The Red Scare: The Evolution and Impact of Russian Computer Hackers

**A thesis submitted to the Miami University
Honors Program in partial fulfillment of the
requirements for University Honors with Distinction**

by

Justin Allen Wilmes

**May 2006
Oxford, Ohio**

ABSTRACT

This thesis includes a discussion of hacker self-image and motives, the public perception of hackers, and the economic impact of Russian hackers. It looks at popular categories of hacker activity in Russia, such as phreaking and worm creation, and how these activities relate to Russian hacker motivations. I will show that the roots of hacking in Russia are tied to the following cultural and historical motivations: intellectual challenge, prestige among the hacker community, a desire for profit, nationalism, disenchantment and underemployment in post-1991 Russia, the Soviet Union's history of state-sponsored hacking, and a culture of opportunism. Finally, I will analyze specific case studies that illustrate many of these arguments and observations.

…

The Red Scare: The Evolution and Impact of Russian Computer Hackers
by Justin Allen Wilmes

Approved by:

_____, Advisor
Dr. Benjamin Sutcliffe

_____, Reader
Dr. Margaret Ziolkowski

_____, Reader
Dr. Scott Campbell

Accepted by:

_____, Director,
Dr. Carolyn Haynes
University Honors Program

Acknowledgements

I would like to thank my thesis mentor, Dr. Ben Sutcliffe, for his guidance and ideas and for the countless hours he put into this project. Much thanks to Dr. Douglas Troy and Dr. Scott Campbell for their time and comments. Thanks to Dr. Paul Mitchell for the craic. Thanks to my friends and roommates who have weathered the brooding that resulted from my long hours of research. Finally, thank you to Marisa Bowersox for keeping me in line, and also for the perpetual loan of your laptop, on which much of this thesis was written. And for Bella.

Table of Contents

Introduction

Until recently study of Russian literature, history, and politics has generally precluded serious analysis of anything in the realm of popular culture. For instance, Russian literature has traditionally been viewed in terms of competing forces (low culture versus high culture), which for Catriona Kelly "produces a history in which questions about the relative popularity of literary texts, or other cultural artifacts are not asked, and where popular cultural forms play a role only in so far as they impinge upon the production of culture proper" (Kelly 5). In recent years, however, scholars have begun applying a cultural studies approach to traditional areas of Russian scholarship as well as new ones, and this has allowed for a more comprehensive understanding of Russian culture. The cultural studies approach, "allows for the study of previously un- or under-valued cultural products and identities" (12).

Hackers are one such under-valued cultural phenomenon. While the news media is replete with stories about hacker activity and the information technology industry regularly releases studies addressing the economic impact of hackers, few studies attempt to encompass the wide range of pertinent issues: the roots of hacker culture, hacker motivations, hacker public perception and misperception, statistical analyses of hacker activity and impact, etc. Hackers are not purely an economic, ideological, or technological phenomenon. They are intrinsically linked with culture. My analysis will therefore employ a cultural studies approach to the subject of Russian computer hackers

in order to achieve a more holistic understanding both of this subculture and, by extension, Russian culture in general.

This thesis includes a discussion of hacker self-image and motives, the public perception of hackers, and the economic impact of hacker activities. It looks at popular categories of hacker activity in Russia, such as phreaking and worm creation, and analyzes how these activities relate to Russian hacker motivations. I will show that the roots of hacking in Russia are tied to the following cultural and historical motivations: intellectual challenge, prestige among the hacker community, a desire for profit, nationalism, disenchantment and underemployment in post-1991 Russia, the Soviet Union's history of state-sponsored hacking, and a culture of opportunism. Finally, I will analyze specific case studies that illustrate many of these arguments and observations.

“Khaker”: A Loaded Word

There have been countless attempts to categorize, define, demonize and romanticize hackers. A popular Internet encyclopedia for tech-savvy users defines a hacker as “A person who enjoys exploring the details of programmable systems and how to stretch their capabilities,” or “One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations” (Everything2.com). Security in Computing, a computer security textbook used by universities and security professionals, fails to even define the term hacker, instead classifying users who manipulate or attack systems into three groups: “amateurs,” “crackers,” and “career criminals” (Pfleeger 30). These disparate definitions highlight the polemic that surrounds hacker culture in society. The term “hacker,” all-encompassing yet ill-defined, promotes a false assumption that everyone knows what a hacker is.

Studies reveal a remarkable number of computer attacks on companies and government agencies. For instance, between January and March, 2003, verifiable digital attacks worldwide caused economic damage of $16 billion dollars (Computer-Related Crime Impact 8). A survey conducted by Ernst and Young in 2000 showed that 70 percent of American companies had experienced computer attacks that year, and 65 percent of Russian companies had been attacked. A 1995 U.S. Department of Defense report, which was widely used as justification for computer security systems in the late 1990s, revealed 165,520 computer attacks on the Department of Defense’s computer network in the year 1994 alone (Skibell).

However, in *The Myth of the Computer Hacker*, Reid Skibell asserts that hackers are demonized and the proportion of hackers who act maliciously is greatly exaggerated: "The seriousness of computer hacking is not exaggerated, it is far worse than [exaggerated]; a thorough analysis of the statistics demonstrates that the majority of computer intruders are neither dangerous nor highly skilled, and thus nothing like the mythical hacker" (336). Yet Skibell fails to emphasize the serious threat posed by "exceptional" hackers who do participate in criminal and malicious hacking. The growing role of e-commerce makes even the remote possibility of a security breech unacceptable for many companies.[1] When two Russian hackers, Vasily Gorshkov and Alexei Ivanov, broke into PayPal's databases in the late 1990s and stole over a million credit cards, many companies changed their attitudes regarding computer security.[2] If a single attack could potentially yield millions of credit card numbers, such attacks clearly had to be prevented at all costs.

However, Mark Twain's famous line—"There are three kinds of lies - lies, damned lies, and statistics"—has particular relevance for computer security. The statistics reported in the famous 1995 Department of Defense Security Report, the very statistics used to convince many companies and government agencies to adopt expensive new security systems in the late 1990s, are arguably skewed. Of the 165,520 documented attacks, many are occurrences that most experts would hesitate to classify as genuine security concerns. These occurrences include failed logins, which are often the result of a mistyped username or password, and port scanning, the computer equivalent of knocking

[1] E-commerce, or electronic commerce, is the buying and selling of goods via the Internet.
[2] Paypal is the preeminent e-commerce facilitator on the Internet.

on a door where no actual break-in occurs.[3] A subsequent review of the Department of Defense's same 1994 computer logs took place by a third-party panel and estimated only 559 successful attacks. "A conflict of interests may have tainted the [original] findings" (Skibell 349). Similarly, virus activity is frequently sensationalized by a security industry that is eager to sell its products.[4] "The industry has regularly released reports arguing that there are between 30,000 and 50,000 viruses in circulation, when in reality most of these have never infected a computer and only 200 are in general circulation" (345).

Hacker apologists cite bloated statistics as evidence that hackers are demonized and their potential for harm exaggerated in the interest of a profiteering computer security industry. They also point out that computer security firms, authors of security textbooks, and the like, are ensured contracts, book sales, and large profits if the perception of computer security risks by businesses and the general public is high. Emmanuel Goldstein, a prominent hacker icon, argues, "By demonizing hackers, the lawmakers and the media get what they want— control and ratings. People fear what hackers can and will do next and they wind up supporting all kinds of draconian measures that will wind up invading their privacy far more than any hacker could" (Goldstein). It is not difficult to see the parallel between the computer security industry and national security— speculation arises about the motives of security advisors in any field potentially influenced by industries or lobbies with vested financial interests in their

[3] Port scanning is the act of searching a network host for open ports. This tactic is used by hackers to discover vulnerable computers.

[4] The term virus is often applied to all forms of malicious software (worms, Trojan horses) but its strict definition is a self-replicating computer program that attaches itself to executable code or other documents on a computer and, when executed, both replicates itself and causes undesirable events to occur. In this context, it is used as an umbrella term for various malicious programs.

recommendations. Even studies that purport to give an "objective" analysis of hacker culture often betray biases, legitimizing or condemning hackers by using selective statistics or through subtle word choice. The answer to the question "What is a hacker?" thus depends most upon whom you ask.

Some hackers claim to live by a strict code of ethics and feverishly dissociate themselves from any sort of illegal behavior, claiming as Goldstein did in a 2001 editorial, "People who steal, threaten, vandalize, torture, murder, etc. are not hackers" (Goldstein). Others routinely perform malicious attacks on systems with the primary motive of self-amusement or hacker prestige. For instance, in 1998 a Russian teenage boy masqueraded as a 14-year-old girl on America Online and tricked a corrupt Florida police officer into opening a pornographic image of the girl he was pretending to be. When the officer opened the image, a Trojan horse secretly downloaded and installed on his computer (Zetter).[5]

Hacker attacks are often exaggerated, but malicious hackers do exist. Their potential for damage should not be overlooked. In Russia, "Hackers are not a criminal guild, they are a subculture. Among the members of this subculture you will find full-time programmers, computer break-in artists, virus designers, 'crackers,' and 'phreakers'" (Dougaev). Some hackers are motivated by a love of the craft or a desire for the unfettered flow of information, while others are simply trying to profit through theft. Because of these complexities, it is meaningless to attempt a narrow definition of the

[5] Trojan horses are backdoor programs that masquerade as legitimate programs or files. Often users will run innocuous Trojan horse programs, unaware that they are performing undesirable functions in the background—generally the ulterior function of a Trojan horse is to provide a backdoor for remote access into the computer, thus rendering the computer a "zombie" computer.

term hacker. Only by looking at their various behaviors, motivations, and cultural context (in particular public views of hackers), can one gain a thorough understanding of hacker culture.

The Evolution of Hacking

Hacking began in earnest with the rise of the personal computer in the late 1970s. The early days of hacking in America involved skilled programmers working in the industry and "a small number of youths trading pirated copies of computer games and discussing ways to get free phone calls" (Skibell 340). Most people were unfamiliar with the term "hacker" and had little or no experience with computers. Adults were generally more averse to learning computer skills than adolescents, who possessed the energy and curiosity necessary to explore new technologies.

The concept of hacking was first popularized in America by the movie *War Games* (1983), in which a charming and mischievous Matthew Broderick breaks into a military computer network. He ultimately outwits military computer scientists and defeats an artificial intelligence program to prevent a global nuclear catastrophe. The film's teenage hero inspired the first generation of young people to investigate computer hacking. Not only did *War Games* invigorate the hacker movement, it provided it with a face, an icon, where none had existed before. Phreakers and hackers flocked to bulletin boards where they exchanged tips and tried to impress one another by breaking into systems.[6] Hacker activity increased exponentially and with it stories about hackers began getting public attention. Films such as *Sneakers* (1992), *Hackers* (1995) and *The Net* (1995) continued to glamorize hacking for young people, while raising fears in the minds of adults (Skibell 341).

---

[6] Phreakers are hackers who manipulate telephone systems.

The term “hacker” soon accrued some serious, negative connotations. The former image of a charismatic, curious computer whiz shifted to that of an antisocial, obsessive youth. The smiling Broderick was replaced by the dark and morally ambiguous Kevin Mitnick in *Takedown* (2000).Young people continued to be drawn to the hacker lifestyle, which was glamorized by films, but many in society developed fears about hackers and expressed concerns about their own safety. In the early 1990s, businesses began demanding law enforcement intervention and new legislation, which resulted in government crackdowns such as Operation Sundevil, the first major action by federal law enforcement against computer hackers in 1990. In this raid, the secret service seized 40 computers and 23,000 floppy disks across America. “The (early) raids were well coordinated, with agents busting into suburban homes with guns drawn to issue search warrants on 14-year-old kids running computer bulletin boards” (Skibell 344). Hollywood immortalized such tyrannical images in the minds of young people as in *Hackers,* when federal agents with rifles and dogs storm the house of the eleven-year-old protagonist and drag him into custody.

It was not until the advent of e-commerce, however, that hacking and computer security gained the significance that it has today. Companies began selling products and conducting transactions over the Internet, creating a new and remarkably vulnerable arena for hackers. Credit cards, social security numbers, bank account numbers, and medical records were being transmitted via fledgling technologies. As a result, hackers were able to intercept an unprecedented amount of sensitive information. The hacker public image took an unfavorable turn in the era of e-commerce. Soon a large percentage

of society regarded hackers as predominantly credit card and identity thieves or malicious vandals, when in reality only a small percentage of hackers were involved in these activities (Voiskounsky 58). These misconceptions inspired a small but vocal movement of hacker apologists to attempt to distinguish "true hackers" from "crackers," [7] "script kiddies," [8] and other sub-classes of hackers. In this way two main schools of thought developed in society, both of them polarized and oversimplified: those who defend hackers and attempt to redefine them as a well-intentioned, highly-skilled group of professionals who abhor criminal activity, and hackers as thieves and vandals.

The term "hacker" evolved similarly in Russia. It was virtually unknown until a translation of Joseph Weizenbaum's influential book *Computer Power and Human Reason* reached Russia, which described a hacker in the following manner (see Appendix for translation):

> Одержимый программист посвящает работе над своими великими проектами столько времени, сколько ему удается. "Работать" - это, однако, не то слово, которое он использует; то, что он делает, он называет "хакированием". "To hack", согласно словарю, - это "рассекать беспорядочно, неумело или без определенной цели; кромсать с помощью или как бы посредством многократных ударов какого-либо рубящего инструмента" [*Прим. перев.*: Явление, о котором пишет здесь автор, не проявляется в советских

[7] Cracker refers to any hacker who acts maliciously; however, it can also mean hackers who break copyright protection on software.
[8] Script kiddies is a derogatory word for inexperienced or low-skill hackers who use existing scripts or programs to perform malicious hacks.

вычислительных центрах в такой крайней степени, хотя для части программистов, действительно, очень характерно пренебрежение к документированию программ и особенно оповещению других о вносимых ими постоянно или время от времени изменениях. Поэтому, насколько нам известно, в отечественном программистском жаргоне соответствующее понятие отсутствует. Поэтому нам, к сожалению, при передаче этого термина пришлось прибегнуть к транслитерации. Так возникли "хакирование" и "хакер" (кстати, в английском языке последний также является неологизмом)].

Я уже отмечал, что одержимый программист, или хакер, как он сам себя называет, обычно превосходный "технарь". Казалось бы, он не действует "неумело', как это указывается в определении. Однако определение справедливо здесь в том более глубоком смысле, что хакер "действует без определенной цели"; он не в состоянии поставить перед собой ясно сформулированную долгосрочную цель и выработать план ее достижения, поскольку он обладает лишь умением, но не знанием. Он не располагает ничем, что он мог бы анализировать или синтезировать; короче говоря, у него нет предмета для построения теорий. Его мастерство, таким образом, бесцельно, даже беспредметно. Оно просто не имеет никакого отношения к чему-нибудь, кроме того инструмента, с помощью которого оно может быть реализовано. Его мастерство напоминает искусство

> переписчика в монастыре, хотя и неграмотного, но первоклассного каллиграфа. Следовательно, все эти великолепные проекты должны неизбежно сопровождаться иллюзиями, а именно иллюзиями грандиозности. Он создаст одну грандиозную систему, в рамках которой все остальные специалисты будут потом писать свои системы. (Следует отметить, что не все хакеры страдают патологией одержимого программиста, в самом деле, если бы не эта в высшей степени творческая работа людей, гордо называющих себя хакерами, немногие из сегодняшних изощренных вычислительных систем с разделением времени, трансляторов машинных языков, систем машинной графики и так далее вообще существовали бы.) (Weizenbaum)

As the passage indicates, the first hackers in Russia were simply “obsessive programmers” and there was no initial connotation of criminality. After this book was published in the USSR (1987), a few computer scientists began using the term “khaker.” However, in contrast with Weizenbaum’s description of a hacker (“Его мастерство, таким образом, бесцельно, даже беспредметно”), the Russian hackers of today demonstrate a number of goals and motivations, such as the desire for hacker prestige, profit, or malice.

The primary khaker activity in the 1980s in Russia was the adaptation of brand-name applications and operating systems to Soviet computers.[9] Soviet companies and government agencies, unable to afford American products, resorted to hacking and modifying imported technology to fit with their architectures and software. These early instances of unauthorized modification initiated longstanding traditions of cracking[10] (breaking software copy protection) and piracy.[11] Cracking and software piracy remain arguably the two most widespread types of cybercrime in Russia today. Low wages mean that virtually no one in Russia can afford the high cost of commercial software products. Consequently, "the programmers have to be competent in cracking the safety systems in order to copy operating systems and applied computer programs and to adapt them in unauthorized computers as needed" (Voiskounsky 64).

Public opinion regarding hacking in Russia shifted during perestroika (1985-1991). At that time ideas spread among the relatively small khaker population about the free flow of information: "computer software should be distributed freely, […] the information contained in the governmental, corporate and private databases should be publicly available, and […] security systems should be abolished" (Voiskounsky 58). From 1987 to 1990, the term hacker became a popular term of discussion and was mentioned numerous times in Russian newspapers and other publications. Though the

[9] "Khaker" is a transliteration of the Russian word for a hacker ("хакер").
[10] Cracking was used earlier as an umbrella term for all malicious forms of hacking. For most of my study, it refers to the practice of breaking software copy protection. This can take the form of breaking the encryption scheme used to protect a piece of software or data, or bypassing other copyright protection schemes. Most commercial software includes some form of copyright protection that is intended to prevent its free distribution. The most common method of cracking commercial software involves reverse-engineering the executable code of a program. This is generally done using a decompiler. After obtaining the decompiled source code, crackers then modify it to change the behavior of the program, often bypassing the copyright protection portion of the software.
[11] Piracy refers to the copyright infringement of electronic media, such as software, music, and film.

initial image of hackers in Russian culture was a fairly positive one of talented programmers, it quickly shifted. "When and if hackers performed illegal actions or disobeyed instructions for computer use, positive attitudes towards them changed immediately" (59).

Hacker activity and awareness of it in society continued to increase in the 1990s. Phreaking became a major hacker activity in Russia as cell phones became the primary means of communication in Moscow and mobile networks grew rapidly[12]. Technical publications about hacking were released, including the first hardcopy of the preeminent hacker magazine in Russia today, *Khaker* magazine, in 1999. Technical audiences enjoyed discussions about the protocols of computer attacks, lists of poorly administered websites, vulnerable computer networks, and descriptions of new types of software for hacking (Voiskounsky 60).

Conferences and courses at universities pertaining to computer security and hacker methods appeared in the late 1990s. Russians, especially teenagers, watched (often pirated) movies such as *War Games*, *Hackers*, and *The Net* and began idolizing hacker heroes. The Internet grew rapidly in Russia, facilitating the rise of hacker activity. In 2005 some 22 million Russians had access to the Internet—about 15.5 percent of the total Russian population. This is a large increase from only one million Internet users in

[12] Phreaking refers to the manipulation of telephone systems, including both landline networks and mobile networks. Phreaking originated in the United States in the 1950s when technical enthusiasts first discovered how to manipulate phone connections by playing certain tone frequencies into the phone. Today phreaking on landline phone networks is virtually nonexistent in developed countries because of improved telephone networks. However, mobile-phone networks presented new opportunities to phreakers around the globe, who discovered ways to obtain free service by charging their calls to other user accounts, and to eavesdrop on other users' conversations using tools such as scanners. In recent years, mobile networks have responded by improving the security of their protocols to prevent unauthorized calls and eavesdropping, but in many developing countries (i.e., Russia) these changes have been slow to occur.

1996 (Solovyova). Moreover, a study conducted by the Moscow Aviation Technologies University in 1999 found that, “Almost all the respondents—Muscovites from 13.5 to 63—recognize the word ‘hacker’ and have at least limited knowledge about the forms of their activities. Thus the social changes are very rapid: about 4-5 years ago the terms ‘Internet’ or ‘hacker’ were known only to a few people in Russia” (Voiskounsky 76).

Hacker Self-Image

Hacker conceptions of identity vary. Some hackers subscribe to explicit ethical codes, but most operate via principles that are not formally defined. The credos of hackers who subscribe to explicit ideologies generally fall into two categories—those who perform malicious or illegal attacks, and those who, spurning such activity, manipulate systems in the interest of improving their own technical ability, improving software security and quality, and promoting knowledge. This dichotomy has changed during the brief history of hackers, generally adhering to the following oppositions: security professionals versus hackers, hackers versus crackers, and white hats versus black hats.[13]

One of the few attempts to explicate hacker values is the famous "Hacker Manifesto." It was first published in January, 1986 in Phrack e-zine by a hacker called "The Mentor," but it is reproduced to this day on websites and chat rooms across the Internet. The "Hacker Manifesto" portrays hackers as people of superior intellect who are oppressed by the government and excluded by their peers: "We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us

[13] Black hats are hackers who engage in malicious or criminal hacking. White hats are hackers who typically use their expertise to improve computer security and software quality. A black hat might break into a system and steal information or vandalize, while a white hat would break into a system for learning purposes, and promptly inform the system's administrator of its vulnerabilities. Black hats include crackers, phreakers, virus writers, and web vandals. White hats are often security specialists, network administrators, or simply computer enthusiasts who are interested in improving the quality of technology and their own skills.

believe it's for our own good, yet we're the criminals" (Hacker Manifesto). The images and language of the "Hacker Manifesto" recall the oppressive characterization of the government in *Hackers* and the "draconian measures" that Immanuel Goldstein warns against. This youth-oriented, self-righteous stance appeals to many hackers, a large number of whom are highly intelligent, disenchanted middle-class teenagers and young men.

Internet communities such as chat rooms, newsgroups, and online forums are the primary means of hacker interaction. They reinforce hacker values. Hackers use these cultural spaces to exchange ideas and socialize. Russian hackers use IRC, as well as the web forums of popular Russian hacker magazines like Xaker.ru and hackzone.ru.[14] In America, hacker conventions such as H2K and Defcon provide opportunities for hackers to meet in person, exchange technical ideas, and debate hacker ethics (though a relatively small percentage of hackers attend hacker conventions).

[14] Internet Relay Chat is a popular chat protocol that is used throughout the world.

Russian Hacker Culture

Russia is fertile ground for hackers. This is due to a number of cultural and historical factors, including Russians' unique computer talent, the social acceptability of cybercrime in Russia relative to other types of crime, a history of government-endorsed cracking, the un- and under-employment of computer scientists and a concomitant disenchantment with society. Moreover, Russian hackers share many of the motivations of the global hacker population, including a feeling of belonging to the electronic community, a distinct pride in one's craft, and a desire for profit.

Russians' unique computer talent is starting to gain global recognition as the country's hackers design increasingly damaging computer worms, hack into high-profile systems, and emmigrate en masse to America and EU countries to work for and, in some cases, found computer companies. Max Levchin, the founder of PayPal is Russian, as are Vasiliy Gorshkov and Alexei Ivanov, the hackers who broke into PayPal's databases and stole over a million credit cards in the late 1990s (see my discussion of this in Case Study: *United States vs. Ivanov, Gorshkov*). Sergei Brin, one of two co-founders of the dominant search engine Google, is originally from Moscow. Countless Russian hackers have authored worms, including Zotob, Mytob and MyDoom, which have caused serious damage to Western firms (see Case Study: Zotob, Mytob and houseofdabus). In a survey, Muscovites commonly expressed the opinion that Russian computer scientists are more skilled than those of other countries, because "the lack of access to the most updated hardware and software products in Russia forces Russian experts in computer programming to seek—and to find—creative solutions," and "education in technical

sciences and mathematics is of a higher level in Russia, compared to ordinary (i.e., non top-level) universities outside Russia" (Voiskounsky 83). These views reflect Russian society's pride in its intellectual abilities, which has lingered despite the collapse of the Soviet Union.

Hacking and cybercrime are often buoyed by some degree of social acceptability. People generally view electronic crime as less severe than its physical equivalent (resulting in polemics like that surrounding the piracy of music in America). For instance, people tend to view stealing a credit card from an online database as less severe than physically stealing a credit card. In Russia, the social acceptability of cybercrime relative to other types of crime is especially high. "Those accused of cybercrimes (carding, hacking, etc.) are usually put on probation, not in prison, indicating that the Russian courts consider this sort of crime relatively minor" (Voiskounsky 68). Indeed "common Russians have a much more amenable attitude toward hackers than the media gives. Most respondents believe that cybercrime should be distinguished from ordinary crime" (Voiskounsky 74).

Russian society in many ways seems to condone or even glorify hacking. Films such as *Hackers* and *War Games* are very popular in Russia. A recent Russian comic book called "Dimich and Timich" features two young Russian hacker heroes "trying to protect their country from foreign cyber-enemies" (Bratersky). Russians enthusiastically follow news stories about hackers: "General audiences prefer verbal descriptions of

current sensational performances by hackers, crackers, carders, etc., and of the security personnel's attempts to arrest and prosecute hackers" (Voiskounsky 60).[15]

Pirated software and other forms of media are readily available on the street at kiosks and markets. Hacker magazines are available electronically and in print in Russia. Russian hacker publications provide detailed descriptions of how to perform attacks. According to Ken Dunham, director of malicious code at iDefense in Virginia, "In Russia, perhaps more than in most other countries right now, hacking magazines and software are sold on the streets of Moscow. It's not a secret as you'd expect, but right out there in the open" (Blau). There is even a hacker school in Moscow called the Civil Hacker School.

The Russian hacker mentality originated in the Soviet era. Hackers were not only tolerated in Soviet society, they were often sponsored by the government. Soviet institutions instructed computer scientists to crack copyrighted software from the West for use on Russian systems. A Russian computer scientist commented on the computer industry under the Soviet Union: "The state used to be one collective hacker. We heroically ripped off capitalists for the sake of strengthening the country's defense potential. If we didn't hack, we would have still been in the Stone Age" (Solovyova).

Hackers were considered heroes by many people in the Soviet Union deeming their work a form of charity. Indeed, many hackers claimed to be providing a public service: "It was like our donation to society. It was a form of honor; [we were] like Robin Hood bringing programs to people" (Blau). But such claims by hackers are suspect:

[15] Carding refers to the practice of stealing credit cards via the Internet. This can occur in a number of ways, but most often involves one of two methods—phishing or breaking into databases.

hackers may purport to be acting magnanimously when in fact there is a strong element of self-interest. Today in Russia it seems that the motivation of hackers is overwhelmingly one of self-interest, not charity. In an interview, several Russian hackers—one software pirate, one virus writer, one carder, and three specializing in illegal penetrations into remote systems—dismissed charity as a motivation. "They disagree with the Robin Hood-like romantic descriptions of their motives; they insist that the actual motives include getting money, cognitive interests, and the prospect of becoming famous" (Voiskounsky 80). Like Americans, the Russian public has some misperceptions about hacker motives and activity.

Cracking computer software in the Soviet Union in the late 1970s and early 1980s reflected certain Soviet mores. State-sponsored theft was certainly not limited to cracking software, but took place in many forms within the bureaucracy. Government employees who were unable to obtain essential resources, neither in the workplace nor in stores, resorted to unconventional and often unethical means, stealing money and other resources from their own institutions. Eventually stealing from the state became widespread and took on an element of social acceptability. Steven Solnick observes that this created a bank-run mentality around the time of the collapse of the Soviet Union. When authority over government institutions became decentralized during perestroika, government bureaucrats were emboldened by a lack of accountability to higher-ups, and open theft was unleashed. This spread the "erosion of authority within the organizational structure, as local officials who were still loyal began to wonder whether their subservience might leave them completely disenfranchised if the center collapsed" (Solnick 7).

Viktor Shklovsky touched on another reason for opportunism, focusing on the Russian Civil War era:

> This book is called *Knight's Move*. The knight moves in an L-shaped manner…There are many reasons for the strangeness of the knight's move…the knight is not free—it moves in an L-shaped manner because it is forbidden to take the straight road…
>
> […]
>
> --In Russia there is something else.
>
> --In Russia everything is so contradictory that we have all become witty in spite of ourselves.
>
> […]
>
> One more word--don't think that the knight's move is the coward's move. I'm no coward. Our tortuous road is the road of the brave, but what are we to do if we see with our own two eyes more than honest pawns and dutiful kings. (Shklovsky)

In a society where opportunistic theft goes unpunished and is, because of bureaucracy and poverty, the only way to survive, hacker mentality is much more likely to flourish. The acceptability of opportunism and state-sponsored and private theft in the Soviet Union has carried over into post-Communist Russian culture and is partially responsible for the disproportionate number of Russian hackers.

State support of hackers continues in the modern age. The United States has a number of agencies that engage in forms of hacking. The FBI's cybercrime taskforce often employs hacker techniques to investigate and combat hackers. These are essentially hackers who work for the public good, but some abuse their power. In pursuing Gorshkov and Ivanov, the Russians who hacked PayPal in 1999, the FBI allegedly used "illegal methods." Michael Schuller, an FBI special agent, was charged by the FSB (the successor to the KGB) for hacking into Russian web servers in order to investigate the files of Gorshkov and Ivanov. An FSB spokesman quipped, "Hacking the hackers is wrong" (Abdullaev). However, in Russia the FSB allegedly employs hackers who engage in cyber warfare with Chechen hackers and other groups. "Reportedly, the FSB even started offering jobs instead of sentences to hackers caught committing cybercrimes" (Mulvey).

Several American companies have recently initiated hacker-friendly policies bordering on sponsorship in the hope of curbing hacker damage. Microsoft, a frequent target of hackers because of its Windows monopoly and alleged bullying of rival companies, made efforts to improve its public image by throwing a party for hackers and security professionals at a Las Vegas night club in 2005. Kevin Kean, director of security response at Microsoft, explained the party in Las Vegas: "One alternative is to take an acrimonious relationship. Another is to recognize that these people are passionate about security. The party is an honest attempt to develop that community" (Tipping Point, a computer security firm, began a program in 2005 called the Zero Day Initiative, that pays

hackers as much as $20,000 for information about “zero-day” flaws in software. [16] Such private sponsorship of hackers is “controversial, since they reward hackers for uncovering computer loopholes and, to some outsiders, look like the payoffs of a protection racket. But security firms argue that this free-market approach will give them critical information so they can boost protection for their clients” (From Black Market). Government and private sponsorship of hackers contributes to an atmosphere where cybercrime is more socially accepted and considered a less egregious form of criminality. However, it may help to curb hacker damages as it will provide companies with the opportunity to patch[17] their products before major exploits[18] can become widespread.

Following the collapse of the Soviet Union (1991) and default (1998), many highly skilled computer scientists found themselves newly unemployed. These programmers, network administrators, and security experts sometimes turned from more legitimate computer activities to hacking as a means of livelihood or revenge. Vladimir Levin, the first person ever to be convicted of a cybercrime, said after his 1995 sentencing, “If your own country robs you for your 50 honestly earned grand, there is nothing else left to do but to start robbing others." Levin stole $5 million from Citibank accounts from his home computer in St. Petersburg and remains a hero and role model to many Russian hackers today. As the “Hacker Manifesto” implies, hackers feel more justified in stealing because they believe they are victims of society (Solovyova).

---

[16] Zero-day flaws are software flaws that have either not been discovered or have not been fixed by the authoring companies, and thus the software companies have a “zero day” notice to fix their products before knowledge of the vulnerability spreads.

[17] A patch is a modification to a software program in order to fix a flaw or vulnerability.

[18] Exploits take advantage of a discovered vulnerability in a piece of software. An exploit can be an actual program that takes advantage of a vulnerability, or a set of instructions describing the vulnerability and how it can be exploited.

The disenchantment of Russian computer scientists is related to another major cultural trait in contemporary Russia—nostalgia for the Soviet Union. Many Russians create a selective personal sense of history by romanticizing the Soviet Union, even under Stalin's rule, but more often the period under Brezhnev when at least steady jobs and basic needs were generally provided. This compounds the feelings of hopelessness and disenchantment with post-1991 society, and increases the tendency to legitimize criminal activity as Levin's comments show. As Svetlana Boym asserts in The Future of Nostalgia, "Unreflected nostalgia breeds monsters," which is evident within the malicious hacker subculture, whose only guiding principle seems to be their own survival (Boym xv).

In 2001 the Russian police arrested a gang of computer hackers, headed by a 63-year-old retiree. "The former computer programmer for a Moscow institute was apparently bitter over receiving no royalties from his work, so he teamed up with a former policeman and three others to steal the details of credit cards from individuals in the U.S. and Europe and use them to make online purchases. The gang then channeled their income back to Moscow through a bogus Internet site" (Blau). Such sentiments of disenchantment recall the alienation evident in the "Hacker Manifesto": "You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal."

Hacker activities often reveal a strong sense of nationalism. This is ironic, considering that many of the hackers who do so also subscribe to some version of the "Hacker Manifesto" ideology: feeling oppressed by the government, disillusioned with

society, even isolated from their fellow citizens. Nevertheless, hackers team up and engage in cyberwar against companies and foreign nations. DDoS attacks[19] and mass web defacement[20] are commonly used in coordinated attacks. The infamous "Code Red" worm is suspected to have been part of a cyberwar between American and Chinese hackers. The worm exploited a vulnerability in the Windows operating system (an American invention), and upon breaking into a system would display on the screen "Hacked By Chinese!" The worm lay dormant on infected machines and ultimately performed DDoS attacks on specific targets; one of the prime targets was the U.S. White House website (Internet Put On Code Red).

When U.S.-led NATO conducted a bombing campaign in former Yugoslavia against the Serbian government in 1999, Russian and Serbian hackers teamed up to perform DDoS, spam,[21] and web defacement attacks on the White House, NATO, and various American military websites (see *Web Defacement and Other Forms of Electronic Vandalism*). In this sense, Russian hackers reflect Russian culture at large.

---

[19] A Distributed Denial of Service (DDoS) attack is a hacker technique that consists of a large number of computers simultaneously making requests on a web server or other publicly available network service, and thereby overburdening it by using up all of its resources. Often, the computers used for such attacks are networks of "zombie" computers controlled by one or a group of hackers. Hackers gain access to zombie computers using Trojan horses. The motivations behind such attacks vary, but often they are performed by hackers with vendettas against a company or organization, or by hackers seeking prestige among their peers.

[20] Website defacement is a malicious hacker activity in which hackers break into web servers and modify the content of a website. Often this is done for hacker prestige, but sometimes it can have other motivations, as in the case of the defacement of the NATO website by Russian hackers during the bombing of Yugoslavia.

[21] Spamming is the practice of indiscriminately sending out mass emails to large groups of strangers. Generally this is done to sell a product or lure users to a website. Previously spamming was often done from one's own mail server, but as government restrictions on spamming have increased, it has gone underground. A recent development in the spam industry is the use of zombie networks, previously used for DDoS attacks, as staging points for spamming. Many security experts believe much of the spamming industry is linked to organized crime in Eastern Europe. (Fisher)

Phreaking in Russian Society

Little has been written on the subject of phreaking in Russia. Whereas in America phreaking was a major hacker movement in the 1970s and 1980s, in Russia, "of all the hackers' subgroups, the phreakers seem to be the least numerous […] due to the fact that Russian phone lines are mainly non-digital, and in general far from being modernized […] Compared to phreakers, groups of criminal hackers such as computer pirates and crackers turned out to be much more numerous" (Voiskounsky 64). However, cell phone phreaking has had a significant impact on Russian society in recent years. Cell phones are ubiquitous now in urban Russia. This is a result of the lack of infrastructure for landline phones and, in Moscow at least, a burgeoning middle class since the 1990s.

The first major object of phreaking in Russia was Altai, a private mobile phone network used by ministers of the State and other wealthy or powerful members of society. The exclusive access of elites to Altai demonstrates the de facto inequalities that existed under the Communist system, which purported to be egalitarian. The urban and rural working and middle class did not have access to this new and useful technology. It is no surprise, then, that disenfranchised members of society discovered ways to exploit Altai, a system from which they were excluded. "Since the center would not supply what people needed, they struggled to do so themselves, developing in the process a huge repertoire of strategies for obtaining consumer goods and services. These strategies, called the 'second' or 'informal' economy, spanned a wide range of quasi-legal to the definitely illegal" (Verdery 10).

Similar circumstances continue to motivate hackers, crackers, and phreakers. One obvious example is the rampant piracy of music in America, which many justify by pointing to exorbitant record prices. It is Shklovsky's "knight's move," to which the exploited feel they must resort. Many hackers and phreakers purport to act in the name of equality, the free flow of information, and redistribution of wealth. Whether these motives are genuine or mere rationalizations for greed or self-interest is situational and often unclear.

Two mobile phone networks flourished after the fall of the Soviet Union—Bi-Line (Beeline) and Moskovskaia Sotovaia (Moscow Network). Moscow Network was the first system to be seriously infiltrated by phreakers. As is the case with many fledgling technologies, Moscow Network failed to provide security checks on its mobile network. It openly transferred access codes to base stations on unencrypted connections, which a phreaker could intercept with the aid of a common scanner and a simple computer program. Later, Moscow Network attempted to add a specialized security code to each call, but this too was quickly circumvented by skilled phreakers. Moscow Network lost a great deal of money as a result of security exploits (Rotkin).

Beeline realized the flaws in its system and switched over to an American mobile phone standard developed by Bell Labs, AMPS (Analog Mobile Phone System). AMPS continued to operate uncompromised for roughly a year and a half. Its success was largely due to the fact that no one in Russia was able to obtain the specifications of the system and consequently no one was able to manipulate it. Of course, someone eventually discovered a way to exploit Beeline's AMPS system, and soon its security was

severely compromised. The primary phreaking technique used on the AMPS system was conceptually the same technique in practice on mobile phone networks in Russia today—so-called *levye trubki* ("altered phones"). Levye trubki are cellular phones that have been physically modified. A typical cellular phone has an ESN (Electronic Serial Number) associated with it. By modifying the ESN in a phone, it is possible to impersonate another user's phone. This gives a phreaker free service and is virtually untraceable (Rotkin).

The second generation of the AMPS system implemented in Russia in the mid 1990s, D-AMPS (Digital AMPS), improved the capacity of the system by a factor of three by dividing the frequencies on which signals traveled into three time slots. Also, because D-AMPS transmitted a digital signal, it prevented phreakers from using analog scanners (the original tool of Altai and Moscow Network phreakers) to intercept codes and other sensitive information. Still, this system did not solve the altered phone problem, and the quantity of altered phones in Russia grew rapidly as common users began finding out about the exploit. At this time, "scan lists"—lists of hundreds or thousands of potentially vulnerable ESNs— circulated in Moscow (and to a lesser extent St. Petersburg). The practice of scan lists still persists today via the Internet on phreaker websites and forums. In the late 1990s, about 20 percent of all cellular phone traffic in Russia was generated by users who were illegally receiving free service through the use of altered phones (Rotkin).

Beeline responded by coming out with a new security scheme—now every call consisted of two lines with identical serial numbers and connection numbers; it became more difficult for phreakers to impersonate a base station, because they now had to create

two parallel phone connections with identical identification and serial numbers. In the event of an invalid serial number, a woman's recorded voice would respond: "obnaruzhen nesanktseonirovannyi dostup, obratites' k operatoru" (invalid access has been discovered, contact the operator). Legal subscribers contacted the operator and resolved the problem. Illegal users were thwarted. This technique, however, was not completely effective (Rotkin).

The advent of A-Key (Authentication Key) brought about the death of classical phreaking in Russia. In systems using A-Key, phones each have a unique and complicated encryption algorithm. Each time a phone wishes to place a call, the base station sends the phone some numbers and the user's phone runs the numbers through the algorithm and returns the answer. The answer, however, is different each time because the numbers sent by the base station vary and depend only on the validity of the algorithmic function's output of a given number, not on a fixed output. This prevents phreakers from listening for the number outputted by user phones and sending those each time—they are only valid for one particular call. A-Key established secure encryption of data via phone lines, thus virtually eliminating interception and snooping. It also established a strong authentication system to prevent the use of altered phones. Of course, this only occurred in those Russian mobile phone networks that could afford to implement it (Rotkin).

Mobile phone networks in Moscow were the first to implement A-Key. It took operators in Russia's provinces much longer to adopt the new technology because it is expensive. Still, upgrading Moscow's systems was most critical because the vast majority

of Russian phreakers resided there. “Sometimes a ‘craftsman’ appears in the interior of the country who creates an altered phone for himself and a couple of friends. In small cities combing out these people is simple. Nothing good will come to them. Regional operators come and offer money to [phreakers] in Moscow who know who is involved and how these things work” (Rotkin).

Interestingly enough, Altai still exists and remains completely unencrypted and vulnerable to attacks, though few people use it. Today, virtually all networks in Russia are on one of two modern standards—GSM (Global System for Mobile Communications) or CDMA (Code Division Multiple Access). AMPS and D-AMPS were replaced by these two standards, both of which continue to use a version of A-Key today. GSM uses several cryptographic algorithms for security. The A5/1 and A5/2 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in countries that may not be able to support the infrastructure necessary for A5/1. A large security advantage of GSM is that the “Ki” (from the Greek letter), the variable stored on the SIM card central to any GSM ciphering algorithm, is never sent over the air interface. Weaknesses have been found in both algorithms, and it is possible, though extremely difficult, to break its code. It is possible to purchase devices on the black market that can break the modern authentication technologies of GSM, but these devices cost approximately $100,000. Moreover, devices used to decrypt GSM encryption schemes can run in the area of $35,000. Few people can afford these devices (Rotkin).

Web Defacement and Other Forms of Electronic Vandalism

One of the most interesting types of hacker activity is web defacement because it often reflects the values of the hacker community. Russian hackers are typically middle-class citizens, which makes them a good barometer for national values. Web attacks can involve a number of motives, but most often they are performed by politically motivated hackers or those seeking prestige among their peers.

When NATO carried out a bombing campaign against Serbia in 1999, Russian and Serbian hackers joined forces and performed a number of politically charged web attacks. Russian hackers were sympathetic to Serbs, with whom they share ancestral roots and a common Eastern Orthodoxy. They were also opposed to international intervention, particularly by America and NATO, both of which were their enemies during the Cold War. "A survey taken by the 'Public Opinion' Foundation of 1,500 [Russians] during the first week of the campaign found that 92 percent opposed the bombing and only two percent supported it" (de Waal).

In response to the bombing campaign, Russian and Serbian hackers performed distributed denial of service (DDoS) and spam attacks on NATO, the White House, and various American websites. Hackers used ping flooding to perform a DDoS attack on the NATO website, which was hosted by a NATO web server in Brussels.[22] They successfully brought this site down for several hours. Russian hackers also launched a

[22] A technique in which an attacker overwhelms the victim with ping packets (a packet that gauges the response time of a remote computer). It succeeds when a user has more bandwidth than the target computer and thus hackers often use several computers or entire networks of zombie computers to attack a single target.

large-scale spamming campaign against the mail servers on NATO's Brussels system. The NATO webserver received about 10,000 emails a day in 1999. Some emails were laden with virus-infected executable programs. "However, many emails are perfectly legitimate expressions of public opinion for and against the NATO airstrikes," although, "Russian emails tend to be pro-Serb/anti-NATO" (Campbell).

Russian hackers allegedly crashed the U.S. White House's website for roughly 36 hours that same year. One hacker living in Moscow stated, "Many of us felt that what the U.S. was doing to the Serbs was wrong, and we retaliated by attacking government websites and big companies. I know that your White House was attacked many times, and so was the defense computers. Did your newspapers not mention this?" (Delio). An inordinate number of attacks were recorded by Defense Department networks in 1999. Investigations indicated the attacks originated in Russian networks, but it is unknown whether the attacks were government-sponsored (Campbell).

At the time of the bombings in former Yugoslavia, Russian hackers were not always selective in deciding which sites to hack—they apparently attacked anything loosely related to NATO or the American military. The U.S. Navy website was broken into by Russian hackers, who "blotted out the Navy data and inserted their own obscenities" (Campbell). In one case Russian hackers even attacked the politically neutral website of Orange Coast College in California, defacing the pages of the site with messages including, "Asses out of Serbia" and "Russian hackers demand to stop terrorist aggression against Yugoslavia" (Campbell).

The numerous instances of Russian hacker attacks aimed at America, particularly those targeting political organizations, suggest an element of patriotism among Russian hackers. This is ironic considering the anarchistic attitudes ascribed to many hackers as described in the "Hacker Manifesto": "We seek after knowledge... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity." This language implies an inverse relationship between intellect and patriotism. However, this passage also reveals hacker elitism through the assumption that intellect cannot coexist with patriotism.

The technical aspects of these particular attacks are undocumented, but a web attack of this type requires that an attacker gain access to the files that are being distributed by a website's web server. Web servers contain bugs and they are always evolving. As new vulnerabilities are discovered, programmers work diligently to patch them. The most common web server in use today, Apache, is used by approximately 50 million systems around the globe. Apache regularly releases new versions that attempt to fix vulnerabilities in previous versions. Hackers exploit vulnerabilities, both new and old (as many web administrators do not stay current on the most recent patches and bugs), and get access to files on web servers. Once they have achieved the privileges to view and modify the files on a web server, they can alter the appearance of websites with their own content, like the politically charged phrases of the Russian hackers above.

Russian hackers attack their own government as well. This is no surprise when considering that the impetus of many Russian hackers for their exploits is their own un-

or under-employment as a result of the collapse of the Soviet government in 1991 and the Russian economic crisis in 1998. Dissatisfaction with the government remains a common trait among hackers in Russia. Many articles have been printed in Russian newspapers in recent years discussing the high volume of attacks on Russian President Vladimir Putin's website. In June 2002, the site was attacked roughly 9,000 times. The attacks fell into one of two categories—probing or actual attempts to gain unauthorized access.[23] An article published by the notably state-funded Itar-Tass boasted that, "Not a single attack has been successful," and, "The web site of the president has also proven to be resistant to viruses. None has managed to infect the site with a virus, specialists say" (Voskoboinikova).

A different article published in June, 2002 by a popular American computer magazine Wired pointed out that, although the Kremlin had been toting the site has "hacker-proof," "independent tests of the Russian president's website revealed Friday that it was running an outdated version of the popular Apache Web server that could be vulnerable to a recently discovered security bug" (McWilliams). The site had been running on Apache version 1.3.20, which is vulnerable to the chunked-encoding bug.[24] The author then noted, "According to Netcraft, more than a dozen websites operated by the Russian Federation were also running unpatched versions of Apache."

---

[23] Probing is also known as port scanning.

[24] Apache versions 1.2.2 to 1.3.24 contain a flaw in the way that invalid http requests are encoded using chunked coding. The impact of this vulnerability depends on the platform on which the web server is being run—for some systems an exploit of this bug could result in a denial of service attack, while on other platforms it can be used as a remote exploit. To read more about this vulnerability see Apache Security Bulletin 20020617.

It is interesting that an author of Wired magazine would write an article solely about the vulnerability of Russian government websites. This is likely the result of the author's indignation in response to the obvious biases of the government-run news service Itar-Tass (a concept wholly offensive to the West, and particularly to hackers). Brian McWilliams was also reacting to the Titanic-esque claims of the Kremlin, which challenges a basic tenet of hacker culture—*everything is hackable*. (Because security systems are designed by other programmers, it is assumed that all code is flawed and contains some vulnerabilities, whether obvious or obscure; moreover, as time passes and software becomes outdated, it is increasingly vulnerable to new techniques that are discovered after it is conceived.) Despite the author's warnings, no successful attacks on Putin's website have been documented to date, which suggests that the author may have had some patriotic biases of his own.

Anti-Putin sentiment did surface on the Itar-Tass website itself when Chechen hackers defaced it in December, 1999. The Chechens broke into the Itar-Tass webserver and left a message on the home page of the site declaring, "We're here to fight evil and our power is growing" (Hackers Attack Russian News Site). They also sent an email to Itar-Tass explaining their attack as a protest of "the murder of peaceful Chechens," demanding that Russia stop the war in Chechnya. This use of computer prowess for political ends fits well with the self-image of ideological hackers, who purport to act as a check on the government when it infringes on the civil liberties of its citizens. Chechens resort to unorthodox methods of expressing political dissent, such as hacking websites, in

defiance of the monolithic Russian government (which controls most media outlets). Chechen subversive activities are “tactics” as defined by philosopher Michel de Certeau:

> Tactics are a calculus which cannot count on a ‘proper’ (a spatial or institutional localization), nor thus on a borderline distinguishing the other as a visible totality. The place of a tactic belongs to the other. It has at its disposal no base where it can capitalize on its advantages, prepare its expansions, and secure independence with respect to circumstances. The ‘proper’ is a victory of space over time. On the contrary, because it does not have a place, a tactic depends on time—it is always on the watch for opportunities that must be seized ‘on the wing.’ Whatever it wins, it does not keep. It must constantly manipulate events in order to turn them into opportunities. (de Certeau xviii)

Allegedly, Russia’s FSB has responded to Chechen cybercrime by employing hackers of their own: “ ’There are organized groups of hackers tied to the FSB and pro-Chechen sites have been hacked by such groups,’ said Vladimir Veinstein, a 25-year-old computer security specialist in St. Petersburg who works for the Internet company Red Net. ‘One man I know, who was caught committing a cybercrime, was given the choice of either prison or cooperation with the FSB and he went along’” (Varoli). Coincidentally, shortly after the Chechen attack on Itar-Tass in December, 1999, “a pro-Chechen Web site, Kavkaz.org, was shut down by hackers working for the FSB.” In addition to the FSB computer unit, the Ministry of Internal Affairs in Russia also has a special cybercrime task force, which has been dubbed “the spider group.” The

effectiveness and activities of these groups are relatively unknown because of the classified nature of the information.

The Impact of Russian Cybercrime on America

The problems Russian hackers and cybercriminals pose for American citizens and firms are significant. The majority of these threats fall into the following categories: phishing,[25] worms, carding,[26] and piracy. The gravity of these problems is increasing as the number of Russians connected to the Internet grows rapidly. “For all its disadvantages, the former Soviet Union had one hugely overlooked advantage; it kept hackers, crackers, and virus writers confined inside the country by restricting their access to the Internet” (Blau).

According to the Russian Ministry of Internal Affairs, the number of cybercrime cases in Russia doubled in 2003, with 11,000 reported cases. About 70 percent of the attacks documented by the Ministry of Internal Affairs were cases of hackers stealing usernames and passwords from other Russians for the purpose of obtaining free Internet access. The credit card numbers and passwords were obtained by hackers primarily using phishing techniques or breaking into databases. Although this type of Russian-on-Russian crime generally does not affect American firms, it was a problem for America Online and CompuServe in 1997, when after opening branches of their internet providers in Russia,

[25] Phishing is the practice of tricking users into volunteering their credit card information. This can be done using one of various social engineering techniques, for instance, sending an email purporting to be a company with which the user subscribes and asking for some sort of verification of a credit card number. Phishers often create replica websites with similar domain names, such as “www.e-bay.com” in place of “www.ebay.com” and attempt to trick users into sending their credit card numbers that way. Recently, the method of planting key loggers (programs that record every keystroke typed on a computer) via worms or Trojan horses onto victim computers has become a popular way of finding out user credit card numbers and other sensitive information.

they were forced to shut them down due to widespread usage of fake credit card numbers and stolen passwords running up the bills of the online services.

In 2000, the Kostroma police took first place in a country-wide contest that gauges the quality of computer crimes law enforcement. They reported that, “Most of [our] crimes follow the same pattern. The hackers find out the log-ins and passwords of other people or organizations and use them, forcing the victims to pay for their time in the Internet” (Sossinsky). The phenomenon of unauthorized access to Internet resources is not a significant threat to American firms, except perhaps in that it reinforces the criminality of hackers in Russia who might go on to attack American firms and contributes to an environment in which cybercrime is socially acceptable simply because it is widespread.

Phishing is apparently gaining popularity around the world. In September 2003, MessageLabs Inc., a New York-based email security company, saw 279 phishing-related email messages. In March 2004 that number had jumped to 215,643. Similarly, the Anti-Phishing Working Group, a volunteer consortium that monitors online scams, reported that it tracked 402 unique phishing scams in March, 2004— an increase of 43 percent from February 2004 (Fisher).

Russian phishers are affecting Americans as well as Russians. Traditionally, phishing has been performed using email, websites, or messaging clients. These methods often employ social engineering techniques in order to dupe Internet users into divulging their sensitive information. However, phishing techniques are becoming much more sophisticated. Instead of relying on social engineering, the newest phreaking techniques

employ worms, viruses, and Trojan horses, to get access to sensitive information. One example is Sepuc, an email Trojan horse that has been used by phishers since 2004 to harvest sensitive information. Sepuc operates in the following manner: a blank email is sent that, when opened and read, exploits a weakness in Microsoft's Internet Explorer and downloads a download manager. The download manager in turn downloads a series of small programs that are capable of harvesting data from a computer and sending it to a remote location. Generally the harvesting programs involve a key-logger.[27] These blended attacks are the next generation in phishing.[28]

Perhaps the most publicized and most daunting attacks are those that employ worms. This type of attack is highly publicized because it often targets large corporations or indiscriminately attacks a large volume of Internet users. Russian hackers are responsible for a disproportionately large number of these attacks. Many of the most harmful worms in recent years were designed by Russian hackers, including the Zotob/Mytob family of worms in 2005, the Sobig worm in 2002-2003, and the MyDoom (or Norvig) worm in 2004. Such attacks have a variety of motives, including but not limited to malice (both general and aimed at specific targets), experimentation, profit, and hacker prestige.

Usually worms are designed to exploit specific vulnerabilities in operating systems or applications. Often companies will discover these vulnerabilities in their own products and announce them to the public and encourage them to download patches of

---

[27] A key-logger in this context is a program that keeps track of keystrokes typed on a computer.
[28] Blended attacks are attacks that combine traditionally separate hacking methods in order to achieve a more versatile or effective attack.

the software. But hackers also read these announcements. Indeed many hackers read these security warnings religiously, looking for new vulnerabilities with which to experiment. This was the case with Zotob and MyDoom, both of which were designed after Microsoft announced flaws in its products, such as Windows NT and 2000. The general public is far from vigilant in checking these security announcements and often do not download patches until much later, sometimes after they have already been infected by worms or viruses. Thus, it seems security announcements for products currently generate almost as much harm as they do protection.

After infiltrating a system through a specific software vulnerability, worms can be used to achieve a number of different hacker ends, including the creation of zombie networks, phishing, and various other goals, like the strain of the Zotob worm that lowered the privacy settings of the Internet Explorer browser so marketing firms could more successfully deliver pop-up ads to infected users.

Worms are able to create backdoors on infected systems that allow hackers to access them remotely.[29] In this way, hackers usually attempt to create zombie networks. Hackers sometimes perform DDoS attacks against large corporations or organizations with whom they have a grievance, as was the case with MyDoom, which in one wave of attacks specifically targeted Microsoft and the Recording Industry Association of America (RIAA)—two organizations that are reviled by many hackers. In such cases, hackers are primarily motivated by revenge, malice, or the desire to bring down a

[29] Backdoors are ways of bypassing authentication in order to gain remote access to a computer. This often takes the form of a backdoor program, or a modification of an existing, legitimate program on a computer.

company. In other cases, however, hackers have used zombie networks to blackmail companies to make a profit.

> Today, hundreds or even possibly thousands of skilled Russians desperate for cash are scouring the Internet looking for security vulnerabilities in the computer networks of companies, particularly in the U.S. and Europe. They are creating worms and Trojans for stealing credit card and other financial information, or turning infected computers into zombie hosts to establish illegal spam farms, or extorting money by threatening companies with a distributed denial-of-service attack if they don't pay (Blau).

According to one estimate, a quarter of a million computers unknowingly become zombie computers every day. “Nobody knows how many zombies are out there, but a quarter of a million new ones every day is 90 million a year. That sounds like a lot, but […] with about 3000 million usable IP addresses, the attackers have a fair bit of time before they run out of addresses to use” (Betts).

The MyDoom (or Norvig) worm has been described as “The most virulent email virus ever” (Delio). It propagates via email and typically consists of a blank subject line and a message that masquerades as an innocuous email from a colleague or friend, with a vague instruction that encourages the recipient to download a “text” file attached to the email. The attachment is actually a zip file that contains various executable programs. Once the zip file is opened, the MyDoom worm attempts to delete files on the computer, install a backdoor program (rendering the computer a “zombie”), and propogate itself further through the user’s email address book. The first version of MyDoom attacked

Microsoft and a software firm called SCO in January, 2004. Later versions also attacked the RIAA, Lycos, Alta Vista, and Google (Urbanowicz).

London-based security firm mi2g estimated the damage of the MyDoom virus to be about $38.5 billion dollars, although this estimate was termed “absurd” by Vmyths, a site that describes itself as being dedicated to the eradication of computer virus hysteria. This illustrates the plurality of information that exists about the seriousness of hacker threats and the theory that computer security firms exaggerate hacker damage in their own interest. An mi2g spokesperson explained the algorithm that was used to compute the estimate: "The EVEDA algorithm is a component of SIPS and estimates economic damage on the basis of help desk support, overtime payments, contingency outsourcing, loss of business, bandwidth clogging, productivity erosion, management time reallocation, cost of recovery and software upgrades” (Varghese).

The Zotob worm (see Case Study: Zotob, Mytob and houseofdabus) also attempted to create a zombie network, though it intended to use the network for spamming. Spammers are difficult to combat because the Simple Mail Transfer Protocol (SMTP) does not require authentication. It is not difficult to create emails that falsely claim to come from legitimate sources, an act known as email spoofing. In October, 2004 CipherTrust, an Atlanta-based computer security firm, analyzed about 4 million of their customers’ emails and found that roughly 1/3 of the zombie machines sending phishing messages were from the U.S. “However, these findings do not mean that these attacks are originating from inside these countries. The global nature of the Internet allows attackers anywhere in the world to compromise machines in any location. In fact, many experts

believe that the majority of phishers are in some way connected to organized crime groups in Russia or Eastern Europe and that most such attacks begin there" (Fisher).

Carding is another major hacker activity in Russia. It is also a high profile activity because it typically involves large amounts of money and it affects a large volume of people, as it raises serious concerns about the reliability of bank and e-commerce websites. Probably the most famous instance of this was the Vasily Gorshkov and Alexei Ivanov attack on Paypal (see Case Study: *United States vs. Ivanov, Gorshkov*).

After stealing credit card numbers, carders can use them to make online purchases, as was the case with Gorshkov and Ivanov, or they can attempt to blackmail the company from which they stole the numbers. In April, 2001, a 21 year-old university dropout in Surgut, Russia hacked a web server containing the financial records of a New York state bank and subsequently used that information to blackmail the bank. The hacker posted 1,500 account numbers online to corroborate his threat, and asked for $1,000 from the bank in exchange for keeping the rest of the numbers private. The bank appealed to law enforcement, and the U.S. Embassy in Russia contacted Russian law enforcement, who then arrested the hacker and prosecuted him. The New York bank's damages were estimated at about $250,000 (Abdullaev).

Carding can also result in identity theft, which has been a serious problem in Russia as in other countries around the world. In fact, "identity theft" is often used synonymously with "carding" to mean unauthorized use of a credit card (as discussed above). Identity theft, however, can also take the form of obtaining fraudulent loans using

information such as social security numbers, bank account numbers, or generating fraudulent passports.

> As Russia has long been dubbed a hub of tech fraud, credit-card holders have been justifiably wary about using their plastic there. Travelers have been warned that after charging a dinner to their card in Russia, that number could be copied and used even after the owner left the country…Apart from anecdotal evidence, there are some solid reasons for switching to a paranoid "cash only" existence. Notably, an unknown number of PIN codes giving access to credit- and debit-card accounts were stolen in mid-1999 after a security breach at a Moscow card-processing center. Subsequently, many cardholders had their checking accounts cleaned out, in a rare example of massive PIN theft (Blagov).

In 2001, Russia was eighth on the list of countries with the most perpetrators of identity theft, but it did not make the list in 2003 or 2004 reports. Data indicates that Russia's identity theft activity has decreased in severity relative to several other countries around the world. This is probably due to the relatively small role that credit cards and electronic transactions play within Russia.

Another major threat that Russian hackers pose to America is cracking and copyright infringement. Although this problem is widespread in most countries, it is especially bad in Russia, where the roots of hacking grew out of government-endorsed cracking schemes and where law enforcement is exceptionally bad at curbing copyright violations. A classic example of how this can affect American firms is the Sklyarov case

discussed previously (see Case Study: *United States vs. Sklyarov*), in which a Russian programmer cracked Adobe's e-Book software, allowing full-length books to be easily copied and distributed on the Internet. The global nature of the Internet makes such international violations of copyright wholly unacceptable for American firms. In the case of e-Book, the entire book industry could have been undermined had the government not forced Elcomsoft to stop posting their crack for e-Book.

One self-proclaimed hero in the hacking community, alias Ivanopulo, has taken it upon himself to crack every product created by the U.S. software giant Macromedia, which specializes in multimedia-related programs. Each time Macromedia releases new software, Ivanopulo displays its areas vulnerable to hacking on one of his websites. Ivanopulo claims he is presenting the software's holes for educational purposes, but not everyone agrees. Steve Wozniak, Macromedia's piracy manager and a co-founder of Apple Computer, wrote in an email to Ivanopulo in March, "Judging from your work, you are an intelligent man who can pursue much more fruitful and valuable ventures than this. These cracks are simply a well-advertised aid to theft." Ivanopulo shot back, "I just like to investigate different protection schemes and show people how weak they can be" (Solovyova 68).

Case Study: United States vs. Sklyarov

Viktor Sklyarov, a twenty-six year-old Russian computer scientist, made Russian and American news headlines when he was arrested after speaking at an international gathering of hackers called Def Con in Las Vegas, Nevada in July, 2001. At Def Con, Sklyarov presented a program he had created, which cracked the copyright protection of Adobe Systems' recently-created eBook—a software package that makes possible the electronic distribution of entire books and protects these books from piracy through encryption. Sklyarov's program essentially accessed the document's source data in encrypted form, decrypted the text using an algorithm Sklyarov had devised, and then saved the clear text to a new file, which could be stored and freely distributed. Sklyarov was arrested by FBI agents a few days after the conference just as he was about to fly back to Russia.

Sklyarov was an employee of Russian software firm Elcomsoft, which sold Sklyarov's cracking program commercially for a period of time until negotiations between Sklyarov and Adobe Systems dictated that Elcomsoft cease sales of the program. Elcomsoft's web site also offered programs for generating serial numbers to crack Microsoft Word and ICQ products. It was believed that the primary motivation behind Sklyarov's eBook program was profit, but Sklyarov, along with Alexander Katalov, the company's general manager, wished to prove otherwise. Katalov called Adobe and the U.S. government's bluff—the program was promptly made available free of charge on the Internet. This circumvented the court's ruling that Elcomsoft stop selling the product in Russia; its free distribution was not prohibited in the agreement. This is an example of

hacker ethics in practice. By making the software available as freeware, Katalov demonstrated the priority of the free flow of information over profit and showed that he and his software developers were smarter than the software powerhouse Adobe Systems. Katalov said, "We have published the web address from which the program can be taken for free, and in the future we will probably publish the cracking algorithm for eBook" (Vedomosti). When questioned about patches that will be made to Adobe's eBook that will attempt to guard against Elcomsoft's cracking algorithm, Katalov added that his software people could crack the new Adobe eBook encryption "within half an hour, maximum." It seems that Katalov takes a definite pride in his ability to thwart Adobe's business ventures, but it is also worth noting that Katalov originally had no qualms with selling the product as well.

The software package created by Sklyarov and distributed by Elcomsoft was called Advanced eBook Processor and sold for $100. Katalov said Adobe itself is to blame for the software since it marketed a faulty product: "Adobe is promoting an incomplete technology and isn't concerned about its safety. No wonder that in an analogy with the musical format MP3, the electronic book world has produced its own Napster and MP3.com," he said (Vedomosti). Katalov claims the Advanced eBook Processor was sold mostly to people with poor eyesight who were unable to use eBook, considering its limitations on reading text aloud and zooming.

Sklyarov was charged under the United States' 1998 Digital Millennium Copyright Act, an act which has caused a great deal of controversy for allegedly being overreaching and giving media conglomerates too much control over digital distribution

(Can the World Be Copyrighted?). Sklyarov was not arrested until he came to America because at that point Russia had yet to adopt the DMCA. The DMCA would allow copyright organizations abroad to go after a programmer like Sklyarov and either charge him domestically or extradite him. Sklyarov faced charges of up to five years in prison and a $500,000 fine, but ultimately all charges were dropped. Immediately after the charges were dropped, a hacker organization called the Electronic Frontier Foundation (EFF) hosted a congratulatory party for Sklyarov and soon thereafter he returned to Russia.

Case Study: United States vs. Ivanov, Gorshkov

Two hackers from Chelyabinsk, Russia, Vasily Gorshkov and Alexei Ivanov spent the years 1998-2000 victimizing several American companies. On several occasions Gorshkov and Ivanov exploited vulnerabilities in the Windows NT Operating System and gained access to the computers of American companies, including Central National Bank in Waco, Texas and, most notably, PayPal, the world's largest online payment company. After breaking into these systems, the two young hackers stole over one million credit card numbers and other sensitive files. The hackers then used the stolen credit cards to pay for computer parts purchased from other vendors in the United States. A patch for the NT vulnerability had been available on the Microsoft website for over two years prior to the attacks, but the victim companies had not yet updated their software.

In addition to breaking into systems with the intention of stealing credit card numbers, Gorshkov and Ivanov also broke into the systems of American companies, copying sensitive information, and contacting the system administrator of the company demanding anywhere from $15,000 to $100,000 to be "security consultants" who would protect the data from being published on the web. One company, Lightrealm Communications of Kirkland, Washington, agreed to hire the two men as consultants for a sizable fee. Additionally, "on at least one occasion, the duo was hired on as consultants at an unnamed e-commerce company they had hacked into, but they went ahead and published the credit card numbers anyway" (Thornburgh).

The FBI had known for some time that Gorshkov and Ivanov were linked to assorted acts of hacking and extortion, but without jurisdiction in Russia or reliable extradition policies they had to lure them to America. In June, 2000 the FBI created a bogus computer security firm, aptly named Invita, and invited the two hackers to Seattle for a job interview with their firm. On November 10, Gorshkov and Ivanov arrived in Seattle and participated in the interview, in which they demonstrated their hacking skills by breaking into Invita's intentionally vulnerable network. "The FBI agents' descriptions of the meeting portray Ivanov and Gorshkov as not only blissfully ignorant of their impending arrest, but also somewhat cocky about their hacking skills. At one point in the meeting, as Gorshkov glibly detailed how he and Ivanov extorted money from a U.S. Internet service provider after hacking into its servers, he told the room of undercover agents 'that the FBI could not get them in Russia'" (Thornburgh).

Perhaps even more interesting is how the FBI used hacking techniques to collect evidence to use against the two Russian hackers. FBI agents ran a key logger on their Invita computer while Gorshkov was using it. They were able to obtain several passwords used by the hackers from these logs and subsequently used them to break into the hackers' computers in Russia and download an immense amount of evidence implicating them in various crimes. A search warrant for this data was not filed until well after the data had already been retrieved by the FBI agents. In 2001, Gorshkov's lawyer filed a Motion to Suppress evidence on the grounds of an illegal search, but the motion was ultimately denied. The judge defended his ruling by stating that the hackers had no right to the expectation of privacy for information transferred over an electronic network

because such information is commonly captured and logged in transit anyway, and could have been read by various third parties. This ruling set a precedent for cybercrime cases and is now commonly referred to as “no expectation of privacy.” This essentially means that computer criminals cannot suppress evidence brought against them that was obtained via an electronic network, because such data is inherently insecure and not private.

Ultimately Gorshkov was found guilty of 20 charges of conspiracy, computer crimes and fraud. He was sentenced to three years imprisonment and a fine of $700,000 in California. Ivanov received 48 months in prison followed by 3 years of supervised release from Connecticut court.

Case Study: Zotob Worm and houseofdabus

The biggest technical assault of 2005 came from the Zotob worm and its derivatives.[30] Zotob exploits a security flaw in three Microsoft operating systems—Microsoft 2000, 2003, and XP. The vulnerability is more difficult to exploit in Windows 2003 and XP systems, though the 2000 operating system is especially vulnerable. The majority of Windows 2000 users are corporate networks, therefore Zotob affected primarily large businesses. More than 100 large corporate networks were significantly affected by it in August, 2005, including ABC, CNN and the New York Times. CNN, whose computer network was brought down for an hour and a half by the worm, broke into their regular programming the day of the assault on their network to give a special announcement about details of the outbreak (Sullivan).

The worm was created by an 18-year-old Russian-born Moroccan national named Faris Essebar who goes by the handle "Diab10." He allegedly authored the worms and sold them to a 21-year-old Turkish hacker named Atilla Ekici (handle "Coder"). Both were later arrested and are currently facing charges of computer crime in their respective countries. Turkey, like Russia, is known as a hotbed of hacker activity, though Morocco is not. Mikko Hypponen, a chief research officer at Finnish security firm F-Secure, said

[30] Worms are similar to computer viruses in that they are self-replicating, but unlike viruses, they are also self-contained and do not attach themselves to existing programs. The chief aim of most worms is to propagate over networks, causing network congestion and infecting as many computers as possible, while the chief aim of viruses is to spread to as many files as possible within a single computer. Thus worms and viruses are quite different, and in recent years worms have taken on a greater significance as the importance of the networks and the Internet to businesses and users has increased dramatically. The Zotob and Mytob worms, largely a Russian innovation, caused significant damage in 2005, and will be discussed in detail later in this analysis.

of Essebar, “Morocco is a real surprise. It’s the first time I’ve heard of any activity coming from there. Significantly, Mr. Essebar was originally from Russia where much malicious code is generated and many hi-tech crime groups operate” (Ward).

Essebar’s design of the Zotob worm was not completely original. Essebar employed a vulnerability that another Russian hacker “houseofdabus” allegedly discovered and wrote about in detail. Houseofdabus publishes several such exploits on a website hosted in Russia, including executable C++ code that can be used to gain control of vulnerable systems. The global nature of the web makes these exploits available to everyone in the world. However, law enforcement has not been able to prosecute houseofdabus for simply describing the exploit in technical detail and not performing them, much as someone who published bomb schematics cannot be punished for a student terrorizing a high school with a homemade bomb.

The motivation behind Zotob is more complicated than many of the worms in recent years. Whereas many worms are intended to circulate through the Internet leaving a hacker’s “stamp” on computers for the purpose of prestige, Zotob was designed to create a network of zombie computers. In the past, the chief use of such zombie networks was DDoS attacks (described above), though recently hackers have taken to using zombie networks to distribute spam in order to make profit from interested parties. Many experts believe that zombie networks are frequently being purchased by criminal organizations in Russia and Eastern Europe to make profits through spamming schemes. In addition, the worm operated in such a way that infected computers would contact an Internet Relay Chat chatroom to report its availability as a zombie computer. In this way, Essebar and

his associates could gain notoriety in the hacker community by demonstrating how many hits the chatroom received from zombie computers. Essebar was motivated by both profit and hacker prestige.

Zotob exploits a vulnerability in Microsoft's Plug and Play hardware feature. This programming flaw allows a remote computer to contact a victim computer via ports 139 or 445 and execute code that raises the attacker's privilege level to that of administrator. Once a hacker has administrator rights, they can read any file on the computer, modify settings on current applications, or install new software. As a result, several variants to Zotob have sprung up which exploit the same basic vulnerability, but have different goals once they have administrator privileges.

"Diab10" also authored a variant of the Zotob virus, Mytob, which lowers the security settings in Microsoft's Internet Explorer web browser. In doing so, Mytob makes it possible for users to receive pop-up advertisements in their web browsers that would have otherwise been prevented by the security settings of the browser. Essebar allegedly expected to be paid by various companies who were sponsoring these pop-up ads, but was arrested before obtaining any profits (Ward).

Conclusion

This thesis employs a cultural studies approach to analyze the phenomenon of Russian hackers in order to gain a more holistic understanding both of Russian hacker culture and Russian culture in general. In contrast with the scant literature that currently deals with this subject (such as anecdotal news articles or statistics put out by the computer industry), it attempts to encompass a wide range of pertinent cultural issues that have led to the rise of the Russian hacker phenomenon. It enumerates and connects these cultural factors, such as the history of Soviet-sponsored cracking and the relative social acceptability of electronic crime in Russia today, in order to explain the development of the uniquely skilled and influential Russian hacker subculture.

This thesis has used case studies and other examples to illustrate the motivations and cultural factors associated with Russian hackers. At one point in the mid-1990s, 20 percent of all cellular phone traffic in Russia was generated by phreakers who were illegally receiving free service through the use of *levye trubki* ("altered phones"). Such widespread phreaker activity reflected the longstanding cultural tendency toward opportunism that has stemmed from years of theft from Soviet bureaucracies; phreakers and common users, motivated by monetary savings and buoyed by the social acceptability of small thefts, went to great lengths to obtain scan lists and altered telephones, which they illegally used to get free service.

Russian web vandals frequently demonstrate nationalism as when Russian hackers attacked U.S. and NATO websites during the bombing of Yugoslavia; they also often attack their own government, as in the case of Russian hackers who have repeatedly

attempted to hack into President Vladimir Putin's website. Their activities reflect many of the popular views of mainstream Russian society, like the anti-Western sentiment during the bombing of Kosovo, and anti-Chechen sentiment in the ongoing cyberwar between allegedly FSB-sponsored Russian hackers and Chechen hackers.

Crackers in Russia enjoy a lax legal system and a relatively hacker-friendly attitude in society that stems from government-sponsored cracking in the Soviet Union. The social acceptability of electronic crime that has stemmed largely from this government-sponsored activity applies not only to crackers like Viktor Sklyarov and others who break the copyright protection of foreign software, but to all forms of electronic crime in Russia, including web defacement, carding, and worm creation..

The worm attacks coming out of Russia, such as the Zytob and MyDoom worms, reflect the hacker motivations of profit, hacker prestige, and vendettas against specific organizations. Such worms often exploit vulnerabilities in foreign-made software (often Microsoft operating systems) in order to create zombie networks that can be used for mass spamming or DDoS attacks against companies and government organizations that are reviled by Russian computer hackers (e.g., MyDoom targeted Microsoft and the RIAA). Worm authors demonstrate a desire to profit as they sell their inventions to interested parties. Faris Essebar sold Zotob to Atilla Ekici. Both Essebar and Ekici then attempted to use the worm to make a profit from advertising companies who would pay them for using the worm to lower the security settings of IE Explorer. Ekici also attempted to DDoS attack Microsoft, RIAA, and others, and Essebar bragged extensively

on IRC chatrooms about his accomplishments. Essebar and Ekici demonstrate a desire for hacker prestige and also vendettas against specific organizations.

Russian hackers will likely continue to engage in these and other types of hacking in the future. Only through a more comprehensive understanding of their motivations and cultural context can they be successfully counteracted and ameliorated. Rather than reinforcing and promoting simplistic, polarizing characterizations of hackers that currently prevail in the West, Russia and other countries would be wise to analyze the roots of hacker culture, hacker motivations, hacker public perception and misperception, and statistical analyses of hacker activity and impact, as this thesis has attempted to do, in order to more effectively enact social change and legislation.

Appendix – Translation of Weizenbaum passage

An obsessive programmer is dedicated to working on his own great projects as much as time allows him. "To work"-- this is not, however, the wording he uses; he calls that which he does "hacking." "To hack" according to the dictionary, is "to cut haphazardly, clumsily or without a definite target; to cut unevenly with the help of or by means of repeated blows." [The phenomenon which this author is writing about here is does not reveal itself in Soviet computer centers to such a degree, although for programming it is very characteristic to have disdain for documentation and especially the notification of others about changes/alterations to software. Therefore, as far as we know, in native programming jargon, computer understanding is absent. Unfortunately for us, the transmission of this term comes from transliteration. Thus arose "hackers" and "hacking" (incidentally, in English these terms are also neologisms].

I have already noted that obsessive programmers or "hackers" as they call themselves, are usually excellent technicians. One would think that he does not act "clumsily" as this definition indicates. However, the definition is correct here in a deeper sense, that hackers "act without a definite target"; the hacker is not in a position to place his own clearly formulated long-term goals and develop a plan of his own achievement, as long as he has the ability and not the knowledge. He does not consider anything that he might analyze or synthesize; in short, he has not intention of forming theory. His mastery, in this way, is without target, even without goal. It simply does not have any sort of relationship with anything other than his instrument, through which it is realized. His

mastery reminds one of a scribe copying manuscripts in a monastary, although not literate, he is a first-class calligrapher. All of these magnificent projects should be accompanied by illusions, by illusions of grandiosity. He creates one grandiose system, within the bounds of which all remaining specialists will write their own systems (it follows to note that not all hackers suffer from a pathological obsession with programming, in fact, if there were not such a high degree of creative work by these people, proudly naming themselves hackers, several of today's most-refined computer systems with time-sharing, translated machine language, systems of machine graphics and so forth, would not exist. (Weizenbaum)

Works Cited

"3Com's Zero Day Initiative Uncovers Microsoft Vulnerability Disclosed and Patched Today." LinuxWorld.com.au. 15 March 2006. Linux World. 20 March 2006 < http://www.linuxworld.com.au/index.php/id;453467771>.

Abdullaev, Nabi. "FSB Calls FBI Agent an Illegal Hacker." Moscow Times. 16 August 2002. 7 February 2006 < http://dlib.eastview.com/sources/article.jsp?id=4278290>

---. "Suspected Hacker Detained in Surgut." Moscow Times. 5 Jan. 2006 < http://dlib.eastview.com/sources/article.jsp?id=244296>.

Benner, Jeffrey. "Russian Hacker Has a Party." Wired. 20 Dec. 2001. 25 Nov. 2005 < http://www.wired.com/news/politics/0,1283,49272,00.html>.

Betts, Bryan. "Dawn of the undead." Techworld. 9 Feb. 2006. 28 Feb. 2006 < http://www.techworld.com/networking/features/index.cfm?featureid=2238>.

Blagov, Sergei. "Identity Theft Rife in Russia." Wired. 19 Aug. 2002. 22 Feb. 2006 < http://www.wired.com/news/business/0,1367,54427,00.html>.

Blau, John. "Viruses: From Russia, With Love?: As Internet Access Spreads to the Soviet Union, So Does Malicious Code." 28 May 2004. PC WORLD. 25 Jan. 2006 < http://www.pcworld.com/news/article/0,aid,116304,00.asp>.

Boym, Svetlana. The Future of Nostalgia. New York: Basic Books, 2001.

Bratersky, Alexander. "It's a Bird! It's a Plane! It's a Hacker!". Moscow Times. 8 Feb. 2002. 15 Nov. 2005 < http://dlib.eastview.com/sources/article.jsp?id=244565>.

Burns, Enid. "Baltic States Internet Population." Clickz Networks. 3 Nov. 2005. 25 Feb. 2006 < http://www.clickz.com/stats/sectors/geographics/article.php/3561451>.

Campbell, K.K. "Serbian War Moves to Cyberspace." Toronto Star. 15 Apr. 1999. 15 Mar. 2006 < http://www.kkc.net/toronto-star/1999/ts0415.shtml>.

Certeau, Michel de. From The Practices of Everyday Life. New York: Routeledge, 1998.

"Computer-Related Crime Impact: Measuring the Incidence and Cost." Joint Council on Information Age Crime. Jan. 2004. 25 Mar. 2006 < http://www.jciac.org/docs/Computer-Related%20Crime%20Impact%20010904.pdf>.

Delio, Michelle. “Inside Russia’s Hacking Culture.” Wired. 12 Mar. 2001. 15 Feb. 2006 < http://www.wired.com/news/culture/0,42346-0.html>.

---. “New MyDoom Virus Packs a Wallop.” Wired. 24 Feb. 2004. 28 Feb. 2006 < http://www.wired.com/news/infostructure/0,1377,62401,00.html>.

De Waal, Tom. “Russian Public Demands Action.” BBC News. April 9, 1999. 15 Jan. 2006 < http://news.bbc.co.uk/1/hi/world/europe/315582.stm>.

Dougaev, Daniil. “Hackers Are Just Human Beings.” Moscow Times. 10 June 1999. 15 Feb. 2006 < http://dlib.eastview.com/sources/article.jsp?id=234916>.

Evers, Joris. “Microsoft Puts Bounty on Virus Writers.” PC World. 5 Nov. 2003. 15 Feb. 2006 < http://www.pcworld.com/news/article/0,aid,113293,00.asp>.

Fisher, Dennis. “Fighting Back Against Cybercrime.” eWeek. 7 July 2004. 22 Jan. 2006 < http://www.eweek.com/article2/0,1895,1607369,00.asp>.

---. “Phishing Scams Get Savvier.” eWeek. 2 May 2004. 25 Jan. 2006 < http://www.eweek.com/article2/0,1895,1582698,00.asp>.

---. “Worldwide Phishing Attacks May Stem from Few Sources.” eWeek. 19 Oct. 2004. 25 Jan. 2006 < http://www.eweek.com/article2/0,1895,1679953,00.asp>.

“From Black Market to Free Market.” BusinessWeek Online. August 22, 2005. 15 Feb. 2006 < http://www.businessweek.com/magazine/content/05_34/b3948022_mz011.htm?chan=tc>.

Goldstein, Emmanuel. “Will The Media Ever Get It Right?” 2600. 9 Mar. 2001. 8 Sept. 2005 < http://www.2600.com/news/view/article/109>.

Golubev, Vladimir. “Criminals in Computer-Related Crime.” Crime-research.org. 15 Feb. 2006 < http://www.crime-research.org/library/Golubev_nov1.html>.

“Hacker.” Everything2.com. 19 June 2001. 15 Dec. 2005 < http://www.everything2.com>.

“Hackers Attack Russian News Site.” BBC News. 12 Dec. 1999. 15 Jan. 2006 < http://news.bbc.co.uk/1/hi/world/europe/561576.stm>.

“Hacker Manifesto”. Phrack. 8 Jan. 1986.15 Feb. 2006 < http://www.phrack.org/show.php?p=7&a=3>.

"Internet Put on Code Red Alert." BBC News. 31 July 2001. 15 Feb. 2006 < http://news.bbc.co.uk/1/hi/sci/tech/1464337.stm>.

Kelly, Catriona and David Shepherd. Russian Cultural Studies. New York, NY: Oxford University Press, 1998.

McClure, Stuart. Hacking Exposed: Network Security Secrets & Solutions. Emeryville, CA: McGraw-Hill, 2005.

McWilliams, Brian. "Kremlin Site Vulnerable to Attack." Wired. 21 June 2002. 28 Jan. 2006 < http://www.wired.com/news/technology/0,1282,53412,00.html>.

"Microsoft Security Bulletin MS05-039." Miscrosoft.com. 9 Aug. 2005. 25 Jan. 2006 < http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx>.

Mulvey, Stephen. "Russian Internet Politics." BBC News. 5 Mar. 2001. 25 Jan. 2006 < http://news.bbc.co.uk/1/hi/world/europe/1198603.stm>.

Nosik, Anton. "Internet Wars." Moscow News. 10 Mar. 1999. 25 Jan. 2006 < http://dlib.eastview.com/sources/article.jsp?id=223278>.

Pfleeger, Charles. Security in Computing. New York: Prentice Hall, 2002.

Rotkin, Aleksandr. "Friker: vce shto nuzhno…" Dec. 2002. 8 Dec. 2005 < http://phriker.narod.ru/phrik_lib01.html>.

Seltzer, Larry. "Spotting Phishing and Fighting Back." eWeek. 2 Aug, 2004. 25 Jan. 2006 < http://www.eweek.com/article2/0,1895,1630161,00.asp>.

Shklovsky, Viktor. Knight's Move. London: Dalkey Archive Press, 2005.

Skibell, Reid. "The Myth of the Computer Hacker." Information, Communication, and Society. Sept. 2002. Vol. 5 Issue 3, p336-356, 21p.

Solnick, Steven L. Stealing the State: Control and collapse in Soviet institutions. Cambridge: Harvard University Press, 1998.

Solovyova, Yulia. "Hacking Away from Vandalizing Web Sites to Online Bank Theft, Russia's Cybercriminals Have Proven Talents." 28 May 1999. 28 Nov. 2005 < http://dlib.eastview.com/sources/article.jsp?id=234713>.

Sossinsky, Sergei. “Society, Computers, and Hackers.” Moscow News. 26 Mar. 2003. 15 Jan. 2006 < http://dlib.eastview.com/sources/article.jsp?id=4800003>.

Sullivan, Bob. “Computer Worms Strike Media Outlets.” New York Times. August 17, 2005. 15 Feb. 2006 < http://msnbc.msn.com/id/8975840/>.

“Survey Says: ‘Everything is Hackable.” Gizmodo: The Gadgets Weblog. 22 Sept. 2005. 18 Mar. 2006 < http://www.gizmodo.com/gadgets/cracks/survey-says-everything-is-hackable-127039.php>.

Thornburgh, Nathan. “Two Russian Hackers Nabbed in FBI Sting.” Moscow Times. 28 Apr. 2001. 15 Nov. 2005 < http://dlib.eastview.com/sources/article.jsp?id=231481>.

Urbanowicz, Vincent. “MyDoom Computer Bug Causes Global Havoc.” Moscow News. 4 Feb. 2004. 28 Feb. 2006 < http://dlib.eastview.com/sources/article.jsp?id=5853845>.

“U.S. has 33% share of Internets users Worldwide Year-end 2000.” Computer Industry Almanac Inc. 24 Apr. 2001. 15 Feb. 2006 < http://www.c-i-a.com/pr0401.htm>.

Varghese, Sam. “Mydoom damage estimate termed absurd.” The Age. 6 Feb. 2004. 28 Feb. 2006 < http://www.theage.com.au/articles/2004/02/06/1075854035648.html?oneclick=true>.

Varoli, John. “In Bleak Russia, a Young Man’s Thoughts Turn to Hacking.” New York Times Online. 29 Jun. 2000. 25 Jan. 2006 < http://www.ssl.stu.neva.ru/psw/misc/29hack.html>.

Vedomosti, Yuriy. “E-Book Duplicator hits Barnes and Noble.” Moscow Times. 4 July 2001. 28 Nov. 2005 < http://dlib.eastview.com/sources/article.jsp?id=232266>.

Voiskounsky, Alexander and Julia D. Babaeva and Olga V. Smyslova. “Attitudes Towards Computer Hacking in Russia.” In Thomas, Douglas, and Brian D. Loader (Eds.). Cybercrime: law enforcement, security, and surveillance in the information age. New York: Routledge, 2000. pages 56 – 84

Voskoboinikova, Veronika. “Attacks of Hackers at Putin Official Web Site on Decline.” Itar-Tass. 22 Sept. 2002. 15 Feb. 2006 < http://dlib.eastview.com/sources/article.jsp?id=4368609>.

Wang, Wally. Steal this Computer Book II: What They Won't Tell You About the Internet. San Francisco, 2003.

Ward, Mark. "Money Motive Drove Virus Suspects." BBC News. 5 Sept. 2005. 25 Jan. 2006 < http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4205220.stm>.

Weizenbaum, Joseph. Computer Power And Human Reason. From Judgment to Calculation. Перевод на русский язык, предисловие и примечания, издательство "Радио и связь", 1982. Пер. с англ./ Под ред. А. Л. Горелика. - М: Радио и связь, 1982.

Zetter, Kim. "Database Hackers Reveal Tactics." Wired. 25 May 2005. 25 Jan. 2006 < http://www.wired.com/news/business/0,1367,67629,00.html>.

"Zotob and Mytob were originated by Russian hacker." Computer Crime Research Center. 30 Aug, 2005. 15 Jan. 2006 < http://www.crime-research.org/news/30.08.2005/1462>.