Terrorism or Civil Disobedience:

Toward a Hacktivist Ethic

Mark Manion & Abby Goodrum
Drexel University, Philadelphia, PA

In this era of global commerce via the Internet, strikes against the hegemony of bureaucratic capitalism and the commercialization of the Internet will inevitably be carried out on the World Wide Web. In fact, recent proliferation of hacking activity has shocked the commercial Internet world. On February 8, 2000 hackers attacked Yahoo, Amazon, eBay, CNN and Buy.com, closing them for several hours. Through "denial of service" attacks originating from hundreds of independent computers, the sites were flooded with millions of simultaneous requests. This increase in fake service requests effectively blocked legitimate users from accessing the site.

These hacks have led to widespread speculation regarding the motivation of the perpetrators. Are they mere nuisance attacks perpetrated by malicious teenagers, more serious acts of cyberterrorism, or evidence of growing outrage over an increasingly commodified Internet? Although at present no individuals or groups have officially claimed responsibility, MSNBC reported receipt of an 18-page letter claiming responsibility by an individual who angrily criticized the sites for their "capitalization of the Internet." Hundreds of reports in the popular press have portrayed the hackers as vandals, terrorists and saboteurs, yet no one seems to have considered the possibility that this might be the work of electronic political activists or "hacktivists."

Perhaps these attacks are evidence of a new form of civil disobedience, which unites the talents of the computer hacker with the social consciousness of the political activist. Adapting a variation of civil disobedience, with its practices of "trespass" and "blockade" to the electronic age, participants in what has been called electronic civil disobedience, or hacktivism, can attack the websites of any individual, corporation, or nation that is deemed responsible for oppressing the ethical, social, or political rights of others. Through an investigation of hacktivism, this essay seeks to elucidate the cooperative and liberal ideology of the originators of the "electronic frontier," speaking in the name of social justice, political decentralization, and freedom of information, and the more powerful counteracting moves to reduce the Internet to one grand global "electronic marketplace."

Hacktivism has the potential to play an active and constructive role in the overcoming of political injustice, to educate, inform and be a genuine agent of positive political and social change. However, there is the fear that cyber-activism could reduce to more radical and violent forms of cyberterrorism (Arquilla & Ronfeldt, 1993). How governments and societies react to this new form of social activism have not been sufficiently addressed in the computer ethics literature. Researchers concerned with ethical issues in computing, policy makers, and computer professionals must come to terms with the complex set of issues surrounding the potential power of hacktivism.

Background

Hacktivism is defined as the (sometimes) clandestine use of computer hacking to help advance political causes. Hacktivist groups such as the Electronic Disturbance Theater, the Cult of the Dead Cow and the Hong Kong Blondes have used electronic civil disobedience to help advance the Zapatista rebellion in Mexico, protest nuclear testing at India's Bhabba Atomic Research Center, attack Indonesian Government websites over the occupation of East Timor, as well as protest anti-democratic crackdowns in China. In addition, hacktivism has been used to inveigh against the corporate domination of telecommunications and mass media, the rapid expansion of dataveillance, and the hegemonic intrusion of the "consumer culture" into the private lives of average citizens.

These concerns give rise to two institutional forces which hactivist protests aim to confront: the commodification of the internet at the hands of corporate profiteers and violations of human rights at the hands of oppressive governments. Hacktivism thus poses a potential threat at two levels: the private industry/intellectual property level and the national government/national security level. Both of these issues will be discussed in this paper.

Electronic Civil Disobedience

Civil disobedience entails the peaceful breaking of unjust laws. It does not condone violent or destructive acts against its enemies, focusing instead on nonviolent means to expose wrongs, raise awareness, and prohibit the implementation of perceived unethical laws by individuals, organizations, corporations or governments. In a civil society, it is the re-

sponsibility of all ethical individuals to take a stand against oppression, inequality, and injustice (Honderich, 1997). Civil disobedience is a technique of resistance and protest whose purpose is to achieve social or political change by drawing attention to problems and influencing public opinion. Breaking specific laws, which are unjust, constitutes direct acts of civil disobedience. Symbolic acts of civil disobedience are accomplished by drawing attention to a problem indirectly. Sit-ins and other forms of blockade and trespass are examples of symbolic acts of civil disobedience.

The Internet has created a brave new world of digital activism by providing forums for organizing, communicating, publishing, and taking direct action. The use of the computer as a tool of civil disobedience has been termed Electronic Civil Disobedience (ECD) (Wray, 1998). Electronic civil disobedience comes in many forms, ranging from conservative acts such as sending email and publishing websites, to breaking into computer systems. A distinction must be made between the use of computers to *support* ECD, and the use of computers as an *act* of ECD. If a U.S. citizen wishes to speak out against the government's actions in Kosovo, it is legal to publish a web site or host mailing lists or chat rooms for this purpose. This activity does not constitute an act of civil disobedience, electronic or otherwise. These types of activity are usually referred to as "electronic activism," which uses the Internet in fully legitimate ways to publish information, coordinate effective action, and to directly lobby policy makers. Running a program such as FloodNet, however, that posts the reload command to a web site hundreds of times a minute constitutes an act of symbolic ECD since the intended aim of such programs is to create an electronic disturbance akin to a sit-in or blockade.

The effect of hundreds of persons reloading a targeted page on the "web" thousands of times effectively blocks entrance by outsiders and may even shut down the server, as occurred in the attacks on the commercial websites of Yahoo, Amazon, etc. In 1998 pro-Zapatista activists took this kind of action against Mexican government web sites (Cleaver, 1999). This is easily seen as a symbolic act of ECD because it tries to draw attention to a perceived violation of rights, rather than attacking the suspected violator(s) directly. The purpose of most ECD is to disrupt the flow of information into and out of institutional computer systems. The point is not to destroy information or systems, but to block access temporarily. This results in virtual sit-ins and virtual blockades. Since institutions today are no longer localized in physical structures but exist in the decentralized zones of cyberspace, electronic blockades can cause financial stress that physical blockades cannot (Critical Art Ensemble, 1994).

The changing nature of authoritative and repressive power has necessitated qualitative changes in resistance to this power. Power/Capital, having constituted itself in a new electronic form in cyberspace, requires that opposition movements have to invent new strategies and tactics that counter this new nomadic power of capital. This entails that certain old ways of trespass and blockade– such as street demonstrations—are being modified through electronic civil disobedience, or hacktivism, to meet the new conditions (Critical Art Ensemble, 1996).

Hacktivism and Electronic Civil Disobedience

Nothing has fired debate about ECD so heatedly as the issue of hacktivism. The central question is whether hacking can reasonably be defined as an act of civil disobedience. Now the refusal to obey governmental commands, even if it entails breaking the law, is often morally sanctioned if certain preconditions are met. Even though philosophers often disagree as to when the breaking of a law actually constitutes an act of civil disobedience, most would agree on the following set of core principles as forming the necessary conditions, and hence ethical justification, for acts considered civilly disobedient. They are:

- No damage done to persons or property
- Non-violent
- Not for personal profit
- Ethical motivation—i.e., the strong conviction that a law is unjust, unfair, or to the extreme detriment of the common good
- Willingness to accept personal responsibility for outcome of actions

Are acts of hacktivism consistent with the philosophy of civil disobedience? In order for hacking to qualify as an act of civil disobedience, hackers must be clearly motivated by ethical concerns, be non-violent, and be ready to accept the repercussions of their actions. Examined in this light, the hack by Eugene Kashpureff clearly constitutes an act of ECD. Kashpureff usurped traffic from InterNIC to protest domain name policy. He did this non-anonymously and went to jail as a result. Further evidence of ethical motivation for hacktivism can also be seen in the messages left behind at hacked sites (Harmon, 1998):

- "China's people have no rights at all, never mind human rights..."
- "Save Kashmir" overlaid with the words "massacre" and "extra-judicial execution."
- "Free East Timor" with hypertext links to Web sites describing Indonesian human rights abuses in the former Portuguese colony."

In order to justify hactivism's direct action praxis and to legitimate it's theoretical foundations, two things must be demonstrated. First, it must be shown that hacktivism is not the work of curious teenagers with advanced technical expertise and a curiosity for infiltrating large computer networks for mere intellectual challenge or sophomoric bravado. Moreover, the justification of hacktivism entails demonstrating that its practitioners are neither "crackers"—those who break into systems for profit or vandalism (Anonymous,

1998), nor are they cyber cyberterrorists—those who use computer technology with the intention of causing grave harm such as loss of life, severe economic losses, or destruction of critical infrastructure (Denning, 1999). Hacktivism must be shown to be ethically motivated. Second, politicized hacking must be shown to be some form of civil disobedience – a form of civil disobedience that is morally justified. In order to determine the motivations of hactivists, one place to look is what hactivists themselves say is their motivation.

On October 12, 1998 the website of Mexican president Erenesto Zedillo was attacked. From all accounts, the Zedillo hack was not the work of bored teens. It was a political act, according to the Electronic Disturbance Theatre, to "demonstrate continued resistance to centuries of colonization, genocide, and racism in the western hemisphere and throughout the world" (Harmon, 1998). Earlier, in August of the same year, the hactivist group "X-Ploit" hacked the website of Mexico's finance ministry, defacing it by replacing the contents with the face of the revolutionary hero Emiliano Zapata, in sympathy with the Zapatista rebellion in the Chipas region of southern Mexico. These acts are political protests, which draw attention to what is perceived to be grave social injustice. The reason for these actions is clear: they are motivated by a socio-economic system that perpetuates discrimination, racism, and economic inequality, not the mere thrill and challenge of breaking into networks for fun.

In June of 1998 the hactivists group "MilwOrm" hacked India's Bhabba Atomic Research Centre to protest against recent nuclear tests. Later, in July of that year, "MilwOrm" and the group "Astray Lumberjacks," orchestrated an unprecedented mass hack of more than 300 sites around the world, replacing web pages with an anti-nuclear statements and images of mushroom clouds. Not surprisingly, the published slogan of MilwOrm is: "Putting the power back in the hands of the people" (Hesseldahl, 1999). These examples seem to be motivated by belief in the positive forces of democracy and freedom rather than the mere thrill of vandalism or the nihilism of "cyberterrorism."

Mail-bombs were delivered and several other Chinese government web sites were hacked to protest the targeting of Chinese and Indonesian citizens for torture, rape, and looting during the anti-Suharto riot in May of 1998 (Hesseldhal, 1999). On August 1, the Portuguese group "Kaotik Team" hacked 45 Indonesian government websites, altering web pages to include calling for full autonomy of East Timor and the cessation of the harsh military crackdown on dissidents (Hesseldhal, 1999). Again, fighting for social justice and human rights is motivated by ethics, not anarchy. Many, many other hactivist activities can be sited to demonstrate the ethical motivation behind this new form of political activism.

These messages, and many others like them, demonstrate a striking change from hacker messages of the past. Prior hacks have had little if any socio-political content, and bear a closer resemblance to "tagging" and other forms of boasting graffiti. There has been a certain juvenile style to messages left by hackers in the past. The hacks listed above, however, represent a new breed of hacker: one who is clearly motivated by the advancement of ethical concerns and who believes such actions should be considered a legitimate from of (electronic) civil disobedience.

Hacktivism and Cyberterrorism

If hacktivism can be defined as an act of electronic civil disobedience, then the punitive outcomes must be brought into alignment with other forms of civil disobedience. Traditional penalties for civil disobedience are mild compared to penalties for hacking. Penalties for hacktivism are meted out with the same degree of force as for hacking in general, regardless of the motivation for the hack or the political content of messages left at hacked sites. Most governments do not recognize hacking as a political activity, and the penalties for breaking into computers can be extreme (Jaconi, 1999). For example, the hack of China's "Human Rights" website by the Hong Kong Blondes, attacks on Indonesian Government websites regarding policy in Kashmir, attacks on India's nuclear weapons research center websites to protest nuclear testing, as well as the hacks on the commercial websites of Yahoo, CNN, etc. are all subject to felony prosecution if apprehended. All of these examples provide convincing evidence in support of our thesis that hacktivism should be considered a legitimate form of civil disobedience, and not the work of "cybervandals" or "cyberterrrorists." Under U.S. law, terrorism is defined as an act of violence for the purpose of intimidating or coercing a government or civilian population. Hacktivism clearly does not fall into this category, as it is fundamentally non-violent.

Since many acts of hacktivism have been perpetuated against government websites, however, hacktivism is increasingly being equated with acts of information warfare and cyberterrorism (Kovacich 1997, Furnell & Warren 1999). In August of 1998, the Center for Intrusion Control was established by a coalition of various government agencies to respond to these "cyber-warfare threats" (Glave 1998b). Similarly, organizations such as RAND and the NSA have categorically denied the existence of hacktivism as an act of civil disobedience and repeatedly refer to all acts of hacking as cyberwar or cyberterrorism in an attempt to push for stronger penalties for hacking, regardless of ethical motivations (Bowers 1998, Gompert 1998).

In order to determine the kinds and range of threats to its critical infrastructures posed by possible cyberterrorists, the U.S. government established the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP findings have led to the development of the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIA), the National Infrastructure Assurance Council (NIAC) and the Joint Task-Force

Computer Network Defense (JTF-CND), established by the Department of Defense. The threat posed by cyberterrorism is very real. However, it is a mistake to identify cyberterrorism with hacktivism. As we have established above, acts of hacktivism are more akin to acts of civil disobedience than to acts of terrorism and it is important to keep this distinction clear.

In fact, potential acts of cyberterrorism are explicitly condemned by hacktivists. During a December 1998 press conference, one member of the hacktivist group, which call themselves the Legion of the Underground (LoU), declared "cyberwar" on the information infrastructures of China and Iraq. This declaration of war prompted a coalition of hacktivists groups to condemn the "irresponsible" declaration or war. In a "Joint Statement by 2600, The Chaos Computer Club, The Cult of the Dead Cow, !Hispahack, L0pht Heavy Industries, Phrack and Pulhas," the leaders of the hacktivist community denounced the LoU declaration of war, saying

> We strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of any country, for any reason. Declaring 'war' against anyone, any group of people, or any nation is a most deplorable act... this has nothing to do with hacktivism or the hacker ethic and is nothing a hacker can be proud of (Hackernews, 12/29/98).

This immediately prompted a quick response from the leaders of LoU who issued a statement saying that the declaration of war did not represent the position of the group. The letter states:

> The LoU does not support the damaging of other nations' computers, network or systems in any way, nor will the LoU use their skills, abilities or connections to take any actions against the systems, network or computers in China or Iraq which may damage or hinder in any way their operations. (Hackernews, 01/799).

Why is it, then, that a growing number of experts refuse to make this distinction, and insist on conflating hacktivism and cyberterrorism? It may be that describing hacktivists as criminals helps entrench a certain conception of, and control over, intellectual property, and obscures the larger critique about the ownership of information, and the legal system's need to protect the powerful economic interests of corporations attempting to dominate and completely commercialize the Internet. Moreover, labeling the hacktivist as a national security threat provides further legitimation for the erasure of individual privacy at the hands of the national security state, which compiles and stores vast databases on hundreds of thousands of citizens each year. The demonization of the hacker may also be an attempt to obscure the violation of our privacy at the hands of corporations. As one critic put it

> Through the routine gathering of information about transactions, consumer preferences, and creditworthiness, a harvest of information about an individual's whereabouts and movements, tastes, desires, contacts, friends, associates, and patterns of work and recreation become available in the form of dossiers sold on the tradable information market, or is endlessly convertible into other forms of intelligence through computer matching. Advanced pattern recognition technologies facilitate the process of surveillance, while data encryption protects it from public accountability" (Ross, 1998).

Hence, one rationalization for the vilification of hacktivism is the need for the power elite to rewrite property law in order to contain the effects of the new information technologies. As a result of the newly evolving intellectual property laws, information and knowledge can now be held as capital. Since new information technology supports easy reproduction of information, the existence of these laws effectively curtails the widest possible spread of this new form of wealth. However, unlike material objects, information can be shared widely without running out. As two experts put it

> Intellectual property is not a tangible, material entity. It is nothing more than a volatile pattern of electrons arrayed in patterns of open and closed gates to form intelligible numerical or textual symbols. Information, documents, and data reside inside computers in a form that can be 'stolen' without ever being removed, indeed without ever being touched by a would-be thief, or depriving the 'owner' from still using and profiting off of the 'property' (Michalowski and Pfuhl, 1991).

Although the information inside of computers is clearly of value, the form of this value is both intangible and novel. Its character as "property" remained legally ambiguous until a rapid proliferation of computer crime laws took place in order to create the legal environment that helped define and delimit the debate over the nature of intellectual property. These laws and rulings ultimately served to protect the immediate financial interests of the corporate techno-elite, and directed the state to protect the profit potential of telecommunications industries, financial investors and entrepreneurs capitalizing on the Internet.

Ironically, this rapid proliferation of computer laws during the 1980s, which saw 47 states enact computer crime laws, as well as two Congressional pieces of compute crime legislation which entered the legal system at the same time, resulted in relatively few arrests or prosecutions. For example, "Operation Sundial" the largest FBI sting on suspected hackers, led to no serious charges. A few hackers pled guilty and paid a total of $233, 000 in fines (Halbert, 1997). This rapid criminalization of computer abuse represents, moreover, an exception to the gradual and reformist nature of typical law formation in common law jurisdiction (Hollinger and Lanza-Kaduce, 1998). Michalowski and Pfuhl conclude form this that "the violations of computer security posed a

broad challenge to the hegemonic construction of property and authority relations, and it was this challenge, more than the concrete losses resulted form unauthorized computer access, that created a climate of fear about computer crime that led to the swift and non-controversial passage of computer crime laws" (Michalowski and Pfuhl, 1991).

The power elite, often synergistically intertwined with the design and operation of information technologies, will always come to the aid and defense of technologies of control, making revolt difficult and reform hard. Intellectual property laws attest to this, as do the excessively stringent laws against hacking. Nevertheless, if we say we support civil disobedience as a legitimate form of social protest, then we must support the computerization of these efforts as well. This means bringing penalties for hacktivism, or electronic civil disobedience, in line with penalties for traditional mechanisms used for the breaking of what are perceived to be unjust laws.

Toward a Hacktivist Ethic

Every technology releases opposing possibilities towards emancipation or domination, and information technology is no different. The new information technologies are often portrayed as the utopian promise of total human emancipation and freedom. However, the promise of freedom from work, e-democracy, and global community, once hailed as the hallmarks of the computer revolution, are nowhere to be found. As critics are quick to point out, the only entities that seem to benefit from the Internet are large transnational business corporations.

For such critics, advanced information technology threatens to turn into an Orwellian nightmare of totalitarian domination and control, a dystopia of complete repression of free thought. They remind us that the Internet is quickly becoming subordinated to the pecuniary interests of the techno-elite, which merely pays lip service to the growth of electronic communities and participatory democracy. These interests are devoted to shutting down the anarchy of the Net in favor of virtualized commercial exchange. Hence, the power elite must destroy the public cyber-sphere for its own survival. This may account for the vilification of hacktivists, as well as why the charges against hacktivism are so high.

As is well known, however, the lifeblood of the hacker ethic has always been the freedom of information and the full democratization of the public sphere. The core principles of the hacker ethic were spelled out in Steven Levy's book, *Hackers: Heroes of the Computer Revolution* (Levy, 1984). Three of these principles are relevant here. They are:

1. Access to computers—and anything that might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-On Imperative!
2. All information should be free.
3. Mistrust Authority—Promote Decentralization

Hackers prioritize freedom of information and are suspicious of centralized control or private ownership of information. Hackers question why a few corporations can own and sell huge databases of information about others and control information helpful to the public at large. Hackers are frustrated to discover that their coveted "electronic agora," a true marketplace for the free-play of ideas, which was the original ideal behind the formation of the Internet, has been invaded and taken-over by avaricious and enterprising entrepreneurs who prefer dollars to the free-flow of information and knowledge. In sum, this ethic puts hackers on a collision course with the commercial-industrial complex who wish to own and control the Internet.

One of the most pervasive popular arguments against the panoptical intentions of the "Captains of Technology" is that their system does not work. Every successful hack in some way reinforces the popular perception that the rise of the total panoptic surveillance society is not inevitable. Hence, the hacker ethic, libertarian and anarchist in its right-to-know principles and its advocacy of decentralized technology, is a principled attempt to challenge the tendency to use technology to form information elites.

The debate over the control of intellectual property demands that we address issues of social justice such as wealth distribution and equality of opportunity. Politically, the resistance to corporate domination of the Internet must force not only the question of privacy and property, but it must also place the critique of the technological society itself into the center of pubic consciousness and debate. Hacktivist activities put theses issues of techno-control on the political agenda, by performing acts of symbolic electronic civil disobedience.

Furthermore, resistance to political oppression and corporate manipulation must be embedded in a well-articulated theory, one that is morally informed and widely shared. Movements acting out of outrage often dissipate. They need to be durable and sustain a commitment, lasting through adversaries of repression. This leads to the necessity of creating a form of technocultural activism that can bring to reality the ideas of human emancipation. Activism today is no longer a case of putting bodies on the picket line; it requires putting minds and virtual bodies "on-line." This is the promise of hacktivism, the fusion of the political consciousness of the activist with the technical expertise of the computer "hacker."

Conclusion

Hacktivism is in its infancy, but, given the ubiquity and democratizing possibility of the Internet, we will certainly bear witness to the movement's growing pains and increasing maturity. One thing is sure, however. Incidents of cyberactivism are on the rise, and will continue to be on the rise in the near future.

Never in the long and storied history of political and social activism have dissidents had at their disposal a tool as far-reaching and potentially effective as the Internet. Sadly, this inherently civil strategy of disobedience is being deliberately and officially mis-construed through mis-information as cyberterrorism, which it is clearly not. Steps must be taken to separate political direct action in cyberspace from organized criminality or cyberterrorism.

When is it legitimate to practice direct action on the Internet? Some will inevitably argue that electronic civil disobedience is never justifiable, while others will argue that it is always justified. What are the limits of political protest in cyberspace? How far can activists go without infringing on the legitimate rights of the people and institutions against whom they are protesting? These questions demand a more extensive argument that extends beyond the scope of this essay. One way or another, in order for hacktivism to become a legitimate form of social protest, it must be provided sound ethical foundations. This, in turn, means expanding the ethical justification of civil disobedience to include acts of hacktivism.

As we envision the possibilities of resistance taking place increasingly on the Internet, it is important to remember that civil disobedience has been an important part of the history of political growth and change in this country, from the Boston Tea Party to the Civil Rights movement to contemporary environmental activism. However, while it is useful to consider the role that the theory and practice of civil disobedience has taken up until now, we must demand more than the right to speak; we must demand the right to act in the "wired world" on behalf of the public good. If we lose the right to protest in cyberspace in the coming Information age, we are in jeopardy of losing the greater part of our individual and collective freedom. ◆

References

(Anonymous), (1998), "The language of hacking," *Management Review* 87 (9), pp. 18-21.

Arquilla, J. and Ronfeldt, D. (1993), "Cyberwar is coming," *Comparative Strategy*, Volume 12, no. 2, 141-165.

Bowers,S. (1998). "Information warfare: the computer revolution is altering how future wars will be conducted," *Armed Forces Journal International*,, August, pp. 38-49.

Cleaver, H. (1998), "The Zapatistas and the electronic fabric of struggle," www.eco.utexas.edu/faculty/Cleaver/zaps.htm (accessed 5/18/99)

Critical Art Ensemble. (1996), Electronic Civil Disobedience and Other Unpopular Ideas. Brooklyn, NY: Autonomedia.

Critical Art Ensemble. (1994), The Electronic Disturbance. Brooklyn, NY:Autonomedia.

Denning, Dorthy (1999). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", paper presented at the *Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking Workshop*, Georgetown University, Washington, D.C.

Furnell, S. & Warren, M. (1999), Computer hacking and cyberterrorism: The real threats in the new millennium, Computers & Security, 18, 28-34.

Glave, J. (1998). "Hacker raises stakes in DOD attacks," Wired News, available at: http://www.wirednews.com

Gompert, D. (1998). "National security in the information age," Naval War College Review, 51 (4), pp. 22-41.

Hackernews, available at http://www.hackernews. com/archive.html

Halbert, D. (1997), Discourses of danger and the computer hacker, *The Information Society*, 13, 361-374.

Harmon, A. (1998), Hacktivists of all persuasions take their struggle to the web, *The York Times*, October 31, 1998, page 1 column 5.

Hollinger, R. and Lanza-Kaduce, L. (1988). "The Process of Criminalization: The Case of Computer Crime Laws," *Criminology* 26 (1), pp. 1010126.

Honderich, T. (1997), Hierarchic democracy and the necessity of mass civil disobedience, in Bontekoe, R. ed. Justice and democracy: cross-cultural perspectives. University of Hawaii Press: Honolulu.

Hesseldhal, Arik (1999). "Hacking for Human Rights?," *Wired News*, 21 May. Available at: http://www.wirednews.com/news/news/politics/story/13693.html.

Jaconi, J. (1999), Federal Cybercrime Law, Section 1030 "Computer Fraud & Abuse Act, " www.antionline.com (accessed 6/17/99)

Kovacich, G. (1997), Information warfare and the information systems security professional, Computers & Security, 16, 14-24.

Levy Stephen (1984).Hackers: computer heroes of the computer revolution, New York: Delta Trade Paperbacks.

Michalowski, R. and Pfuhl, E. (1001). "Technology, property and Law: The case of Computer Crime," *** (need to provide full reference).

Ross, Andrew (1998). "Hacking away at the counterculture," in *Technoculture*, Penley and Ross, Eds. Minneapolis: University of Minnesota Press, p. 126.

Wray, S. (1998). Electronic civil disobedience and the word wide web of hacktivism: a mapping of extraparliamentarian direct action net politics, available at: http://www.nyu.edu/projects/wray/wwwhack.html.