Communication Law Review
Volume 12, Issue 1

The Rhetoric of the Web: The Rhetoric of the Streets Revisited Again

Brett Lunceford, University of South Alabama

Abstract

Protest rhetoric has always provided a prime example of how communication can work to change the human condition, but strategies of protest have evolved as the United States has transformed into an information economy. Although protest remains "on the streets," it has also moved into the digital realm. This essay builds on the work of Franklyn Haiman by considering the ethical and rhetorical dimensions of hacktivism (politically motivated computer hacking). After briefly tracing the historical development of hacktivism, I discuss several recent politically motivated website defacements and denial of service attacks, concluding that Haiman's argument that the rhetoric of the streets should be held to different rhetorical and ethical standards still holds true in the online world.

In Franklyn Haiman's essay, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," the author defended protest tactics that were, at the time, criticized. Haiman revisited his arguments 15 years later in the essay "Nonverbal Communication and the First Amendment: The Rhetoric of the Streets Revisited," in which he discussed various legal cases involving symbolic nonverbal acts.[1] The advent of the information age has allowed for forms of protest unimaginable in 1967 and 1982. In this essay, I wish to reconsider protest that falls outside of traditional and legal boundaries by exploring the current practice of politically motivated computer hacking, also known as "hacktivism," "cyberactivism," or "electronic civil disobedience."

First, a disclaimer: this essay makes no argument concerning the legality of computer hacking. Unauthorized access to computer systems constitutes an illegal act under United States law.[2] However, this essay suggests that hacktivism is a special case of computer hacking and that ethical and rhetorical considerations surrounding hacktivism should be considered independent of its legality. Actions can be rhetorical regardless of their legality, and ethical and legal are by no means synonymous. Other scholars have defended the rhetorical value of uncivil discourse and action: Robert Doolittle explains that even riots can be viewed as rhetorical phenomena; Haig Bosmajian defends obscenity and heckling; Theodore Windt defends the diatribe.[3] At issue here is not the legal status of computer hacking, but the rhetorical function of hacktivism.

Although hacking and political action have long been intertwined, the political component is often overshadowed by the illegality of the action. The ways that particular actions are defined has been a continual problem for social movement and protest groups. Thomas Benson and Bonnie Johnson describe the problems of definition in their observations of a Vietnam War protest:

> Was the action primarily a rhetorical one, designed to persuade the government, public, and participants to work for an end to the war? Or was it, as some said, an act of resistance, designed to cripple the war effort by attacks upon the government's time and property? Even the labels used to describe the event were dichotomized: some called it a *march, rally,* or

> *demonstration*, others a *resistance,* or *mobilization.* The word *confrontation,* chosen by its organizers as the official title of the event, seems to be capable of synonymity with either side of the dichotomy, depending on the user.[4]

Since the events of September 11, 2001, it has become fashionable in some circles to define acts of political resistance as "terrorism," and hacking has not escaped this fate. Under the provisions of the USA PATRIOT Act, computer hacking is listed under the banner of "cyberterrorism."[5]

Re-examining Haiman's assertions concerning the rhetoric of the streets seems particularly timely because the strategies of hacktivism build on the strategies of the past. Stefan Wray writes, "The same principles of traditional civil disobedience, such as trespass and blockage, will be applied, but more and more these acts will take place in electronic or digital form: The primary site for [electronic civil disobedience] will be in cyberspace."[6] Two particular strategies, website defacement and denial of service attacks, have clear analogues in the physical world. Website defacement can be described as electronic graffiti. Winn Schwartau states, "Graffiti on billboards, graffiti on web sites, same difference, different medium."[7] Denial of service (DoS) attacks can be described as a form of electronic sit-in; both seek to deny access to a particular venue by occupying that space. But despite the similarities in the strategies, Marshall McLuhan reminds us that the medium still matters because "the personal and social consequences of any medium—that is, of any extension of ourselves—result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology."[8] It is not enough to examine the strategy itself; one must examine the consequences of employing a particular strategy in a particular medium or place.

Who Engages in Hacktivism and What do They Do?

The term "hacktivism" was coined in 1996 by Omega, a member of the hacker collective Cult of the Dead Cow.[9] Douglas Thomas identifies Cult of the Dead Cow 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."[10] Thomas also argues that hackers had more limited political agendas in the 1970s and 1980s and that at that time most attacks were directed at the phone company; after the breakup of the phone monopoly this changed. "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."[11] But there are problems with this account of hacker politicization. Although the term hacktivism may be relatively recent, the actions underlying the term have a long history, reaching back at least to the early 1970s when the Technological American Party (TAP) advocated phreaking (the hacking of telephone systems) as a way to avoid paying the War Tax levied on telephone bills and provided schematics for blue boxes in their Youth International Party Line (YIPL) publications.[12] Other hacker collectives, such as the Chaos Computer Club and *2600*, have long had a political slant. Steven Furnell explains that "the exploits of [Chaos Computer Club] over the years have had a considerably political slant," and that members were linked to an espionage case in the late 1980s.[13]

In some cases, hacker collectives have automated the work of the hacktivist. One of the more widely known instances of this kind of automation took place in 1998 when the Zapatista movement in Mexico employed a program called Floodnet to engage in politically motivated denial of service attacks.[14] This program allowed others to take part in the protest in the form of a digital sit in. A similar action took place in 1999 against the World Trade Organization (WTO) when the electrohippies, a UK hacker collective, orchestrated a client-side distributed denial of service attack. The electrohippies note that client-side actions require a large amount of individuals taking part in the actions for them to be successful: "The fact that service on the WTO's servers was interrupted on the 30th November [and] 1st of December, and significantly slowed on the 2nd and 3rd of December, demonstrated that there was significant support for the electrohippies action."[15] In defending their actions, the electrohippies argue that "as another part of society's public space the Internet will be used by groups and individuals as a means of protests. There is no practical difference between cyberspace and the street in terms of how people use the 'Net."[16]

Other politically motivated hacks have been the product of small groups of hackers rather than the result of large numbers of participants. In 1998, a group of hackers called HFG, or H4ck1ng for Girl13s (Hacking for Girlies) defaced the *New York Times* website in support of Kevin Mitnick. The hack seemed to be a belated response to a July 4, 1994, article by John Markoff demonizing Mitnick that appeared on the front page of the *New York Times*.[17] Other hacks in that time period also attempted to raise awareness of the plight of Mitnick, whom hackers believed was being treated unfairly, largely as a result of Markoff's attempts to portray Mitnick as a kind of superhacker. More recently, The Recording Industry Association of America (RIAA) was hacked repeatedly in response to a wave of lawsuits against those who used peer-to-peer file sharing programs to download music.[18]

Ethical Considerations Concerning Hacktivism

These hacks provide a framework to consider four ethical considerations concerning hacktivism. First, there is the question of inclusiveness. Do large numbers of participants make the action more defensible? The electrohippies argue that "distributed clientside DoS action is only effective if it has mass support, and hence a democratic mandate from a large number of people on the Net to permit the action to take place. These type[s] of actions are directly analogous to the type of demonstrations that take place across the world. One or two people do not make a valid demonstration – 100,000 people do."[19] Other hacker groups disagree on this point. Cult of the Dead Cow opposed the electrohippies action, arguing that it went against principles of free speech, but they also dismissed the notion that there is little difference between cyberspace and physical space: "Where a large physical mass is the currency of protest on the street, or at the ballot box, it is an irrelevancy on the Internet. Or more correctly, it is not always necessary . . . . But to think that it takes a lot of people to execute an act of civil disobedience on the Internet is naive. Programs make a difference, not people."[20]

Because it takes place online, hacktivism frees protestors from several constraints of the physical world. Most importantly, when activism takes place online political action is no longer relegated to where and when one happens to be. Maria Bakardjieva writes, "Ordinary people . . . have not been able to afford to 'leave what you are doing now and go' . . . The handiness of the Internet access to these institutions—from amid everyday life—now generates the feeling that they are within 'attainable reach,' that people, as citizens, can actually perform action onto them, that they are part of the subjective everyday lifeworld and not a detached 'province of reality.' Thus 'easy' may actually mean 'it is now possible for me to act politically from where I stand.'"[21] Also, because there is no longer a need to physically assemble, one need not risk direct bodily harm by engaging in protest activity. Thomas points out that a virtual presence can be a powerful tool when considering the legal implications of one's actions: "The virtual presence of the hacker is not enough to constitute a crime—what is always needed is a body, a real body, a live body."[22] In the case of distributed attacks, such as those enacted by the Zapatistas and the electrohippies, one need not have the skills of the hacker to participate; one need only have a computer and an Internet connection. Hugh Martin notes, "electronic protesting these days is a simple matter of downloading easy-to-use software from the Web, or of visiting a protest site where you can set your browser to bombard a target site with requests for information. Anyone can be a hacktivist."[23]

Whether greater numbers of protestors participating in electronic protest actions, such as denial of service attacks, provides greater legitimacy for the action depends on one's views concerning democratic practice, the importance of dissent, and the role of the media in civil society. Alain Touraine explains that protest and democracy are intertwined:

> Far from being antithetical, social movements and democracy are, in contrast, indissociable. On the one hand, if a political system regards social movements simply as violent expressions of demands that cannot possibly be satisfied, it ceases to be representative and loses the trust of the electorate. . . . A government that tries to legitimize its actions in terms of the constraints of the system loses its democratic character, even if it remains tolerant and liberal. On the other hand, a social movement can exist only if a collective action has social objectives, or in other words, recognizes that society has general interests or values. In other words, a social movement can exist only if collective action does not reduce political life to a confrontation between camps or classes, even though it organizes and extends conflicts.[24]

Acts of hacktivism serve mainly as a means for dissent or to voice grievances; as such, these actions create a space in which alternative viewpoints can be expressed and heard. The purpose of the electrohippies action against the WTO was to silence the WTO in order to open a space in which the concerns of anti-globalization activists could be heard. By silencing the WTO, they also drew media attention to their action. Dissent is an integral part of deliberative democracy. This is not to say that all forms of dissent are created equally. Burning down a factory that opponents claim is polluting the environment sends a strong message to the corporation that owns the factory, but is it ethical? Perhaps not, but it is certainly rational. J. Glenn Gray states, "A happy person will never—or almost never—give way to the destructive passions of rage and resentment. On the other hand, the unhappiness that arises from the frustration of action and consequently thwarted self-realization and deprivation of freedom is nearly bound to be violent."[25] The question then becomes whether there were other effective possibilities open to those that opposed the polluting corporation. Still, although ethicist John Rawls suggests that civil disobedience is a last resort after "the legal means of redress have proved to no avail," he notes that legal means need not have been completely exhausted.[26] Hannah Arendt notes that "Civil disobedience arises when a significant number of citizens have become convinced either that the normal channels of change no longer function, and grievances will not be heard or acted upon," although Arendt also notes the potential for disobedience in the face of governmental actions that move into realms of dubious legality.[27]

Secondly, there is the nature of the medium in which the protest action takes place. The online world can best be described as fluid and transient. Thus there is the issue of permanence and duration. Web pages are constantly altered and sites appear and disappear hourly. Denial of service attacks are likewise transitory; to perform them requires significant computing resources. Therefore, any act of hacktivism will necessarily be short-lived. Despite its transitory nature, hacktivism remains an important part of modern protest. John McKenzie argues, "as the site of power moves from physical locations into digital networks and as universal knowledge gives way to situated knowledges, new forms of resistance also emerge. Long-entrenched practices of political activism—street protests, strikes, sit-ins, boycotts—are becoming less and less effective and in their place have arisen practices of 'electronic civil disobedience' and 'hacktivism.'"[28] The ease with which website defacements can be remedied is likely one reason why hacktivists tend to disavow any concern for potential damage to the website.

In the online world, then, nothing is permanent. As such, one must consider acts of hacktivism as at least less harmful than destructive acts in the physical world. If one burns down a building as a means of protest, that building must be rebuilt, but if a web site is defaced, it can often be fixed quickly by uploading the original version again. However, some may see such acts as equivalent. Following HFG's hack of the *New York Times* website, Bernard Gwertzman, editor of the *New York Times* on the Web, stated, "This is the equivalent of somebody blowing up a press... A lot of people, I'm sure, were planning to read our coverage of the Starr report and were deprived of it."[29] Elsewhere, Gwertzman stated, "We consider this very serious. They are interfering with the press' ability to function."[30] But hacking is *not* the equivalent of blowing up a press. Hackers are not defacing property so much as they are defacing a presentation of self that can quickly be reclaimed.

By hacking the *New York Times* website, HFG was able to air grievances concerning the *New York Times* to both the *Times* and the general public by hijacking a well known and heavily trafficked website. Robert McChesney has pointed out that as the mass media have consolidated, viewpoints and frames have become less and less varied.[31] Hacktivism provides a way to express dissent with the same magnitude of those in the mass media by allowing protestors to temporarily hijack those media, providing the potential for a more level playing field of discussion.

Rawls provides a framework for considering justice based on a "veil of ignorance," in which the parties in the transaction would decide the justice of a particular situation without knowledge of which position they would hold.[32] For example, one may be quite accepting of the institution of slavery, so long as he or she was the owner and not the slave; for the situation to be considered truly just, one must find either position acceptable. Using such a framework, one could consider the relative power differential between the media and the individuals, especially in the case of Mitnick. The front page of the *New York Times* is a powerful means of demonizing an individual to millions of people. How can one correct such information? As Dean Barnlund and Franklyn Haiman explain, "When one person or a few people in a group or society possess all the guns, muscles, or money, and the others are relatively weak and helpless, optimum conditions do not exist for discussion, mutual influence, and democracy. Discussion in such circumstances occurs only at the sufferance of the powerful; and generous as these persons may sometimes be, they are not likely voluntarily to abdicate their power when vital interests are at stake."[33] From Rawls' perspective the power dynamic is so great as to make justice impossible. Rawls' theory of justice allows for inequalities but only if the inequalities are to the benefit of all, including the least advantaged in society.[34]

In considering the restriction of protest activities in residential neighborhoods, Haiman asks, "The question, I think, is what price a society is willing to pay to insure that the messages of minority groups are not screened out of the consciences of those to whom they are addressed. For once the principle is invoked that listeners may be granted some immunity from messages they think they would rather not hear, or which cause them annoyance, a Pandora's box of circumstances is opened in which the right of free speech could be effectively nullified."[35] In the information age, it is difficult for dissenters to be heard at the same volume as those who control media. It seems that Haiman's concerns still hold at this point—can one really have free speech if one cannot be heard? Can one really dissent if those you oppose can reach millions, as in the case of the *New York Times*? Such hijacking of the media can be seen in staged actions at media events such as press conferences or sporting events. Such action is similar to heckling, which Haig Bosmajian explains is an important element of civic discourse: "Although it may be more comfortable to silence the heckler, such action may be detrimental to the proper functioning of a democratic society."[36] Hijacking the media may be one way for dissenters to express their messages and be heard.

Third, there is the question of who is targeted. In the case of denial of service attacks the whole point is to disrupt the smooth functioning of the target organization—much like the sit-ins of the 1960s. In other cases, the hacked websites may be unrelated but serve as a means of mass-media that serves to equalize power between those who generally control the mass media and the hacktivists whose messages have been silenced my those media outlets. Here we find a case where the ethics become murkier. Unlike the "innocent bystanders" discussed by Haiman that were by no means innocent, some acts of hacktivism simply scan for unprotected servers and replace the page with the message of the hacktivists. What should be said of such collateral damage? In the case of completely unrelated websites, I would suggest that such actions are unethical. There are some exceptions, however, such as the case in which a group is protesting against those of a particular nation. As Haiman notes, "Every citizen who supports the status quo, either actively or by passive acquiescence, is a legitimate target for the communications of the dissenter."[37] Such hacktivism may function in a way similar to economic sanctions, which affect governments and citizens alike.

Fourth, there is the question of responsibility. Some may consider hacktivism to be something other than civil disobedience because it is less public than other forms of protest and because the hacktivists generally evade capture. Arendt observes that many point to Socrates and Thoreau who willingly accepted their punishment; "Their conduct is the joy of jurists because it seems to prove that disobedience to the law can be justified only if the lawbreaker is willing and even eager to accept punishment for his act."[38] Yet Howard Zinn asks, "Why must the citizen 'accept the result' of a decision he considers immoral," arguing, "to support a wrong rule of law does not automatically strengthen the right rule of law, indeed may weaken it."[39] One need not go to jail in order to participate in civil disobedience.[40]

Defacing a website or engaging in denial of service attacks can be an act of civil disobedience. There are, of course, hacks that do little more than engage in online vandalism, but in the case of the *New York Times* hack, for example, the hackers were protesting what they saw as unfair journalistic practices that amounted to libel. Markoff's front-page story describing Mitnick states that "as a teen-ager, [Mitnick] used a computer and a modem to break into a North American Air Defense Command computer, foreshadowing the 1983 movie 'War Games.'"[41] Markoff provides no evidence for this assertion, which Mitnick claims is completely false: "No way, no how did I break into NORAD. That's a complete myth. And I never attempted to access anything considered to be classified government systems."[42] In their coverage of the hack, the *Times* downplayed allegations against Markoff: "The group that took over the *Times* site directed some of its comments at John Markoff, a reporter for The Times who covered Mr. Mitnick's arrest."[43] But Markoff had done more than simply cover the arrest—he had taken an active role in tracking Mitnick down and by the time the hack occurred, Markoff had co-written two books about Mitnick and cut a movie deal from the book about Mitnick's pursuit and arrest.[44] Breaking into the *New York Times* website forced the *Times* (and other news outlets) to bring the controversy concerning Mitnick into the public arena.

The Rhetoric of Recent Hacktivism

Thousands of websites are hacked every day, and although many of them resort to the equivalent of graffiti tagging, leaving messages along the lines of "ZafT 0wnZ Ur B0x!!!!," some defacements are overtly political.[45] Kovacich writes, "The hackers of the world are using the Internet to communicate and attack systems on a global scale. Much of the attacks are aimed at totalitarian governments, government agencies, political parties, against the slaughter of animals for their fur, all of which can be considered politically-motivated attacks."[46] This section examines some recent politically motivated hacks to explore how hackers use the medium of the Internet to promote their messages.[47]

Although hacks that target a particular site still occur, they seem to be increasingly rare. The website itself is incidental to the message, serving only as a receptacle for the message. But not all parts of the website are created equally and hackers recognize that a homepage defacement is much more valuable in displaying their message than a random page in the website. This is demonstrated in two hacks by the hacker group RedHack. In one hack, a webpage is replaced by the simple message, "HackeD By RedHack HURRAY WORLD PROLETARIAN REVOLUTÝON."[48] However, when they defaced a homepage, they posted an elaborate image file and long message.[49] The image has the slogan "workers of the world unite!" in several languages surrounding the border of the image. At the top is a logo for RedHack with the Soviet hammer and sickle in the place of the "R" and a red hat on the "H," a symbol for Red Hat, a common version of Linux. An image of Lenin is prominently placed to the right. I did not recognize the language of the text, so I was unable to get a translation, but in these defacements I am focusing on the differences in approach rather than the text. In the language of graffiti, these hacks demonstrate the difference between a simple tag and an elaborate mural.

Another hacker group, Ayyildiz Team, uses website defacement to both spread a message and to comment on the nature of hacking itself.[50] As majestic orchestral music plays, the viewer first sees a large image with "Don't believe the Armenian lies" on the left and the lyrics to "Invaded" by Turkish metal band Notwithstanding.[51] The hack responds to accusations of genocide by the Turks against the Armenians. The hackers identify themselves by stating, "UNCLE H0tTurk Uykusuz001 And OzeLHarekat AyHan HeRo SAYS THERE IS NO FUCKING GENOCIDE." Although much of the hack is written in Turkish, the imagery is striking. The first photo shows a child lying on the ground and the second shows a close-up of a man hanging from a tree. The neck is elongated and his eyes are open. The hackers make a powerful emotional counterargument against the Armenians by juxtaposing these photos with the lines at the top, "Where's my granddad to tell me the truth??? He was massacred by the Armenians." The hackers take their main image from a website opposing System of a Down, a metal band comprised of Armenian-Americans who have tried to raise awareness of genocide against the Armenians by the Turks through songs (P.L.U.C.K.), benefit concerts, and public relations campaigns.[52] These hackers are waging their own counter-information campaign online.

The hackers define their website defacement not as a hack but as a way to enlighten the masses: "IT IS NOT HACKING OPERATION. IT IS ONLY IT IS ONLY SHOWING REALITY. DON'T PANIC. AYYILDIZ TEAM WAS HERE!" Other hackers more forcefully argue against the criminalization of hacking. Hackers from D.O.M team leave this message: "El hacking no es un delito es un buen hobby, Hay asesinos sueltos,hay violadores y ustedes piensan ke somos criminales?? en verdad estan locos, no eh tocado nada solo eh subido mi index."[53] (Translation: Hacking is not a crime, it is a good hobby, There are assassins loose, there are rapists and you think that we are criminals? In truth they are crazy, I have touched nothing, I have only uploaded my index). PowerDream also combines their message with a philosophy of hacking: "No War..! No Terror..! hack just for fun and real messages for test... lol (:"[54]

Some hackers use visual imagery to craft their arguments. For example, a defacement by anonyph states, "This is a cyber-protest against climatic change!! Stop contamination! Fuck to all governs that allow the contamination of the world!"[55] Above this text are two photos, one labeled "1918" and the other labeled "2004." The 1918 photo shows a large ice shelf that is non-existent in the 2004 photo. In each photo, there is a person in a small boat, providing symmetry to the photos and linking them together. In another website defacement, heIdI, a member of tw0team, places at the top of the page a photo of a man (possibly homeless) lying under garbage on the sidewalk. On the fence above him are the words "Contruindo Qualidade" (trans. "Building Quality"). The translation of the text reads:

> Shit, the world is coming to an end, fighting for power, fighting for possessions, and what you see is a lot of greed from those who have more, or countries fighting for stupid reasons. Global warming is here, but why all these "treaties/protocols" if the countries that are the most at blame are unwilling to give up their greed for capital? Exploitation and inequalities are the most common sights in this world, whilst people die of hunger/thirst and live in sub-human conditions, others couldn't care less. At least we have "faith."[56]

heIdI provides a strong visual counterpart to the anti-capitalist text. Rather than simply discussing the plight of those who "die of hunger/thirst and live in sub-human conditions," the hacker shows these conditions, all under the ironic caption "building quality."

When acting alone, hackers sometimes change their messages. For example, a hack by Uykusuz001, one of the members of Ayyildiz Team, replaced a site with the following message on a simple black background under a white crescent and star:

> h4(k3d
> [uykusuz001]
> 0n3 [Turk]-494!n57 7h3 w0r1d
> n0 w4r-f0r3v3r w0r1d p34(3
> ...4nd ju57!(3 f0r 411[57]

(Hacked, uykusuz001, one Turk against the world, no war – forever world peace . . . and justice for all.) This message is still political, but when acting alone the hacker no longer presumes to speak for the rest of the group and thus does not use the prefabricated message of Ayyildiz Team. Also, the hacker uses "leet speak," a stylized form of writing common in hacker culture. In doing so, the message becomes more universal, mirroring the general nature of the message, and the hacker chooses not to target a particular group or address a specific issue. This defacement also incorporates White Lion's anti-war song "When the Children Cry" to augment his or her anti-war message.

Some hacks are directed at current events in the Middle East. Delta Hacking Team left the following message on a defaced website: "Nuclear Energy is our right, Iranian is not Terrorist."[58] Iranian Hackers Sabotage makes a more general plea concerning the plight of Muslims in the current "War on Terror" and the war in Iraq:

> All Muslim's nation condemned all terorist activities in everywhere Do you think that all muslims are terrorists? we are for peace...humanity. friendshp, kindness this is wrong.. we all are brothers, Muslims has been more harmed by this kinde of actvities than the other believes Dont you guys see what has been hapenning to muslims in the last 50 years in Israel? Dont u see in iraq how many casualties have muslims pr day? Dont u see the attitude of americans towards muslims in goantanamo?"[59]

Both of these hackers paint an image of Iranians as anti-terrorist and peaceful. The message of Iranian Hackers Sabotage, although describing specific American and Israeli actions, seems directed to the world in general rather than to these specific countries—a "you" that is outside of these situations. Although the situations concerning Muslims in Iraq, Guantanamo, and Israel are each implied, the reader is expected to fill in the rest of the enthymeme. This allows the reader to become an active participant in constructing the argument and come to the conclusion that Muslims are under attack.

Four main themes emerge in this sampling of website defacements. First, there is an explicit political message in these hacks. In each hack, the audience does not seem to be specific except in two important ways—the hackers assume that the audience is informed and that the audience has already been somehow deceived. For example, the Ayyildiz Team hacks assume an understanding of the questions surrounding accusations of genocide against the Armenians and that the audience has already been targeted by "Armenian lies." At one point, they exclaim: "People! We call you! Don't forget Armenian lies! That's reality!" This assumes that the audience was already familiar with the accusations, but despite the prevalence of Turkish writing in the hack, the hack also has elements in English. Thus it seems aimed not only at Turks and Armenians, but the English speaking world as well. Delta Hacking Team's hack also seems directed at the English speaking world as an attempt to counter American (specifically then President George W. Bush's) descriptions of Iran as part of an "Axis of Evil" that promotes terrorism. Their wording—"nuclear energy is our right"—reinforces the assertion that the aim is the peaceful generation of electrical power. Had they used the term "nuclear power," the message could have been interpreted more readily as a military goal.

Second, the implied authors of these messages are also more universal and certainly more westernized than one would think, especially in the case of the Iranian Delta Hacking Team. There is no Arabic script on the site. The entire defacement, including the logo, is in English. Many of the hacks seem to follow this pattern. Iranian Hackers Sabotage not only wrote the defacement in English, but their handles (hacking names)—C0d3r, NT, Rupture, and LorD—are also English. Although anonyph hacked a Mexican website and identified themselves as Spanish, Mexican, and Argentine, they still wrote the text in English. Perhaps this reveals an implicit assumption that their target audiences—governments that allow the contamination of the world—are those that would understand English. Even the Turkish hacks have English interspersed throughout and some are completely in English or "leet."[60]

Third, some of these hacks reject the description of hacking as a criminal endeavor. In fact, Ayyildiz Team claims that they were not actually hacking. But if breaking into a website and defacing it is not hacking, then what is? Perhaps they are responding to the common misconception that hackers are breaking in to systems in order to steal information, generally for the purposes of identity theft. Political hacking, at least this form of it, does not seek to take anything from the website but its online presence. Hacktivists temporarily silence the voice of the website owner and replace it with their own. For the most part, the sites seem to be taken as a matter of convenience; the site itself did not seem to be the target. Rather, the sites serve only as a means to disseminate a message to more people. I previously discussed this as an ethical problem for the hacktivists. Even Zinn, who is quite celebratory of civil disobedience, argues that "the force of any act of civil disobedience must be focused clearly, discriminately on the object of protest."[61] However, despite the questionable ethics of taking over an unrelated site, one can see analogues in the offline world in stickering campaigns that attempt to get the message out to as many people as possible through sheer ubiquity.

Finally, hacktivists seem quite aware of the potential uses of their medium, incorporating sound and/or imagery into the website defacement to create and augment their message. Many of them seem to recognize the utility of prepackaging their hack into short, easily digestible messages. Rhetorical scholars have noted that society is moving away from detailed argument and toward a culture of the sound byte.[62] With some exceptions—Ayyildiz Team's lengthy text, for example—these hacks reflect an understanding of this cultural shift. But easily reproducible, short arguments also reflect the constraints of the medium and the action. A defaced website generally has a very short shelf life. If one is to make an impression, he or she must do so quickly and efficiently. When one may have only a few moments to make an impression, there is no time for the intricacies of a complex argument.

The Future of Protest?

Individuals that engage in hacktivism demonstrate a commitment to symbolic action as an integral part of democratic practice. Perhaps one product of hacktivism is what Richard Gregg refers to as the "ego function of the rhetoric of protest," in which the protestors engage in the action in order to gain psychic rehabilitation rather than to enact real change.[63] Acts of hacktivism may not accomplish much in the long term (at least not on a specific site), but such actions provide a way for activists to embrace the illusion that their words will be read by many people, despite their ephemeral nature.

Acts of hacktivism can also be considered image events. Kevin Deluca's explanation of how environmental groups uses image events seem well suited to hacktivists' use of the Internet as a political tool: "Although the image events of radical environmental groups are often spectacular, they are not the displays of the rulers but, rather, the discourse of subaltern counterpublics (Fraser, 1992, 123) who have purposely been excluded for political reasons from the forums of the public sphere by the rules of reason and the protocols of decorum."[64] That hacktivists can, to some extent, flaunt the protocols of decorum may be one source of its power. In an age of professionalized social movement organizations, hacktivism is one possible way for individuals to disseminate an uncensored message.[65] Hacktivism precludes any possibility that the message will be opposed in the sphere of argument because it works not by opening alternative spaces of discourse but by hijacking already existing ones and silencing all others in that sphere. For example, HFG silenced the *New York Times* by placing their own message on their website, if only for a brief period of time. Likewise, the electrohippies' action against the WTO silenced the WTO website in order to draw attention to their message. Despite its invisibility, the electrohippies action was certainly an image event.

But hacktivism may carry heavy consequences, for both the actors and those acted against, in the information age. Denial of service attacks are less publicized now and more often used as a form of "hackstortion" in which the hackers launch denial of service attacks as a way to extract money from their targets, but politically motivated denial of service attacks still take place. When Estonian officials decided to remove Soviet war monuments from their capital, local Russians rioted and looted in protest. But the battle also took place online. An article in *The Economist* describes the cyber-attacks: "Some have involved defacing Estonian websites, replacing the pages with Russian propaganda or bogus apologies. Most have concentrated on shutting them down. The attacks are intensifying. The number on May 9th—the day when Russia and its allies commemorate Hitler's defeat in Europe—was the biggest yet, says Hillar Aarelaid, who runs Estonia's cyber-warfare defences. At least six sites were all but inaccessible, including those of the foreign and justice ministries."[66]

Franklyn Haiman explains, "It would seem that even the 'rhetoric of the riot,' mindless and indiscriminate as it may be, has its positive function in contemporary America."[67] However, in an information society, the rhetoric of the online riot has consequences that go beyond the property and personal damage that may take place in a physical riot. As Thomas explains, "Hackers realize that at some level, *all* machines are insecure."[68] Much as civil disobedience calls into question the laws of the nation, electronic civil disobedience calls into question the security of the online world that many have come to depend on.

Hacktivism also blurs the line between the online and the offline worlds. Concerning the denial of service attacks against Estonia, *The Economist* article notes, "NATO has been paying special attention. 'If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?' asks a senior official in Brussels. Estonia's defence ministry goes further: a spokesman compares the attacks to those launched against America on September 11th 2001."[69] The full implications of politically motivated hacking are still being considered, but it seems that in an increasingly connected world such disruptions will become progressively more severe in impact; Marshall McLuhan, Quentin Fiore, and Jerome Agel declare that "real total war has become information war."[70] The lines between warfare and protest, the physical and the digital, are becoming more blurred.[71] Even so, such defacements and denial of service attacks have not yet reached the point at which one can reasonably equate them with the loss of life that would accompany a traditional military campaign.

As the boundaries between physical and digital space become more permeable, actions that take place in the digital realm have implications for the physical world, and in the digital realm protestors are able to transcend some of the constraints of corporeality and physical space. One hacktivist can automate the process of hacking with scripts to become quite prolific in his or her hacks. For example, according to Zone-h, as of May 24, 2007, uykusuz001, one of the hackers described above, had completed 430 total defacements, of which 324 were single IP and 106 were mass defacements, with 92.56 percent of them politically motivated. On January 19, 2012 that number had risen to 9291 total defacements, of which 4840 were single IP and 4451 were mass defacements. The ability to perform mass defacements is one of the core advantages of hacktivism and demonstrates the stark difference between website defacement and its closest physical analogs, graffiti and stickering.

Because the world has become increasingly wired, hacktivism is a useful rhetorical strategy. Norman Solomon notes that there was little media attention when the World Bank planned to hold meetings in cyberspace rather than in a physical location in Barcelona Spain to avoid disruption: "If global corporatization is to achieve its transnational potential, the discourse among power brokers and their favorite thinkers can happen anywhere at once—and nowhere in particular. Let the troublemakers try to interfere by doing civil disobedience in cyberspace!"[72] But this is exactly what is happening; people are engaging in online protest. And they must; Michael Margolis and David Resnick write, "The evidence shows that those who have been powerful in the past—the established organizations, the wealthy, and the privileged—are moving into cyberspace and taking their advantages with them."[73]

Haiman was quite clear that he was not suggesting a "lowering of the standards to be espoused for the ideal conduct of public discussion and debate. On the contrary, every effort should be made to help create the conditions under which the achievement of those standards becomes a possibility."[74] What Haiman calls for is a state in which dialogue can occur, but in a state of drastic inequality this is impossible. Calls for obedience to the rule of law and propriety serve only the existing structures of power and those who benefit from them.

Hacktivism levels the playing field to some extent. Tim Jordan argues that "hacktivists are not so much bending, twisting and reshaping information flows as creating alternative infrastructures to enable new types of flow.[75] In an information society, decentralizing discourse is an essential component of democracy. Lewis Friedland suggests, "as networks become structurally decentralized, even wider publics gain access to them in ways that lead to an increase in the rate and density of public exchange."[76] But decentralization is only part of the equation for creating the potential for greater equality among the various participants in the public sphere. There are still cases in which certain groups (e.g., government, corporations) are able to control the discourse in ways that silence alternative voices. Hacktivism allows dissent to be heard through the very channels that would silence them. Thus it seems that Haiman's assertion that the rhetoric of the streets should be held to different ethical standards still holds true in the digital realm. Four decades later, his words still raise a call of caution: "Perhaps the best one can do is to avoid the blithe assumption that the channels of rational communication are open to any and all who wish to use them."[77]

Notes

[1] See Franklyn S. Haiman, "Nonverbal Communication and the First Amendment: The Rhetoric of the Streets Revisited," *Quarterly Journal of Speech* 68, no. 4 (1982): 371-83, Franklyn S. Haiman, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," *Quarterly Journal of Speech* 53 (1967): 99-114.

[2] See "Fraud and Related Activity in Connection with Computers," Title 18 *U.S. Code*, Pts. 1030, 2006 ed.; *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.

[3] See Haig A. Bosmajian, "Freedom of Speech and the Heckler," *Western Speech* 36, no. 4 (1972): 218-32; Haig A. Bosmajian, "Obscenity and Protest," *Today's Speech* 18 (1970): 9-14; Robert J. Doolittle, "Riots as Symbolic: A Criticism and Approach," *Central States Speech Journal* 27 (1976): 310-17; Theodore Otto Windt, Jr., "The Diatribe: Last Resort for Protest," *Quarterly Journal of Speech* 58 (1972): 1-14.

[4] Thomas W. Benson and Bonnie Johnson, "The Rhetoric of Resistance: Confrontation with the Warmakers, Washington, D.C., October, 1967," *Today's Speech* 16 (1968): 35-36.

[5] See *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.

[6] Stefan Wray, "On Electronic Civil Disobedience," *Peace Review* 11, no. 1 (1999): 108.

[7] Winn Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction* (New York: Thunder's Mouth Press, 2000), 25.

[8] Marshall McLuhan, *Understanding Media: The Extensions of Man* (Cambridge, MA: MIT Press, 1994), 7.

[9] 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 May 6, 2011).

[10] Douglas Thomas, *Hacker Culture* (Minneapolis: University of Minnesota Press, 2002), 96.

[11] Ibid., 89.

[12] 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.

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

[14] Jill Lane, "Digital Zapatistas," *TDR: The Drama Review* 47, no. 2 (2003): 129-44.

[15] DJNZ and the Action Tool Development Group of the electrohippies collective, "Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?" *the electrohippies collective*, February, 2000, http://www.fraw.org.uk/projects/electrohippies/archive/op-01.html (accessed May 6, 2011), 3.

[16] Ibid., 2.

[17] See John Markoff, "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit," *New York Times*, July 4, 1994.

[18] See Robert Menta, "RIAA Site Hacked Again," *mp3newswire.net*, August 27, 2002, http://www.mp3newswire.net/stories/2002/hackedagain.html (accessed May 6, 2011); Robert Menta, "RIAA Web Site Hacked" *mp3newswire.net*, July 30, 2002, http://www.mp3newswire.net/stories/2002/riaahacked.html (accessed May 6, 2011); Robert Menta, "A Third Hack on RIAA Site," mp3newswire.net, August 31, 2002, http://www.mp3newswire.net/stories/2002/thirdhack.html (accessed May 6, 2011).

[19] DJNZ and collective, *Occasional Paper No. 1*, 5.

[20] Oxblood Ruffin, "Hacktivismo," *Cult of the Dead Cow*, July 17, 2000, http://w3.cultdeadcow.com/cms/2000/07/hacktivismo.html (accessed May 6, 2011).

[21] Maria Bakardjieva, *Internet Society: The Internet in Everyday Life* (London: Sage, 2005), 127.

[22] Thomas, *Hacker Culture*, 182.

[23] Hugh J. Martin, "Hacktivism: The New Protest Movement?" *Spark-Online*, 2000, http://www.spark-online.com/april00/trends/martin.html (accessed May 6, 2011), para. 6.

[24] Alain Touraine, *What is Democracy?* trans. David Macey (Boulder, CO: Westview Press, 1997), 57.

[25] J. Glenn Gray, *On Understanding Violence Philosophically, and Other Essays* (New York: Harper & Row, 1970), 29.

[26] John Rawls, *A Theory of Justice* (Cambridge, MA: Belknap Press of Harvard University Press, 1971), 373.

[27] Hannah Arendt, *Crises of the Republic; Lying in Politics, Civil Disobedience, on Violence, Thoughts on Politics, and Revolution* (New York: Harcourt Brace Jovanovich, 1972), 74.

[28] John McKenzie "!Nt3rh4ckt!V!Ty," *Style* 33, no. 2 (1999): para. 32.

[29] David Noack, "Hack Attack Sends Chill through News Web Sites," *Editor & Publisher*, September 19, 1998.

[30] Arik Hesseldahl, "All the News That's Fit to Hack," *Wired News*, September 14, 1998, http://www.wired.com/news/politics/0,1283,14990,00.html (accessed May 6, 2011), para. 24.

[31] See Robert Waterman McChesney, *Corporate Media and the Threat to Democracy* (New York: Seven Stories Press, 1997).

[32] Rawls, *A Theory of Justice*.

[33] Dean C. Barnlund and Franklyn Saul Haiman, *The Dynamics of Discussion* (Boston: Houghton Mifflin, 1960), 12.

[34] See Rawls, *A Theory of Justice*, 78-82.

[35] Haiman, "The Rhetoric of the Streets," 106.

[36] Bosmajian, "Freedom of Speech and the Heckler," 219.

[37] Haiman, "The Rhetoric of the Streets," 105-6.

[38] Arendt, *Crises of the Republic*, 51-52.

[39] Howard Zinn, *Disobedience and Democracy: Nine Fallacies on Law and Order* (New York: Random House, 1968), 27.

[40] See Ibid., 121.

[41] Markoff, "Cyberspace's Most Wanted."

[42] Adam L. Penenberg, "Mitnick Speaks!" Forbes.com, April 5, 1999, http://www.forbes.com /1999/04/05/feat.html (accessed May 6, 2011).

[43] Amy Harmon, "Hacker Group Commandeers the New York Times Web Site," *New York Times*, September 14, 1998.

[44] See Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Simon & Schuster, 1991); 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). The movie, *Track Down*, which has been heavily criticized, both in terms of artistic merit and accuracy, was finally released in 2004 on DVD.

[45] A casual examination of www.zone-h.org, a security site that maintains an archive of website defacements, demonstrates the sheer quantity of websites that are hacked every day. For example, at 12.45 p.m. on May 5, 2011, the site had already logged 5522 website defacements.

[46] Gerald L. Kovacich, "Hackers: Freedom Fighters of the 21st Century," *Computers & Security* 18, no. 7 (1999): 575.

[47] Unless noted otherwise, all of these hacks were retrieved from www.zone-h.org but at the time I retrieved them, most of the website hacks were still live. Although there are many spelling and grammatical errors, I have chosen to leave them uncorrected in the interest of accuracy.

[48] The hacked webpage was found on http://www.teolandia.ba.gov.br/fotos

[49] The hacked webpage was found on http://gokceada.gov.tr

[50] The hacked webpage was found on http://www.cheu.gov.hk/eng

[51] A similar image can be found at http://www.anti-soad.org/ (no longer active).

[52] The website, Anti-Soad.Org, is no longer active, but was retrieved August 13, 2007. For System of a Down's efforts, see "System of Down Steps up Armenian Genocide Awareness Campaign." *Armenian National Committee of America*, May 1, 2001. http://www.anca.org /press_releases/press_releases.php?prid=75 (accessed May 6, 2011).

[53] The hacked webpage was found on http://www.fosis.gov.cl

[54] The hacked webpages were found on http://chwcc.bjchy.gov.cn/hacked.html and http://distamben.kalsel.go.id/delta.php

[55] The hacked webpage was found on http://extranet.isssteson.gob.mx

[56] The hacked webpage was found on http://www1.thaicyberu.go.th. The text was translated from Brazilian Portuguese by Nuno Ribeiro.

[57] The hacked webpages were found on http://music.zggs.gov.cn/eng and http://qc.zggs.gov.cn/Qcyg

[58] The hacked webpage was found on http://distamben.kalsel.go.id/delta.php

[59] The hacked webpages were found on http://jam1.kids.krs.yahoo.com/index.htm, http://jam2.kids.krs.yahoo.com /index.htm, http://jam3.kids.krs.yahoo.com, and http://kr.olympus.kids.yahoo.com

[60] PowerDream's defacement of http://chwcc.bjchy.gov.cn/hacked.html is one example of Turkish hackers who replaced the site with completely English text.

[61] Zinn, *Disobedience and Democracy*, 121.

[62] See J. Michael Hogan, *The Nuclear Freeze Campaign: Rhetoric and Foreign Policy in the Telepolitical Age* (East Lansing: Michigan State University Press, 1994); Kathleen Hall Jamieson, *Eloquence in an Electronic Age: The Transformation of Political Speechmaking* (New York: Oxford University Press, 1988).

[63] Richard B. Gregg, "The Ego-Function of the Rhetoric of Protest," *Philosophy and Rhetoric* 4 (1971): 74.

[64] Kevin Michael DeLuca, *Image Politics: The New Rhetoric of Environmental Activism* (New York: Guilford Press, 1999), 20.

[65] For more on the professionalization of social movements, see John D. McCarthy and Mayer N. Zald, "The Trend of Social Movements in America: Professionalization and Resource Mobilization," in *Social Movements in an Organizational Society: Collected Essays*, ed. Mayer N. Zald and John D. McCarthy, 337-91 (New Brunswick, NJ: Transaction Books, 1987); Suzanne Staggenborg, "The Consequences of Professionalization and Formalization in the Pro-Choice Movement," *American Sociological Review* 53, no. 4 (1988): 585-605.

[66] "A Cyber-Riot." *The Economist*, May 12, 2007.

[67] Haiman, "The Rhetoric of the Streets," 105.

[68] Thomas, *Hacker Culture*, 88.

[69] "A Cyber-Riot."

[70] Marshall McLuhan, Quentin Fiore, and Jerome Agel, *The Medium Is the Massage: An Inventory of Effects* (San Francisco, CA: HardWired, 1996), 138.

[71] See Brett Lunceford, "Cyberwar: The Future of War?" in *War and the Media: Essays on News Reporting, Propaganda and Popular Culture*, ed. Paul M. Haridakis, Barbara S. Hugenberg, and Stanley T. Wearden, 238-51 (Jefferson, NC: McFarland, 2009).

[72] Norman Solomon, "Hiding out in Cyberspace," *The Humanist* 61, no. 4 (2001): 17.

[73] Michael Margolis and David Resnick, *Politics as Usual: The Cyberspace "Revolution"*, *Contemporary American Politics* (Thousand Oaks, CA: Sage Publications, 2000), 208.

[74] Haiman, "The Rhetoric of the Streets," 114.

[75] Tim Jordan, *Activism!: Direct Action, Hacktivism and the Future of Society* (London: Reaktion Books, 2002), 135.

[76] Lewis A. Friedland, "Electronic Democracy and the New Citizenship," *Media, Culture & Society* 18, no. 2 (1996): 187.

[77] Haiman, "The Rhetoric of the Streets," 114.