cent), and minority hackers were rare exceptions. Over 93 percent of the hackers in the sample were Whites, a fraction that substantially exceeds their percentage in the U.S. population. Another noteworthy finding is the fact that Asians (5 per cent) were the largest minority in the sample. This result reflects the racial distribution in most IT professions (Zarrett & Malanchuk, 2005). The near uniformity with regard to the sex and race distributions, however, stood in sharp contrast to the strong emphasis of many attendees on individualism. Many hackers conveyed their individualistic nature in conversations with the researcher as well as through their physical appearances. Their physical expressions of individualism ranged from extravagant haircuts and hair colors, to unusual clothing styles, to large tattoos on various body parts, sometimes even on faces.

The two most important inadequacies of the hacker stereotype seem to be the notions that hackers are invariably young and that they are socially inept. The average hacker in the sample was 30 years of age, a finding that calls the common notion of the prototypical hacker as a delinquent teenager (Yar, 2005) into question. It is reasonable to assume that the higher average age in this study of convention attendees was caused by the sampling frame of this particular research project. The attendees' profile at the ShmooCon convention was geared more toward security experts and computer professionals than to teenagers who pursue their hacking interests merely as a leisure-time hobby. Thus, while the distribution in this particular sample is certainly not enough to refute claims that the majority of hackers are teenagers, nevertheless, it indicates that the hacking community is by no means limited to youth. To the contrary, it involves many mature security experts and many seasoned hackers who pursue their hacking activity in a professional manner. The data clearly show that hacking is not just a "young man's game." The oldest active hacker in the sample was 52 years old, and he reported to have been hacking for close to three decades. Most importantly, the data also revealed that hackers undergo a maturation process over the course of their hacking careers and that the more experienced and seasoned hackers tend to be the most dangerous ones. They are more likely to attack higher profile targets, and some engage in their illegal hacking activities with financial profits as their primary motivation. Young and inexperienced hackers can certainly cause damage with their activities, but the study shows that these hackers attack primarily private targets and do so out of intellectual curiosity, love for knowledge, experimentation, or boredom. Many hackers first become interested in hacking in their teenage years, and, typically, they are not driven by a pronounced initial criminal intent or the desire to make financial profits. As their hacking activities continue to become habitualized, however, many of them develop into more professional and ambitious hackers. Over the course of their hacking careers, many intensify their hacking activities and begin to also attack higher profile targets such as governmental and corporate information systems. Some hackers even reported having turned their once merely deviant juvenile behavior into a criminal business activity. A total of 15 percent of all respondents said that hacking has become their main source of income and that they would reject a target unless it was profitable. Undoubtedly, these experienced veteran hackers should receive the bulk of attention from law enforcement.

Although the comparatively high fraction of unmarried hackers showed that many of them may indeed be hesitant to engage in serious relationships and commitments, the vast popularity of social hacking methods and their high success rates also indicated that the commonly presumed social incompetence of hackers is misleading. The falseness of this assumption was further reaffirmed by some of the observations the researcher made during the convention. Most attendees appeared to be outgoing and sociable. Many attended the convention together with their friends, and most of the attendees seemed to share a distinct sense of humor and mingled quickly. Certainly, the informal observations during the convention and the finding that hackers are skilled in manipulating and “programming” other persons, oftentimes managing to exploit the trust or carelessness of other computer users for their hacking purposes, are not sufficient evidence to strongly reject of the notion that hackers are social hermits. It might be that the sociability of hackers is limited to interactions with likeminded technophiles and that, although many appear to be skilled manipulators, genuine and affectionate social relations are of lesser importance to them. Additional examinations of the social networks of hackers; including their amount, frequency and quality of interactions with close contacts, the types of contacts they engage in (face-to-face or online), and the importance they attribute to these social contacts, are needed.

The debate about the sociability of hackers aside, one of the most important findings of the study was the significant role of social hacking methods. While many persons think of hacking attacks as performed solely through technical means and exploits, they are in fact more diverse and oftentimes involve a combination of technical methods, social methods, and circulations of different kinds of malicious code, such as viruses or

Trojan horses (Erickson, 2008). In the context of hacking attacks, the term social methods denotes a variety of attacking techniques that can be summarized as attempts to establish and subvert trust relationships with victims or to predict the behaviors of victims. Once such a relationship is established, the attacker tricks the victim into revealing information or performing an action, such as a password reset, for example, that can then be used in the attack. To gain a clearer picture of the prevalence of each of the three types of attacks and to obtain a better understanding of the composition of typical hacking attacks, all three types of attacks were assessed independently.

The separate analyses of the three main hacking techniques showed that many hackers combine social and technical methods and launch attacks that are comprised of both tactics. The more detailed examination of preferences for certain types of technical hacking attacks confirmed that many hackers combine different reconnaissance methods with different intrusion and cover-up techniques. Of the different technical methods to gain access to a system, the various techniques to obtain passwords were the most frequently used. These results suggest that the classic exploitation of password weaknesses remains popular today. Overall, the success rate reported by all respondents showed that, personally, they estimated about half (48 per cent) of all their technical intrusions to have been successful. While a close to 50 percent success rate of all technical intrusions is high, the estimated success rate of social methods was even higher (62 per cent). This very high success rate for social methods was one of the most surprising findings in this study. It demonstrates that the popular image of hackers as social hermits who launch their hacking attacks solely through remote computer and network technology, or even do so mainly to compensate for social deficits, has to be revised. The opposite seems to be the case. Hackers seem to be socially capable persons who know how to successfully manipulate and trick other persons. Moreover, the study showed that hackers who combine social and technical attack methods were the most successful ones. The common perception of hacking attacks as being executed solely through technical means and the perception of hackers as socially incompetent are most likely part of the reason why the danger posed by social engineering attacks is oftentimes underestimated. Unless these perceptions are revised and the awareness of social hacks is raised, social engineering methods will predictably continue to be very successful and will continue to pose a serious threat to individuals and organizations.

Different from social and technical attack strategies, which were very popular and oftentimes used in combination, the reported distribution of malicious codes was rare. Thereby, the surveyed hackers demonstrated having a strong preference for directed attacks on selected targets over widely dispersed and randomly distributed attacks without specific targets. It appears that phishers, spammers and virus coders are a group of cybercriminals that is distinctively different from “traditional” hackers.

Policy Implications

The conclusions that can be derived from this study are not limited to contributions to the scientific discourse about cybercrime offenders. They also hold some important implications for efforts to combat cybercrimes. Experts agree that current strategies to combat this threat face a multitude of challenges that have to be addressed. Aside from the resource shortages and other practical difficulties, law enforcement efforts to combat cybercriminals are also hampered by a shortage of substantive and reliable information that can be used for the creation of offender profiles. Detailed profiles of the different types of cybercriminals, their skill levels, and their motivations are critical because they provide helpful guidance for ongoing investigation of cybercrimes and, thereby, increase the effectiveness of current prosecution efforts. A more effective response by both the criminal justice system and the private sector is urgently needed—not only because it would increase the number of convicted cybercriminals but, more importantly, because it would also have a preventive deterrence effect on the larger hacking community.

In relation to law enforcement, the findings of this study suggest that the creation of a deterrent effect through enhanced apprehension and prosecution is an essential component of efforts to combat cybercrime. Unfortunately, present efforts to curb cybercrimes are hardly suited to accomplish this goal. Despite the annually increasing number of cybercrimes, only a relatively few high profile cases are successfully tried at present, and many of them do not lead to swift or severe punishments (Brenner, 2006). The continuing unlikeliness of punishment is particularly problematic because it severely undermines any efforts to deter criminal behavior in cyberspace. Indeed, the findings of the present study demonstrate that many hackers are aware of the slim chances of being detected and punished. The current improbability of becoming prosecuted even led some hackers to report that they have never been afraid of being apprehended or prosecuted. Furthermore, the risk awareness of most hackers seems to decrease over time as they repeatedly learn that their actions have no negative consequences for them.

Nevertheless, several findings from this study also signify that deterrence can be a successful strategy to prevent cybercrimes. The study revealed that many hackers have a nuanced risk awareness. For example, the majority of hackers report having become more concerned about risks in recent years, a finding that suggests that increased efforts to combat cybercrimes do not go unnoticed in the hacking community. Furthermore, many hackers evidently distinguish between the chances of becoming detected and apprehended and the consequences of these two events. Most importantly, the data also indicate that the most successful hackers are the ones that also have the highest risk awareness. Thus, these hackers seem to be the ones that are most susceptible to changes in risk estimates.

Deterrence undoubtedly is an indispensable component in the control of all criminal behaviors, but is seems to be particularly suited to prevent cybercrimes. Unlike other, less deliberately acting types of criminals, hackers plan their hacking attacks, and they oftentimes do so in an explicitly rational manner. Consequently, they should be more easily dissuaded than criminals who commit their crimes spontaneously when opportunities arise. Taken together, the findings of this study suggest that a more pronounced deterrence perspective needs to become a central addition to the existing technical approaches to cybercrime prevention. However, merely adding deterrence as one separate component will not suffice. To be effective, a deterrence perspective has to be integrated into currently existing national policy efforts beyond the criminal justice system. One promising approach to establish deterrence policies in the private sector could be directed at businesses and organizations. The study showed that most hackers pursue legal careers in legitimate jobs and companies. Organizations and companies that offer IT security services or are otherwise attractive to hackers should be encouraged to promote awareness of the potential consequences of committing cybercrimes. For example, they could distribute information about punishments that have been given to convicted computer criminals as well as other informational materials that directly highlight what constitutes a crime under the law. Other informal control mechanisms, such as extra-legal social stigmata or the systematic introduction of negative effects on job opportunities, might also be strong incentives to prevent particularly young, middle-class computer experts from becoming involved in computer crime. Unquestionably, the establishment of effective deterrence efforts as an integral part of cybercrime prevention strategies will not be an easy undertaking. The vast range of cybercrime activities and the multitude of different offenders considerably complicate the selections of the most appropriate deterrence policies. Strategies that are most effective for leisure-time juvenile hackers will most likely be unfit to deter destructive computer-security experts or other seasoned hackers from attacking computer systems for monetary gains. Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishments can prevent some crime incidents and provide some protection from an increasingly serious problem. Companies in branches that typically employ hackers can certainly be particularly helpful in deterring computer crimes, but the results of this study also indicate that all companies and organizations need to do more to actively prevent victimization, regardless of their branch. The analysis of the different hacking methods showed that, of the three main types of attack methods, social engineering attacks are the most successful ones. It also revealed that the various methods to obtain user passwords, whether the systematic guessing of weak or standard passwords or the theft of user logins, remain the most common ways hackers gain access to their targets. Thus, it seems that the weakest points of companies and organizations are their employees. Corporations have to educate their employees about social hacking methods. They need to raise awareness of the seriousness and frequency of the problem, educate their staff about the wetware tactics commonly used by hackers, and give them instructions of how to avoid becoming victimized.

The education of employers, while definitely an important protective measure, is not the only contribution that will be required from organizations. They also need to start reporting all their victimization incidents to the authorities. The current situation, in which many organizations refrain from reporting incidents to protect their own interests and thereby harm the interest of all businesses, needs to be changed because, unless more incidents are reported, computer crimes are unlikely to become controllable. The benefits and detriments of a mandatory reporting system are debatable, but a reporting requirement would certainly benefit efforts to manage cybercrimes. It would put law enforcement agents in the position to decide which cases to devote their attention to rather than be dependent on the willingness of organizations to submit their cases in order to press charges.

Concluding, it has to be pointed out that cybercriminology is only just beginning to develop and our knowledge about cybercrime offenders remains fragmentary at best. The present study yields some important insights into the composition of the hacking underground, and it sheds some light on the motivations and maturation processes of hackers. Nevertheless, it is but one step toward the establishment of cybercriminology as a distinct subfield of criminological research and the development of successful strategies of prevention and apprehension by law enforcement and prosecution by the courts.

References

Aguila, N. (2008). The fifteen greatest hacking exploits: The birth of hacking. March 16. Retrieved from http://www.tomshardware.com/2008/03/14/the_fifteen_greatest_hacking_exploits/index.html.

Bednarz, A. (2004). Profiling cybercriminals: A promising but immature science. May 3. Retrieved from http://www.networkworld.com/supp/2004/cybercrime/112904profile.html.

Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 11*(1), 1-16.

Brenner, S. (2006). Defining cybercrime: A review of state and federal Law. In R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution, and defense of a computer-related crime* (pp. 13-94). Durham, NC: Carolina Academic Press.

Chirillo, J. (2001). *Hack attacks revealed: A complete reference with custom security hacking toolkit*. New York: John Wiley.

Curran, K., Morrissey, C., Fagan, C., Murphy, C., O'Donnell, B., Firzpatrick, G., et al. (2005). Monitoring hacker activity with a honeynet. *International Journal of Network Management, 15*(2), 123-134.

Erickson, J. (2008). *Hacking: The art of exploitation* (2nd ed.). San Francisco: No Starch Press.

Grecs. (2008). ShmooCon 2008 infosec conference event. April 25. Retrieved from http://www.novainfosecportal.com/2008/02/18/shmoocon-2008-infosec-conference-event-saturday/.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1-6.

Jewkes, Y. (2006). Comment on the book 'Cyber crime and society' by Majid Yar. September 09. Retrieved from http://www.sagepub.co.uk/booksProdDesc.nav?prodId=Book227351.

Johnson, B. (2008). Nato says cyber warfare poses as great a threat as a missile attack. May 2. Retrieved from http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.

Johnston, P. (2008). Tories want new cybercrime police unit. March 07. Retrieved from http://www.crime-research.org/news/06.03.2008/3236/.

Jordan, T., & Taylor, P. A. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Landler, M., & Markoff, J. (2007). Digital fears emerge After data siege in Estonia. *The New York Times*. August 25. Retrieved from http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1&ei=5070&en=15ee9940d96714da&ex=1188187200.

Mann, D., & Sutton, M. (1998). Netcrime. More change in the organisation of thieving. *British Journal of Criminology, 38*(2), 210-229.

Mitnick, K. D., & Simon, W. L. (2005). *The art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers*. New York: John Wiley.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The art of deception: Controlling the human element of security*. New York: John Wiley.

NCIRC. (2008). NATO opens new centre of excellence on cyber defense. May 3. Retrieved from http://www.nato.int/docu/update/2008/05-may/e0514a.html.

Newsted, P. R., Chin, W., Ngwenyama, O., & Lee, A. (1996). *Resolved: Surveys have outlived their usefulness in IS research.* Paper presented at the Seventeenth International Conference on Information Systems, Cleveland, OH.

Nuwere, E., & Chanoff, D. (2003). *Hacker cracker: A journey from the mean streets of Brooklyn to the frontiers of cyberspace*. New York: Harper Collins.

Schell, B. H., Dodge, J. L., & Moutsatsos, S. (2002). *The hacking of America: Who's doing it, why, and how*. New York: Quorum.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London and New York: Routledge.

Taylor, P. A. (2000). Hackers - cyberpunks or microserfs. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Zarrett, N. R., & Malanchuk, O. (2005). Who's computing? Gender and race differences in young adults' decisions to pursue an information technology career. *New Directions for Child and Adolescent Development, 2005*(110), 65-84