Media History Monographs 11:2 (2008-2009)

ISSN 1940-8862

Building Hacker Collective Identity One Text Phile at a Time: Reading *Phrack*

Brett Lunceford
University of South Alabama

Research concerning computer hackers generally focuses on how to stop them; far less attention is given to the texts they create. *Phrack*, an online hacker journal that has run almost continuously since 1985, is an important touchstone in hacker literature, widely read by both hackers and telephone and network security professionals. But beyond its instantiation as a compendium of illicit technical knowledge, *Phrack* was, above all, a rhetorical publication. The files in each issue of *Phrack* created a shared rhetorical vision concerning the place of the hacker underground within society and in relation to law enforcement officials, as well as what it means to be a hacker. This essay examines two important events in the evolution of the hacker movement through the lens of *Phrack*—Operation Sundevil and the arrest of Kevin Mitnick. How these events were framed in *Phrack* both shaped and reflected emerging shifts in hacker collective identity.

Building Hacker Collective Identity One Text Phile at a Time: Reading *Phrack*

Stephen Segaller describes the formation of the Internet as "one of the twentieth century's most productive accidents," explaining that the "seeds of the Internet were planted by the U.S. government in the wake of nationwide concern over the Soviet launch of *Sputnik*."[44] Hackers were an integral part of the construction of this network. Scholars have traced the origins of the computer hacker to the computer programmers of the 1950s and 1960s who, for the most part, worked in universities on projects funded almost exclusively by the government.[45] These programmers were instrumental in the formation of ARPANet, created as a communication system that could be used in the event of a nuclear attack. Randall points out that while ARPANet was a military venture, there are several interpretations of the origins of ARPANet, including a decidedly non-military version that explains ARPANet as a way to develop a network that people wanted anyway. After all, he explains, it was the height of the Cold War and military spending was at an all time high and by framing a project as useful for the military, one could more easily gain funding.[46] Hackers were useful to government and industry for the same reasons that they are now perceived as a threat—hackers are inquisitive, driven by internal rather than external motivations, and refuse to accept boundaries concerning what can and can not be done.

Although public fear of hackers, with increasing concern over cyberterrorism and identity theft, seems to be a fairly recent trend, this sentiment began in the early 1980's. Headlines such as "Raising Security Consciousness; A Monthly Guide for Managers that Helps Protect Corporate Data from Assaults by the Hackers" and "The World of Data Confronts the Joy of Hacking," which begins, "The recent electronic escapades of a group of Milwaukee youths have brought national attention to the growing problem of computer security,"[47] demonstrate the early concerns over hackers in the media. Eric Raymond explains that 1984 marked the time "that serious cracking episodes were first covered in the mainstream press—and journalists began to misapply the term 'hacker' to refer to computer vandals."[48] Socially constructed views of hackers have considerable weight and, in large measure, these views have been influenced by popular press and network security journals that describe hackers as a threat.

A commonly held myth concerning hackers is that they break into computer systems because they want to intrude on other networks or steal information such as credit card numbers or passwords. These hackers do exist, and, unfortunately, this is the kind of hacking that has received the most attention from law enforcement, the media, and the government. But other motivations may also lead to hacking. Some hackers are interested in computer security. Others may simply want to know that they can access a particular network—in other words, it is not the actual utility of accessing a network, but the potential of realizing that utility if necessary. There are lesser acknowledged professional interests as well; many hackers are also computer industry professionals. In other words, the people who build word processing programs, Internet browsers, and computer systems may be the

Brett Lunceford is Assistant Professor of Communication at the University of South Alabama where he serves as the head of the Interpersonal / Rhetoric track. This manuscript is partially derived from his doctoral dissertation, "Democracy and the Hacker Movement: Information Technologies and Political Action," directed by Thomas W. Benson at the Pennsylvania State University.

same people who are interested in breaking into the code of these programs and systems to examine how they can be made more efficient and more secure.

As a group, hackers defy a clear, overarching definition because they exist in the liminal space between the fears and the dreams of how technology is shaping society. Inquisitiveness and a desire to push the boundaries of what something can do comprise the essence of hacking. For example, Levy describes the MIT Tech Model Railroad Club as an early hacker group because they modified and incorporated discarded telephone equipment into their existing model railroad systems.[49] This is an excellent example of hacking that does not conform to the vernacular usage of the term. Jon Erickson states, "There are some who will still argue that there is a distinct line between hackers and crackers, but I believe that anyone who has the hacker spirit is a hacker, despite what laws he or she may break."[50] Yet, like hackers themselves, the "hacker spirit" is also difficult to define.

Perhaps another difficulty in solidifying a clear definition of hackers stems from the competing definitions that come from hackers themselves, the mass media, government and law enforcement agencies, and legislation. Even within the hacker community, definitions of what it means to be a hacker are contested. The various definitions may have different criteria for inclusion and exclusion but the imposition of a definition may carry serious consequences. Yar points out that "the contested nature of the terms [hacking and hackers] . . . shows how hacking, as a form of criminal activity, is actively constructed by governments, law enforcement, the computer security industry, businesses, and media; and how the equation of such activities with 'crime' and 'criminality' is both embraced and challenged by those who engage in them."[51] A particular group's self-definition is not the only possible definition, and questions of definition are important—especially when such definitions carry the possibility of a prison sentence. As hackers have become rhetorically constructed as terrorists in government and media discourses, hackers have worked to provide alternate definitions of hackers and hacking.

Despite the intricacies and contradictions of hacker identity, some core tenets can be distilled through their writings. *Phrack*, an online hacker journal, is one of several hacker texts that provide hackers with a way of seeing themselves and their place in the world by reporting on and defining the exigencies that spurred hackers into creating a shared identity. This essay examines how *Phrack* framed two such exigencies, Operation Sundevil and the arrest of Kevin Mitnick, which helped shape hacker collective identity. Other scholars have traced the history of more mainstream hackers[52]; this study seeks to provide an alternate history of the more subversive elements of the hacker movement by closely examining these two defining moments as recorded in the pages of *Phrack*.

The Politicization of Hackers

Before delving into *Phrack*, we must first examine the events that led to its creation. Some scholars argue that the politicization of the hacker is a relatively new phenomenon. Douglas Thomas states that hackers had more limited political agendas in the 1970s and 1980s and that most attacks were then directed at the phone company but that "more recently, in the wake of the AT&T break up, with the rise of the Internet, and with the increasing globalization of technology, hackers have begun to engage in more concerted political action, at both local and political levels."[53] Thomas identifies Cult of the Dead Cow (cDc) as "the first hacker group dedicated to a kind of political action based on principles of civil disobedience and visibility, and . . . the first group to connect hacker identity with the notion of political action."[54]

There are some problems with this account of hacker politicization. Hackers have long understood the power that comes with understanding technology. Gareth Branwyn put it this way: "One of the first 'a-ha's' I had about computer terrorism in the late '80s was that the possibilities for insurrection and for a parity of power not based on brute force had changed radically with the advent of computer networks and our society's almost complete reliance on them. There was now at least the possibility that groups or individual hackers could seriously compromise the U.S. military and/or civilian electronic infrastructure."[55] Michael Synergy, a hacker, echoes this point: "Anyone who was around in the Sixties is aware of the concept that all political power comes from the barrel of a gun and the power to control is the power to destroy. . . . Now, with information tools, people like me have the capability and the access—because of the way the system is structured—to shut everything down—not just locally, but globally. And, it's getting worse every day."[56] Political uses of hacking and phreaking (the hacking of phone equipment to make telephone calls for free) can easily be traced to the early 1970s when the *Youth International Party Line* (YIPL) published by the Technological American Party (TAP) (an offshoot of the Yippies), advocated defrauding the phone company as a way to avoid paying the War Tax levied on phone bills and provided schematics for blue boxes.[57] According to Tim Jordan and Paul Taylor, TAP's newsletters "provided a raft of detailed technical information, predominantly about how to phone-phreak (obtain free phone calls through the technical manipulation of the phone system), but also on a range of artifacts including burglar alarms, lock-picking, pirate radio and how to illegally alter gas and electric meters."[58]

In 1981, Chaos Computer Club (CCC) began in Germany. They describe themselves as "a global community, which campaigns transboundarily for the freedom of information and communication without any censorship - by any government or company, and which studies the impacts of technology for the society and the individual."[59] Although this statement was written in 2003, Steven Furnell explains that "the exploits of [CCC] over the years have had a considerably political slant," and that members were linked to an espionage case in the late 1980's.[60]

Shortly after the Chaos Computer Club began, *2600*, named after the frequency that allowed phreakers to make free phone calls from pay phones, began publishing in the United States in 1984. In contrast to the phile based virtual publications of *Phrack* and *Cult of the Dead Cow, 2600* was print based and, as Jim Thomas notes, was "oriented primarily toward telecommunications technology."[61] The publication date is significant; the publisher operates under the pseudonym Emmanuel Goldstein, the enemy figure in George Orwell's novel *1984*. *2600* demonstrated a political slant from the first issue, which included a list of phone numbers for the White House.[62] *2600* is still operating and has had its share of legal battles, most notably due to its publication of the DeCSS code which allows individuals to circumvent DVD copy protection.[63] Yet Douglas Thomas observes that "*2600* reveals a great deal about the history and commitments of hacking. Its political and social message, however, tells us relatively little about the underground world of hackers as a culture."[64]

Also in 1984, Cult of the Dead Cow (cDc) formed, which is perhaps one of the most politically active and high profile hacker groups. One of their members, Omega, is said to have coined the term "hacktivism."[65] Cult of the Dead Cow is best known for revealing security flaws in software, specifically with their "Back Orifice" utility, which demonstrated significant security flaws in the Microsoft Windows operating system. In 1999, they began to draw more explicit links between activism and computer technology by forming "Hacktivismo." cDc is arguably the longest running group of phile writers. They have the most in common with *Phrack*, employing a mix of technical information, literary musings, and strategies for social disruption, yet many of cDc's philes tend toward stories and philosophical writings.[66] In his Phrack Pro-Phile, Grandmaster "Swamp" Ratte' observes that "what makes CULT OF THE DEAD COW different and has enabled us to last is that cDc has never been about technology... we didn't form to trade 'inpho' and hack together like the other groups. We used technology, be it hand - hacked MCI codes or the Internet to get our 'messages' out there. Hacking is a means to an end. I don't give a rat's ass about hacking or any of that crap on its own. I just want to make cool stuff. Now we're starting a 'paramedia' concept which means the end of cDc as a 'hacker group that puts out text files.'"[67] Where *Phrack* and *2600* are the technical journals, *Cult of the Dead Cow* are the beat poets of the hacker underground. cDc remains an active part of the hacker underground, yet they have also gained some mainstream attention, even appearing in *Spin* magazine.[68]

In 1985, shortly after the creation of cDc and *2600*, *Phrack* began publishing digitally. It is difficult to know the relative influence of *Phrack* compared to other hacker texts, but Jim Thomas calls *Phrack* "the most influential and visible of the hacker e-zines,"[69] and Douglas Thomas argues that "*Phrack* has had its finger on the pulse of hacker culture."[70] *Phrack* stuck mainly to the practical aspects of technology and important developments in the hacker scene could be found in the pages of Phrack World News. Phrack World News was a feature that set *Phrack* apart from other hacker publications and through their reporting a hacker identity began to take shape. *Phrack* was a place not only for information, but also for indoctrination and a repository for shared history. In the introduction to *Phrack* 31, DH proclaims, "Phrack is more than just a technical newsletter that comes out every now and then, it's a symbol of our hacking history."[71] *Phrack*'s unique blend of technical information and reporting on current events that had a direct impact on the hacker community makes it particularly worthy of closer examination.

Of the major texts that have persisted from the early days of the hacker community—*2600*, *Phrack*, *Cult of the Dead Cow*—all seemed to have differing visions and, therefore, would appeal to different factions of the hacker/phreaker community. Moreover, these groups tended to share members, which further blurred the lines between them. Certainly there were other many other texts that were housed on BBS systems that are now virtually unknown.[72] Other texts that emerged in the early days of the cyberculture, such as *Mondo 2000* and *Wired*, seemed more interested in the impact on society than on the intricate workings of technology itself and thus would mainly be interesting from a lifestyle perspective. More importantly for this study, they mainly dealt with hacker issues tangentially.

Hackers also became increasingly connected in both virtual and physical space as hackers began to meet at conventions. Some of the more notable conventions have included Chaos Communication Congress (organized by the Chaos Communication Club), SummerCon, HoHoCon (organized by Cult of the Dead Cow), Hackers on Planet Earth (H.O.P.E.) (organized by *2600*), and DefCon. These meetings provided a way to exchange information and, by most accounts, drink heavily. But these meetings also helped hackers to organize. In his description of Drunkfux, the organizer of HoHoCon, Rodney Palmer writes, "HoHo Con is serious business to him. Drunkfux is part of the hacker movement that is beginning to turn its curious computer talent into a legitimate political movement. . . . Drunkfux has designed HoHo as a place where hackers can learn they are part of an important social movement."[73] Groups like cDc, 2600, Chaos Computer Club, and the publishers of *Phrack* recognized that politics and hacking were related. Indeed, because unauthorized hacking (which was the main means of access for many early hackers who could not afford the prohibitively expensive computer equipment) has always existed in the nebulous grey area of legality at best (before the law caught up with the possibility of hacking), the act of hacking is a political act in itself.

With action comes ideology, which can be seen in the justifications and slogans employed by hackers. Jim Thomas notes that "the romantic view of being part of a social revolution was the core of the hacker identity and provided the justification for computer intrusion and attempts to subvert authority."[74] The slogan "information wants to be free," reveals an ideology opposed to the notion of commodified, proprietary information. Dan Verton writes, "Hackers look at themselves as Internet-age Robin Hoods, stealing from the information rich to give to the information- and connectivity- starved poor. Their aim is to open up and expose information held closely by corporate America and government and expose the truth. The world's knowledge belongs to the world, not a select few with the money and political influence to claim ownership of it. The freedom of information and knowledge is another core belief of the hacker community."[75] If hackers view the structures of power to be skewed in such a way as to make control over technology virtually impossible for the average user and difficult—legally and physically—for the expert, the belief may emerge that change can come only from working outside of the system.

In the Beginning There Was Phrack

Phrack began November 17, 1985 on the Metal Shop Bulletin Board System (BBS) run by Taran King. *Phrack* is made up of "philes," or text files that covered topics ranging from the home manufacture of methamphetamines to highly technical schematics of telephone systems and computer equipment. In the inaugural phile, Taran King writes (in all of these philes, I have left the spelling as found in the original and because several of these philes have many spelling and grammatical errors, I have omitted the traditional use of [*sic*] in order to ease readability):

> Welcome to the Phrack Inc. Philes. Basically, we are a group of phile writers who have combined our philes and are distributing them in a group. This newsletter-type project is home-based at Metal Shop. If you or your group are interested in writing philes for Phrack Inc. you, your group, your BBS, or any other credits will be included. These philes may include articles on telcom (phreaking/hacking), anarchy (guns and death & destruction) or kracking. Other topics will be allowed also to an certain extent. If you feel you have some material that's original, please call and we'll include it in the next issue possible. Also, you are welcomed to put up these philes on your BBS/AE/Catfur/Etc. The philes will be regularly available on Metal Shop. If you wish to say in the philes that your BBS will also be sponsering Phrack Inc., please leave feedback to me, Taran King stating you'd like your BBS in the credits. Later on.[76]

With this simple introduction began one of the most well-known and influential online sources for hacker information and indoctrination.

Although these philes were read by many different kinds of people, there seems to be a male slant to them. Edwin Black notes that within rhetorical discourses, there exists the image of an ideal auditor, for whom the discourse is designed, and this implied auditor can often be linked to a particular ideology.[77] Black states, "What the critic can find projected by the discourse is the image of a man, and though that man may never find actual embodiment, it is still a man that the image is of."[78] Thus, I suggest that the implied audience for *Phrack* is an adolescent male; the preferred topics of "telcom (phreaking/hacking), anarchy (guns and death & destruction) or kracking" tap into a current of adolescent male rebellion.[79] By adolescent, I do not simply mean those of a particular age; rather, I am describing a kind of mindset—one of tension between adulthood and responsibility and childhood, exploration, and play. For example, if an adult were to make an acetylene balloon, such behavior could still be described as "juvenile."

Yet there may be some overlap between the implied auditor and the actual hackers at whom this discourse is directed. Paul Taylor notes the male domination of the hacker subculture, arguing that there may be many reasons for this, including misogyny, discomfort with females in the physical world, and a projection of their sexuality into hacking itself. In short, a successful hack is penetration and orgasm.[80] Elsewhere, Taylor postulates that societal factors, the masculine environment of computer science, and male gender bias in computer languages can also account for this lack of females in the hacker subculture; other scholars have likewise argued that cyberspace is largely masculine space.[81]

The first issue of *Phrack* exposes an already evident tension between the technical and the antisocial. Technical documentation is juxtaposed with philes that teach the reader how to pick locks and make acetylene balloon bombs. Issue two contains an in-depth overview of MCI Communications Corporation that includes data such as subscriber figures and descriptions of various services, as well as philes that provide instructions for making homemade guns and blowguns. Issue four contains a phile guiding the reader through the process of making methamphetamines. In essence, *Phrack* seemed to live up to its mission statement; it was obviously geared toward the mischievous adolescent male.

Yet one can find clues early on in *Phrack* that foreshadow the beginnings of the end of adolescence for the hacker community and recognition of the realities of the sociopolitical world in which hackers lived. For example, an article by The Mentor begins, "Occasionally there will be a time when destruction is necessary. Whether it is revenge against a tyrannical system operator or against a particular company, sometimes it is desirable to strike at the heart of a company . . . their computer."[82] In the same volume, an article concerning telephone company regulatory changes ends with the following postscript: "The above text was written primarily for people in marketing telephone technologies. In the interest of the phreaking world, I hope that you can focus on the business side of telecommunications which may be in your future."[83] From the beginning, some hackers and phreakers understood the larger implications of their actions, recognizing that these telecommunication systems were embedded within societal systems they may eventually fight against and/or become assimilated into. Levy describes how many hackers eventually went on to use their skills in the service of corporate and government empires. Thus, one can observe early on the apparent tension between youthful abandon and the realization that adolescence would one day fade away.

Phrack's mission was to bring technical information to the hacker/phreaker collective with a decidedly anarchist/countercultural bent. *Phrack* stuck mainly to practical aspects of technology, teaching nascent hackers the tricks of the trade, but it was also a repository of hacker culture that was self-generated. Hackers' discussion of hackers and hacking functioned much like the discourse described by Habermas in his discussion of the eighteenth century public sphere: "The public that read and debated this sort of thing read and debated about itself."[84] Important developments could be found in the pages of

Phrack World News, and through their reporting a hacker identity began to take shape. *Phrack* was not only a source of information, but a site of indoctrination.

Throughout *Phrack*'s history, many descriptions of what it means to be a hacker have emerged. Perhaps the most visible description of what it means to be a hacker can be found in "The Conscience of a Hacker," a touchstone text for hackers written by The Mentor (real name Loyd Blankenship).[85] This document is prefaced with the words, "The following was written shortly after my arrest," which provides a way to understand the words that will follow. In this manifesto, The Mentor conjures an image of a highly intelligent youth that has been left behind by an education system that caters to the lowest common denominator. He proclaims that his crime is "curiosity," a theme that is common to most discussions of what it means to be a hacker. The manifesto prescribes a way of being in the digital age and is an important indicator of the norms of hacker collective identity, putting forth such ideals as intelligence and a hunger for knowledge.

There has been relative stability concerning how hackers define themselves in the pages of *Phrack*. Chris Goggans (a.k.a. Erik Bloodaxe) defines a hacker as "someone who wants to find out everything that there is to know about the workings of a particular computer system, and will exhaust every means within his ability to do so."[86] In 1990, Crimson Death took a similar approach, defining a hacker as one "who enjoys pushing the envelope, bypassing limits, discovering knowledge, inventing solutions, <and> adventuring into uncharted areas."[87] Scut, a German hacker states, "All hackers share the enthusiasm for technology and creativity."[88] Outside of *Phrack*, similar sentiments concerning what it means to be a hacker are put forth. At *Cult of the Dead Cow*, Dissident writes, "A true hacker DOESN'T get into the system to kill everything or to sell what he gets to someone else. True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place they've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool we live in."[89]

Yet certain events have called into question what it means to be a hacker. For example, the 1983 movie *War Games* demonstrated to the general public the potential damage from unauthorized access to computerized military systems when the protagonist, David Lightman, played by Matthew Broderick, hacked into a military computer to play a game called "Global Thermonuclear War."[90] Other events have included the release of the Morris Worm[91] in 1988 and the arrest of Markus Hess, a German hacker who was selling information to the KGB.[92] In his description of the Morris Worm, Rick Howard notes, "On the day his experiment went awry, Morris invented 'malcode.' It was so scary at the time that the US CERT formed just to combat this kind of threat."[93]

Although many events helped to shape hacker identity, the remainder of this essay closely examines two important occasions that played out in the pages of *Phrack*: Operation Sundevil and the arrest of Kevin Mitnick. However, in doing so I want to note that this study is less concerned with whether or not the hacker community as a whole interpreted these events in the same way that they were portrayed in *Phrack.* Rather, this study explores how the contributors to *Phrack* framed these events and how these controversies and struggles over meaning played out in the publication itself.

"We Are Being Hunted": Operation Sundevil

Operation Sundevil was a widespread crackdown on computer hackers conducted primarily by the Secret Service at various locations all over the country. Law enforcement officials seized computer equipment, notebooks, and anything else that could be connected to hacking activities. According to Bruce Sterling, "Of the various antihacker activities of 1990, Operation Sundevil had by far the highest public profile. The sweeping, nationwide computer seizures of May 8, 1990, were unprecedented in scope and highly, if rather selectively, publicized."[94] That hackers may be arrested by the authorities was already understood within the hacker community; in the second issue of *Phrack*, Phreak World News reported three different instances of phreakers and hackers being charged with various offenses. But Operation Sundevil was an unprecedented wide-scale assault on hackers that seemed to take hackers largely by surprise. After Operation Sundevil, hackers began to recognize the need for solidarity and organization.

Sterling states that "Sundevil's motives can only be described as political. It was a public relations effort, meant to pass certain messages, meant to make certain situations clear: both in the mind of the general public and in the minds of various constituencies of the electronic community. First—and this motivation was vital—a 'message' would be sent from law enforcement to the digital underground."[95] This message was clearly received by the hacker community. The opening lines of the May 28, 1990, edition of Phrack World News began: "May 9th and 10th brought on two days [that] would be marked in every hackers history book. The reason we assume these days will be important to many, is that maybe it's time we opened are (sic) eyes and saw the witch hunt currently in progress," concluding, "Yes, we are the witches, and we are being hunted."[96]

This should not have come as much surprise to the hacker community; hackers had already encountered similar operations by law enforcement agencies. The July 28, 1987 edition of *Phrack* begins with this introduction by Knight Lightning: "Hi and welcome to the final regular issue of Phrack Newsletter. Most of you already know about the nationwide arrest of many of the phreak/hack world's most knowledgeable members. I may receive a visit from the authorities as well and because of this and other events, I am going to leave the modem world."[97] Even so, his decision to reprint "The Conscience of a Hacker"—also known as the "Hacker's Manifesto"— by The Mentor, with its unapologetic conclusion, "you may stop this individual, but you can't stop us all," demonstrates an attitude of defiance.[98] Shortly thereafter (August 7, 1987), the editorship changed hands with the following message: "So, did you miss us? Yes, Phrack is back! Phrack Magazine's beloved founders, Taran King and Knight Lightning, have gone off to college, and the recent busts (summarized completely in this month's Phrack World News) have made it difficult to keep the magazine going. TK and KL have put the editorship of Phrack in the hands of Elric of Imrryr and Sir Francis Drake. SFD is primarily responsible for PWN. As of yet we have no 'Official Phrack BBS.'"[99]

By 1990, when Operation Sundevil took place, the hacker community had already realized that law enforcement agencies had finally caught up with them. In 1988, Phrack World News had reprinted an article called "Illegal Hacker Crackdown" from *California Computer News* that detailed the first adult conviction for hacking.[100] *Phrack* had also moved from simply reporting raids to explaining what to do when the reader is actually involved in a raid. The April 25, 1989 edition of *Phrack* features an article called "Getting Caught- Legal Procedures" by The Disk Jockey that provides an overview of the legal process, from informing the phone company to sentencing at the trial.[101] The first explicit phile dedicated to legal issues is "The Laws Governing Credit Card Fraud," published in 1987.[102] Later philes, such as "Can You Find Out If Your Telephone Is Tapped?" "Big Brother Online," and

"Hacking: What's Legal And What's Not," demonstrate that by the time Operation Sundevil occurred, hackers had already abandoned the belief that they could simply hide in the relative anonymity of the ether.[103]

The law enforcement community had issued a wakeup call not only to the hacker community, but also to the general public. There had already been media coverage of the potential threat that hackers represented to the general public. This was now brought back into the public eye in a dramatic way, but only for those who read reports of the raid. The raid made the front page of *USA Today*,[104] but other outlets did not see this event as front page news and it was not even mentioned in the *New York Times*.[105] Thus, Operation Sundevil may have been somewhat newsworthy but it did not seem to be particularly noteworthy at the time. Maxwell McCombs and Donald Shaw argue that the mass media, especially the news media, set the agenda of what is important in political campaigns.[106] By relegating coverage of Operation Sundevil to the interior of the newspaper, the news media sent a clear message to the reader—this was not something with which they should be terribly concerned. Thus, although Operation Sundevil is largely credited for raising the consciousness of the public mind concerning the hacker threat, a brief evaluation of the news coverage suggests that Operation Sundevil may not have been the watershed event that fostered this shift. On the other hand, the change in relationship between industry and the law enforcement community was unmistakable. Sterling writes, "Sundevil was greeted with joy by the security officers of the electronic business community. After years of high-tech harassment and spiraling revenue losses, their complaints of rampant outlawry were being taken seriously by law enforcement."[107] From that point, the aggressive stance against hackers has only intensified.

The scars from Operation Sundevil are still visible within the hacker community. In a phile commemorating the fifteenth anniversary of Operation Sundevil, Dark Sorcerer spends much of the early part of the essay attacking an informant called "The Dictator." Dark Sorcerer reinforces the value of loyalty in the hacker community: "I reserve a special hatred for snitches and narcs of all types. In my view, there is no lower creature in the world than the professional snitch. Law enforcement personnel are simply doing their job: they might be clueless, on a power trip, or what have you, but you can't fault law enforcement for doing what they do – if you throw bananas in a cage of orangutans, for example, you simply don't expect them to do anything but grab them and shove them in their mouths. Likewise, if you are on the "other side", you should at least know who your enemies are."[108] Dark Sorcerer concludes the attack with a comparison to Christ's betrayal by Judas Iscariot: "Enjoy your 30 pieces of silver, and don't be surprised if you're born in Haiti during your next life."[109]

The loyalty that Dark Sorcerer extols marks a shift away from individual skill as the measure of one's worth in hacker culture. Hacker culture celebrated rugged individualism rather than loyalty. But times had changed, the stakes had been raised, and hackers were under attack. Operation Sundevil provided the catalyst that helped bring hackers together. Law enforcement, government officials, and industry were all united against hackers; hackers needed to also become united. This helped reinforce a common theme in hacker collective identity—an "us versus them" mentality. Hackers tend to make a clear distinction between hackers and non hackers. Kenneth Burke writes, "To the extent that a social structure becomes differentiated, with privileges to some that are denied to others, there are the conditions for a kind of 'built in' pride. King and peasant are 'mysteries' to each other."[110] With separation came protection.

Hackers had long maintained a culture of secrecy, most obviously through their use of handles. Creative names like Oxblood Ruffin, Erik Bloodaxe, Mudge, DilDog, and The Mentor carefully distanced the online persona from one's physical embodiment. Some handles were more open than others. For example, in an interview Emmanuel Goldstein provides a list of six other handles, then states, "There are others that I keep quiet about."[111] But this secrecy was coupled with an unhealthy measure of braggadocio, which was also reflected in the handles (i.e., Lex Luthor, Lord Digital, The Executioner, Doom Prophet) and in the names of the hacker groups (i.e., Legion of Doom, Masters of Deception). As hackers began to organize and meet in person at conventions, the potential for identification increased considerably, especially in a culture where bragging about one's exploits is a measure of one's status. Operation Sundevil reinforced the culture of secrecy and marked the end of an era in which an arrest record was not a stigma but, in some ways, a badge of honor.

Kevin Mitnick and the Myth of the Superhacker

Operation Sundevil provided an impetus for hacker organization, but the capture and imprisonment of Kevin Mitnick provided an opportunity for the hacker community to explicitly define themselves. Mitnick was a figure who both galvanized and polarized hackers. He had been arrested on multiple occasions for computer crimes and few hackers argued that he was innocent when he was arrested in 1995 with the help of computer security expert Tsutomu Shimomura and journalist John Markoff. But hackers protested that the caution with which Mitnick was held was unreasonable and that these precautions served mainly to instill within the general public a sense of fear and awe of the hacker. Although his crimes were rather pedestrian and far from threatening to the general public, the image of Mitnick created by the prosecution and the media is one of a dangerous "dark-side hacker" with almost superhuman powers. Mitnick's legal issues and fugitive status would be played out not only on the front page of the *New York Times*, but also in the text files of Phrack World News.

John Markoff's front page article in the *New York Times* helped create the myth of "Kevin Mitnick the superhacker." Markoff had previously written about Mitnick, describing him as the "Dark-Side Hacker"[112] and after Mitnick's arrest, he wrote *Takedown* with Tsutomu Shimomura, describing Mitnick as "a loner and an underachiever" who "was seduced by the power he could gain over the telephone network."[113] Such descriptions reinforce the image of the pathological hacker who is driven to crime in a quest for power and control. Hackers protested the film version of *Takedown*, which, they argued, was fictionalized to demonize Mitnick.[114] Emmanuel Goldstein of *2600* stated, "If this film is made the way the script reads, Kevin will be forever demonized in the eyes of the public, and mostly for things that everyone agrees never even happened in the first place." Some of the things that Goldstein criticized included "Mitnick changing medical records, Mitnick clobbering Shimomura on the head with the top of a metal garbage can, and Mitnick whistling touch tones into a pay phone to avoid having to pay," none of which actually took place.[115] Such portrayals likely had a significant impact on the perception of hackers in general and on Mitnick's abilities specifically. Conway explains that "the US Department of Justice labeled Kevin Mitnick, probably the world's most famous computer hacker, a 'computer terrorist.' On his arraignment, Mitnick was denied access not only to computers, but also to a phone, because the judge believed that, with a phone and a whistle, Mitnick could set off a nuclear attack."[116]

But not all media outlets accepted the depiction of Mitnick as a superhacker. Like the discussions that took place in *Phrack*, a *Chicago Tribune* article casts doubt on Mitnick's ability to accomplish the feats attributed to him. The article cites Katie Hafner who, with Markoff, had previously written about Mitnick, stating that there was no evidence for some of the claims that Markoff had made concerning Mitnick, specifically that Mitnick had broken into the North American Aerospace Defense Command (NORAD). She conceded that "Kevin really takes the rap for a lot of stuff he didn't do."[117] Mitnick himself stated that Markoff was the main reason that he was still in custody: "Markoff has single-handedly created 'The Myth of Kevin Mitnick,' which everyone is using to advance their own agendas. I wasn't a hacker for the publicity. I never hacked for personal gain. If I was some unknown hacker, accused of copying programs from cell phone companies, I wouldn't be here. Markoff's printing false and defamatory material about me on the front page of *The New York Times* had a substantial effect on my case and reputation. He's the main reason I'm still in custody."[118] Mitnick has also sought to redefine hacking by publishing his own book on social engineering—his chosen brand of hacking—in which he describes the various means by which he would gain access to systems by attacking the most vulnerable component of any computer system: the user.[119]

Even some members of the law enforcement community noted that Mitnick was treated unfairly and served more as a scapegoat than as an example of a real threat. Gerald Kovacich, a veteran law enforcement and information security professional, states:

> The Mitnick case was an example of the criminal justice system gone awry, with the FBI agents and prosecutors more interested in forthcoming fame and fortune than justice. Mitnick may have been a pain in the ass, but he was no Capone, although he was treated as if he was that dangerous. Yes, in what he could have done if he wanted to but not what he actually did. He was an embarrassment to the government agencies with their political and public relations egos being damaged while he was on the [loose] . . . . so when he was found—not by the FBI by the way—it was get even time. This is mentioned only as an example of what millions of federal dollars can not accomplish and also what power the federal government can bring to bear on an individual.[120]

Kovacich paints a picture of vindictive federal agencies interested more in revenge and self-interest than justice. With the advent of the USA PATRIOT Act, hackers have been lumped into the category of "cyberterrorist" and the stakes are even higher.[121] Kovacich also illustrates the extreme power differential between the hacker and the federal government, but demonstrates that even with this power differential, there is still a possibility of evading the law, if only temporarily.

Kovacich's suggestion that revenge was a motivation for the treatment of Mitnick overlooks the genuine fear of Mitnick within the federal law enforcement community. After all, this was a person who, according to John Markoff's front page coverage of Mitnick in the *New York Times*, used to break into NORAD as a teenager.[122] In one portion of Phrack World News, Kenneth Siani, a security specialist, had this to say about Kevin Mitnick's arrest:

> Unfortunately he is thought of as some kind of a "SUPER HACKER." The head of Los Angeles Police Dept's Computer Crime Unit is quoted as saying, "Mitnick is several levels above what you would characterize as a computer hacker." No disrespect intended, but a statement like this from the head of a computer crime unit indicates his ignorance on the ability of hackers and phone phreaks. Sure he did things like access and perhaps even altered Police Department criminal records, credit records at TRW Corp, and Pacific Telephone, disconnecting phones of people he didn't like etc. But what is not

> understood by most people outside of the hack/phreak world is that these things are VERY EASY TO DO AND ARE DONE ALL THE TIME.[123]

Siani's argument both redeems Mitnick from his demonization by placing him on a level of the average, above novice hacker, while simultaneously raising questions of what the advanced hackers are capable of. But his description also casts aspersions on Mitnick's skill, which defines what it means to be a true hacker.

Siani explains why Mitnick was perceived as such an advanced hacker: "The only thing special about Kevin Mitnick is that he is not a "novice" hacker like most of the thirteen year old kids that get busted for hacking/phreaking. It has been a number of years since an "advanced" hacker has been arrested. Not since the days of the Inner Circle gang have law enforcement authorities had to deal with a hacker working at this level of ability. As a general rule, advanced hackers do not get caught because of [their] activity but rather it is almost always others that turn them in. It is therefore easy to understand why his abilities are perceived as being extraordinary when in fact they are not."[124] Siani provides a blueprint concerning what it means to be an "elite" hacker. Several hackers note that the main problem with Mitnick is that he got caught. But many of the old guard of the hacker underground had been arrested or raided, yet they were generally not ridiculed by the hacker community. This illustrates a shift to a belief that is still held today within the hacker community: a real hacker can cover his or her tracks well enough to evade detection and capture. Perhaps this is one reason for Siani's disparaging remarks concerning Mitnick's skills—the collective identity had shifted, and what was once a peril of hacking had become an unpardonable sin.

When asked about Mitnick, Agent Steal, a hacker turned FBI informant, also criticizes Mitnick's skill: "I had never met him before I was busted. When I went to work for the bureau I contacted him. He was still up to his old tricks so we opened a case on him and Roscoe. It's a long story but they wound up getting busted again. Mitnick got tipped off right before they were going to pick him up. So he's on the run again. Roscoe wasn't so lucky. This will be Mitnick's fifth time to get busted. What a loser. Everyone thinks he is some great hacker. I out smarted him and busted him. [Kevin] Poulson blows him away as well."[125] Later in the interview, Steal goes on to explain how he himself was caught and arrested, which make his comments concerning Mitnick seem ironic and hypocritical. Such sentiments illustrate the sometimes contradictory nature of hacker collective identity.

Many issues of Phrack World News do little more than reprint mainstream news coverage of Mitnick with little additional comment.[126] However, once Mitnick was caught, *Phrack* provided reprints and excerpts of mainstream news stories and headlines about Mitnick with the following commentary: "Just a sampling of the scores of Mitnick articles that inundated the news media within hours of his arrest in North Carolina. JUMP ON THE MITNICK BANDWAGON! GET THEM COLUMN INCHES! WOO WOO!"[127] For the news media, the Mitnick case was the ideal hacker story. He had been captured after a nationwide manhunt—the kind of journalism that made sense; tracing someone though server hops is boring for readers, but a man on the run is interesting. This arrest was far different from what took place during Operation Sundevil during which many of the hackers were raided in their parent's homes, much to their surprise. Mitnick was a fugitive on the FBI's most wanted list and he was caught with the help of a journalist. Other elements also made the Mitnick case attractive from a journalistic perspective. Mitnick fit the hacker stereotype: geeky, glasses, overweight, a bit petty at times. He was also an identified computer criminal.

In other words, he was not like the average reader. Many of the individuals raided in Operation Sundevil were typical white kids from the suburbs who had not previously been in trouble—they could be anybody. Mitnick was someone who could be safely viewed as "other" by both the journalists and by the readers.

Hackers are skeptical of the supposed facts of the Mitnick case as reported by Markoff. A *Phrack* editorial lays out an argument that casts doubt upon the entire case, establishing ties between Mitnick and Shimomura and illuminating the prior relationship between Markoff and Mitnick: "I guess Markoff has had a hard on for Mitnick for ages. Word always was that Mitnick didn't really like the treatment he got in Markoff's book 'Cyberpunk' and had been kinda screwing with him for several years. (Gee, self-proclaimed techie-journalist writes something untrue about computer hackers and gets harassed…who would have thought)."[128] After outlining the reasons why the charges against Mitnick seemed overstated, the editors suggest that Mitnick's arrest was little more than a get rich quick scheme for Markoff and Shimomura:

> Less than a month after the whole bust went down, Markoff and Tsutomo signed with Miramax Films to produce a film and multimedia project based on their hunt for Mitnick. The deal reportedly went for $750,000. That is a fuckload of money. Markoff also gets to do a book, which in turn will become the screenplay for the movie. (Tsutomo commented that he went with Miramax "based on their track record." Whatever the fuck that means). Less than a month and they are signed. Looks to me like our duo planned for all this.
>
> "Hey Tsutomo, you know, if you went after this joker, I could write a book about your exploits! We stand to make a pretty penny. It would be bigger than the Cuckoo's egg!"
>
> "You know John, that's a damn good idea. Let me see what I can find. Call your agent now, and let's get the ball rolling."
>
> "I'll call him right now, but first let me write this little story to recapture the interest of the public in the whole Mitnick saga. Once that runs, [the] publishers are sure to bite."
>
> Meanwhile Mitnick becomes the fall guy for the world's ills, and two guys methodically formulate a plot to get rich. It worked! Way to go, guys.[129]

Arguments that Markoff had motives other than journalistic inquiry have been largely ignored by the popular media. Even when the *New York Times* was hacked in protest of Markoff's reporting and the hackers explicitly pointed out that Markoff had greatly profited from Mitnick's arrest, this point was glossed over in the reporting of the hack.[130]

Within the hacker community, not all thought that Mitnick's arrest was a bad thing. Debate concerning Kevin Mitnick extended beyond the pages of *Phrack,* taking place also on the pages of defaced websites. The day after the *New York Times* hack, a group calling themselves H4G1S hacked *Slashdot*'s website with the following message: "Fuck Kevin Mitnick! People like Eric Corley have dedicated their whole miserable lives to help 'free' guilty Kevin Mitnick. The truth of the matter is Eric Corley is a 'profiteering glutton,' using Kevin Mitnick's misfortune for his own personal benefit and profit."[131] The archive containing the hack questions the authenticity of the hack, noting that "the group allegedly taking responsibility (H4G1S) has hacked pages in the past with pro-Mitnick sentiments . . . Just further proof that in the world of web hacking, nobody's in control."[132] However, Hacking For Girlies (HFG), the group that hacked the *New York Times* website, had ridiculed H4G1S in the code of the hack, so the hack may have simply been retaliation against HFG.

The plight of Kevin Mitnick brings to the forefront some of the paradoxes of hacker identity. Although many of the old guard hackers had also been arrested, hackers ridiculed Mitnick because of his capture. Moreover, because he had been captured, Mitnick's skills were called into question and maligned. It is clear that Mitnick was skilled, at least in social engineering, and may have been more skilled than his detractors gave him credit for but Mitnick was far from the skill level ascribed to him by law enforcement officials, members of the press (especially John Markoff), and the justice system. It seems that Mitnick served as the scapegoat for both the justice system and the hacker movement. Kenneth Burke notes that "when the attacker chooses for himself the object of attack, it is usually his blood brother; the debunker is much closer to the debunked than others are."[133] By casting their collective inadequacies upon Mitnick, hackers could avoid considering the possibility that each of them was more like Mitnick than they would like to admit and that, but for the grace of God and the inadequacies of law enforcement officials, they could be the next one to fall.

The Dialectical Construction of Hacker Collective Identity

Events such as Operation Sundevil and Mitnick's arrest have left a lasting impression on hacker collective identity. Michael McGee writes, "Each political myth presupposes a 'people' who can legislate reality with their collective belief. So long as 'the people' believe basic myths, there is unity and collective identity."[134] Mitnick is the substance and embodiment of one of the core basic myths of the hacker movement. Hackers do not argue about whether he broke the law; rather, the arguments range from whether or not the law is just to disagreements concerning the severity of the punishment. Mitnick serves as synecdoche for the entire hacker movement. The disagreements over the imprisonment of Mitnick reveal the cleavages within hacker collective identity. Moreover, the way hackers defined the events of Operation Sundevil also revealed the way they viewed themselves in relation to the rest of society. For hackers, to argue about Mitnick and Operation Sundevil is to argue about themselves.

But hackers are not the only group that is working to define what it means to be a hacker; other entities, such as the government and the media, have already formulated definitions of "hackers" and "hacking." When hacking was subtly redefined as terrorism by the USA PATRIOT Act, little concern raised by the general population.[135] Anti-hacker propaganda supports the law enforcement efforts against hackers and helps justify the resources being expended on this target. Kovacich argues that with major crimes decreasing and funding to government law enforcement agencies also decreasing, these agencies must find new threats in order to remain relevant: "The new mission? Hype the hacker threat and the FBI gets $30 plus million to go after the teenage hackers - at a time when the Chinese have stolen and continue to steal our nuclear secrets. At a time when the Russian bear is coming out of hibernation. At a time when real terrorists are gaining new weapons and attacking the interests of the free world in the old fashioned way - by blowing it up! Talk about misallocation of available resources!"[136] The demonization of the hacker has implications both for public policy and in how hackers define themselves. Authorities have increased the pressure on hackers, which, in turn, invites hackers to adopt a siege mentality. Perhaps this is one reason Dark Sorcerer levels such harsh criticism against "The Dictator," the informer in Operation Sundevil. For those who have been marginalized, a betrayal by one's own is the worst possible violation of trust.

In addition to legislation, popular culture influences hacker identity. Thomas notes that "hacker identity is created and shaped by the split between a culture of expertise and a culture of end-users, but it is also heavily influenced and defined by images from popular culture, even among hackers themselves."[137] Popular movies portray hackers in conflicting ways; *The Matrix* portrays hackers as saviors of humanity while *The Net* portrays hackers as murderous criminals able to erase and replace another's identity. Popular press and network security journals describe hackers as a threat. Even within the hacker community there are different opinions concerning what constitutes a "true" hacker. Even if hackers were able to agree on a definition, theirs would be only one of many competing definitions. Which definition is correct? To some extent, all of them are correct. Hackers are feared, romanticized, intriguing, and mysterious. The mosaic of definitions surrounding hackers reflects the complexity of hacker identity. Hackers are much more than artisan programmers who write elegant code. Hackers are both the creators and the destroyers of the emerging technological society. Rather than accept technology at face value, hackers learn to understand it and shape it to fulfill their own ends. The differences in how hackers are defined reflect different societal views concerning those who control and shape technology.

The battle to define hackers is waged on many fronts, which is one reason it is so difficult to come to any consensus on what constitutes hacking and hackers. Perhaps this explains why hackers have chosen to define themselves not in affirmative terms but in negative ones. Eli Zaretsky suggests that "the notion of identity involves negation or difference—something *is* something, *not* something else."[138] Hackers have always been a group of outsiders and have thrived on this form of ostracism. The fact that they are not like everyone else is worn like a badge of honor, but it is more than the idea of not being like everyone else—rather, the hacker believes that he or she is *better* than everyone else. For hackers, intelligence and skill are the gold standard; these attributes allow hackers to maintain a sense of superiority because the general public remains largely ignorant concerning technical matters. Manuel Castells writes, "Only hackers can judge hackers. Only the capacity to create technology (coming from any context), and to share it with the community, are respected values. For hackers, freedom is a fundamental value, particularly freedom to access their technology, and use it as they see fit."[139] The values questioned during Operation Sundevil—real hackers are too smart to get caught—and (re)constructed and reinforced during through discussions concerning Kevin Mitnick seem to remain in force even now.

Dark Sorcerer explains that the fifteen years after Operation Sundevil has brought about a sea change in the hacking community. Making the comparison between pioneers and those who come in to settle after them, he writes:

> When I look at the old, mid 80's *Phrack* versus articles written in the last few years, you can see the change: in are complicated things like Polymorphic Shellcode Using Spectrum Analysis, out are recipes for bathtub crank manufacture. This is a generalization, but the early articles – dumb and inarticulate as they usually were – showed more of a wide-ranging desire to conquer time and space. If you're going to sail around the world, then lock picking and acetylene balloon bomb making are definitely good skills to have, but if you're going to stay in London and work on maps, there's not much that's going to benefit you other than a slightly improved recipe for ink or parchment making.[140]

Dark Sorcerer notes the evolution of the hacker community and reminds the reader of the inherent tension between the desire for illicit knowledge in general and the need for specific technical knowledge that has existed since the first issue of *Phrack*. Hackers, it seemed, had become domesticated.

The (Latest) Death and Resurrection of Phrack

Phrack was pronounced dead in 2006, and despite previous occasions in which the pronouncement of death may have been premature, it seemed that this time the pronouncement had been made not only by the editors of *Phrack* but by the hacking community as well. Dark Sorcerer asks, "Is Phrack more or less popular than it was five years ago? Ten years ago? I don't know. It does seem as though Phrack has followed a classic organic cycle: a naive, exuberant youth paving the way for a stodgier, more establishment-minded adulthood. That's not to say that it's irrelevant, but rather that it was doing what it should have. Evidently now - whether due to exhaustion, boredom, or just plain realizing it's time to move on - someone has decided to give it a rest. Twenty years was definitely a good run - so RIP, Phrack."[141]

But *Phrack* had been traveling down the road to legitimacy for over a decade before it ended. In the March 1, 1993 issue, Erik Bloodaxe took over the editorship and proclaimed, "There are a few very distinct differences beginning with this issue of *Phrack*. First and foremost, Phrack is now registered with the Library of Congress, and has its own ISSN. Yes, boys and girls, you can go to Washington, D.C. and look it up. This adds a new era of legitimacy to Phrack in that with such a registration, Phrack should never again face any legal challenge that would bypass any paper based magazine."[142] *Phrack* also began to cover itself in other ways, such as the implementation of a PGP key and the requirement that all government and industry members register and pay a fee for access.

There was an early impulse toward inclusion in *Phrack*. For example, the September 25, 1986 issue begins, "Anyone can write for Phrack Inc. now. If you have an article you'd like published or a story for Phrack World News, get in touch with one of us (Knight Lightning, Taran King, and Cheap Shades) and as long as it fits the guidelines, it should make it in. If you have been one of the many ragging on Phrack Inc., please, write a phile and see if you can improve our status with your help."[143] Taran King re-emphasizes this message in issue 9: "Let me once again stress that ANYONE can write for Phrack Inc. You aren't required to be on a particular board, much less a board at all, all you need is some means to get the file to us, as we do not discriminate against anyone for any reason."[144] But the times changed quickly in light of events such as Operation Sundevil with more attention from law enforcement agencies and the telephone industry, most notably due to a document detailing the 911 phone system.[145] Because of these exigencies, the editors of *Phrack* had to become more discriminating in the articles that they chose to publish.

The urge for legitimacy can be seen in other parts of the hacker community. Part of this impulse has resulted in visibility for hackers. Members of L0pht testified before Congress. Cult of the Dead Cow appeared in *Spin* magazine.[146] Other groups have made explicit efforts to alter public perceptions of hackers. For example, 2600 meetings implemented a dress code in 2005 that requires formal business attire for attendees, explaining that "dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society. There simply is no reason to convey another image. While some will see this as an unreasonable restriction on their freedom of expression and individuality, we think that that is an irresponsible attitude for these times. Can we really put a price on the importance of maintaining a good image? Is the comfort of walking around in blue jeans and tank-tops really worth sabotaging our futures? The answer should be obvious. These are difficult times and we all must make sacrifices."[147] Hackers have become more visible and the mainstreaming of hackers seems to be happening on multiple fronts, even becoming an integral part of popular culture. Hackers have been both demonized and celebrated in popular films, and the genius child computer prodigy has become somewhat of a cliché in television shows.

In the desire for legitimacy, perhaps the hacker community had reached a point where recipes for homemade methamphetamines and grenades made out of shotgun shells could no longer stand side by side with technical documentation. It seems that the adolescent phase of hacking had ended and the death of *Phrack* marked a transition to adulthood. Even so, much as adolescence shapes individual adulthood, the adolescence of the hacker movement has left an impression upon the collective identity of the movement. This is illustrated by the continued relevance of *Phrack's* most lasting contribution to the shaping of the hacker movement—the early text phile entitled "The Conscience of a Hacker."[148]

However, like previous pronouncements of death, reports of the demise of *Phrack* have been greatly exaggerated. *Phrack* is now under new editorship, and still seems to be an active player in the construction of hacker collective identity. The most recent issue maintains the serious technical documentation for which *Phrack* had become known while seeking to reclaim the irreverence of the previous generation of hackers. This issue provides clues for the continued shifting of collective identity even as the editors look to the past for guidance. For example, Duvel laments that new hackers do not understand the history of the hacker community: "Nowadays, I'm pretty sure that new hackers don't read old Phrack articles anymore. Because they are lazy, because they can find information elsewhere, because they think old Phracks are outdated... But reading old Phracks is not only to acquire knowledge, it's also to acquire the hacking spirit."[149]

There is also some evidence for revision of hacker identity through the reconceptualization of figures from the past. Duvel offers this description of Kevin Mitnick:

> This guy really was amazing and I have a total respect for what he did. I don't want to argue about his present activity, it's his choice and we have to respect it. But nowadays, when new hackers talk about Kevin Mitnick, one of the first things I hear is: "Kevin is lame. Look, we have defaced his website, we are much better than him." This is completely stupid. They have probably found a stupid web bug to deface his website and they probably found the way to exploit the vulnerability in a book like Hacking Web Exposed. And after reading this book and defacing Kevin's website, they claim that Kevin is lame and that they are the best hackers in the world... Where are we going? If these hackers could do a third of what Kevin did, they would be considered heroes in the Underground community.[150]

This passage demonstrates how collectives can alter their perceptions of the figures of the past. Mitnick has now embodied the roles of fugitive hacker and cause célèbre, unskilled pariah, and revered elder statesman in the hacker community, all within the pages of *Phrack*.

The new editorship of *Phrack* seems intent on reclaiming the countercultural spirit that has waned since the early days.[151] In the most recent issue, Gladio provides a description of revolutionary tactics that is one part pragmatism and one part conspiracy theory.[152] In the same issue, Keptune contributes a phile entitled, "Hacking Your Brain: The Projection of Consciousness," which provides techniques for inducing lucid dreaming and out of body experiences. The introduction to this article anticipates the skepticism of readers who consider it unrelated to computer hacking and justifies its publication by stating that "before being a computer hacking magazine, phrack is dedicated to spread the occult knowledge, unrecognized and subversive."[153] For hackers, the brain is merely one of many systems to hack. Keptune's article hearkens back to early texts in *Phrack* that described various means for altering consciousness, although at the time it was mainly through drug use.[154] There has long been an intersection of technology and psychotropic elements in the history of cyberculture. R.U. Sirius of *Mondo 2000* explains the realization that the magazine staff had that simple drug usage was not enough to enact real, lasting change: "If, for instance, we were able to change ourselves biologically, that would be a more interesting change than a million people dropping acid. ... I started to become aware that the ability to manipulate information -- and the huge carrying capacity of information, all that stuff that is related to silicon and digital stuff -- was also going to be related to any other kind of technical change."[155]

It seems that the new editors of *Phrack* are attempting to bring about a renaissance of hacker identity by looking to the past to reclaim a spirit of hacking that they perceive as lost. "All the people who make up The Circle of Lost Hackers agree that Phrack should come back to its past style when the spirit was present. We really agree . . . that Phrack is mainly a dry technical journal. It's why we would like to give you some idea that can bring back to Phrack its bygone aura."[156] For Duvel, this is a matter of life and death for the hacker underground. "We have to get back the old school hacking spirit and afterwards explain to the new generation of hackers what it is. It's the only way to survive."[157] Thus, *Phrack* is explicitly attempting to shape hacker collective identity in the image of a hacker collective that draws primarily from the time frame that Jim Thomas describes as the "golden age" of hacking.[158]

Even so, although not explicitly described in Duvel's history of the hacker underground, there is also an appropriation of still earlier impulses to hack. In the comments to Duvel's article, one respondent, Ahzzmandius, states, "I fear that this article will fall mostly upon ears that are deaf to the captnCrunch whistle. Hacking is a state of being. An irresistable urge to see what is on the other side of the fence. The desire to find out what little gnome resides in that black box. Hacking is a way of life, not a skill set that you learned. Anyone can learn tricks. Anyone can collect data. A hacker makes sense of it all in ways that others don't see. A hacker makes something new out of seemingly unrelated things."[159] Such a description of hacker motivation seems reminiscent of Levy's description of the MIT Tech Model Railroad Club's desire to see if they could repurpose unrelated telephone equipment and assimilate it into their railroad systems.[160] Moreover, his comments subtly remind hackers of their roots with the early phreakers such as Captain Crunch.

Finally, we see in the new editorship of *Phrack* a desire to create a kind of pan-hacker unity. In the introduction to the phile, "International Scenes," the editors note that in the past, hackers were isolated but as networks became more widespread,

> They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles. With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there.[161]

The phile provides a brief accounting of the past and present hacker scenes in Brazil, France, and Quebec, with each author enshrining their own heroes and chronicling tribulations with law enforcement. As could be expected, these narratives reaffirm cultural values that define what it means to be a hacker and how they view their place in the world. For example, Ankara describes the plight of a French hacker who had pioneered radio hacking in France: "Larsen got busted later on, as he was getting out of his home in bicycle, by weaponed authorities who considered him as a terrorist, while he was just a happy hacker making no profit from his research."[162] Such a description reaffirms the view of hacking as harmless, the authorities as overbearing, and the imperative that information should be free. These narratives also demonstrate how texts such as *Phrack* can help shape a hacker collective identity that transcends national boundaries. There also remains a kind of optimism that such hacker unity can be achieved, an optimism that can be seen even in the early days of *Phrack*.

Although the values of hacker collective identity continue to shift and evolve, a few common elements emerge. First, there is a consistent impulse to valorize one's predecessors in the hacker movement. Despite Mitnick's excoriation in the press—and in *Phrack*—at the time he was arrested, he is now valorized by the new editorship as someone worthy of respect. Douglas Thomas notes that many of the Pro-Philes focus on hackers that are no longer active that "pass into a state of veneration or even apotheosis."[163] Thomas also notes that "almost all of the hackers pro-philed have also been arrested, signaling a kind of symbolic death . . . It is also a culturally constructed narrative of male sacrifice for the community."[164] Thus Mitnick's redemption is a continuation of a long held cycle of veneration of those who have been destroyed by the enemies of the hacker community.

Second, there is a continued desire for novelty, creativity, and inventiveness. Knowledge and skills are the coin of the realm in the hacker underground. For hackers, there is no system that is unworthy of deconstruction and examination, including human consciousness itself. In the most recent issue of *Phrack,* Anonymous laments the death of the hacker underground while suggesting that a new underground will form:

> Hackers, not black hat nor white, not professionals, not amateurs (surely none of this matters), are still out there in this world today, still with all the potential to be something great. The question is not then how to artificially group these people into a new underground movement. The question is not how to mourn the passing of the golden days, how to keep the memories alive. . . . All that remains is to relax, to do what you enjoy doing; to hack purely for the enjoyment of doing so. The rest will come naturally, a new scene, with its own traditions, culture and history. A new underground, organically formed over time, just like the first, out of the hacker's natural inclination to share and explore.[165]

Anonymous' imperative to "hack purely for the enjoyment of doing so" and the belief that the rest will come naturally betrays a belief in an essential nature of hackers. This belief has long been held in the hacker community. In 1986, the Mentor wrote, "I'm smarter than most of the other kids, this crap they teach us bores me," and "My crime is that of curiosity." This belief has persisted. In his *Phrack* prophile, Mudge, a member of l0pht, makes a clear distinction between computer geeks and hackers by noting their creativity: "Computer geeks seem not to have that creative twist in many cases that hackers have. This is the same twist that says: I don't care what it's _supposed_ to do - I bet I can make it do *this*."[166] Mudge also notes that "it's all about information and learning. If you stop learning... you're not doing it right."[167]

Finally, the perception that hackers stand in opposition to the rest of the world remains in force. Hackers must remain distrustful of non-hackers, particularly authorities, partially out of individual disposition—hackers seem particularly resistant to rules and authority—and partially out of a shared collective memory of past trials within the hacker community such as Operation Sundevil and the treatment of Mitnick in both the media and the legal system. But this was a long standing problem. From the second issue of *Phrack* onward, *Phrack* World News was filled with accounts of hackers who had been busted. In 1988, Knight Lightning compiled news from

Phrack World News to explore how the hacker/phreaker community had let down their guard. "Today's phreak/hacker must learn to be more security conscious. . . . Safety first; the stakes in this game are a lot higher than no television after school for a week because once a hacker's phone number falls into the wrong hands, the law enforcement community or organizations like the Communications Fraud Control Association (CFCA) can find out everything about you. I know because I have seen their files and their hacker data base is so incredibly large and accurate . . . its unbelievable."[168] The events of the past shape and reinforce hacker identity, yet, as seen with the status of Mitnick, the cultural landscape is always subject to revision.

As *Phrack* continues to reach an international audience, it is likely that the vision of hacker collective identity that they promote will continue to influence the hacker community around the world. Fernback notes that "cyberspace is a repository for collective cultural memory"[169]; the continued presence of *Phrack* provides a greater understanding of the events that shaped the hacker movement and how these events were interpreted by that community. The hacker community as a whole seems quite unwilling to let *Phrack* die, despite a series of previous deaths and resurrections. As such, *Phrack* will likely remain an important site of hacker collective identity formation and indoctrination for years to come. As DH proclaimed in 1990, "Phrack is not dead. On the contrary, Phrack will and can't ever die."[170]

Notes

[44] Stephen Segaller, *Nerds 2.0.1: A Brief History of the Internet* (New York: TV Books, 1998), 29.

[45] Stephen Levy, *Hackers: Heroes of the Computer Revolution* (New York: Penguin, 1984); Douglas Thomas, *Hacker Culture* (Minneapolis: University of Minnesota Press, 2002), 12-14.

[46] Neil Randall, *The Soul of the Internet* (London: Thompson Publishing Inc., 1997), 1-18.

[47] Erik Sandberg-Diment, "Raising Security Consciousness," *New York Times*, July 28, 1985; "The World of Data Confronts the Joy of Hacking," *New York Times*, August 28, 1983.

[48] Eric S. Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (Cambridge, MA: O'Reilly, 1999), 19.

[49] Levy, *Hackers*, 21-27.

[50] Jon Erickson, *Hacking: The Art of Exploitation* (San Francisco: No Starch Press, 2003), 4.

[51] Majid Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal of Criminal Justice* 44, no. 4 (2005): 390.

[52] See Levy, *Hackers*; Raymond, *The Cathedral & the Bazaar*; Segaller, *Nerds 2.0.1*.

[53] Thomas, *Hacker Culture*, 89.

[54] Ibid., 96.

[55] Gareth Branwyn, introduction to *Secrets of a Super Hacker* by The Knightmare (Port Townsend, WA: Loompanics Unlimited, 1994), iii.

[56] A. J. S. Rayl, "Secrets of the Cyberculture," *Omni*, November 1992, 67.

[57] See Al Bell, "Blue Box Is Linked to Phone Call Fraud," *Youth International Party Line,* July, 1971; "Remember the Blue Box?" *Youth International Party Line,* October, 1971. Blue boxes created tones that allowed individuals to use pay phones without paying.

[58] Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004), 14.

[59] Chaos Computer Club, "CCC Summary: What Is the CCC?" May 10, 2003, http://www.ccc.de/club/?language=en (accessed January 27, 2006).

[60] Steven Furnell, *Cybercrime: Vandalizing the Information Society* (Boston: Addison-Wesley, 2002), 72.

[61] Jim Thomas, "The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the 'Golden Age' of Hacking," *New Media & Society* 7, no. 5 (2005): 604.

[62] "White House Phone Directory," *2600,* January, 1984.

[63] For extensive documentation on this legal battle, see http://www.2600.com/dvd/docs/.

[64] Thomas, *Hacker Culture*, 120.

[65] See Oxblood Ruffin, "Hacktivism, from Here to There," *Cult of the Dead Cow*, March 28, 2004, http://www.cultdeadcow.com/cDc_files/cDc-0384.html (accessed February 1, 2006).

[66] Sometimes these stories tend toward the perverse. For example, one text file details the torture, anal rape, and killing of a lab rabbit by two men. See Tippy Turtle, "Ted and Dave's Animal Fun: Session I: Bunny Lust," *Cult of the Dead Cow*, 1987, http://www.cultdeadcow.com/cDc_files/cDc-0018.php (accessed March 22, 2006). On the other hand, there are also many philosophical writings, for example, a detailed consideration of the nature of love. See Trammel, "Modern Love," *Cult of the Dead Cow*, February 14, 2006, http://www.cultdeadcow.com/cDc_files/cDc-0403.php (accessed March 22, 2006).

[67] Phrack Staff, "Phrack 51 Prophile: Grandmaster Ratte'," *Phrack* 7, no. 51 (September 1, 1997): article 4.
[68] Mike Romano, "The Politics of Hacking," *Spin*, November 1999, 168-74.
[69] Thomas, "The Moral Ambiguity of Social Control in Cyberspace," 604.
[70] Thomas, *Hacker Culture*, 121.
[71] DH, "Introduction to Phrack 31," *Phrack* 3, no. 31 (May 28, 1990): phile 1.
[72] Some of these are mentioned in Thomas, "The Moral Ambiguity of Social Control in Cyberspace," 599-624.
[73] Rodney Palmer, "New Hack City," *Cult of the Dead Cow*, http://www.cultdeadcow.com/oldskool/NewHackCity.html (accessed April 9, 2008).
[74] Thomas, "The Moral Ambiguity of Social Control in Cyberspace," 606.
[75] Dan Verton, *The Hacker Diaries: Confessions of Teenage Hackers* (New York: McGraw-Hill/Osborne, 2002), 191.
[76] Taran King, "Introduction," *Phrack* 1, no. 1 (November 17, 1985): phile 1. AE (ASCII Express), Catfur, and BBS (Bulletin Board System) were all methods of connection and file transfer and served similar functions.
[77] Edwin Black, "The Second Persona," *Quarterly Journal of Speech* 56, no. 2 (1970): 112.
[78] Ibid., 113.
[79] It is important to note that these files indicate an interest in these topics rather than a disposition to actually enact them. When researching the commonly held belief that adolescent males like things like fire and explosives, I was surprised to find that there was little research on *interest* in these topics. Most of the psychological and sociological literature dealt with adolescents that actually displayed seriously antisocial behavior, and rightfully so. Thus, although it seems intuitive, it is difficult to find scholarly literature concerning those who may harbor antisocial feelings or fantasies rather than display them, or those who are simply interested in information deemed dangerous or inappropriate.
[80] Paul A. Taylor, "Maestros or Misogynists? Gender and the Social Construction of Hacking," in *Dot.Cons*, ed. Yvonne Jewkes, 126-46 (Portland, OR: Willan Publishing, 2003).
[81] Paul A. Taylor, *Hackers: Crime in the Digital Sublime* (London: Routledge, 1999), 33. See also Melanie Stewart Millar, *Cracking the Gender Code: Who Rules the Wired World?* (Toronto: Second Story Press, 1998); Graham Thomas and Sally Wyatt, "Access Is Not the Only Problem: Using and Controlling the Internet," in *Technology and in/Equality: Questioning the Information Society*, ed. Sally Wyatt, et al., 21-45 (London: Routledge, 2000); Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995).
[82] The Mentor, "Crashing DEC-10's," *Phrack* 1, no. 4 (March 13, 1986): phile 6.
[83] Leslie Albin and Jester Sluggo, "Centrex Renaissance: 'The Regulations,'" *Phrack* 1, no. 4 (March 13, 1986): phile 7.
[84] Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, trans. Thomas Burger (Cambridge, MA: MIT Press, 1989), 43.
[85] The Mentor, "The Conscience of a Hacker," *Phrack* 1, no. 7 (1986): phile 3, available at http://www.phrack.com/issues.html?issue=7&id=3.
[86] S. Leonard Spitz, "Phrack XXXV Prophile Presents Sincerely Yours, Chris Goggans," *Phrack* 3, no. 35 (November 17, 1991): file 3.

[87] Crimson Death, "Phrack Classic Newsletter Issue XXXII Index," *Phrack* 3, no. 32 (November 17, 1990): file 1.
[88] Phrack Staff, "Prophile on Scut," *Phrack* 11, no. 62 (July 13, 2004): phile 4.
[89] Dissident, "The Ethics of Hacking," Cult of the Dead Cow, http://www.cultdeadcow.com/cDc_files/cDc-0037.txt (accessed February 16, 2009).
[90] *War Games*, film, directed by John Badham (Las Angeles: MGM/UA, 1983).
[91] See Andy Gray, "An Historical Perspective of Software Vulnerability Management," *Information Security Technical Report* 8, no. 4 (2003): 34-44; Rick Howard, "The Tipping Point," *Computer Fraud & Security* 2009, no. 1 (2009): 11-13.
[92] Clifford Stoll, "Stalking the Wily Hacker," *Communication of the ACM* 31, no. 5 (1988): 484-500; Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).
[93] Howard, "The Tipping Point," 11.
[94] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992), 153.
[95] Ibid., 161.
[96] Phreak_Accident, "Phrack World News," *Phrack* 3, no. 31 (May 28, 1990): phile 8.
[97] Knight Lightning, "Introduction," *Phrack* 2, no. 14 (July 28, 1987): phile 1.
[98] "The Conscience of a Hacker" is a touchstone text for hackers, written by Loyd Blankenship, otherwise known as "The Mentor." The document bears the heading, the heading, "The following was written shortly after my arrest…" See The Mentor, "The Conscience of a Hacker."
[99] Shooting Shark, "Phrack XV Intro," *Phrack* 2, no. 15 (August 7, 1987): file 1.
[100] The Smuggler, "Phrack World News," *Phrack* 2, no. 17 (February 1, 1988): file 11.
[101] The Disk Jockey, "Getting Caught - Legal Procedures," *Phrack* 3, no. 26 (March 24, 1989): file 3.
[102] Tom Brokaw, "The Laws Governing Credit Card Fraud," *Phrack*, no. 16 (September 19, 1987): file 5.
[103] Fred P. Graham and VaxCat, "Can You Find out If Your Telephone Is Tapped? 'It Depends on Who You Ask,'" *Phrack* 2, no. 23 (December 30, 1988): file 9; Thumpr Of ChicagoLand, "Big Brother Online," *Phrack* 2, no. 23 (June 6, 1988): file 10; Hatchet Molly, "Hacking: What's Legal and What's Not," *Phrack* 3, no. 25 (March 8, 1989): file 8.
[104] Debbie Howlett, "Hackers Run up $50 Million Phone Bill," *USA Today*, May 10, 1990.
[105] See "Computer Hacker Ring with a Bay Area Link," *San Francisco Chronicle*, May 9, 1990; "Lawmen Seek Hackers - Raids in 15 Cities," *San Francisco Chronicle*, May 10, 1990; Tom Schmitz and Rory J. O'Connor, "Fed Program Pulls the Plug on Hackers," *Houston Chronicle*, May 13, 1990.
[106] See Maxwell E. McCombs and Donald L. Shaw, "The Agenda-Setting Function of Mass Media," *Public Opinion Quarterly* 36, no. 2 (1972): 176-87.
[107] Sterling, *The Hacker Crackdown,* 163.
[108] Dark Sorcerer, "Operation Sundevil... 15 Years Later," *Cult of the Dead Cow*, May 9, 2005, http://www .cultdeadcow.com/archives/2005/05/operation_sundevil_1.php3 (accessed March 21, 2006).
[109] Ibid.

[110] Kenneth Burke, *Language as Symbolic Action* (Berkeley, CA: University of California Press, 1966).
[111] Taran King, "Phrack Pro-Phile XXIX," *Phrack* 3, no. 29 (November 12, 1989).
[112] Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Simon & Schuster, 1991). In this book, Hafner and Markoff devote 121 pages to Mitnick's story.
[113] Tsutomu Shimomura and John Markoff, *Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--By the Man Who Did It* (New York: Hyperion, 1996), 236.
[114] The movie, *Track Down*, which has been heavily criticized, both in terms of artistic merit and accuracy, was finally released in 2004 on DVD. See *Track Down*, DVD, directed by Joe Chappelle (New York: Dimension, 2000).
[115] Wendy Grossman, "Hackers to Shake Down Takedown," *Wired*, July 15, 1998, http://www.wired.com/culture/lifestyle/news/1998/07/13712 (accessed April 16, 2008). See also Maureen Callahan, "A Low-Key Mitnick Protest," *Wired*, July 16, 1998, http://www.wired.com/culture/lifestyle/news/1998/07/13792 (accessed April 16, 2008).
[116] Maura Conway, "Hackers as Terrorists? Why It Doesn't Compute," *Computer Fraud & Security* 2003, no. 12 (2003): 13.
[117] Elizabeth Weise, "Some Calling Super Hacker More Myth Than a Danger," *Chicago Tribune*, February 1, 1996.
[118] Adam L. Penenberg, "Mitnick Speaks!" Forbes.com, April 5, 1999, http://www.forbes.com/1999/04/05/feat.html (accessed April 29, 2003), para. 15.
[119] Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis, IN: Wiley, 2002).
[120] Gerald L. Kovacich, "Hackers: Freedom Fighters of the 21st Century," *Computers & Security* 18, no. 7 (1999): 573-574.
[121] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Public Law 107–56, 107th Cong. 1st sess. (October 26, 2001), § 814, 816.
[122] John Markoff, "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit," *New York Times*, July 4, 1994.
[123] Kenneth Siani, "Kenneth Siani Speaks out About Kevin Mitnick," *Phrack* 3, no. 27 (June 20, 1989): file 10.
[124] Ibid.
[125] Mike Bowden (Agenta Aka Agent 005), "An Interview with Agent Steal," *Phrack* 4, no. 44 (November 17, 1993): file 16. Kevin Poulson (a.k.a. Dark Dante) was another hacker who had been apprehended by law enforcement.
[126] For some examples, see Knight Lightning, "Phrack World News," *Phrack* 2, no. 23 (January 25, 1989): file 11; Knight Lightning and Taran King, "Phrack World News," *Phrack* 2, no. 22 (December 23, 1988): file 9; Disorder, "Phrack World News," *Phrack* 8, no. 53 (July 8, 1998): article 14.
[127] Datastream Cowboy, "Phrack World News," *Phrack* 6, no. 47 (April 15, 1995): file 22.
[128] Phrack Staff, "Phrack Editorial," *Phrack* 6, no. 47 (April 15, 1995): file 2a.
[129] Ibid.

[130] Amy Harmon, "Hacker Group Commandeers the New York Times Web Site," *New York Times*, September 14, 1998.
[131] H4G1S, "RoTSHB," *2600*, September 14, 1998, http://www.2600.com/hackedphiles/ slashdot/hacked/ (accessed March 27, 2006).
[132] *2600*, "2600 | Slashdot," September 14, 1998, http://www.2600.com/hackedphiles/slashdot/ (accessed March 27, 2006).
[133] Kenneth Burke, *A Grammar of Motives* (New York: Prentice-Hall, 1945), 406-07.
[134] Michael C. McGee, "In Search of 'the People': A Rhetorical Alternative," *Quarterly Journal of Speech* 61, no. 3 (1975): 245.
[135] To be fair, the entire USA PATRIOT Act was passed with little concern expressed by much of the population. For more on the connection between hacking and the USA PATRIOT Act, see *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, § 814, 816.
[136] Kovacich, "Hackers: Freedom Fighters of the 21st Century," 575.
[137] Thomas, *Hacker Culture*, 170.
[138] Eli Zaretsky, "Identity Theory, Identity Politics: Psychoanalysis, Marxism, Post-Structuralism," in *Social Theory and the Politics of Identity*, ed. Craig J. Calhoun, 198-215 (Oxford: Blackwell, 1994), 200.
[139] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford: Oxford University Press, 2001), 60.
[140] Dark Sorcerer, "Operation Sundevil... 15 Years Later."
[141] Dark Sorcerer, "A Short Requiem for _Phrack_ . . . Life Sucking in the Middle East," *Cult of the Dead Cow*, April 22, 2005, http://www.cultdeadcow.com/archives/2005/04/ a_short_requiem_for_.php3 (accessed March 21, 2006).
[142] Erik Bloodaxe, "Introduction," *Phrack* 4, no. 42 (March 1, 1993): file 1.
[143] Taran King, "Introduction," *Phrack* 1, no. 7 (September 25, 1986): phile 1.
[144] Taran King, "Introduction," *Phrack* 1, no. 9 (December 1, 1986): phile 1.
[145] See Sterling, *The Hacker Crackdown*, 261-281 for the document in question and the trial surrounding it.
[146] Romano, "The Politics of Hacking."
[147] *2600,* "2600 Meetings Today - Formal Attire Required," April 1, 2005, http://www.2600.com/ news/ view/article/2200 (accessed March 27, 2006).
[148] The Mentor, "The Conscience of a Hacker."
[149] Duvel, "A Brief History of the Underground Scene," *Phrack*, no. 64 (May 27, 2007): phile 4.
[150] Ibid.
[151] For more on the connection between the counterculture and cyberculture, see Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism* (Chicago: University of Chicago Press, 2006).
[152] Gladio, "The Revolution Will Be on Youtube " *Phrack*, no. 64 (May 27, 2007): phile 7.
[153] Keptune, "Hacking Your Brain: The Projection of Consciousness," *Phrack*, no. 64 (May 27, 2007): phile 14.
[154] See Anonymous, "Line Noise Part I: Making Methcathinone," *Phrack* 7, no. 48 (September 1, 1996): file 3; The Leftist, "The Tried and True Home Production Method For 'Methamphetamine,'" *Phrack* 1, no. 4 (March 13, 1986): phile 8.

[155] Jack Boulware, "Mondo 1995," SF Weekly, http://search.sfweekly.com/1995-10-11/news/mondo-1995/full (accessed April 11, 2008).
[156] Duvel, "A Brief History of the Underground Scene."
[157] Ibid.
[158] Thomas, "The Moral Ambiguity of Social Control in Cyberspace."
[159] Duvel, "A Brief History of the Underground Scene."
[160] Levy, *Hackers*, 21-27.
[161] Nicholas Ankara, g463, and sandimas, "International Scenes," *Phrack*, no. 64 (May 27, 2007): phile 15.
[162] Ibid.
[163] Thomas, *Hacker Culture*, 134.
[164] Thomas, *Hacker Culture*, 134-135.
[165] Anonymous, "The Underground Myth," *Phrack*, no. 65 (April 11, 2008): phile 13.
[166] Phrack Staff, "Phrack Prophile on Mudge," *Phrack* 7, no. 49 (November 8, 1996): file 4.
[167] Ibid.
[168] Knight Lightning, "Shadows of a Future Past: Part One of the Vicious Circle Trilogy: A New Indepth Look at a Re-Occurring Problem," *Phrack* 2, no. 21 (August 6, 1988): file 3.
[169] Jan Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," in *Virtual Culture: Identity and Communication in Cybersociety*, ed. Steve Jones, 36-54 (London: Sage Publications, 1997), 37.
[170] DH, "Introduction to Phrack 31."