Hackers and the Battle for Cyberspace

Helen Nissenbaum

HACKERS NEVER were part of the mainstream establishment, but their current reputation as villains of cyberspace is a far cry from the early days when, first and foremost, they were seen as ardent if quirky programmers, capable of near-miraculous, unorthodox feats of machine manipulation. True, their dedication bordered on fanaticism, and their living habits bordered on the unsavory. But the shift in popular perception to hackers as deviants and criminals is important not only because it affects the hackers themselves and the extraordinary culture that has grown around them (fascinating as a subject in its own right), but because it reflects shifts in the development, governance, and meaning of the new information technology. These shifts should be questioned and resisted. They unfairly cast hackers in a disreputable light and, more important, they deny the rest of us a political opportunity.

In *Hackers: Heroes of the Computer Revolution*, Steven Levy traces the roots of evolving hacker communities to the Massachusetts Institute of Technology in the late 1950s. Here, core members of the Tech Model Railroad Club "discovered" computers first as a tool for enhancing their beloved model railroads and then as objects of passion in their own right. They turned their considerable creative energies to the task of building and programming MIT's early mainframes in uneasy but relatively peaceful coexistence with formal employees of the university's technical staff. In parallel, hacker communities developed and flourished in other academic locales, particularly Stanford and Carnegie-Mellon, sometimes spilling over into nearby cities such as Cambridge, Palo Alto, and Berkeley.

Formidable programmers, these hackers produced and debugged computer code at an astonishing rate. They helped develop hardware and software for existing computer functions and invented, sometimes as playful challenges, novel algorithms and applications that were incorporated into subsequent generations of computers. These novel functions not only extended recreational capabilities—gaming, virtual reality, and digitized music—but also increased practical capabilities such as control of robots and processing speeds. Obsessive work leavened with inspired creativity also yielded a host of basic system subroutines and utilities that pushed operating capacities and efficiency to new heights, steered the field of computing in novel directions, and became a fundamental part of what we experience every time we sit in front of a computer.

Levy and others who have written about this early hacker period describe legendary hacking binges—days and nights with little or no sleep—leading to products that surprised and sometimes annoyed colleagues in mainstream academic and research positions. The "pure hack" did not respect prescribed methods or theory-driven, top-down approaches to computer science and engineering. To hack was to find a way, any way that worked, to make something happen, solve the problem, invent the next thrill. There was a bravado associated with being a hacker, an identity worn as a badge of honor. The unconventional lifestyle did not seem to put off adherents, even though it could be pretty unwholesome: a disregard for patterns of night and day, a diet of junk-food, inattention to personal appearance and hygiene, and the virtual absence of any life outside of hacking. Nor did hackers come off as "nice" people; they did little to nourish conventional interpersonal skills and were not particularly tolerant of aspiring hackers with lesser skills or insufficient dedication.

It was not only single-minded attachment to their craft that defined these early hackers but their espousal of an ideology informally called the "hacker ethic." This creed included several elements: commitment to total and free access to computers and information, belief in the immense powers of computers to improve people's lives and create art and beauty, mistrust of centralized authority, disdain for obstacles erected against free access to computing, and an insistence that hackers be evaluated by no other criteria than technical virtuosity and accomplishment. In other words, the culture of hacking incorporated political and moral values as well as technical ends.

In the early decades—1960s and 1970s—although hacker antics and political ideology frequently led to skirmishes with the authorities (for example, administrators at MIT), hackers were generally tolerated with grudging admiration. Even the Defense Advanced Research Projects Agency (DARPA), the funding agency widely credited for sponsoring invention of the Internet, not only turned a blind eye to unofficial hacker activities but indirectly sponsored some of them. For example, research it funded at MIT's Artificial Intelligence Laboratory was reported online in 1972 as a catalog of "hacks," HAKMEM (ftp://publications.ai.mit.edu/ai-publications/pdf/AIM-239.pdf). The report is prefaced, tongue-in-cheek, as follows: "Here is some little known data which may be of interest to computer hackers. The items and examples are so sketchy that to decipher them may require more sincerity and curiosity than a non-hacker can muster." In *A Brief History of Hacking*, Eric Raymond, prolific philosopher of the Open Source movement, suggests that for DARPA "the extra overhead was a small price to pay for attracting an entire generation of bright young people into the computing field."

Heroes to Hooligans

Nowadays, though, when we hear about hackers it is usually as anti-social and possibly dangerous individuals who attack systems, damage other people's computers, compromise the integrity of stored information, create and distribute viruses and other harmful code, invade privacy, and even threaten national security. They flout the law by cracking into communications networks and copying and distributing copyrighted intellectual work. They care nothing for the norms of common morality and etiquette. They stay up all night, eat pizza and Twinkies, bathe infrequently, and take on bizarre and menacing names like Legion of Doom, Acid Freak, The Knights of Shadow, Scorpion, Terminus, Cult of the Dead Cow, and The Marauder. To top it off, the essential credo of old-style hackerdom, creative brilliance above all, has given way to a culture of "script kiddies" or "copycats," who merely mimic the technical ingenuity of a few creative hackers in order to further anti-social and often selfish ends.

In interoffice memos, government advisories, and stories in the popular media and trade press, systems administrators and security experts stress the importance of protecting vulnerable systems against hackers, peppering their rhetoric with cautionary tales (all of them true): the hacker "Maxim," who threatened to post three hundred thousand stolen credit-card numbers on the Net unless the online music-retailer CDUniverse paid him a hundred thousand dollars; master-hacker-addict Kevin Mitnick, at one point the most wanted hacker in the world, who gained access to corporate trade secrets worth millions; the loss of a ship at sea when a hacker brought down the weather forecasting system for the English Channel; the distribution of damaging viruses and worms, such as Klez, Nimda, Kalamar, Melissa, and ILOVEYOU; denial-of-service attacks on Yahoo!, America OnLine, and more. Each story is a reminder of the damage done and the millions of dollars lost in equipment, time, and productivity.

What accounts for the transformation in our conception of hackers from Levy's "heroes of the computer revolution" to white-collar criminals of the information age? There are simple, straightforward answers. One is that hackers themselves have changed. They no longer discriminate in their targets, victimizing not only carefully chosen centralized bureaucracies but unsuspecting users and consumers of the digital media. Having cut themselves adrift from their idealistic moorings, they are no better than other common criminals,

intruders, vandals, and thieves. We see them as villains now because they now are villains. Another explanation points not to a change in hackers themselves but to a change in us. Because our standards and values have changed, what we used to admire or tolerate we now deplore. Value shifts like these are not unprecedented; consider the cases—more significant, obviously—of slavery, racism, sexism, and corporal punishment.

But these answers, though each is true to some extent, tell only a fraction of the story, for the change in popular conception of hacking has as much to do with changes in the meaning and status of the new digital media and the powerful interests vested in them as with hacking itself. I will go further, and suggest that the shift is, to a significant degree, a product of purposeful political maneuvering that serves the ends of interested parties in our technology intensive society. Only by bringing these background factors into focus can we understand the significance for society of the transformation in moral status of hackers, and in turn, appreciate why it is important to question what is happening.

In the United States and other technologically advanced nations where digital electronic systems and devices are in widespread, everyday use, the rapid evolution of the technology has been accompanied by lively social and political responses. The progression of cause and effect is too complex to cover here in meaningful detail—technology to ideology and vice versa—but I would like to highlight a few relevant points. As is generally acknowledged by writers and scholars, the artifacts of information technology were incubated in the cooperation between the military establishment (mainly through its funding agencies) and academic research institutions, diffusing from these specialized and closely knit communities outward in many directions. Popular chroniclers of the information age, such as John Perry Barlow, Howard Rheingold, and Nicholas Negroponte, created a certain mindset, or interpretive lens, through which many people understood the social role of these new technologies. Writing in the eighties to mid-nineties, they elaborated a mythology of the Internet and World Wide Web as new frontiers, where great freedoms and opportunities lay, where brave (if sometimes bizarre) cowboys and "homesteaders" would create a cyberspace embodying these ideals. Their works both echoed and nurtured the earlier hacker culture.

But this was only half the story; the other half is a story of normalization. From early obscurity, through the phase of mythological idealism, the technologies of information finally reached the mainstream of everyday experience. The demographics of cyberspace normalized as the exotic constellation of camgirls, BBS (electronic bulletin boards), avatars (graphic icons representing characters in online games and other exchanges), ISPs (Internet Service Providers), chatrooms, portals, MUDs (multi-user dungeons/domains/dimensions—online computer-managed games or structured social experience involving many players, bearing some resemblance to the game "Dungeons and Dragons"), MOOs (multi-user object-oriented settings, a further variation of MUDs), and hackers were joined by familiar transplants—collective and individual—from more ordinary, physically bounded space. Local retailers, global corporations, credit card companies, traditional media corporations, governments (local, state, and federal), grandmothers, preachers, and lonely hearts sought their fortunes online. Pragmatic economic visions (from the likes of Al Gore) competed with the romantic mythologies of futurists as cyberspace became increasingly domesticated, encompassing the mundane and being encompassed by it.

These familiar presences brought familiar practices and modes of interaction, with their associated norms and institutions. Among the most vigorous was the commercial marketplace, which, in turn, required mechanisms for the enforcement of contracts and the protection of private property. Indeed, private property leached into and became central to all the multiple layerings of the online world, from the physical infrastructure on up. Global telecommunications corporations took over possession and oversight of the fiber-optic cables, airwaves, and switches from government agencies. Commercial Internet service providers (such as AOL) and others, including cable and phone companies, became dominant provid-

ers of popular online access. (The small percentage of users granted access through government and educational institutions, who typically have experienced little interference from their sponsors, now face greater restriction and regulation. Fearful of lawsuits and worried by the overuse of resources, these providers must keep a watchful eye for conduct such as exchange of MP3s (music files), online postings of copyrighted software, linking to pornographic sites, and so forth.) Some observers note that even open nonproprietary protocols, including TCP/IP, the fundamental building blocks of the Internet and Web, are under challenge as private entities attempt to replace open standards with proprietary ones.

The property metaphor has crept into the informal culture of the Web. Web sites are conceived as spaces *belonging* to people and organizations. People take pride and claim credit in the design of *their* Web sites. There is a growing sense of what one can and cannot do when visiting another's *home*page: wander around but touch only when authorized, link but do not deep-link. (To deep-link is to bypass the front page of a Web site, linking directly to desired content on another page within it, for example, bypassing the *New York Times* front page and linking directly to a particular story. Owners of commercial Web sites fear the loss of revenues from advertisements on their front-page portals and argue that deep-linking constitutes a copyright violation.)

The growing acceptance of property in computerized environments is seen in other arenas, too. For example, on the question of electronic surveillance in the workplace—employers reading employee e-mail and keeping track of their Web-surfing— the tide has turned dramatically, as shown in a survey of one thousand adults, reported by the Angus Reid Group in May 2000. The survey found that three of four workers believe employers are within their rights to monitor employee e-mail and Internet use at work. More surprising than the result itself, given vigorous objections just a few years ago, is the primary rationale for acceptance of these practices: because the employers own the computer resources, they have the right to monitor them.

Private ownership over content, long a feature in other media, plays an increasingly dominant role in the so-called "new media." Moreover, property claimants in software, images, music, movies, and other intellectual works are finding a body of law, including for example the controversial Digital Millennium Copyright Act (DMCA), that is tailored for the online environment and increasingly supportive of their interests. International treaties aimed at global harmony ensure that such rules prevail beyond and across national boundaries. This push to turn infrastructure, technical systems, and content into private property leads legal scholars such as James Boyle and Yochai Benkler to talk of a second enclosure movement, where the enclosure is not of land and physical property but of the creations of the intellect and the web of conduits through which they travel.

Though property has had the greatest public visibility, other arenas have seen efforts at regulation: online speech, online gambling, the assignment of domain names, and tighter controls on access (admitting authorized users only). All these have contributed to the transformation of a relatively intimate, mildly anarchic environment to one marked by institutionally imposed order. With some nostalgia, Larry Lessig, in his book *Code and Other Laws of Cyberspace*, describes the passage from Net95—the open online world that readily suggested Barlow's new frontier—to the enclosed, gated, regulated world of Net01.

It may already be obvious how this sea change strands hackers. While the exotic personae of cyberspace can be tolerated as long as they play by the rules of the new order, hackers are fundamentally inimical to it. The credo of their early years, which included a commitment to the free flow of information, to unrestricted access to computer resources, and to the idea of computer technology as an instrument of the public good runs counter to the new order. For corporate and government agents, this remnant of the old anarchy poses a terrifying threat.

Hackers as Bad Guys

The response of these agents has been to cast hackers as the bad guys of computerized and computer-mediated social reality: sociopaths, thieves, opportunists, trespassers, vandals,

Peeping Toms, and terrorists. These labels are more than negative public relations. They transform social meaning, refashioning the concept of hacking into one that is imbued with negative content. Our language is full of normative terms: "murder" when we mean an unlawful, wicked, premeditated killing; "theft" when we mean the wrongful taking of something one does not own; "weed" when we mean wild and unwanted plants. Words like these constrain what a speaker can say without stumbling into awkward inconsistencies; they foreclose certain moral discussions. To ask whether murder is wrong is odd, for by conceding that a killing is a murder we have already passed moral judgment. A philosopher might patiently explain that murder is wrong; did the questioner, perhaps, mean to ask whether it can sometimes be excused? In many cases, terms such as murder are useful, for they enable expressive precision—as in courts of law or in strong personal judgments: "As far as I'm concerned factory owners who dump toxins into drinking water are murderers." But in other cases, affixing a moral label can stunt exploratory deliberation—as it does, I believe, in the case of hacking. If hackers are thieves, vandals, and terrorists, it makes no sense to ask whether hacking is good or bad, whether we're for it or against it.

How such conceptual shifts occur is an important question. In the case of hackers, the media have played a critical role, bringing us countless stories of the sort already described. According to Eric Raymond, in *A Brief History of Hackerdom*, as early as 1984 the mainstream press began covering episodes of unauthorized breaking into computer systems and "journalists began to misapply the term 'hacker' to refer to computer vandals, an abuse which sadly continues to this day." Consider examples drawn from the print media within the past three years:

- The *New York Times*, June 13, 1999: "Computer hackers attacked the United States Senate's main Web site on Friday, the second such electronic assault on the high profile Internet page in just over two weeks." Later in the same article, "In an obvious taunt directed at the F.B.I.—which is conducting a national crackdown on computer hackers—they wrote on part of the page: "You can stop one, but you cannot stop all."

- The *Boston Herald*, August 1, 1999: "It was the kind of threat for which computer hackers are famous, a declaration of war dripping with the risk-free bravado so common on the anonymous Internet. The warning, which appeared on a hacked Web page of the U.S. Interior Department in late May, promised unrelenting attacks against government computers to avenge an FBI roundup of hackers associated with the group Global Hell."

- *Time* magazine (Canadian edition), May 22, 2000, headline: "School for Hackers: The Love Bug's Manila birthplace is just one of many Third World virus breeding grounds," suggests that De Guzman, who is suspected of unleashing the virus, is an example of a growing force of hackers in the "third world." Law-enforcement officials warn that "small cells of hackers—some at colleges, others in contact only electronically—pose an unprecedented threat to the computer systems of the industrialized world. . . "

- The *Boston Herald*, July 12, 2000, headline: "Don't have a cow Mr. Gates: Hacker cult opens doors for assault on Windows."

- In *LA Times.com*, November 7, 2000: "A 20 year-old hacker who seized control of sensitive computer programs at the Jet Propulsion Laboratory in Pasadena and at Stanford University pleaded guilty to federal charges Monday." http://www.latimes.com/cgi-bin/print.cgi.

- *Horizon Air*, January 2001: "A hacker in the Philippines can reach out to computers around the world and cause havoc," (62) and in comparing cyber criminals to regular burglars who cannot resist boasting about their exploits, "Modern-day hackers do the same, posting their exploits on hacker Web sites."

- The *Washington Post*, May 7, 2001: "A series of sophisticated attempts to break into Pentagon computers has continued for more than three years, and an extensive investigation has produced 'disturbingly few clues' about who is responsible, according to a member of the National Security Agency's advisory board . . ."

- The *San Jose Mercury News*, July 10, 2002: "Security Flaw Afflicts Popular Technology for Encrypting E-mail: The flaw allows a hacker to send a specially coded e-mail—which would appear as a blank message followed by an error warning—and effectively seize control of

the victim's computer. The hacker could then install spy software to record keystrokes, steal financial records or copy a person's secret unlocking keys to unscramble their sensitive e-mails."

• CNET News.com, July 15, 2002 headline: "House OKs Life Sentences for Hackers: The House of Representatives on Monday overwhelmingly approved a bill that would allow for life prison sentences for malicious computer hackers. . . . The Cyber Security Enhancement Act had been written before the Sept. 11 terrorist attacks last year, but the events spurred legislators toward Monday evening's near-unanimous vote."

The steady stream of media reports about hackers who are vandals, intruders, thieves, terrorists, and trespassers plays a role in establishing a new hacker profile, and we are led to see these hackers not as exceptions but the rule. They become prototypes of a newly defined category.

WE DO NOT HAVE to posit a massive conspiracy to understand why the media have followed this path. As Todd Gitlin argues in *The Whole World is Watching: Mass Media in the Making and Unmaking of the New Left*, established institutions, as compared with opposition movements, exert a formidable influence in how the mass media construe reality. Besides the obvious trappings of wealth and power, established institutions are able to provide duly selected spokespersons who present a coordinated, authoritative account of these institutions' positions and perspectives. By contrast, opposition movements typically lack such mechanisms. Although a sense of solidarity binds many hacker-comrades, and a dispersed, loosely associated network of small bands convenes around electronic discussion groups (such as Slashdot.com) and magazines (such as *2600: The Hacker Quarterly*), forming what Bruce Sterling once called a "digital underground," there are no formal entry requirements and no clearly representative organizations or individuals to express substantive positions from the hacker perspective. In such circumstances, as Gitlin would predict, media presentation of hackers falls prey to serendipity and the media's taste for celebrity and melodrama, even where it is not systematically shaped by the voices of the establishment.

For law enforcement and security agencies, hackers represent anarchy and disobedience, and for corporate agents they represent stubborn resistance to the imposed order of private property and restricted access. Hackers are not readily "tamed"; they explicitly eschew the rules of centralized authorities. This is a bad enough threat. How much worse if the rest of us were to identify with hackers and their "ethic"? The seventy million people who downloaded Napster and the even greater numbers who ignore the threats of established authorities and subscribe to file-sharing services such as Aimster and KaZaA are a corporate executive's nightmare.

One remedy is to separate the interests of hackers from those of the rest of us, construe public representations so as to make "us" see "them" as enemies, not friends. Lest we sympathize with hacker intentions, established institutions focus attention on destructive viruses, vandalism, intrusion, and theft. They fashion tools, technological and political, to "save" us from the negative impacts of these hacker attacks. Congress rises to the occasion with laws addressing the hacker "problem," from the 1986 Computer Fraud and Abuse Act to the 1998 Digital Millennium Copyright Act. In well-publicized sting operations of the 1980s, which Bruce Sterling calls "hacker crackdowns," police and FBI agents arrested hackers and "phreaks" (hackers who break into telecommunications networks), confiscated equipment, and pursued public indictments of infamous hackers such as Kevin Mitnick, Robert Morris, and Craig Neidorf.

Courts demonstrate their readiness to cooperate in such crackdowns by handing down guilty verdicts and imposing stiff punishments, from fines to jail sentences. In recent, highly visible cases, courts shut down Shawn Fanning's Napster and prohibited publication of DeCSS, a program that decrypts DVD disks for Linux machines, in Eric Corley's *2600 Magazine*. (In January 2002, Jon Johansen, a sixteen-year-old Norwegian hacker, was indicted by the Norwegian government, at the request of Norwegian and U.S. motion picture

associations, for his part in creating DeCSS. If convicted, he faces two years in prison.) In the wake of the September 11 attacks, hacking became even less tolerable, as it feeds the fear of cyber-terrorism.

But old-fashioned hackers—who worship the pure hack, resent centralized control of computer power, and believe computing to be a source of public good—have not disappeared. They have receded into the background, relegated to the margins of a revised category that now is filled by vandals and criminals. The question that remains is whether we are well-served by this revision. I believe we are not, but not because I condone the actions of those who apply programming skills to stealing information or money, to damaging and vandalizing systems, or to placing critical systems at risk of malfunction. The problem is that we are robbed of a concept that once suggested an alternative to the new, imposed order of cyberspace.

IT IS A MISTAKE to allow hacker ideas, ideals, and ideologies to drift toward the margins. Consider Richard Stallman and his followers in the Free Software Movement. Though many scoffed when they insisted that software should be free—"as in speech," Stallman would quip, "not beer"—the enormous body of free software, including Linux, poses a formidable challenge to glib truisms about intellectual property and innovation. Eric Raymond, referring to the origins of the phenomenal Open Source Movement, notes that "the hacker culture, defying repeated predictions of its demise, was just beginning to remake the commercial-software world in its own image." Hacker ideology also inspired such luminaries of the information age as Tim Berners-Lee, dubbed "the inventor of the World Wide Web," who sees his efforts as continuous with projects and ideologies of such earlier hackers as Ted Nelson. Contributions to social welfare included more than free software, Raymond says, because "many of the hackers of the 1980s and early 1990s launched Internet Service Providers selling or giving access to the masses."

In the political arena, self-identified hackers have publicly supported causes of liberty and individual autonomy. In 1994-1995, for example, they were among those who doggedly resisted the Clinton administration's Clipper proposal, which would have limited individual access to strong encryption. In 1996, they joined the broad coalition opposing, and ultimately defeating, the Communications Decency Act, arguing that it would lead to unacceptable censorship of the Internet.

Hackers have also joined fights against political oppression, devising ingenious forms of political protest. In a historic case in 1998, "hacktivists" supporting Mexican Zapatista rebels developed Floodnet, which temporarily shut down the Web site of Mexican president Ernesto Zedillo by a coordinated bombardment of client-requests. The attack was carefully planned and controlled in the tradition of peaceful civil disobedience not to destroy, but, as described by Ricardo Dominguez, one of its leaders, "to create a disturbance that becomes symbolic, so a certain community can gain a voice in the media." More recent hacktivist concerns include the growing presence of video surveillance technologies in private and public spaces. The hacktivist group Institute for Applied Autonomy charts routes of least surveillance through Manhattan streets, and an anonymous Web site at http://rtmark.com/cctv/ offers advice on how to disable cameras. In his article in the *Guardian*, published March 2001, Stuart Millar characterizes hacktivism as a "highly politicized underground movement using direct action in cyberspace to attack globalization and corporate domination of the internet," and, as such, an ideological heir to the great protest movements of the nineteenth and twentieth centuries.

In the end, it is protest that ties together the many variations of what I have called "old-fashioned" hacking. These hackers flail against encroaching systems of total order where control is complete and dissent dangerous. They defy tendencies of established powers to overreach and exploit without accountability. With their specialized skills they resist private enclosure and fight to preserve open and popular access to online resources, which they consider a great boon to humanity. Ornery and irreverent, they represent a degree of freedom; they open an escape hatch from a system that threatens

to become too regulated and controlled.

As noted earlier, there are people who apply technical know-how to harming others and committing acts of crime and terror. These people should be found, stopped, and punished no less because their mode, or object, of attack is high tech. But the growing tendency to portray these individuals as typical of the category erases crucial meaning from the concept of "hacking." If I had the power to fix meaning, I would deny criminals and terrorists the term; I would reserve "hacker" for those who turn their technical virtuosity to conscientious pursuit of the specific constellation of social values discussed above.

But it probably isn't possible to determine semantic outcomes, and even if it were, it certainly would not be easy to draw clear lines. I hope simply to have shown what is at stake in allowing conscientious hackers to be identified as criminals and terrorists. This version of conceptual revisionism imposes two critical, if inverse burdens. First, in the wake of the September 11 attacks, when our predicament demands a unified resolve in dealing especially with terror but also with crime, adding hacker-protesters into the mix distorts the mission and exploits its urgency. Second, if we insist that hacker-protesters answer for the actions of criminals and terrorists, we will only distract them from their own task: to challenge the values and interests that are increasingly coming to dominate digitally mediated societies. Hacking deserves our unconfused recognition and warrants a place in a free society alongside other forms of legitimate protest. ●

Helen Nissenbaum has written about privacy, trust, accountability, and other values in the information age. Co-editor of the journal *Ethics and Information Technology*, she serves on the faculty of New York University.