THE ECONOMICS OF COMPUTER HACKING

Peter T. Leeson, Ph.D.[*] *& Christopher J. Coyne, Ph.D.*[**]

ABSTRACT

This paper considers various classes of computer hackers, with a special emphasis on fame-driven versus profit-driven hackers. We use simple economic analysis to examine how each of these hacking "markets" work. The resulting framework is employed to evaluate current U.S. policy aimed at reducing the threat of computer hacking and shows that this policy is largely effective. We consider policy adjustments consistent with the insights of the framework provided as a means of strengthening cyber security.

1. INTRODUCTION

In the digital age cyber security is perhaps the most important form of security with which individuals must be concerned. Banks, schools, hospitals, businesses, governments, and virtually every other modern institution you can think of stores and organizes its information electronically. This means that all of your most sensitive information—from credit card numbers and checking accounts to medical records and phone bills—is accessible for viewing, stealing, or manipulating to anyone with a PC, an Internet connection, and some computer know-how. The increasingly computer-based world is increasingly vulnerable to malevolent computer hackers.

While we know little about these shadowy hackers, we have a very clear picture of the damage they do. In 2003, hacker-created computer viruses alone cost businesses $55 billion—nearly double the damage they inflicted in 2002 (SecurityStats.com 2004). In 2000 the total cost of all hack attacks to the world economy was estimated at a staggering $1.5 trillion (PricewaterhouseCoopers 2000). In a 2004 survey of American companies and government agencies conducted by the Computer Security Institute, over half of respondents indicated a computer security breach in the

[*] Department of Economics, West Virginia University. Email: pete.leeson@mail.wvu.edu.

[**] Department of Economics, Hampden-Sydney College. Email: ccoyne@hsc.edu. We thank Peter Boettke, Tony Carilli and Tyler Cowen for helpful comments and suggestions. The financial support of the Critical Infrastructure Project, the Earhart Foundation and the Oloffson Weaver Fellowship is also gratefully acknowledged.

past 12 months and 100 percent of respondents indicated a Web site-related incident over the same period (CSI 2004).

If anything these figures probably understate the volume of hacker-related security breaches. Firms, especially financial institutions, are extremely reluctant to report hacker-related break-ins for fear of how this may affect customers' and stockholders' impressions of their security. In the survey of American businesses conducted jointly by CSI and the FBI, nearly 50 percent of firms that experienced system intrusion over the last year stated that they did not report this intrusion to anyone. The primary reason cited for this was the perceived negative impact on company image or stock (CSI 2004, pp. 13-14), and similar findings have been corroborated by others (see for instance, United Nations 1994; Schell and Dodge 2002, p. 40). What can we say about the enigmatic community of computer hackers and what can we do about the cost these hackers impose?

This paper uses simple economic analysis to try and better understand the phenomenon of hacking. In particular we are interested in creating a framework for analyzing hacking that is policy relevant. Towards this end we divide the community of hackers into three classes separated by motivation. The first class consists of "good" hackers. These hackers illegally break into computer systems but voluntarily share security weaknesses with those in charge of these systems. The second class of hackers is fame-driven. This class constitutes a dangerous subculture of unethical hacking in which members seek infamy and the accolades of their cohorts by breaking into the electronically stored information of vulnerable parties and wreaking havoc. The third group of hackers is "greedy." These hackers are not motivated by considerations of fame but are instead driven by profits. Profit-driven hackers can be "good" or "bad" depending upon which type of behavior yields the greatest monetary return.

An economic analysis of these distinct hacker categories yields important insights for policy aimed at reducing the security threat posed by computer hacking. In Section 2 we offer a brief history of hacking. Section 3 discusses good hackers. Section 4 examines fame-driven hackers. Section 5 considers profit-driven hackers. Section 6 turns to the policy implications of our analysis, and Section 7 concludes.

2. A BRIEF HISTORY OF HACKING

The history of hacking can be traced to 1960s America where members of the Tech Model Railroad Club at MIT "hacked" the control systems of model trains to make them run faster, more effectively, or differently than they were designed to run. Around the same time MIT introduces its Artificial Intelligence Lab where some of the first large mainframe computers are located. With an innate curiosity for how things work, several club members are drawn to MIT's AI lab. These computers—called PDP-1's—are large, slow, and extremely expensive to operate. To overcome

some of these problems the more clever programmers created "hacks"—system shortcuts that make performing certain operations faster and easier.

MIT is not the only locus of hacking activities. Computing think tanks, like Bell Labs, are at it too. In one of history's most important hacks, in 1969 two AT&T Bell Lab workers, Dennis Ritchie and Ken Thompson, create the forerunner of the open source operating system, which they name UNIX. UNIX quickly becomes the standard language of computing. In its first stages hacking has nothing to do with illicit activities or cyber-crimes. On the contrary, access is consensual, and hackers improve systems rather than defacing them.

In the 1970s, however, things begin to change. Hackers start to realize the potential of hacking for personal benefit. In particular, hacking activities are increasingly directed at the telephone—an activity called "phreaking." In the early 1970s a Vietnam veteran named John Draper discovers that the free plastic whistle that comes in boxes of Captain Crunch cereal identically reproduces the 2600 Hz tone required to make long distance phone calls. By blowing the whistle into the phone at the appropriate time AT&T's switching system believes that legitimate access has been granted to make a long distance call and the caller is granted the ability to do so without paying.

After his discovery Draper takes on the pseudonym "Cap'n Crunch" and quickly generates an underground following among hackers and phreakers for his creativity with long distance calling. Other hackers build on Draper's innovation by constructing "blue boxes" designed to aid in the long distance phone fraud process. Notable hackers engaged in such phreaking at the time include Steve Wozniak and Steve Jobs—the future founders of Apple Computers. In 1978, two hackers from Chicago start a computer to computer bulletin board, creating the first virtual meeting place for the growing hacker community where members can share tips, stolen credit card numbers, and other information going into or coming out of their hacking activities.

Partly spurred by the publicity given to hackers in the 1983 film *War Games*, partly spurred by the new affordability of personal computers, and partly spurred by the increasing presence of the online world (ARPANET during this time is becoming the Internet), the prevalence of computer hacking rises yet again in the 1980s. Among the most important hacking developments of this decade is the emergence of hacker "gangs" like the Milwaukee area's "414" gang that consist of hacker die-hards who live to gain unauthorized access to outside computer systems and wreak havoc. The 414 gang is among the first to be apprehended and punished by the law for their cyber-crimes, which include illegally accessing the computer system at Los Alamos National Laboratory where nuclear weapons are developed and breaking into the system at Sloan Kettering Cancer Center in New

York. The 414's are not alone in the new world of hacker crime. The "Legion of Doom" and the "Masters of Deception"[1]—two leading, rival hacker gangs—are also born in the 80s. In response to the growing number of hacker-related crimes, in 1984 the U.S. government makes it a crime to gain unauthorized access to computer systems.

But hacker activity is not limited to breaking into computer systems. In 1988 the world witnesses the first of a new type of hacker act—the Internet worm, which is inadvertently spread by its creator Robert Morris of Cornell University. Morris is identified, fined $10,000, and sentenced to three years probation. The late 80s also see the first cases of hacker action directed at government. Several members of the West German hacker gang, the "Computer Chaos Club," steal electronically stored information from the U.S. government and sell it to the Soviet KGB.[2]

In the 1990s the growing trend of hacker activity prompts the U.S. government to perform surprise raids on the locations of suspected hacker outfits in 14 cities across the nation ("Operation Sundevil"). Although arrests are made, and many inside the hacking community turn on their cohorts in exchange for immunity, hacker activity continues. No longer is hacking mostly about the pranksterish behavior of teenage boys or petty crime. Now hackers turn their talents to much larger deals. In 1995 two Russian hackers steal $10 million from Citibank. In response to more serious hacker activities like this one, in 1998 the U.S. government unveils its National Information Infrastructure Protection Center, designed to protect America's telecommunications, transportation, and technological systems from hacker attacks.

In the new millennium, hacking—an activity once largely restricted to Americans and Western Europeans—is a worldwide phenomenon. The seriousness of the crimes perpetrated by hackers increases again as well. Hackers design "denial of service" hacks that crash the networks of companies like Yahoo!, eBay, Amazon, and others, costing them millions in lost business. The potency and prevalence of damaging viruses also continue to grow, culminating in May of 2000 with the "I LOVE YOU" virus, which is estimated to have cost the global economy close to $9 billion, and is the most harmful hacker-created virus to date (CEI 2002).

As its history indicates, "hacking" refers to multiple activities. It includes, for instance, breaking passwords; creating "logic bombs;" e-mail bombs; denial of service attacks; writing and releasing viruses and worms; viewing restricted, electronically-stored information owned by others; URL redirection; adulterating Web sites; or any other behavior that involves accessing a computing system without appropriate authorization. Furthermore, although for the most part hacking is restricted to computers, it need not be and may be extended to fraudulent activities relating to telephones

---

[1] For a detailed account of the Masters of Deception see Slatalla and Quittner (1996).

[2] For a detailed account of this story see Stoll (1989).

(e.g., tricking phones into authorizing free long distance calls, so-called "phreaking"), credit cards (for instance, creating gadgets to "steal" the magnetic code stored on credit cards and copy it on to others), subway passes (for example, adulterating passes or pass readers to enable unlimited free rides), parking meters (rigging parking meters to allow unlimited free parking) or virtually any other item with electronic components. We restrict our discussion primarily to computer hacking, although the basic principles we elucidate may be applied to other forms of hacking as well.

Some hackers object to calling many of the destructive activities mentioned above "hacking" and their perpetrators "hackers." These terms, they insist, should be reserved to the harmless (albeit often illegal) activities of computer enthusiasts who break into systems, look around to learn how things work and leave things undisturbed. According to this view the name "cracker" should be applied to the malicious "cracking" behaviors enumerated above that are all too frequently conflated with harmless hacking. While we recognize this difference, we nonetheless opt to refer exclusively to hackers and hacking throughout our discussion. On the one hand, in most cases, both hacking and "cracking" involve unauthorized access and so constitute security threats whether or not the individual breaking in uses her illicitly gained access to do harm. Second, for better or worse, in the parlance of our day "hacking" refers to the activities that we describe and the general public does not have the nuanced appreciation of illegal computer activity that members of the hacking community do to merit the terminological distinction implored by some members of this community.[3]

3. GOOD HACKERS

While the psychology of hacking is still in its nascent stages, initial research seems to have come to some consensus regarding what motivates hackers to hack. Individual hackers and hacker gangs operate in the context of a larger underground social network or community consisting of similar individuals. The best empirically grounded work that examines the hacker mind therefore draws primarily on interviews and surveys administered to members of this underground community. We will briefly overview some recent findings of this small literature below. Before doing so, however, we should point out that members of the hacking community are notorious for lying to journalists, researchers, and others who approach them for information about how they and their associates work. Many hackers seem to "get a kick" out of misleading scientists or generally giving others a false im-

[3] As Dann and Dozois put it: "just about everyone knows what a hacker is, at least in the most commonly accepted sense: someone who illicitly intrudes into computer systems by stealth and manipulates those systems to his own ends, for his own purposes (*Hackers* 1996, p. xii).

pression about their reasons for hacking (Platt 1997, p. 53).[4] Of course, this fact must be kept in mind when considering the results of research aimed at identifying hacker motives. Nevertheless, this data is the best we have to date so we must make use of it unless we are to avoid empirical investigations of the subject altogether.

The most current and comprehensive data regarding hackers' demographics, motives, lifestyles, etc. is that collected by Schell et al. (2002). These researchers surveyed over 200 hackers who attended two of America's largest hacker conventions (yes, there are annual hacker conventions in which hackers from across the globe get together to share tips ranging from the latest computer hardware to how to steal credit card numbers stored electronically) in July of 2000. These conventions included the H2K convention in New York and the DefCon 8 convention in Las Vegas. In addition to administering anonymous surveys, researchers randomly interviewed some hackers with in-depth questions (again on the condition of anonymity) when hackers would agree to do so.

The total size of the hacking community is unclear, though by most accounts it is fairly small. According to Sterling, "some professional informants . . . have estimated the size of the hacker population as high as fifty thousand." However, "This is likely highly inflated . . . . My best guess is about five thousand people" (Sterling 1992, p. 77). While we know little about the total size of the hacking community we have a very good idea about its gender proportions. Consistent with figures from others which suggest the population of hackers is overwhelmingly male, only 9 percent of those surveyed by Schell et al. (2000) were female (see for instance, Taylor 1999; Gilboa 1996). Also consistent with older findings, most hackers surveyed were under the age of 30, with a mean age of about 27, a mode of 24 and a median of 25.

The motivation for hacking varies but a significant proportion of hackers surveyed indicated innocuous reasons for their behavior. Thirty-six percent said they hack to "advance network, software, and computer capabilities," 34 percent claimed they hack "to solve puzzles or challenges," and 5 percent said they hack to "make society a better place to live." If we can believe these numbers the overwhelming majority of hackers are harmless. It is true, in gaining unauthorized access to computer systems they pose potential security threats, but they do not themselves cause damage. Of course, to the extent that they share security holes with other less responsible members of the hacking community they indirectly jeopardize computer users; but it is unclear to what extent "good" hackers do this.[5]

---

[4] Taylor suggests that hacker manipulation of the media is partly in order to "revel in the subsequent notoriety" that stigmatizing themselves creates (1999, p. xiii).

[5] In the early 1980s an elite group of hackers calling themselves the "Inner Circle," formed to pass new information gleaned from their hacking activities between one another without making this information available to unethical hackers who would abuse it.

Among these good hackers there is some part of the population that performs a questionably valuable service to computer users. Some of these hackers report security holes to programmers and systems operators of computer systems where they find security weaknesses. This information can then be used to patch holes or strengthen vulnerabilities, preventing intrusion by less benevolent hackers.

Nevertheless, we say questionable here because the advice of these hackers (as well as the hack itself) is unsolicited. According to one popular hacking analogy, it is a bit as if someone broke into your house, didn't steal anything, but left you a note telling you that your alarm system is weak and your windows unprotected, so you should look into having that fixed. While in one sense you are better off because of it, in another sense you may be justifiably outraged.

Unfortunately, data on what proportion of the good hackers are benevolent in this way is not available.[6] We do know that some such hackers exist because insiders at some companies have hinted that certain patches they have released are in response to "good hacker" tips like these. Complicating the issue of good hackers is the fact that some good hackers are far more adamant that vulnerable programmers and systems operators respond to their advice than others. Some good hackers not only inform organizations of security weaknesses but also threaten to release the hole they've found unless action is taken to correct the problem. This is as if someone broke into your house and told you that if you don't buy a better alarm they will inform the criminal community about how it may plunder you.

Good hackers appear to be the most complicated to deal with because they are not motivated by "base" human desires like money or fame. Fortunately, because they pose the weakest threat and are likely responsible for the least damage to individuals and businesses among the hacking community, we lose relatively little at least in terms of felt costs by this dearth of understanding. Far more important from the standpoint of security are bad hackers—those who perform damaging acts in order to gain peer recognition and those who perform such acts for personal profit.

4. BAD HACKERS: HACKING FOR NOTORIETY

The survey conducted by Schell et al. (2000) suggests that only 11 percent of respondents are malevolently motivated. However small the proportion of bad hackers may be, they are the most important to consider because they are responsible for the costly damage inflicted by hackers each year. Contrary to other work which suggests that a substantial propor-

---

[6] Eight percent of those surveyed by Schell et al. (2000) said that they hack to "expose weaknesses in organizations or their products." It is unclear from this, however, whether the reason behind this motive of these respondents is benevolent or malevolent.

tion of hackers are motivated by fame or reputation inside the hacking community, none of those surveyed by Schell et al. noted this reason as their motivation. It is difficult to say why this is, but this result is evidently counter to other examinations of hacker motivation. Fame or peer recognition ranks among the most prominent hacker motivations cited by security experts and hackers alike, as well as in other discussions of hacker psychology (see for instance, Taylor 1999b; Blake 1994; Sterling 1991; Hannemyr 1999; Platt 1997; Thomas 2002; Verton 2002).[7]

As Denning has pointed out, "Although the stereotype image of a hacker is someone who is socially inept and avoids people in favour of computers, hackers are more likely to be in it for the social aspects. They like to interact with others on bulletin boards, through electronic mail, and in person. They share stories, gossip, opinions and information; work on projects together; teach younger hackers; and get together for conferences and socializing" (1992, p. 60).

Bigger, more difficult, more devastating, or new types of hacks bring their creators notoriety among members of their underground community.[8] Word of a hacker's exploits can be spread among community members in a number of ways. First, hackers may spread this information by their own word of mouth, repeating it to fellow hackers or rival gangs who repeat this to other community members and so on. Second, hackers may publicize their responsibility for acts of hacking on Websites, bulletin boards, or on hacker e-mail lists like "BugTraq,"[9] "rootshell," "RISKS Digest," and "VulnWatch." In these virtual spaces hackers take credit for damage done, make information or software that they have stolen available to other hackers, or share their newest methods of hacking or hacking programs they have created with other members of the community so that these individuals may consume them.

In each of these cases hackers identify themselves as the individuals behind new hacks by posting information under their "handles"—pseudonyms chosen by hackers and hacker gangs to give them identity within the hacking community and yet retain their anonymity from authorities.[10] Pseudonyms selected by hackers tend to the memorable and dra-

---

[7] Some other hacker motivations such as the "feeling of power" and "ability to share knowledge" can also be collapsed into considerations of fame. For instance, the more notorious a hacker becomes, the greater her feeling of power. Similarly, her ability to share knowledge will increase with the amount of new information she collects and disseminates, which will also increase her fame.

[8] We should also note that the general public's fascination with the mysterious hacking underworld has helped to fuel fame for members of the hacking community as a whole. Numerous popular movies, for instance, glorify hacking, contributing to this phenomenon. *War Games*, *The Net*, *Hackers*, *Sneakers* and others all provide cases in point.

[9] Interestingly, BugTraq was recently purchased by the computer security firm Symantec for $75 million.

[10] Not all hackers identify themselves by their handles all of the time. Most hackers, however, do so most of the time. The survey conducted by Schell et al. (2000), for instance, indicates 63 percent of

matic, for instance, "Dark Dante" (aka Kevin Poulsen), "Captain Zap" (aka Ian Murphy), "The Nightstalker" (a leading member of the influential hacker group the "Cult of Dead Cows"), etc.—a factor that aids hackers' ability to generate notoriety within the community when they post new information. The same is true of names selected by hacking gangs, for example, "World of Hell," "Bad Ass Mother F*ckers," "Circle of Death," "Farmers of Doom," and so on.[11] The fame-based motivation of many bad hackers helps to explain why profane, absurd, and overstated gang names and handles pervade the hacking underground.

Hackers and hacker gangs that generate celebrity status for their hacks can also set trends inside the hacking community. For instance, two of hacking history's most famous hacker gangs, the Legion of Doom and the Masters of Deception, sparked a trend whereby subsequent hackers and gangs created handles based on comic book characters. Similarly, the 414 gang—one of the first hacker gangs raided by authorities—set the trend of creating handles based on numbers (Schell et al. 2000, p. 58).

The underground world of hackers also has its own popular media that publishes hacking-related books, newspapers, and magazines or e-zines. Some examples of the latter include *2600: The Hacker Quarterly*, *Black Hacker Magazine*, *Computer Underground Digest*, *Phrack Magazine*, *Hack-Tic Magazine*, *The Hackademy Journal*, *Hacker Zine*, *H.A.C.K.*, *Bootlegger Magazine* and *Binary Revolution* to name a few. Inside these outlets hackers publish "how to" articles (e.g., how to defraud an ATM machine) and share new information they have gleaned from their most recent hacking exploits. Articles and books are published under the author's handle and give well-published hackers access to large audiences who thus come to know certain hackers as the "best" in their area, increasing the author's fame inside the community. One of the largest of these publications—*Phrack*—even contains a section called "Pro-Philes" in which famous hackers, retired legends, or rising stars in the hacking community are profiled and interviewed for readers, with special highlights on their biographies and most impressive hacks. In this way, outlets like *Phrack* "served as the means to legitimate hackers for the underground . . . presenting them as celebrated heroes to the readers that made up the underground" (Thomas 2002, p. 140).

Becoming famous through these channels has its benefits for hackers who can generate stardom in the digital underground. Some subcommunities within the hacking underworld will only allow relatively well-known hackers into the community. On the one hand, this gives famous hackers who are admitted greater exposure inside the hacking community,

---

respondents typically use their handles when hacking. This finding is also corroborated by Meyer (1989). Obviously, to some extent the use of handles will depend upon the illegality of the activity. Bad hackers, it is safe to assume, rely upon their handles more than good hackers do.

[11] For examples of other hacker gang names see Platt (1997).

and on the other hand, it gives them access to additional information that may only be shared within the group. Peer recognition also enables hackers to enter elite hacker gangs that are well known and highly respected by other members of the community. As one hacker put it: "Peer recognition was very important, when you were recognized you had access to more . . . many people hacked for fame as well as the rush. Anyone who gets an informative article in a magazine (i.e., *Phrack*, *NIA*, etc.) can be admitted to bulletin boards."[12]

When done right, celebrity in the hacker underground can evolve into outright cult star status as other hackers seek to imitate a notorious hacker's methods or view him as a leader within their community. Such was the case, for instance, with Cap'n Crunch, whose name is forever linked to the practice of phreaking and whose big discovery has led to, among other things, one of the largest hacker publications—*2600*—which is named after his discovery.

"Condor," aka Kevin Mitnick, obtained similar superstar status inside the hacking underground and generated a cult-like following of his own. Mitnick, arrested numerous times for his hacking activities, not only gained notoriety within the hacking sub-community, but became well known to the outside world as well. His picture and story appeared throughout the country in newspapers and magazines, and Mitnick told his story on television's *60 Minutes*. In addition to serving as the basis for numerous books, Mitnick's hacking helped inspire use of the term "Cyberpunk" in popular culture, which was famously used partly in reference to Mitnick by authors/journalists Katie Hafner and John Markoff (1991).[13] Following Mitnick's last arrest in 1995, a group of his hacker community followers protested his trial in the late 1990s. This group of hackers, which had organized itself into a gang called "Hacking for Girlies," broke into the *New York Times* Web page and created a message the *Times* could not remove, exonerating Mitnick for all the site's readers.

Select hackers get the reputation among their cohorts as "elite"—the cream of the underground. These individuals are often gang leaders like "Lex Luther" (former head of the Legion of Doom), or "Phiber Optik" (a former leader of the Masters of Deception), who was even heralded by *New York Magazine* as one of the city's "smartest 100 people." These hackers are the most innovative in the underground and are responsible for making hacking programs publicly available to the hacking community at large. Hacking programs can be downloaded from hacker bulletin boards, for in-

---

[12] Quote from a hacker's email interview with Taylor (1999, p. 59).

[13] William Gibson, credited with coining the term "cyberspace," helped spawn the science fiction genre now called "cyberpunk" in the 1980s (see for instance, Gibson 1984). Some believe that this genre contributed significantly to the shape of hacking culture by glorifying cyber anti-heroes (see for instance, Thomas 2002).

stance, and used with minimal knowledge and effort to hack various systems.

Most hackers, of course, do not reach this level of fame. Their inferior programming skills prevent them from creating effective hacking programs, and instead, most of their energies are devoted to finding and reporting relatively small or already known security holes to fellow hackers, or simply downloading information and prefabricated programs like "Trin00," "Tribal Flood Network," or "Stacheldraht," which were developed by superior hackers and using these to attack systems.[14] These "script kiddies," as they are called, are unlikely to gain fame in the larger hacker community for their hacking skills, but some may gain notoriety for the damage they cause using the programs and information created by more elite hackers. It requires little hacking prowess to crash Amazon.com, for instance, as was demonstrated by "Mafiaboy," the 15 year-old script kiddie whose hacking antics cost some of the Internet's largest vendors $1.7 billion in February of 2000.

Most fame-driven hackers explicitly eschew monetary gain as part of their hacking expeditions. They have contempt for profit-driven hackers who operate or work for computer security companies, or other large computer-related corporations, as though these individuals were beneath them. Fame-driven hackers even have a special, derisive name for these hackers—they call them "Microserfs." This negative reaction to profit-driven hacking has much to do with the cultural norms of the fame-driven hacking community, which in large part believes that big businesses are unscrupulous and views such entities as subordinating the creative skills of the hacker to the greedy corporate world.

4.1 The Economics of Fame-Driven Hacking

The fame-based drive of many hackers has particular implications for how this segment of the "hacker market" looks. The "coin of the realm" for fame-driven hacking is, of course, fame. How we model this "market," therefore, differs from traditional markets in which money drives production and price adjusts to equilibrate suppliers and demanders. The fame-driven hacking "market" considers the relationship between fame and the quantity of hacking. It maps supply and "demand" (which as we will see

[14] Other examples of programs created by hackers that can be downloaded and used by virtually anyone to hack systems include "Black Orifice" created by the Cult of Dead Cows and "L0phtCrack" created by L0pht, and "WinNuke"—all used to hack Microsoft Windows. A similar program called "AOHell" can be used to hack AOL. In 1995, Dan Farmer and Wieste Venema released their "Security Administrator Tool for Analyzing Networks," aka SATAN, an automated program to be used by systems administrators to find flaws in their security. This program could also be used, however, by low-level hackers to hack vulnerable systems, and thus there was great concern it would lead to many problems. To date, it has not caused the harm expected by many.

below is not demand in the conventional sense) in fame/quantity of hacking space.

On one side of this "market" are the producers of hacks who desire fame. The supply schedule for these hackers has the conventional positively sloped shape. When hackers stand to become more famous or better known within the hacker community for hacking, they supply a greater quantity of hacking (which may be expressed in terms of the inventiveness of hacks, the severity of hacks, etc.). When they stand to receive less fame or notoriety for hacking, they are willing to supply less.

The position of this supply curve is determined largely by the cost of hacking. Hackers face a moderate initial fixed cost of hacking, which in most cases comes down a computer, a telephone line (or cable), and a modem. For more sophisticated attacks fixed costs may also include training in basic programming and computer languages, though many kinds of devastating hacks require little specialized training at all. Hackers' variable costs consist primarily of the cost of electricity.

The other primary determinant of the supply curve's position is the number of hackers in the industry. This population is constrained significantly by the number of people who desire fame in the hacker underground (your sister, for instance, is probably capable of hacking but does not desire to be famous among hackers and so does not), which is relatively small. This factor—the population of individuals who desire to enter the "Hacker Hall of Fame"—ends up being the limiting factor determining the position of the supply curve for hacking. Thus, although virtually anyone can cause a lot of damage as a hacker because it is so cheap, very few do so because very few desire the reward it offers—fame among hackers.

The other side of this "market" is unusual in that it does not consist of demanders in the usual sense. When hackers supply more hacks the rest of the hacking community becomes happier. This may be because it gives them access to new information, new hacking methods, and software, which they may value for the purposes of undertaking their own hacking activities or because they view these things as goods in and of themselves. Members of the hacking community may view acts of hacking as expressive of their stand against corporate entities or their belief that all information ought to be publicly available and "free."[15] Others may simply be malicious and enjoy seeing the security of big corporations, for instance, jeopardized, or they may view hack attacks as indirectly serving their political ends.[16]

---

[15] A core component of the hacker "code" ascribed to by so many hackers is that access to computers and all information should be unlimited and free. For a more detailed description of this code see Levy (1994).

[16] Many hackers tend to be strongly left leaning and are adamantly against "commodifying" information. This partly stems from their roots in the "Yippie" movement of the 1960s and 1970s,

In the fame-driven case the hacking community does not pay for more hacking with a higher price. The producers of hacks do not seek money and, as we noted previously, often explicitly reject monetary reward. They seek fame. This, in conjunction with the fact other members of the hacking community value additional hacking, leads them to cheer more, so to speak, when additional hacking occurs. Additional cheering is translated into additional fame for the suppliers of hacks. Rather than demanding the output of suppliers in the usual sense, the other side of the fame-driven "hacker market" consists of individuals (the hacking community) who respond to the supply of hacking with greater or lesser applause. In the language of economists, the hacking community has a reaction function, which specifies how this community reacts with fame to various quantities of hacking that are supplied by hackers. More hacking is rewarded with more applause and less with less applause. The hacking community's reaction function is therefore positively sloped like the supply of hacking itself. The interaction of the supply curve for hacking and the hacking community's reaction function creates two possibilities, depicted in Figure 1 and Figure 2.

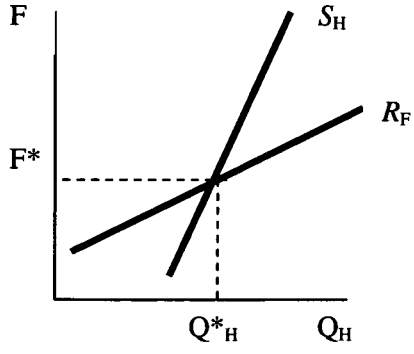

Figure 1.

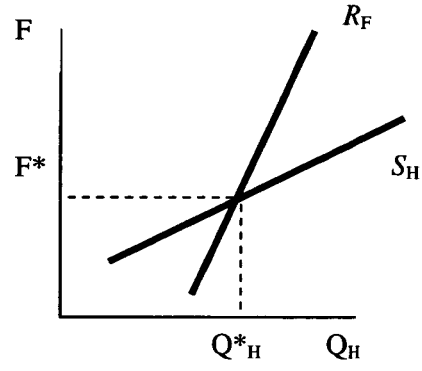

Figure 2.

In Figure 1 hackers' supply curve is less elastic than the hacking community's fame reaction function. In Figure 2 the reverse is true. This means that in Figure 1 the producers of hacks are more responsive (sensitive) to changes in fame than the community of reacting hackers, and in Figure 2 the community of reacting hackers is more responsive to changes in fame than are producers of hacks. These two possibilities have very different (and in fact, contradictory) implications for policy aimed at reducing the quantity of hacking in the fame-driven hacking industry. It is therefore very important to carefully consider the impact of existing policy in each

which in addition to advocating phreaking was largely anchored in the leftist political environment among young people of this time (see for instance, Sterling 1992).

case and, if possible, identify which case is more likely to prevail. We address these issues in Section 6.

5. GREEDY HACKERS: HACKING FOR PROFIT

A third class of hackers is driven by the profit potential of hacking activity. These hackers are concerned with dollars not fame and may come from either pool of hackers, good or bad. From the bad pool are hackers who engage in activities such as credit card fraud, stealing from banks, selling sensitive information stolen from one company to another, or those who are hired by other criminals to do their bidding for a fee.

From the good pool are hackers who work for or operate computer security firms. In 2001 this was a $1.8 billion industry in the United States alone (Wingfield 2002). These hackers sell their skills at finding security weaknesses in computer systems and programs to governmental institutions and private businesses that want to strengthen their security. These organizations hire security firm employees to engage in simulated hacker attacks on their systems and then report vulnerabilities so that they may be corrected. Some of the security experts employed by or running these firms are reformed hackers—individuals who used to hack illegally and either gave it up voluntarily or were caught and punished for their former crimes and so turned to legitimate hacking. Some examples of this include the now defunct, Comsec Data Security operated by four former members of the Legion of Doom, and Crossbar Security operated by Mark Abene (aka Phiber Optik), a former leader of the Masters of Deception. Successful examples of reformed hacker-run security firms include, for instance, ShopIP, run by John Draper (aka Cap'n Crunch) which now has made available a new firewall it calls the "Crunchbox," and Ian Murphy's (aka Captain Zap) IAM Secure Data Systems, Inc.[17]

Out of mistrust, many businesses are reluctant to hire reformed hackers to improve their security. This was ultimately responsible for why Comsec went out of business. Many other organizations, however, are especially drawn to this feature of some security firms because these firms provide the most realistic hack attacks on their systems. Hackers are said to possess a unique way of thinking that leads them to find inventive ways into systems that normal hired hands could not. Major corporations such as American Express, Dun & Bradstreet, and Monsanto, have all hired so-called "tiger teams" to test their systems for vulnerabilities (Roush 1995, p. 39).

The markets for both good and bad profit-motivated hackers look conventional. Since producers seek money, the supply and demand for hacking

---

[17] Former notorious hacker Kevin Poulsen (aka Dark Dante) is now an editorial director for *Security Focus*, an on-line information network for computer security.

are expressed in traditional price/quantity space and price equilibrates the behavior of suppliers and demanders. Both markets exhibit positively sloping supply curves and negatively sloped demand curves. In both cases hackers will provide a larger quantity of hacking if they are paid more and less if they are paid less. Similarly, both criminals and legitimate businesses that hire profit-driven hackers for their purposes demand smaller quantities of hacking when hackers charge more and demand greater quantities when hackers charge less.

The price elasticities of these curves are determined by the standard factors and there is no reason to think that they will be extreme for either the supply of or demand for hacking. Similarly, the position of these curves is determined by the typical elements in each case, with the exception of the fact that the cost of hacking for bad hackers is higher than it is for good hackers because the former involves the possibility of legal punishment while the latter does not. It is therefore reasonable to think that the equilibrium price of hacking in the market for bad profit-driven hacking will be higher than it is in the market for good profit-driven hacking. To the extent that for-profit hackers are willing to supply their services to the highest bidder, the rates of return on bad versus good profit-driven hacking will determine the flow of hackers between these two industries that compete for their labor.

This can be a good thing or a bad thing from the perspective of computer security. If good for-profit hacking is more profitable than bad for-profit hacking, society wins on two fronts from the standpoint of security. The number of bad hackers shrinks endogenously and exogenously. On the one hand more hackers will be employed in activities that do not involve illegally breaking into others' systems, thus reducing the number of potentially harmful hackers out there. Not only this, but the supply of profit-driven hackers no longer employed in harmful hacking is actually employed in fighting the attempts of bad hackers attempting to cause trouble. If, however, bad for-profit hacking is more lucrative, the opposite is true. The supply of hacker threats rises as the best and brightest for-profit hackers are recruited to the dark side.

6. POLICY IMPLICATIONS

The primary federal law in the United States designed to deal with computer hackers is the Computer Fraud and Abuse Act, originally created in 1984 but modified in 1996 by the National Information Infrastructure Protection Act. Originally this law applied only to government computers but it has subsequently been extended to include any computer involved in interstate commerce. This act prohibits under penalty of law: accessing a protected computer without authorization (or exceeding authorized access); accessing a protected computer without authorization and acquiring information; transmitting a program, information, code or command, and as a

result of that conduct, intentionally causing damage to a computer system without authorization (computer viruses); trafficking in computer passwords or other such information through which a computer may be accessed without authorization; and interstate threats for the purposes of extortion to cause damage to a protected computer (Raysman and Brown 2000). The act also prohibits accessing a protected computer without authorization with the intent to defraud where as a result of such action the hacker causes damage in excess of $5,000 over a one-year period.

Most violations of this law can result in up to five years in prison and $250,000 in fines for the first offense and up to ten years in prison and $500,000 in fines for the second offense. Any violation of this law results in a sentence of at least six months. The Computer Fraud and Abuse Act also allows any person who suffers damage as a result of its violation to bring civil charges against the perpetrator for damages. Additionally, since some hacks involve the violation of copyrighted materials, the Digital Millennium Copyright Act punishes those who attempt to disable encryption devices protecting copyrighted work.

In a nutshell, the present law punishes computer hackers, be they good or bad, with stiff fines and jail sentences. It is hoped that through these punishments, hackers will be deterred from hacking. What can our analysis say about this policy?

6.1 Policy and Profit-Driven Hacking

In the case of profit-driven hackers, present policy achieves its desired end. By increasing the cost of bad for-profit hacking through making this behavior criminal, current policy reduces the supply of bad for-profit hacking. The effect of this legislation is two-fold. First, it raises the equilibrium wage of producers who remain in the bad for-profit hacking industry, and second it reduces the quantity of bad for-profit hacking supplied. These effects of current legislation are depicted in Figure 3.

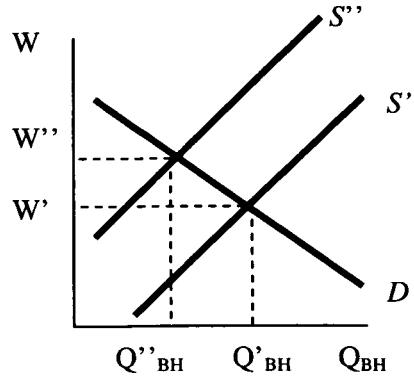

Figure 3.

Although present policy that criminalizes bad profit-driven hacking effectively reduces the quantity of this hacking, this is not all that policy can do towards this end. As we noted earlier, the relative rates of return on working as a bad versus a good for-profit hacker determine which of these markets will garner the best and largest number of profit-driven hackers in general. If it becomes more profitable to be a good profit-driven hacker who owns or works for a legitimate firm, profit-driven hackers currently employed in bad for-profit hacking will be lured out of this industry and into the good profit-driven hacking industry. As we already noted, this has two positive effects on computer security. First, it reduces the number of bad profit-driven hackers, and second, it recruits them to the "good side" in the fight against bad hackers.

One way of making good for-profit hacking look relatively more attractive to for-profit hackers is to raise the cost of bad for-profit hacking, which existing legislation prohibiting this activity does. Another way to increase the competitiveness of good profit-driven hacking, however, is to increase its return vis-à-vis bad profit-driven hacking. To do this, government could subsidize laborers and businesses in the good for-profit hacking industry via outright transfers or through tax breaks and other preferential treatments that result in raising the incomes of those in this industry. The effects of this policy are depicted in Figure 4.

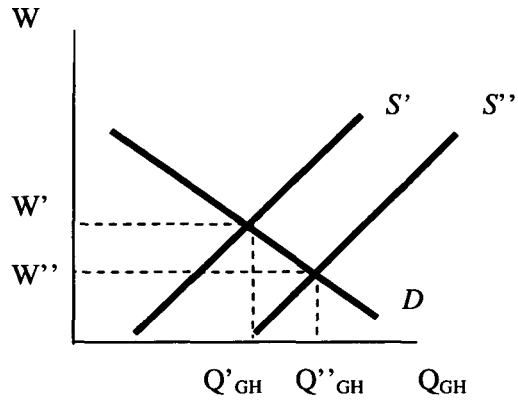

Figure 4.

6.2 Policy and Fame-Driven Hacking

Although current legislation is appropriate for profit-driven hacking, it may not be effective in reducing the quantity of hacking for fame-driven hackers. Recall from Section 4 that the fame-driven hacking industry may look one of two ways. In the first case, the supply schedule for hacking is

less elastic than the fame reaction function for hacking, and in the second case the opposite is true. We also noted in Section 4 that these differing cases have contradictory implications for the effectiveness of present policy. To see why this is so, consider Figures 5 and 6.

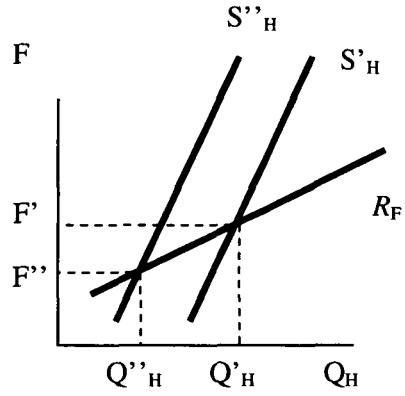

Figure 5.

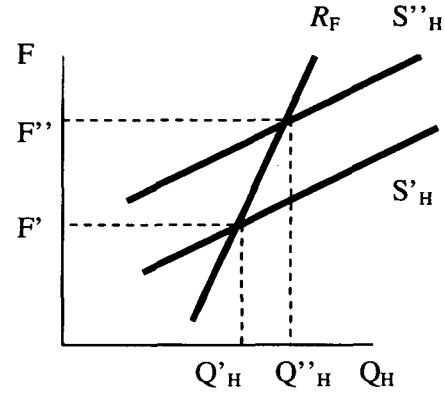

Figure 6.

As with for-profit hacking, current legislation that generically punishes hacking activity raises the cost of fame-driven hacking as well. This leads to a reduction in the supply of hacking, which in Figures 5 and 6 is illustrated by a leftward shift in the supply of hacking from S'_H to S''_H. Note the disparate impact this policy has in each case above. In Figure 5 where the supply of hacking is less elastic than the fame reaction function of the community of hackers, current policy has the desired affect—the equilibrium quantity of hacking drops from Q'_H to Q''_H. Where the supply of hacking is more elastic than the reaction function of the hacking community, the reverse is true. In Figure 6 policy has a perverse effect. Legislation that raises the cost of hacking counter-intuitively leads to more hacking, not less. Specifically the quantity of hacking rises by the amount $Q''_H - Q'_H$. Perhaps strangely, the stiffer the penalty for hacking imposed by law, the greater the increase in fame-driven hacking.

In light of policy's contradictory effects in each of these cases the important question thus emerges: Which of them most likely characterizes the actual fame-driven hacking industry? The "fame elasticity of supply" depends heavily upon hackers' ability to meet increased demand for hacking with additional hacking. Because the marginal cost of hacking is positive and increases with additional output, it is reasonable to think that the supply of hacking is fairly inelastic over at least some range of output.

In contrast, the hacking community's fame reaction function is likely to be relatively elastic. The logic here is simple. The marginal cost of pro-

viding fame is extremely low, if not zero, for the hacking community. Unlike giving up money, which involves sacrificing successively more important alternatives as the price paid rises, providing fame is essentially costless. Increasing the amount of fame the hacking community will "pay" to producers of hacks is very inexpensive. As Cowen points out, "fame remains positive-sum *at its current margin.* Although fame is growing in supply, it is not close to being so plentiful as to lose its exclusive flavor and its power" (2000, p. 114). While the number of famous individuals may grow, fame is not a winner take all, negative-sum game. This is especially true as technologies progress that allow fans to monitor an increasing number of "artists." Increasing fame therefore remains a cheap way to induce more hacking. This means that fame bestowed upon hackers by other members of their community is relatively responsive to changes in the quantity of hacking supplied. Taken together with the fact that the supply of hacking is relatively inelastic, this implies that the fame-driven hacking industry we actually confront most likely corresponds to the case depicted in Figure 5, where raising the cost of hacking does not have a perverse effect. This is good news from the perspective of present policy because it suggests that current legislation is effectively decreasing the quantity of hacking in the fame-driven hacker industry rather than increasing the problem, as it would if the relative elasticities were reversed.

While it is desirable to retain current legislation—which affects the hacking industry through the supply side—demand management could also be effectively used to fight fame-driven hackers. Policies that make it more costly to make the producers of hacks famous—those that reduce the level of fame the hacking community is willing to offer producers for any given quantity of hacking—will further reduce the quantity of fame-driven hacking. Such policies shift the hacking community's reaction function rightward instead of shifting producers' supply curve leftward.

There are at least a few measures that might be taken in this direction. Unfortunately, the most obvious measures towards this end involve violations of basic civil liberties to which many will be opposed. For instance, as we discussed previously, one way by which members of the hacking community give fame to inventive hackers is by publishing them in hacker magazines and books. Prohibiting these publications would not prevent the hacking community from giving fame to hackers, but it would likely force them to find more costly avenues of applauding fame-seeking hackers. The same measures might be taken against hacking community bulletin boards and e-mail lists. Prohibiting hackers from posting hacker programs, tips, etc., it will make it more costly for members of the hacking community to award fame to innovative hackers. Again, for obvious and good reasons, steps like this one are likely to be unpopular. Still, they may remain effective means of reducing the quantity of fame-driven hacking.

7. CONCLUSION

While computer hackers constitute a major security concern for individuals, businesses and public institutions across the globe, hacking and hackers' underground culture remain much of a black box for both lawmakers and those vulnerable to hacker attacks. The mystery that surrounds much of hacking prevents us from arriving at definitive solutions to the security problem it poses; but our analysis provides at least tentative insights for dealing with this problem.

Analyzing computer hacking through the lens of economics gives rise to several suggestions in this vein. First, it is critical to recognize that there are different kinds of hackers characterized by disparate motivations. Because of this, the most effective method of reducing the risk posed by hackers in general will tailor legislation in such a way as to target different classes of hackers differentially. We looked at fame-driven and profit-driven hackers and showed how punishment appropriate for one may actually worsen the problem generated by the other. Current policy directed at reducing hacking by affecting the supply side effectively reduces the quantity of bad profit-driven hacking. Fortunately, there are also good reasons to think that this policy effectively reduces the quantity of fame-driven hacking. If, however, there were strong reasons to think that the elasticities characterized in Figure 6 prevailed over those in Figure 5, supply management that raises the cost of hacking would exacerbate instead of reduce the quantity of fame-driven hacking. We have suggested why we believe this is unlikely to be the case. Still, because of its contradictory policy implications it is important to investigate this issue further.

Our analysis has only touched upon the many and complicated issues regarding computer hacking. In particular, we have not given adequate attention to good hackers who are driven neither by fame nor money, but who voluntarily report security weaknesses to vulnerable computer operators. While the behavior of these hackers is still illegal, it may play an important role in helping to prevent the attacks of more malicious hackers.

We have also not paid sufficient attention to the potential impact that tailoring hacking-related punishments to the age group of the perpetrator may hold for reducing the security threat posed by computer hackers. We noted that most hackers are relatively young—under the age of 30. While this demographic generally cuts across fame-driven and profit-driven hacking groups, there is some evidence suggesting that a disproportionate number of profit-driven hackers are above this age threshold.

The different ages of the individuals in these two different groups suggests that punishments designed to hit each age group where it hurts will be more effective in reducing hacking than a one-size-fits-all approach that may deter the members of one group who are older, but do little to deter the other class of hackers who are younger. In other words, we may want to punish fame-driven hacking, where hackers are younger, with one kind of

punishment that deters younger individuals, and punish bad profit-driven hacking, where hackers are older, with another kind of punishment. This seems relatively simple and yet to our knowledge has not yet been addressed in policy discussions. Presumably 14 year-old script kiddies and 50 year-old men value different things, so effective deterrence will mean differential punishments.

If even after considering these issues it is decided that a uniform punishment for all types of hacking (fame or profit-driven) is desirable, it will still be wise in developing legislation for dealing with hackers to take into consideration the fact that it will inevitably apply primarily to young men. This suggests that effective punishment might be unconventional even if it is uniform across types of hacking. We leave issues like these for future research.

REFERENCES

Blake, Roger. 1994. *Hackers in the Mist.* Chicago, IL: Northwestern University.

Computer Economics Institute. 2002. http://www.computereconomics.com/ article.cfm?id=133.

Computer Security Institute. 2002. *CSI/FBI Computer Crime and Security Survey.* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

Cowen, Tyler. 2000. *What Price Fame?* Cambridge, MA: Harvard University Press.

Denning, Dorothy. 1992. Hacker Ethics. *Computing Security.* New Haven, CT: South Connecticut State University.

Gibson, William. 1984. *Neuromancer.* New York: Ace Books.

Gilboa, Netta. 1996. Elites, Lamers, Narcs and Whores: Exploring the Computer Underground, edited by Lynn Cherny and Elizabeth Reba Weise. *Wired Women: Gender and New Realities in Cyberspace.* Seattle, WA: Seal Press.

Hackers. 1996. Edited by Jack Dann and Gardener Dozois. New York: Ace Books.

Hafner, Katie, and John Markoff. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* New York: Simon and Schuster.

Hannemyr, Gisle. 1999. E-mail interview with Paul Taylor. In *Hackers: Crime in the Digital Sublime.* London: Routledge.

Levy, Steven. 1994. *Hackers: Heroes of the Computer Revolution.* New York: Penguin Books.

Meyer, Gordon. 1989. *The Social Organization of the Computer Underworld.* MA Thesis. http://project.cyberpunk.ru/idb/social_organization _of_the_computer_underground.html.

Platt, Charles. 1997. *Anarchy Online.* New York: Harper Prism.

PricewaterhouseCoopers. 2000. *Security Benchmarking Service/Information-Week's 2000 Global Information Security Survey.*

Raysman, Richard, and Peter Brown. 2000. *Computer Intrusions and the Criminal Law.* http://www.brownraysman.com/publications/techlaw/nylj0300.htm.

Roush, Wade. 1995. Hackers: Taking a Bite Out of Computer Crime. *Technology Review*, April 1995.

Schell, Bernadette, and John Dodge. 2002. *The Hacking of America: Who's Doing It, Why, and How.* Westport, CT: Quorum Books.

SecurityStats.com. 2004. *Virus Statistics*, January 16, 2004. http://www.securitystats.com.

Slatalla, Michelle, and Joshua Quittner. 1996. *Masters of Deception: The Gang that Ruled Cyberspace.* New York: Harper Perennial.

Sterling, Bruce. 1991. *Cyber View 91 Report.* http://www.eff.org/Misc/Publications/Bruce_Sterling/cyberview_91.report.

Sterling, Bruce. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* London: Viking.

Stoll, Richard. 1989. *The Cuckoo's Egg.* New York: Doubleday.

Taylor, Paul. 1999a. *Hackers: Crime in the Digital Sublime.* London: Routledge.

Taylor, Paul. 1999b. E-mail interview with Zoetermeer. In *Hackers: Crime in the Digital Sublime.* London: Routledge.

Thomas, Douglas. 2002. *Hacker Culture.* Minneapolis: University of Minnesota Press.

United Nations. 1994. *International Review of Criminal Policy.* Available at: http://www.uncjin.org/Documents/EighthCongress.html.

Wingfield, Nick. 2002. "It Takes a Hacker," *Wall Street Journal*, March 11, 2002.