Hacktivism and the Future of Political Participation

A thesis presented by

Alexandra Whitney Samuel

to the Department of Government in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the subject of Political Science

Harvard University
Cambridge, Massachusetts

September 2004

Hacktivism and the Future of Political Participation

Thesis Advisor: Prof. Sidney Verba **Alexandra Samuel**

Abstract

This dissertation looks at the phenomenon of hacktivism: the marriage of political activism and computer hacking. It defines hacktivism as the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development.

The dissertation uses data from fifty-one interviews in conjunction with additional primary and secondary source material. This data is used to construct a taxonomy of hacktivism, and to apply the taxonomy to three core issues in political participation.

Chapter 2 presents a taxonomy of hacktivism defined by variation in hacktivist origins (in the hacker-programmer or artist-activist worlds) and orientations (transgressive or outlaw). The dissertation identifies three distinct types of hacktivism: political cracking, which consists of illegal actions like web site defacements and redirects; performative hacktivism, which consists of legally nebulous actions like virtual sit-ins and web site parodies; and political coding, which consists of political software development.

The taxonomy illuminates several key questions in political participation, each examined in a different chapter. Chapter 3 focuses on the role of identity incentives in shaping political participation, and finds a strong correlation between hacktivist origins and the type of hacktivism engaged in. Chapter 4 looks at political coders' strategy of

policy circumvention, which focuses on nullifying rather than changing a targeted law or policy. The success of this strategy depends on political entrepreneurs, low costs of failure, and high political costs of repression. Chapter 5 examines deliberative democrats' suggestion that the Internet may constitute a new public sphere, friendly to democratic discourse. It suggests that variation in how hacktivists handle speech rights and anonymity challenges proceduralist visions of deliberative democracy.

After reflecting on the themes that unite the dissertation, the conclusion reflects on how the post 9/11 political climate has heightened the pressure to erroneously treat hacktivism as cyberterrorism. The author hopes that the rising fortunes of political coding, which is increasingly legitimated by both governments and businesses, will ensure a continued space for hacktivism within the repertoire of political contention.

Acknowledgements

I owe a tremendous debt of gratitude to the many people who made this dissertation possible. The list begins with my very patient and supportive committee, chaired by Prof. Sidney Verba of Harvard University, and including Prof. Torben Iversen (also of Harvard) and Prof. Richard Johnston of the University of British Columbia. All three of them embraced my somewhat unusual topic with remarkable enthusiasm, and helped me shape it into a research project that could speak to political science scholars as well as Internet researchers.

For his great persistence and generous comments I must also thank Prof. Peter Hall of Harvard University, whose early guidance helped me find my way to a feasible area for research. Prof. Peter Shane of Carnegie Mellon University helped shape the paper on hacktivism and deliberation that became the basis for Chapter 5 of the dissertation, and was an extremely helpful and patient editor in the course of preparing that research for publication. Prof. Chip Hauss of George Mason University helped me to find an approach to hacktivism that speaks to the larger community of citizen engagement scholarship, and offered comments on the various pieces of the dissertation that made their way into our joint research. Anthony Williams, now of the London School of Economics, was the first person to introduce me to hacktivism during our collaboration on the *Governance in the Digital Economy* research program.

Institutional support for the dissertation was provided by the National Science Foundation, whose graduate research fellowship supported my early research into the Internet and politics. The German Academic Exchange Service (DAAD) provided

funding for my field research in Germany and the Netherlands, and Harvard's Center for European Studies provided earlier support for the language training that made this research possible. The Political Science Department at the University of British Columbia offered me an institutional home while I completed my dissertation on the opposite side of the continent from the department at Harvard, and provided a terrific opportunity for me to develop my work on Internet politics as a lecturer in its department.

For their longstanding personal support of this project I must thank two people in particular: my husband, Rob Cottingham, and my mother, Deborah Hobson. Both of them extended themselves on every personal and financial front so that I could complete the dissertation, and both of them provided very practical support for its completion through their assistance with proofreading and (in Rob's case) web development.

Finally and perhaps above all, I must thank the more than fifty men and women who very generously agreed to be interviewed for this dissertation. Their cooperation not only made the dissertation possible, but also made it hugely enjoyable, since my interactions with this group were the highlight of the entire dissertation process. The people who fall into the varied universe that I term "hacktivism" are an exceptionally intelligent, engaging, and dedicated bunch. It was a privilege to meet, IRC or correspond with each of them, and I only hope that my dissertation can in some way capture their remarkable contribution to politics in the digital age.

Table of Contents

Table of Tables

Table of Figures

Chapter 1

Introduction: Into the world of hacktivism

January 1997: Visitors to www.plannedparenthood.com are greeted with the words, "Welcome to the Planned Parenthood Home Page!" above an ad for the anti-abortion book, "The Cost of Abortion." The web site is operated not by Planned Parenthood, but by anti-abortion activist Richard Bucci.

April 1998: Visitors to Mexican President Zedillo's web page find that the site has slowed to a crawl. A "virtual sit-in" that has overwhelmed the web site with traffic, in an action aimed at drawing attention to the Zapatista rebellion.

June 2000: Visitors to nike.com find themselves reading information about the problems of global capitalism. Nike's web site has been redirected to the web site of s11, an anti-globalization group.

September 2001: Visitors to the web site of Iran's Ministry of the Interior are met with a picture of Osama bin Laden, and the caption "Osama die." The web site's defacers say that they are "outraged at the acts of terrorism and such which are taking place in this day in [sic] age."[1]

February 2003: Chinese web surfers can visit censored web sites like CNN, NPR, and Playboy. A new software tool lets surfers illegally circumvent China's Internet firewall.

Across the political spectrum and around the world, incidents like these have emerged to spawn a new entry into the political lexicon: hacktivism. Commonly defined as the marriage of political activism and computer hacking (Denning 1999; National Infrastructure Protection Center 2001), hacktivism combines the transgressive politics of

---

[1] One dilemma in reproducing the many quotations from web sites, e-mails, and online chats that are contained in this dissertation is that Internet communications tend to be more relaxed about grammar and spelling. For this reason, as well as due to the fact that many of these quotations come from sources for whom English is a second language, the quotations contained in this dissertation would include a distracting number of typographical, spelling and grammatical errors if reproduced entirely verbatim. As a result, I have copy edited the text of my own IRC and e-mail interviews in order to correct the majority of these errors, making exceptions in cases where deviations from standard written English convey useful information or relevant context, or where I have any grounds for imagining the deviations were deliberate. I have not copy edited quotations from web site defacements or other online materials, since copyediting these sources might make it difficult for interested readers to track down the quotations in their original online contexts; nor have I used the convention of inserting [sic] to denote each anomaly, since that might prove overly distracting. Because all quotations from such sources were inserted into this text by direct copy-and-pasting, I ask for the reader's trust that any anomalies are reproduced from the original text, and not the accident of this author.

civil disobedience with the technologies and techniques of computer hackers. The result has been the rapid explosion and diffusion of a digital repertoire of political transgression, harnessed to a wide range of political causes.

This dissertation is the first empirical study of hacktivism and the people who engage in it. It is based on three years of research, including online and face-to-face interviews with more than fifty people who are directly or indirectly involved in hacktivist activities. While not all of these interview subjects define themselves as hacktivists, all of them have participated in projects that meet the definition of hacktivism that guides this dissertation:

hacktivism is the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends.

This definition attempts to bridge and consolidate the various definitions that have appeared in the small literature on hacktivism reviewed below. Denning's influential 1999 paper defines hacktivism as "the marriage of hacking and activism. It covers operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage."(Denning 1999) Milone uses the term hacktivism to apply to online activism, "[w]hen such activism manifests itself in the form of surreptitious computer access or the dissemination of potentially disruptive and/or subversive software."(Milone 2002) Jordan and Taylor describe hacktivism more broadly than I do, calling it " a combination of grassroots political protest with computer hacking" (Jordan and Taylor 2004); elsewhere Jordan defines it as "politically motivated hacking" (Jordan 2002). Vegh's definition is similarly inclusive: "[h]acktivism is a politically motivated single incident online action, or a campaign

thereof, taken by non-state actors in retaliation to express disapproval or to call attention to an issue advocated by the activists."(Vegh 2003)

While none of these definitions contradict the definition that guides this dissertation, the present phrasing offers several advantages. First, by specifying that hacktivism is nonviolent, it differentiates hacktivism from cyberterrorist acts that harm human beings. Second, by specifying that hacktivism involves illegal or legally ambiguous activity, it differentiates hacktivism from non-transgressive forms of online activism. Third, by generalizing hacktivism to encompass any use of digital tools, it explicitly includes all forms of nonviolent, transgressive digital actions that have sometimes been labeled hacktivism. In other words, it is the broadest possible definition of hacktivism that fits the dual criteria of transgression and nonviolence. This definition situates hacktivism in a political universe that is bounded on all sides by related but distinct types of activity, as per Figure 1.

The lines that separate hacktivism from related areas of political (and apolitical) activity are tactical, principled, and cultural. At a tactical level, hacktivists adopt tools and strategies that are more direct and transgressive than the tools used by online activists, because they believe that the confrontational tactics of hacktivism can be more effective than more conventional forms of online activism. For reasons of principle, they stop well short of cyberterrorism out of respect for human welfare; and turn from hacking to hacktivism because they believe their skills should be harnessed to meaningful social ends. And for cultural as well as tactical reasons, they diverge from the tradition of offline civil disobedience in order to tackle issues on the digital playing field: this field is

both their home turf, and (many hacktivists believe) an increasingly powerful political realm.

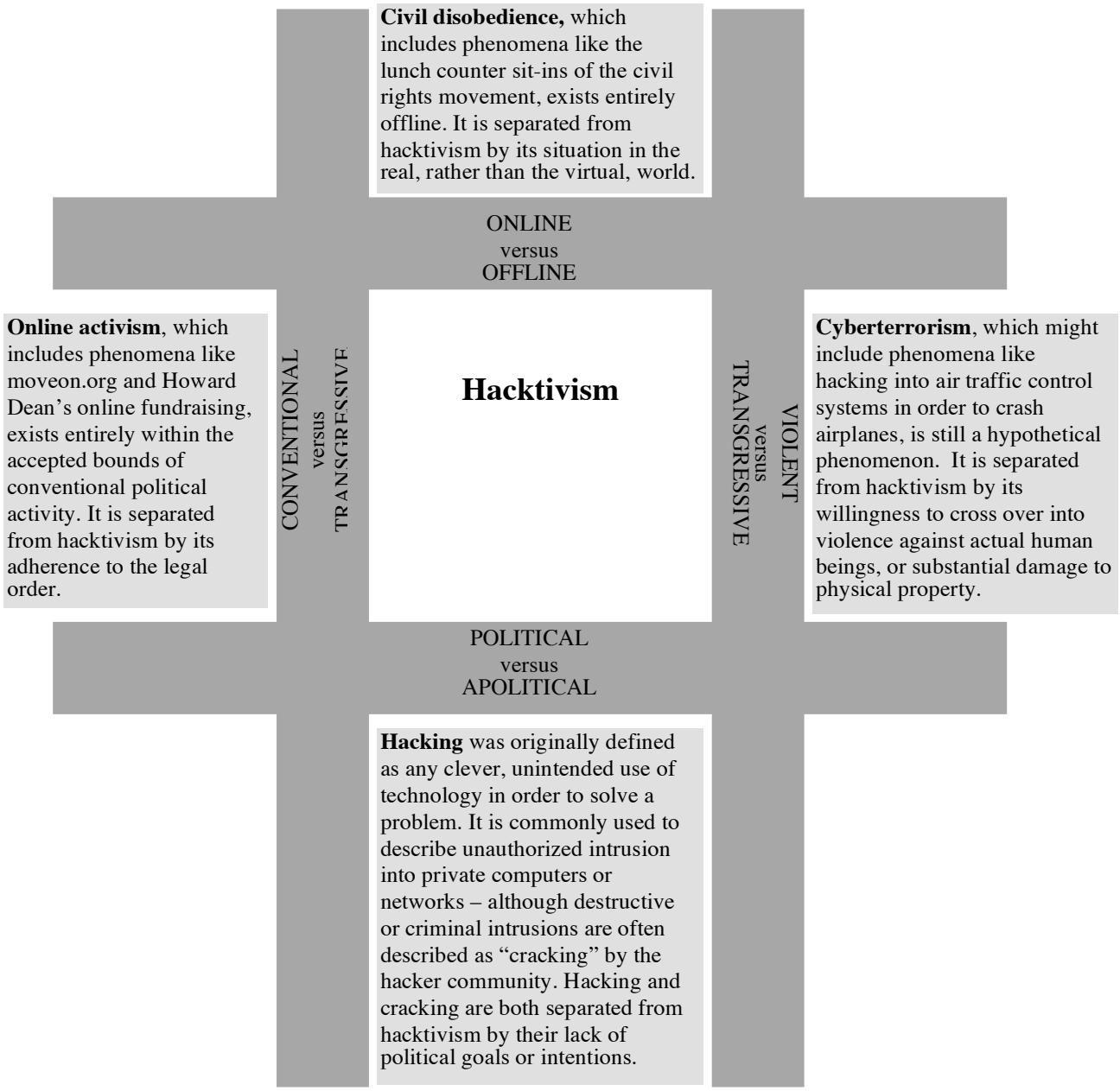


Figure 1. The boundaries of hacktivism

These tactical, principled, and cultural choices have birthed hacktivism as a loose-knit movement that is defined by its repertoire of contention. The "repertoire" concept comes from Tilly, who observed that social movements must draw on a limited repertoire of collective actions, and that this repertoire changes only over time (Tilly 1978). For movements that are choosing among tactical options, a key strategic choice is whether to pursue transgressive tactics:

> The use of transgressive forms offers the advantages of surprise, uncertainty, and novelty, but contained forms of contention have the advantage of being accepted, familiar, and relatively easy to employ by claimants without special resources or willingness to incur costs and take great risks.(McAdam, Tarrow, and Tilly 2001)

In the digital age, an equally important choice is whether to adopt on- or offline tactics, or some combination of the two. The growth and power of the Internet makes it a crucial space for contention, because in the Internet era, "control of communication networks becomes the lever by which interests and values are transformed in guiding norms of human behavior."(Castells 2001) For social movements,

> the many-to-many and one-to-many characteristics of the Internet multiply manifold the access points for publicity and information in the political system. The global dimension of the Web facilitates transnational movements transcending the boundaries of the nation-state. The linkage capacity strengthens alliances and coalitions. Moreover…the values that pervade many transnational advocacy networks….seem highly conducive to the irreverent, egalitarian, and libertarian character of the cyber-culture.(Norris 2001)

And for movements that also employ offline tactics, digital tools can "operate as a powerful facilitator through 'the maintenance of dispersed face-to-face networks.'" (Calhoun 1998, quoted in Diani 2001) Hacktivists' decision to employ online tactics is thus as politically substantive as their decision to employ transgressive tactics, drawing the crucial lines that divide hacktivists from other types of political actors (see t will be detailed in Chapter 2.

Table 1).

This dissertation approaches the phenomenon of hacktivism in two ways. First, it maps the parameters of hacktivism by creating a taxonomy of hacktivism's origins, orientations, and types. Second, it uses hacktivism's unique constellation of characteristics as a testing ground for several distinct questions about political participation.

This introductory chapter sets the stage for both pieces of the dissertation. It begins by outlining the dimensions of hacktivism in greater detail, in order to clarify exactly which types of digital transgression are under examination. As part of this outline it describes each of the forms of hacktivism, offers a chronology highlighting some of the most notorious instances of hacktivism, and introduces the taxonomy of hacktivism that will be detailed in Chapter 2.

Table 1: Different activist repertoires: some examples

	Offline	**Online**
Conventional	**Activism:** Voting Electioneering Non-violent protest marches Boycotts	**Online activism:** Online voting Online campaign donations Online petitions
Transgressive	**Civil disobedience:** Sit-ins Barricades Political graffiti Wildcat strikes Underground presses Political theater Sabotage	**Hacktivism:** Web site defacements Web site redirects Denial-of-service attacks Information theft Site parodies Virtual sit-ins Virtual sabotage Software development

Violent	**Terrorism:** Political bombing Political hijacking Tree spiking	**Cyberterrorism:** Hacking air traffic control Hacking power grid (*note: to date these examples are purely hypothetical)*

The introduction then moves onto the second part of the dissertation: using hacktivism as a window on key questions in political science. It provides a brief overview of the three questions that will be addressed in chapters 3 through 5: Why do people choose to participate in collective political action? When do political actors pursue policy circumvention, rather than policy change? Can the Internet foster new, deliberative forms of political participation? The last section of the introduction clarifies the dissertation's perspective and methodology. It situates the research in the small body of existing work on hacktivism, and describes the dissertation's research methodology.

The phenomenon of hacktivism

The phenomenon loosely known as hacktivism actually comprises at least nine distinct forms of electronic mischief: site defacements, site redirects, denial-of-service attacks, information theft, information theft and distribution, site parodies, virtual sabotage and software development.

Some norms are common to all forms of hacktivism. Hacker culture puts a premium on humor, as does the artist-activist scene from which many hacktivists emerge; no surprise, then, that many hacktions use humor to make their point. Hacktivists usually endeavor to draw attention to their hacktions, whether by contacting the media or by

submitting a defacement to a defacement "mirror" so that it can be preserved for posterity[2]. And hacktivists usually take some pride in their technological prowess – their ability to implement hacktions in an efficient or innovative manner.

But there are also important differences between each form of hacktivism. Different forms of hacktivism reference different political cultures, represent different political orientations, and lend themselves to different kinds of political statements. These differences mean that hacktivists' tactical choices about which forms of hacktivism to engage in represent larger differences in the character of different types of hacktivism. To understand the character of hacktivism, it is therefore crucial to understand what constitutes each of its forms. This requires a brief definition and illustration of each form in turn.

Site defacements consist of hacking into a web server and replacing a web page with a new page bearing some sort of message. An apolitical web site defacement might contain a simple text message like "this page owned by hax0r!", a list of "greetz" to particular fellow hackers, or some sort of (often pornographic) image. A hacktivist web site defacement, in contrast, contains a political message. The message is usually a criticism of the organization that has been hacked, or of some other cause or organization with which it is associated (even if the only association the target web site's nationality).

---

[2] Thanks to the volume of defacements, the biggest mirrors (Attrition and alldas) have stopped archiving defacements. alldas has gone offline entirely; Attrition stopped maintaining its archive in April 2001 (not even halfway through the WFD's lifespan) but has preserved its records of defacements from 1995-2001. Zone-H maintains a defacement list but its "mirror" contains only statistics about each attack, rather than an archive of the defacement itself. As Attrition explained the problem when it shut down its mirroring operation:

> What began as a small collection of web site defacement mirrors soon turned into a near 24/7 chore of keeping it up to date. In the last month, we have experienced single days of mirroring over 100 defaced web sites, over three times the total for 1995 and 1996 combined.("Attrition: Evolution" 2001)

Site defacements may target a single web page or site, but it is quite common to see "mass defacements" which replace tens, hundreds, or even thousands of web sites with the same defacement.

One early example of a site defacement was an attack on the US Department of Justice Web Server. In 1996 an anonymous hacker defaced the DoJ site to protest the Communications Decency Act (CDA). The CDA attracted the ire of the Internet community with its provisions for screening offensive material online. The DoJ defacement protested the CDA with a range of images and invective, such as:

> Free speech in the land of the free? Arms in the home of the brave? Privacy in a state of wiretaps and government intrusion? Unreasonable searches? We are a little behind our 1984 deadline, but working slowly one amendment at a time. It is hard to trick hundreds of millions of people out of their freedoms, but we should be complete within a decade.("Site defacement, US Dept. of Justice" 1996)

The DoJ hack is quite different in character from the defacements that have taken place in the context of subsequent international "cyberwars" between hacktivists. A typical defacement comes from Doctor Nuker, a member of the Pakistani Hackerz Club. Doctor Nuker frequently targets US, Indian and Israeli web sites, replacing their content with messages about human rights violations in Kashmir or Palestine. Using one such defacement to explain his overall approach, Nuker wrote:

> I can't go and fight for all the nations suffering, but i can do something to make the world know about the injustice going around. Defacing a websites will cost nothing to the target….United Nations is responsible to solve disputes among different countries. The United States being the "super power" loves to intercept any country in any of their internal affairs, they do use their powers when they see some income.but loves to neglect in the same way when it comes to the "real" problems. (Doctor Nuker 1999)

Defacements remain the most common form of hacktivism. Between defacements of single sites, and mass defacements that target many web sites at once, thousands of web sites have been defaced by hacktivists in the course of the past decade.

Site redirects involve hacking into a web server and changing its addressing so that would-be visitors to the site are instead redirected to an alternative site, usually one that is critical of the hacked site.

One example of a hacktivist site redirect occurred in 1999, when an anonymous hacker redirected a KKK web site to the anti-bigotry web site of the organization HateWatch. That redirect packed a double wallop; since the director of HateWatch had recently been quoted as critical of hacktivism, the attack was seen as embarrassing to HateWatch as well as being a hit on the KKK (Glave 1999).

Denial of service (DoS) attacks are a common and powerful way to wreak online havoc, but have been only rarely used by hacktivists. A DoS attack is

> an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services. Such attacks are not designed to gain access to the systems.
>
> A DoS attack can be perpetrated in a number of ways. There are three basic types of attack:
> 1. consumption of computational resources, such as bandwidth, disk space or CPU time
> 2. disruption of configuration information, such as routing information
> 3. disruption of physical network components.
>
> In a distributed attack [DDoS], the attacking computer hosts are often personal computers with broadband connections to the Internet that have been compromised by viruses that allow the perpetrator to remotely control the machine and direct the attack. With enough such slave hosts, the services of even the largest and most well-connected websites can be denied.("Denial-of-service attack" 2004)

A DoS attack can target a single company or organization, or it might target many different Internet gateways in order to shut down huge parts of the Net, slowing worldwide Internet traffic to a crawl. Next to computer viruses, DoS attacks probably constitute the most widely recognized form of illegal hacking (“cracking”), because DoS attacks on web sites like Yahoo and Google have been responsible for widespread, well-publicized Internet slowdowns and outages.

One instance of a hacktivist DoS attack was the 2001 attack on US web sites by Chinese hackers. As part of a cyberwar precipitated by a collision between Chinese and US military planes, Chinese hackers launched DoS attacks on hundreds of US web sites (Delio 2001). Ultimately these attacks did not appear to have a major effect on the speed of network access within the United States.

Information theft consists of hacking into a private network and stealing information. While the hack is publicized (and proof offered), the goal is often to embarrass the organization with the laxness of its information security, rather than to get hold of the information itself. In some cases, however, hacktivists publish information stolen online as part of the effect.

One reported case of hacktivist information theft preceded the 2001 meetings of the World Economic Forum in Davos, Switzerland. Hacktivists broke into the WEF's computer system and stole personal information on conference participants, including web sites, e-mail addresses, and travel itineraries. The hacktivists then placed the information on a computer disk, and sent it to a Swiss newspaper (McDonald 2001).

Virtual sabotage consists of online activities designed to manipulate or damage the information technologies of the target. This includes the creation of viruses or worms: self-executing software programs that propagate and distribute messages or sabotage. Viruses, like other forms of electronic sabotage, can vary tremendously in their level of destruction. At the most benign level, they manipulate a system only in order to replicate and spread the virus to other computers; at a more invasive level, they can forward or even destroy private data.

An instance of hacktivist sabotage was the 2001 InJustice worm, which replicated itself by infecting Microsoft's Outlook Express e-mail program, and sending itself to contacts listed in the address book. The message it delivered contained an attachment that began by apologizing for the intrusion, before telling the reader about the death of a Palestinian boy during a conflict between Palestinian protesters and the Israeli military (Weisman 2001).

Virtual sit-ins get hundreds, thousands, or even hundreds of thousands of protesters to rapidly reload web pages on targeted servers, overloading them with traffic until they slow down or crash. While a lone or small group entrepreneur sets up the virtual sit-in code, the success of this tactic depends on the volume of participants; the more people participate, the more the target server gets overloaded. It is the mass nature of the attack (the requirement that actual human beings visit the virtual sit-in page) that differentiates it from the distributed denial-of-service attack. As a mass form of hacktivism, virtual sit-ins can also lay claim to being a more democratic or representative form of hacktivism.

Some of the biggest sit-ins have been organized by the Electronic Disturbance Theater, which developed software that it has since made available to other groups. Instead of asking participants to continually hit the reload button, the EDT created a bit of downloadable code that automatically refreshed the target web page every few seconds. In this way the EDT ensured a steady stream of page requests to the target server, with only minimal effort required from protest participants.

The virtual sit-in technique promulgated by the EDT was adopted by a now-defunct British group, the electrohippies. The e-hippies were most active on globalization

issues, staging sit-ins during the WTO's meetings in Seattle, and during the 2001 Free Trade Area of the Americas meeting in Quebec City. The virtual sit-in they staged during the WTO's Seattle meeting may be the most successful one ever, if we measure success by the number of participants: the electrohippies reported over 237,000 hits on the sit-in web site (MacMillan 1999).

Site parodies spoof a target organization, often by imitating the appearance of its web site, and by locating the spoof at a URL (web address) that is likely to be confused with the address of the original (spoofed) site. While this is arguably the least transgressive form of hacktivism, it can still provoke outrage and even legal action from its target.

One of the most notorious site parodies to date was ®™ark's spoof of the WTO's web site. In November 1999, immediately before the WTO's Seattle meeting, ®™ark (pronounced "art mark") unveiled an anti-globalization web site at http://www.gatt.org. The site's web address capitalized on possible confusion between the WTO and the GATT, its predecessor organization; the site's design maximized that confusion by replicating the look and feel of the WTO's official site. But if the URL and appearance of the site suggested that it was an official WTO site, the content did not; the site's content was highly critical of the WTO and global economic integration more generally. In response, the WTO threatened (but did not pursue) legal action. In 2000, ®™ark transferred the GATT domain to the Yes Men, a group of activist "impostors" who now maintain the site.

Software development can constitute hacktivism if the software tools serve specific political purposes. These tools are usually created and distributed as open source

software, which means that they are free, and that anyone can modify the code – allowing for collaboration and continuous improvement.

One example of hacktivist software development is Six/Four, a program developed to address the problem of Internet censorship. A number of authoritarian regimes, China foremost among them, build digital firewalls that allow them to block their citizens' access to certain banned web sites. A group of software programmers, collaborating online, developed a piece of open source software to circumvent those firewalls. Internet users in authoritarian countries can now tunnel through to the full range of web sites by routing their traffic through a network of computers running the Six/Four software. Note that while this kind of activity is legal in the countries in which most of the developers reside, the use of these tools is illegal and highly dangerous in the countries for which they are intended --- making political software development another example of legally ambiguous activity.

* * *

The issues that hacktivism targets are as varied as its forms. A survey of some of the best-known incidents of hacktivism shows that certain clusters of issues, and certain lines of conflict, appear most frequently: cyberwars between India and Pakistan, Israel and Palestine, and China and the US (as well as general activism against Chinese censorship); anti-globalization hacktivism; anti-corporate hacktivism; actions on behalf of national independence; hacker issue activism; social conservative hacktivism; and domestic US politics (See).

The taxonomy that is developed in Chapter 2 attempts to bring some order to the heterogeneity of hacktivist actors and actions. It identifies three distinct types of

hacktivism: political cracking, performative hacktivism, and political coding. Political cracking is conducted by hacktivists from hacker-programmer activism, and consists of forms of hacktivism that are consistent with what I call an "outlaw" orientation. These are the most illegal forms of hacktivism such as defacements, redirects, denial of service attacks, sabotage, and information theft. Political coding is also undertaken by hacktivists from hacker-programmer backgrounds, but these hacktivists have a "transgressive" rather than an outlaw orientation; they work in the legally ambiguous zone of political software development. Finally, we have performative hacktivism, which is practiced by hacktivists from artist-activist backgrounds who have a transgressive orientation. Its forms are web site parodies and virtual sit-ins, most often as part of anti-corporate, anti-globalization, or pro-independence protests.

Table 2: A chronology of hacktivist incidents by issue area

Timeline	Cyberwar	Anti-globalization	Anti-corporate	Independence	Hacker	Abortion/Christian	US Politics
Feb-97						Planned Parenthood gets injunction against prolife site www.plannedparenthood.com	
Jul-97				IGC shuts down Basque site after emailbomb campaign			
Aug-97				"Internet Black Tigers" attack Sri Lanka web sites with e-mail bomb			
Apr-98				EDT Zapatista Floodnet			
Jun-98	milw0rm hacks Bhabbha Atomic Research Centre						
Sep-98				40 Indonesian servers hacked with "Free East Timor" message, by Portuguese hackers	NYT site revenge hacked by Mitnick supporters		
Oct-98	Bronc Buster hacks China's human rights agency "Save Kashmir" hack against Indian government info site on Kashmir						
Jan-99							moveon.org website redirected to "Impeach Clinton Now!" John Birch Society site
Feb-99						Nuremberg Files site cut off by ISP	
May-99	Chinese hackers attack US after US bombs Chinese Embassy in Belgrade						
Jun-99	Falun Gong site hacked - www.falunusa.net						
Aug-99					Chaos Computer Club holds intergalactic camp	godhatesfags.com redirected to godlovesfags site	
Sep-99							Stormfront KKK site hacked
Oct-99					Jam Echelon Day Jon Johansen releases DeCSS		
Dec-99		WTO meeting Seattle: E-hippies sitin, Rtmark parody site	Rtmark campaign against etoys begins				
Mar-00	Pakistani group MOS hacks more than 600 Indian sites in 1 week				Dave Touretzky creates the Gallery of CSS Descramblers		
Jun-00			Nike site hacked by S-11 with message on global economy				Violence Policy Center (gun control project) hacked
Jul-00	CDC announces Hacktivismo project at H2K conference						
Sep-00		Federation of Random Action and ToyzTech organize online action against IMF-affiliated sites to sync with Sep 26 protests in Prague					
Oct-00	Israeli hackers promote attacks on Hizbullah web site						
Nov-00	Pakistan Hackerz Club steals data from American Israeli Public Affairs Committee						Republican web site hacked on e-day, replaced with Gore endorsement
Apr-01	China-US hacker war after US spyplane seized; primary US group was PoisonBox, who hit 200+ Chinese domains; retaliation from Chinese 1in0ncrew	Ehippies sitin against FTAA(quebec mtg)					
May-01		Virtual MonkeyWrench steals data on attendees of World Economic Forum meeting in Davos					
Aug-01	US gov announces campaign against Chinese firewalls						
Sep-01	Post-9/11 wave of anti-Arab hacking condemned by leading hacker groups						
Jan-02		World Economic Forum web site crashed by virtual sit-in					
Dec-02			Dow Chemical web site hoax put online at www.dow-chemical.com				
Feb-03	Hacktivismo releases the Six/Four anti-censorship tool						
Apr-03	Voice of America announces its new anti-censorship software project						
Jul-03	U.S. House of Congress passes the Global Internet Freedom Act, approving creation of an anti-censorship office						
Jan-04					Software company SCO targeted by MyDoom virus by pro-Linux hacktivists		

The taxonomy presented in Chapter 2 shows how these three types of hacktivism reflect intersecting variations in hacktivist origins (hacker-programmer or artist-activist) and in hacktivist orientations (transgressive or outlaw). It fleshes out the characteristics of each type of hacktivism with in-depth case studies of three hacktivist groups: the World's Fantabulous Defacers (a group of political crackers), the Electronic Disturbance Theater (performative hacktivists) and Hacktivismo (political coders). This taxonomy enhances, organizes and consolidates the knowledge about hacktivism that has emerged out of work by practitioners, journalists, and academics.

Hacktivism and political participation

For academics, hacktivism is more than an intriguing phenomenon: it is an opportunity to examine certain questions that are particularly well-illuminated by hacktivism's unique constellation of characteristics. One crucial characteristic is hacktivism's capacity for solo activity: unlike most forms of political action, which require some degree of mass cooperation, hacktivism can be conducted by a solo actor. Another important element is hacktivism's facilitation of policy circumvention: hacktivists can elude the mechanisms that allow states to enforce policy, pursuing policy circumvention rather than policy change. Also key are the characteristics that go along with hacktivism's digital nature: like most forms of Internet communication it can be anonymous, trans- and multinational, and take advantage of many-to-many and one-to-many communications.

This dissertation takes advantage of these peculiar characteristics, and uses hacktivism as an opportunity to examine three different questions: Why do people choose to participate in collective political action? When do political actors pursue policy circumvention, rather than policy change? Can the Internet foster new, deliberative forms of political participation?

Chapter 3 centers on the first of these questions, examining the incentives for collective political action. Political science has conventionally taken the politics for granted, and instead problematized the collective nature of political action, wondering why some engage in pursuing public goods while others remain free riders. The chapter turns this formulation upside down, and instead asks whether collective action might be its own reward: do people engage in political action precisely because its collective nature offers social benefits?

My investigation into these social benefits hinges on a reappraisal of the existing literature on social incentives for political participation. I identify two very distinct notions of social incentives: one understands social incentives as the benefits of social interaction, while the other sees social incentives in terms of the rewards of a sense of belonging. I then argue that the notion of social incentives as desire for belonging can be clarified and expanded by referencing the literature on social identity. Noting that the identity literature emphasizes the drive for identity as the desire for positive differentiation from other groups, I articulate a notion of *identity incentives* that satisfy that drive by offering the reward of aligning individual identity with identity of a valued group.

I then test both interactive and identity incentive models against the data gathered from my interviews with hacktivists. This data allows us to assess the drivers that shape hacktivists' choices about which type and form of hacktivism to engage in. While I find that collaboration rates among hacktivists are remarkably high, suggesting that interaction may be a significant motivation, the qualitative data indicates that collaboration is motivated by instrumental rather than interactive incentives. Identity incentives, on the other hand, do a terrific job of predicting the relationship between hacktivist origins and the type of hacktivism each respondent engaged in. After demonstrating that hacktivists' self-labeling and discussion of different hacktivist forms further supports the identity model, I reflect on how the identity model helps to resolve the puzzle of hacktivism as a movement in which means precede ends.

Chapter 4 moves onto the next question: when and how do political actors pursue policy circumvention, rather than policy change? Policy change is the implicit or explicit focus of most of the literature on social movements, including the transnational social movements that have emerged as major players in the Internet era. Scholars of transnational social movements typically examine how the political engagement of non-state actors pressures policy makers into adopting new or modified policies.

I argue that this exclusive focus on policy change misses a major part of the picture: the phenomenon of policy circumvention. Policy circumvention is defined as legal noncompliance that is a strategic political response to a specific policy, law, regulation or court decision; that focuses on nullifying the effect of the policy; and that creates some non-excludable benefits. These criteria allow us to differentiate policy circumvention from simple law-breaking: underground currencies, abortion clinic

blockades, and hacktivist anti-censorship software are all examples of the former, while tax evasion, CD piracy, and trespassing are all examples of the latter.

I develop a model for predicting the emergence of successful policy circumvention, hinging on three variables. First, political entrepreneurs are crucial, since they frame the circumvention in response to particular policies, and structure it in a way that creates non-excludable benefits. Second, policy circumventions are more likely to succeed when the costs of failure are low, since this encourages mobilization and mass participation in the circumvention. Third, policy circumventions are more likely to succeed when the state faces political constraints on repression – most common in liberal states that are inhibited from harshly punishing transgressors.

I test this model against two cases of hacktivist policy circumvention. The first is DeCSS distribution: the distribution of banned code that allows the decoding and viewing of DVDs on Linux machines. The second example is Hacktivismo, a project designed to evade Internet censorship in China and other non-democratic regimes. It turns out that DeCSS has been a more successful case of policy circumvention, though there are indications that Hacktivismo may be a significant influence on policy change; this difference in outcomes is consistent with the predictions of the model.

I conclude the chapter by exploring the broader significance of hacktivist policy circumvention. Most crucially, policy circumvention emerges as a significant transnational challenge to the authority of the nation-state – just the sort of challenge that scholars of transnational social movements, with their focus on policy change, attempt to posit. Policy circumvention also appears as an additional pressure for policy change, since widespread evasion undermines the legitimacy of any policy. Finally, policy

circumvention is changing norms about policy compliance, as evidenced by state and business actors who are adopting policy circumvention as part of their own toolboxes.

Chapter 5 uses the case of hacktivism to address one of the central questions in the study of the Internet and politics: can the Internet foster new, deliberative forms of political participation? Those who would answer yes frequently hang their aspirations on a Habermasian vision of a digital, deliberative public sphere. Such a vision necessarily assumes the operation of some sort of free speech principle – a principle that the case of hacktivism renders problematic. Visions of online deliberation must also grapple with the issue of anonymity, another key challenge in online communication. The hacktivist case helps to illuminate this issue, too.

I begin with the problem of free speech, held to be crucial in enabling meaningful online deliberation. The Internet's hospitality towards free speech is one of the reasons that democratic theorists often see it as a promising home for deliberative democracy. But internal battles among hacktivists show that free speech online is a messy and complicated concept. While the Internet may provide many opportunities to speak, the sheer number of speakers offers diminishing opportunities to be heard; this lack of substantive speaking opportunities could prove fatal to online deliberation.

The phenomenon of anonymity online is equally problematic. Democratic theorists have long debated the question of whether anonymity is constructive or destructive to public speech. Some envision anonymity as a platform that enables speech to be separated from the identity of the speaker, so that all voices can be treated equally; others see anonymity as a corrupting influence, allowing people to evade the

consequences of their speech. The advent of the Internet, with its abundant opportunities for anonymous speech, allows us to test speculation against reality.

The case of hacktivism shows that anonymity practices look little like either the worst or best case scenarios envisaged in theory. Some hacktivists use their real names, while others use traceable pseudonyms, and still others use pseudonyms that are completely untraceable. Each of these choices amounts to a type of accountability claim, a political tool that conveys information about the speaker and the speaker's engagement in the public sphere.

While hacktivism raises questions about the way that free speech and anonymity have been formulated by theorists of deliberative democracy, it also poses a larger problem for would-be discursive democrats. Hacktivism illustrates the challenge of enforcing any rules of deliberative discourse; without enforceable rules, the proceduralist vision of deliberative democracy may have to give way to a more amorphous form of online deliberation.

Investigating hacktivism: literature and methodology

Each chapter of the dissertation covers significantly different theoretical ground, and as such, each chapter is situated in relation to a different body of literature. But the dissertation also has a cumulative perspective on the phenomenon of hacktivism, and it is

worth locating this perspective in relation to the small body of literature on hacktivism itself.[3]

This literature spans the fields of sociology, law, philosophy, security studies, and cultural studies, and largely falls into two camps. One camp looks at hacktivism in the context of civil disobedience, and tends to focus on media coverage of hacktivism; this approach has been most fully realized in the work of Tim Jordan and Paul Taylor, and in a dissertation by Sandor Vegh. The other camp looks at hacktivism in the context of computer security, information warfare, and cyberterrorism; its approach has been most fully realized in the work of Dorothy Denning, and RAND researchers David Ronfeldt and John Arquilla. Both camps base their work on incident reports, press coverage, and online statements by hacktivists themselves; the previous academic research on hacktivism has documented very few original interviews.

A key preoccupation of the first camp is the evaluation of some hacktivists' claim on the tradition of civil disobedience. Karam argues that hacktivism meets Rawls' four-part definition of civil disobedience, in that it is conducted openly, is nonviolent, is conscientiously undertaken, and usually adheres to norms of accountability (Karam). Manion and Goodrum (2000) offer a similar evaluation of hacktivism's claim to the civil disobedience tradition, presenting a series of hacktivist incidents and arguing that they "represent a new breed of hacker: one who is clearly motivated by the advancement of

---

[3] My review deliberately excludes the few scholarly and theoretical works produced by hacktivists themselves, such as *The Electronic Disturbance* (Critical Art Ensemble, 1994) and *Electronic Civil Disobedience and Other Popular Ideas* (Critical Art Ensemble, 1996), and *Electronic Civil Disobedience and the World Wide Web of Hacktivism* (Wray, 1999). These works are better approached as primary source materials disclosing hacktivists' own motivations and ideological commitments, than as independent scholarship on the hacktivist phenomenon.

ethical concerns and who believes such actions should be considered a legitimate from [sic] of (electronic) civil disobedience." (Manion and Goodrum 2000) Hushcle has a more exacting definition of civil disobedience, and argues that hacktivism often falls short of the mark by being insufficiently public and insufficiently respectful of the law. While he allows for forms of hacktivism that violate these precepts of civil disobedience, he argues that they are better understood as

> forms of revolutionary protest, analogous to trashing, sabotage, and perhaps forms of terrorism. The effort to label such behavior as civil disobedience will only encourage the media, governments, and legal systems to continue to treat legitimate electronic civil disobedience as 'electronic terrorism.'(Huschle 2002)

Jordan and Taylor's work constitutes the most substantial investigation into the civil disobedience perspective on hacktivism, as realized in their forthcoming book, *Hacktivism: informational politics for informational times*. Jordan and Taylor are interested in hacktivism primarily as a form of resistance to neoliberal globalization. They distinguish "mass action" hacktivism (roughly comparable to what I term "performative hacktivism") from "digitally correct" hacktivism (roughly comparable to what I term "political coding"). In their view, mass action hacktivism rightly adopts forms that are analogous to offline mass protest and civil disobedience, and correctly focuses on anti-globalization activism. Digitally correct hacktivism, on the other hand, focuses on the "human right to secure access to information", which Jordan and Taylor describe as a "second political order, serving the 'first order' rights to health, welfare and full citizenship."(Jordan and Taylor 2004)

This evaluation of the relative significance of different strains of hacktivism rests partly on Jordan and Taylor's overarching interest in the capacity for radical resistance to "the regressive globalization carried out by governments following a neo-liberal agenda"

(Jordan and Taylor 2004) – or as Taylor puts it elsewhere, in "whether hacktivism can successfully confront capitalism's pervasive yet increasingly immaterially networked nature."(Taylor 2001) It also rests on their reliance on the published (or web published) manifestos of different hacktivists, such as Ricardo Dominguez's *Digital Zapatismo* and the Cult of the Dead Cow's *Hacktivismo FAQ*. These manifestos find hacktivists at their most rhetorical, theatrical, and theoretical, leading Jordan and Taylor to a perspective that collectively treats performative hacktivists as rather more ideologically pure and politically ambitious than they turn out to be individually. Similarly, it represents political coders as less political and more technological than they turn out to be, when interviewed.

While Jordan's earlier work acknowledges that "digitally correct hacktivism" may "generate a new, activist politics of information,"(Jordan 2002) *Hacktivism* sees the value of "digitally correct hacktivism" primarily in terms of its influence on how "the hacking community is being reinvented, in part, as a politicized community." Jordan and Taylor's work is perhaps more reflective of the public narrative of hacktivism – a combination of hacktivist self-presentation, and media coverage – than of the substance of actual hacktivist activities and commitments.

In the case of Vegh's dissertation, the focus on media coverage of hacktivism is consistent with a theoretical agenda: to demonstrate the Internet's challenge to elite control of mass communications. As a communications scholar, Vegh argues that control of the media is crucial to the hegemony of political and economic elites: media control allows elites to repress alternative narratives of resistance or protest. The agenda of elite control leads mass media to skew their presentation of "counterhegemonic" online

activities "toward a perspective that is favorable to the ruling powers, no matter how democratic or socially empowering these activities potentially are."(Vegh 2003) His dissertation uses content analysis of mass media coverage of hackers, hacking and hacktivism to "seek support for [his] theories regarding a conscious agenda on the part of the elite to construct hacking and hacktivism through the media as an anti-social, criminal activity to contain their subversive power."(Vegh 2003) He concludes that

> articles on hackers and hacking increasingly use sensationalist tone and language, motivations are not discussed in news articles about hacking, the discourse is shifting from hackers as criminals to hackers as cyberterrorists, there is a larger focus on cyberterrorism now, even if it has not yet happened, the language of the media blurs the differences between hacktivism and cyberterrorism…..True political dissent online is delegitimized by public opinion driven by the peculiar framing of media reports, which presents favorable conditions for passing laws and regulations that limit not only this mode of having alternative voices heard, but also other ways of conduct otherwise protected by the civil liberties and democratic principles. (Vegh 2003)

The perspective that Vegh critiques finds its scholarly representation in the work of Denning, Ronfeldt, Arquilla, and others who examine hacktivism in the context of cyberterrorism. As Vegh himselves argues, the media's conflation of cyberterrorism and hacktivism has leaked into academia. For experts in computer and information security, or scholars of information warfare theory, it is natural to include cyberprotesters in their pool of perpetrators, and hacktivism as a moderate form of cyberterrorism, since the methods of intrusion and disruption are similar, although they differ a lot in motivation, scale, and outcome. (Vegh 2003)

Vegh's comment constitutes a useful confrontation between the civil disobedience and cyberterrorist scholarships on hacktivism. While the latter camp does not explicitly discredit hacktivists' claim on the tradition of non-violent protest, it begins from a commitment to containing threats to information infrastructure. Denning's 1999 paper, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing*

Foreign Policy, is the starting point for this literature, and is referenced by just about every academic article on the subject of hacktivism or cyberwarfare. Denning places conventional online activism on one side of the political divide, and hacktivism and cyberterrorism on the other: she argues that while "the Internet can be an effective tool for activism….those who engage in [hacktivism and cyberterrorism] are less likely to accomplish their foreign policy objectives than those who do not employ disruptive and destructive techniques." Her concluding analysis of cyberdefense strategies "covers domestic and international initiatives aimed at countering a wide variety of cyberthreats, including cyberterrorism, certain forms of hacktivism, and other non-politically motivated computer network attacks." By treating hacktivism as just one point on a continuum of information security threats, Denning underestimates the political significance of distinctions between nonviolent and violent forms of online transgression, and between various forms of hacktivist activity.

Ronfeldt and Arquilla take a still broader perspective in their widely-discussed work on "netwar", a term they coined to describe "numerous dispersed small groups using the latest communications technologies [to] act conjointly across great distances." (Arquilla and Ronfeldt 2001a) This definition encompasses not only cyberterrorists, but also real-world terrorists who use network technology as an organizing tool – as Al Qaeda did in organizing the 9/11 attacks. Ronfeldt and Arquilla distinguish between terrorist and criminal netwar, and what they call "social netwar", in which "networks of activist NGOs challenge a government (or rival NGOs) in a public issue area, and the 'war' is mainly over 'information'"(Ronfeldt et al. 1998) Ronfeldt and Arquilla are careful to note that the "counternetwar" strategies they develop should not necessarily be

applied to social networks: "netwar is not a uniformly adverse phenomenon that can, or should, always be countered. It is not necessarily a mode of conflict that always gets in the way of government aims."(Arquilla and Ronfeldt 2001b) While this caveat allows for a constructive interpretation of hacktivism as a form of social netwar, the militarist paradigm is still problematic for those seeking to locate hacktivism in the tradition of nonviolent direct action.

The difference between the civil disobedience and cyberterrorist camps is a significant one, since it invokes not only a very different theoretical lens but also very different policy prescriptions. Denning argues that "[w]here the [hacktivist] acts are crimes, it needs to be addressed the same way you would address any kind of computer crime, starting with security defenses so you will not be a victim."(Denning 2000) In contrast, Manion and Goodrum suggest that

> the punitive outcomes [for hacktivism] must be brought into alignment with other forms of civil disobedience….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. (Manion and Goodrum 2000)

Milone goes even further, arguing that

> Hacktivists can aid in the defense of the National Infrastructure by testing critical systems, identifying potential weaknesses, monitoring suspicious activity in cyberspace and, possibly, aiding in retaliatory attacks on hostile governments….Recent legislative reforms attempt to secure the National Infrastructure by increasing governmental surveillance power and easing the prosecution of computer-related crimes….In fact, such actions may actually hinder the National Infrastructure by discouraging beneficial hacktivism for fear of prosecution, and instilling enmity between hacktivists and law enforcement, while concomitantly restraining civil liberties. Far better would be to foster a sense of civic duty among groups of ethical hackers, revise existing laws to facilitate cooperation between hacktivists and law enforcement, and develop innovative programs that encourage responsible hacktivism and fuel hacktivists' innate love of a good challenge.

This dissertation takes an evidence-driven approach to this debate. My perspective is certainly closer to the civil disobedience camp than to the cyberterrorist

camp: simply by taking hacktivism as a subject for serious political science inquiry, I accept the premise that it is better understood as political engagement than as terrorism or crime. But the civil disobedience camp is limited by its lack of direct contact with hacktivists themselves (as is, for that matter, the cyberterrorist camp). With so little interview data on the motivations, concerns, and commitments of hacktivists themselves, scholars have had to rely on hacktivist manifestos and media treatments of hacktivism, both of which tend to produce an overly dramatic picture of hacktivists and hacktivist agendas. The picture of hacktivism that emerges through direct contact with hacktivists offers a freshly convincing case for locating hacktivism in the tradition of civil disobedience.

The new data gathered for this dissertation comes from face-to-face, e-mail, Internet Relay Chat (IRC) and phone interviews with fifty-one people either directly or indirectly involved in the hacktivist community. The first of these interviews was conducted in May 2002, and the last was completed in August 2003. Interviews were conducted in a range of media: 26 by e-mail, 19 face-to-face, 4 by synchronous online chat, 1 by phone, and 1 by mail. (I e-mailed a list of questions, and the interview subject responded by mail). In 24 of the e-mail interviews I corresponded with a single respondent; in 2 e-mail interviews the respondents replied on behalf of one or more collaborators. Among the 19 face-to-face interviews, 15 were conducted one-on-one; two interviews were conducted with two respondents simultaneously. The remaining chat, phone, and mail interviews were all one-on-one.

The interview sample was constructed through four basic methods: a mass e-mail sent to participants from the now-defunct hacktivism.ca listserv[4]; personal e-mails sent to known participants in hacktivist activities, identified through mass media and/or online coverage; solicitation of interview subjects from two hacker conferences (one in the US and one in Germany); and "snowball sampling", whereby interview subjects culled from the above methods referred me to additional prospective subjects. Among these interview subjects, the country of residence is as follows:

[4] In the mass e-mailing to hacktivism.ca listserv members, I sent 233 e-mails to addresses culled from the list archives; of these, 88 e-mails failed due to address changes or other technical problems.

Table 3: Interview subjects by country of residence

Australia	1
Canada	8
East Timor	1
France	1
Germany	11
Netherlands	9
Norway	1
Sweden	1
UK	4
Unknown	2
US	20

My sampling methods introduce several potential distortions, some of them necessary, and some of them incidental. The most significant – and crucial --- distortion is that the sample was deliberately chosen from a population that was disproportionately likely to participate in hacktivist activities. Hacktivism is still a rare enough phenomenon that a truly random sample drawn from general population would be unlikely to include any participants in hacktivist activities, and only a few respondents who had even heard of hacktivism. Since my inquiry is into the motivations and dynamics of hacktivist participation, it is more useful to limit myself to a population that is at least aware of the hacktivism phenomenon, and/or the possibility for hacktivist activities. In drawing my sample from populations that are already engaged in discussion of political computer hacking, I ensured that respondents were at least able to consider hacktivism as an option.

In limiting myself to hacktivism-aware populations, however, I ensured that my sample contained a disproportionate number of people actively engaged in hacktivist activities. From the responses I received to my inquiry, I can infer a further skew from self-selection: people who were involved in hacktivist activities were more likely to agree to speak with me than those who were merely observers of the hacktivism phenomenon.

It is possible that my sampling methods introduced additional sources of bias in terms of the kinds of hacktivist participants I was likely to find. Soliciting interview subjects at US and German hacker conferences means that my sample probably contains a disproportionate number of US and German hacktivists, and there is every reason to imagine that there may be some systematic differences between US and German hacktivists, and the larger hacktivist population. Specifically contacting people who had achieved some publicity for their hacktivism meant that I was more likely to speak with people who were public about their hacktivism, and relatively unlikely to speak with people whose hacktivism placed them in a high degree of legal jeopardy (such as political crackers). Finally, my use of snowball sampling – obtaining additional interview referrals from interview subjects I had contacted directly – means that my sample may contain a disproportionate number of hacktivists who have social links to other hacktivists.

Because of the variation in interview media, the type of data gathered in different interviews also varied. The e-mail interviews were the most consistent; they consisted of a common set of questions sent to everyone who agreed to an e-mail interview, with a slightly different set tailored to interview subjects who were identified through their involvement with DeCSS. The face-to-face, phone, and chat interviews were somewhat looser; while I had a core list of questions that I tried to get through with each interview subject, I let the synchronous interviews unfold more organically, so not all questions were posed in the same form or at the same point in the interview. In some cases interview subjects touched on core questions without being prompted, so I let their comments stand in place of formal answers to specific questions. In cases where I had

prior data on the interview subject's activities, I did not ask questions for which I already knew the answer.

The dissertation is informed by several additional sources of material on hacktivism. References to specific hacktivist incidents come from an exhaustive search of the popular and online press, which has covered many of the hacktivist actions conducted since 1998. The specific content of hacktivist web site defacements comes from a review of the leading defacement mirrors. Content analysis of three months of postings to the hacktivism.ca e-mail list, which informed my earliest work on hacktivism (Samuel 2001), also provided a source of comments from a wider range of hacktivists and hacktivist observers. Hacktivist web sites that feature articles and/or manifestos from hacktivists provide additional first-person material. Several computer security sites feature regular interviews with hackers; some of these include politically motivated hackers, and thus provide more hacktivist accounts.

The various chapters of the dissertation deliberately deploy this material in different ways, reflecting the very different agendas of each chapter. Chapter 2 synthesizes a wide range of popular, online, first-person and interview accounts to paint a broad picture of each of the three types of hacktivism. Chapter 3, on the incentives for collective political action, uses a combination of quantitative and qualitative analysis of the full set of interview data. Chapter 4, which looks at the politics of policy circumvention, focuses on two central cases; it uses third party accounts of each of these two cases, along with interviews from the hacktivists involved in each case. Chapter 5 is an exploration of two theoretical issues in deliberative democracy, informed by data gathered from interviews with hacktivists and other first-person accounts.

This wide range of research questions and research methods emerges as both challenge and opportunity. It is a challenge to address three such different areas of political science inquiry in the space of one work, since this demands a degree of efficiency in addressing the literatures and marshalling the data relevant to each thread. But the variety of approaches and agendas also provides an opportunity to make a case for hacktivism that is larger than any one of these questions: hacktivism's ability to speak to each of these issues is the strongest possible evidence for its wider relevance to political science.

The multithreaded approach also paints a more vivid picture of the hacktivist phenomenon itself. Precisely because we are seeing hacktivism in such different research contexts, it is striking when interconnections emerge between chapters, turning chapter topics into larger themes. While these interconnections will be explored more deeply in the concluding chapter, a tabular preview provides a roadmap and summary of the chapters ahead.

Table 4: The dissertation in crosstabs

Bold cells represent the central argument of each chapter. Non-bold cells describe the interlinkages that will be presented in the concluding chapter.

		Chapter Topics			
Interconnecting Themes		Ch. 2: Taxonomy	Ch. 3: Identity incentives	Ch. 4: Policy circumvention	Ch. 5 Deliberative Democracy
	Civil disobedience or cyberterrorism?	It is crucial to acknowledge distinctions among types of hacktivism. Performative hacktivists draw clearest links to civil disobedience, while political crackers are most often confused with cyberterrorists.	The instrumental orientations of hacktivists underline their ethical commitments. The importance they place on social ties and a sense of belonging is consistent with evidence from other examples of civil disobedience.	Policy circumvention is threatening, contributing to conflation with cyberterrorism. The history of civil disobedience includes many examples of policy circumvention.	The strategic use of nymity choices as accountability claims demonstrates adherence to civil disobedience norms of accountability, albeit accountability to different notions of political community.
	Taxonomy	**Hacktivist origins and orientations divide hacktivism into three types: political cracking, performative hacktivism, and political coding.**	The distinction among different types of hacktivists reflects different origins, not different demands for interaction.	The adoption of policy circumvention by state and nonstate actors suggests that the political coding model of hacktivism may be ascendant.	Lines of division on nymity and free speech shows that the taxonomy captures meaningful lines of conflict.
	Identity	The congruence between political origins and type of hacktivist underlines the relevance of group identity.	**Ex ante identity (hacker-programmer or artist-activist worlds) predicts the type of hacktivism (political coding/cracking or performative hacktivism) in which respondents engage.**	The dynamics of policy circumvention are partly a narrative of collective action challenges.	Nymity choices serve as another way of stating and reinforcing ties to a particular community.
	Circumvention	One of the key lines of division among types is the focus on policy circumvention versus policy change.	The efficacy of policy circumvention reinforces motivations for collaboration.	**Successful policy circumvention depends on political entrepreneurs, low costs of failure, and high political costs of repression.**	The transgressive pursuit of audience is an indirect form of policy circumvention.
	Deliberative democracy	The ascendance or decay of different types of hacktivism has practical as well as symbolic significance for democratic deliberation online.	The continued pull of collective engagement puts the lie to fears about the Internet's atomizing potential. Perceptions of efficacy through hacktivism suggest the potential for broadening engagement online by expanding our notion of speech to include speech acts.	The accountability claims encoded in nymity choices reflect pragmatic, self-interested decisions as well as political commitments.	**Proceduralist visions of deliberative democracy are challenged by hacktivist claims to a right to be heard, and by the use of nymity choices as accountability claims.**

Chapter 2

A Taxonomy of Hacktivism

Introduction

The "type" of hacktivism categorizes people: political crackers, performative hackers, and political coders. The "form" of hacktivism categorizes actions: site redirects, defacements, virtual sit-ins, etc.

This chapter provides a broad map of the hacktivist universe, of its participants and their activities. My purpose is to introduce the key lines of variation that define distinct types of hacktivism, and to provide a clear introduction to each of these types. To this end I describe three distinct types of hacktivism: political cracking, performative hacking, and political coding.

The distinctions among these three types are based on two dimensions of variation: origins and orientation. The first part of this chapter discusses each of these lines of variation. It begins by looking at *origins*: the political culture from which each type of hacktivism emerged. Hacker-programmer culture gave rise to political coding and political cracking; postmodern left culture gave rise to performative hacktivism.

Table 5. Types of hacktivism by hacktivist origins and orientation

Hacktivist Origins

Hacktivist Orientations	Hacker-programmer world	Postmodern left (artist-activist)
Transgressive	**Political coding**	**Performative hacktivism**
Outlaw	**Political cracking**	*About this space*[5]

[5] While it might seem theoretically possible for artist-activists to engage in outlaw forms of hacktivism, it is easy to see why such hacktivism has yet to emerge. The outlaw orientation of political crackers, which includes the assumption of greater legal risk and the not-unrelated effort at avoiding accountability, along with a propensity for transnational conflict and an avoidance of large-scale collective action, all run counter to some pretty central principles of postmodern left activism. Artist-activists tend to value mass, accountable action as more democratically legitimate, and eschew transnational conflict due to a more pacifist orientation.

Once I have reviewed the two worlds from which hacktivists originate, I move onto the notion of *orientation*: the playbook that defines different types of hacktivism, and that separates political coders from political crackers (even though both emerge from the same hacker-programmer culture). The transgressive[6] orientation of both political coders and performative hacktivists challenges the legal and political order, but still exists in relation to it and even shares some norms of the liberal democratic order, such as notions of legitimacy and accountability. Political crackers, in contrast, have an outlaw orientation that completely rejects the legal and political order, and seem to exist entirely outside of liberal democratic norms (though perhaps within the norms of some local or radical subcultures). In concrete terms, these differences translate into very different practices around legal risk, accountability, group size, and international cooperation, as seen below.

Table 6. Characteristics of hacktivist orientations (transgressive vs. outlaw)

		Orientation	
		Transgressive	Outlaw
Characteristics	Legal risk	Legally ambiguous	Illegal
	Accountability[7] (naming practices)	Real names, traceable pseudonyms	Untraceable pseudonyms, anonymity
	Group size	Medium-size groups, dependence on mass participation	Solo, small groups
	Transnational cooperation	Multinational (working with hacktivists from multiple nations)	National (vs. own country) Multinational (cooperating across boundaries) International (mirroring international conflicts)

[6] The distinction between the transgressive and outlaw orientations is a distinction of degree, more than of kind – I could describe these orientations as "transgressive" and "even more transgressive.". But to describe them as "conventional" versus "transgressive" would be to radically underestimate the degree of transgression involved in political coding and performative hacktivism.

[7] Variation in naming practices as a type of accountability claim is addressed in Chapter 5.

Once I have provided a brief overview of each of the characteristics that define different hacktivist orientations, I move quickly into describing each of the three types of hacktivism. Political cracking is the most legally risky, and probably the least effective, form of hacktivism: after a brief overview I provide a more in-depth description of one group of political crackers, the World's Fantabulous Defacers. Performative hacktivism looks a bit more like progressive street activism, but with a decidedly postmodern twist: here I provide a case study of the Electronic Disturbance Theater, one of the best-known groups of performative hacktivists. Finally, I introduce political coding, which focuses on political software development: the case study here looks at Hacktivismo, the leading group of political software developers.

These three types of hacktivism are not just useful intellectual constructs. They represent meaningful differences in the origins and orientations of different hacktivists, and translate into fierce internal debates. The later chapters on identity, policy circumvention, and online deliberation will all rely heavily on the differentiation among hacktivist types in order to address key questions in political participation.

And it is in the context of describing each type of hacktivism that we can best see how the difference between a transgressive and an outlaw orientation separates hacker-programmer-coders from hacker-programmer-crackers. The chapter concludes by underlining the commonalities in the shared transgressive orientation of political coders and performative hacktivists, while noting a couple of further distinctions that still separate them.

Hacktivist origins

Hacktivists come from two distinct political cultures. One is the hacker-programmer culture, itself embedded in the broader social and political culture of the Internet. Another stream of hacktivists comes from the world of post-modern left, and its community of progressive artist-activists. These two backgrounds translate into very different identities – and very different kinds of hacktivist practice. As we will see in later chapters, there is some animosity between the two camps; hacker-programmers often see artist-activists as ignorant and careless about the infrastructure of the Internet, and as technically incompetent. Artist-activists often describe hackers as caring more about computers than people, and as technological elitists.

The world of hacker-programmers: a very brief history of hacking

The world of hacker-programmers is a tightly networked community, although the explosive growth of the Internet has expanded that community to the point where ties have necessarily loosened. Its denizens are bound together by their immersion in the culture of the Internet, which generates its own behavioral norms, its own political worldview, and its own political agenda.[8]

---

[8] All of these aspects of hacker history and culture are well-documented online. Indeed, Internet culture sets a new standard for sociological documentation, since the culture has continually articulated, documented and discussed the evolution of its language, technologies and norms. The results of each development – and many of the discussions that drove the evolutionary process – have been preserved in media such as Usenet "Netiquette" guidelines (summarizing online behavioral norms), the Jargon file (tracking online terms and language use), and the Wikipedia (a communal project that documents everything from the overall history of the Internet to individual technical standards – and includes many offline cultural references, too).

The Internet culture in which hackers exist itself emerged out of hacker culture. Before the Internet, hacker culture existing as multiple cultures("Hacker culture") of computer scientists, research assistants, and hobbyists, clustered around whatever mainframes they could get access to. [9] The idea of linking these mainframes together initially arose in a RAND report to the U.S. Air Force, suggesting how communications could be constructed to survive a nuclear attack:

> The report proposed a communications system where there would be no obvious central command and control point, but all surviving points would be able to reestablish contact in the event of an attack on any one point. Thus damage to a part would not destroy the whole and its effect on the whole would be minimized.(Hauben)

In 1969, this abstract idea was given life as the ARPANET, and the disparate communities of hacker-dom were suddenly connected in what was for many years a very small network of users. But where the Advanced Research Projects Agency (ARPA) had envisaged its ARPANET as a means of pooling computing power, the law of unintended consequences took hold.

> By the second year of operation, however, an odd fact became clear. ARPANET's users had warped the computer-sharing network into a dedicated, high-speed, federally subsidized electronic post- office. The main traffic on ARPANET was not long-distance computing. Instead, it was news and personal messages. Researchers were using ARPANET to collaborate on projects, to trade notes on work, and eventually, to downright gossip and schmooze. People had their own personal user accounts on the ARPANET computers, and their own personal addresses for electronic mail. Not only were they using ARPANET for person-to-person communication, but they were very enthusiastic about this particular service -- far more enthusiastic than they were about long-distance computation. It wasn't long before the invention of the mailing-list, an ARPANET broadcasting technique in which an identical message could be sent automatically to large numbers of network subscribers. Interestingly, one of the first really big mailing-lists was "SF- LOVERS," for science fiction fans. Discussing science fiction on the network was not work-related and was frowned upon by many ARPANET computer administrators, but this didn't stop it from happening.(Sterling 1993)

---

[9] These early days are well chronicled; see (Levy 1984; Raymond 2000).

As much as the ARPANET – and later, the Internet[10] – reflected the interests and values of computer scientists, hobbyists and hackers, its characteristics also shaped them. Networks enabled instant, world-wide, synchronous or asynchronous communication – and for many years, that communication was necessarily in plain text form. Network communication demanded a common language, and English emerged as the dominant one. Networks were blind to characteristics like gender, race, age, and accent. Networks depended on common standards, so that different parts of the network could communicate. And networks thrived on access: access to computers (a rare and valuable commodity in the early days of the Internet), access to networks (in order to gather and share information), and above all, access to information itself: information on how to use the emergent tools of network computing.

From this drive for access emerged the "hacker ethic", whose core tenets were articulated by Steven Levy as:

> - All information should be free.
> - Mistrust authority - promote decentralization.
> - Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
> - You can create art and beauty on a computer.
> - Computers can change your life for the better.(Levy 1984, Chapter 2, "The Hacker Ethic")

These tenets constituted a worldview that has been described as inherently political, for,

> although hacking is often perceived as apolitical, hacking always tends to evoke political elements due to the nature of knowledge in our society. The quest for knowledge, which is an unmistakable core component of hacking, is a politics of transgression because the 'knowledge' that is sought is often inaccessible (or potentially so) at either a technological or legal level.(Coleman 2003)

---

[10] The transition from ARPANET to Internet took place in the 1980s with the development and proliferation of the TCP/IP networking protocol, until the ARPANET was finally decommissioned in 1990. (Leiner et al. 2003)

In concrete terms, the hacker "quest for knowledge" translated into a particular politics, which has to some degree become identified as the politics of the Internet more broadly. The motherhood issues for hackers – and the Internet community more generally – are:

- *freedom of speech*, and in particular the fight against online censorship, reflecting hackers' view that "information wants to be free";
- *privacy rights,* especially online, reflecting hackers' mistrust of authority;
- *intellectual property freedoms,* like the ability to share traditionally copyrighted text, music or video files online, again reflecting the view that "information wants to be free";
- *open standards,* which ensure interoperability of the Internet, as opposed to the private standards promulgated by Microsoft and others through the creation of for-profit networks and tools; and
- *free or open source software,* which permit various kinds of modification and distribution, reflecting hackers' quest to use technology for continuous improvement, and to continuously improve technology.

This political agenda manifested itself in a number of illegal hacking ("cracking") campaigns, long before the phenomenon of "hacktivism" is usually said to have emerged. When Kevin Mitnick was arrested and prosecuted for his hacking, thousands of hackers mobilized to support him – in many cases by defacing sites to add "Free Kevin" messages. Was this hacktivism, or plain old hacking? According to the hacker ethic, it is

a false distinction – because hacking is an inherently political act: the liberation of information.

In recent years, however, political cracking has shifted away from the hacker agenda, and political coding has emerged to champion Internet issues. This explains the focus of projects like Hacktivismo (which tackles Internet censorship) and DeCSS (which tackles the narrow construction of intellectual property rights). But the fact that political coders focus on Internet issues should not be taken as a lack of interest in "real world" politics. Over time it has become clear that hackers' online political agenda extends to a distinct perspective on offline issues, too:

> located somewhere between the secular or progressive pole on moral values and the laissez-faire pole on economic values, favoring freedom on both dimensions. Internet enthusiasts favor the private sector more than government intervention to produce economic equality, but they are also strong supporters of the alternative social movements that arose in the counterculture 1960s, such as those seeking to promote gay rights, pro-choice, civil rights, feminism, and environmentalism. (Norris 2001)

If it is hard to know where hacker politics ends and the broader politics of the Internet begins, that is because the hacker-programmer culture has a continually evolving relationship with the larger Internet. In the early years, hacker-programmers constituted the entire Internet community, so hacker politics *were* Internet politics. In the late 1980s and early 1990s, more Internet users came online, but these still tended to be people with a great deal of interest, skills, or enthusiasm for computing; they absorbed many of the norms and values of the hacker world, even if they did not engage in the same level of assisistance or tinkering with the Internet's software and hardware infrastructure. This Internet community has over time been enveloped by a much larger perimeter of Internet users, mostly coming online in the late 1990s or after, who see the instrumental value of the Internet. These users may contribute content or participate in online communities, but

their contributions and participation are defined by offline identities and interests (such as ethnicity, sexual orientation, or political affiliation) rather than by the culture and values of the Internet itself. Throughout each wave of growth, "white hat" hackers have seen it as their particular duty to protect the Internet from private sector encroachment, "newbie" carelessness, and destructive "black hat" hackers who fail to respect the hacker ethic.

People who live in this world might or might not call themselves hackers – many do not, citing media misrepresentation of what hacking actually means. Some call themselves programmers, coders, geeks, or nerds – and some do not use a label at all. But *all* of them identify very strongly with the "true" community of the Internet, as we can see from this programmer's reaction to the Internet's gradual dilution:

> When the Internet first formed, it centered on technical experimentation by academics, scientists, and students. The original connections were almost all free of charge; people recognized that connecting and communicating were really cool, and we helped each other in a general spirit of cooperation. We promoted free speech and grassroots access, because we recognized those things as valuable. Alleged Internet problems, such as child pornography, "bomb making instructions", hate literature, etc., were simply not issues. We could set up real-time chat connections across the continent or the world and get instant response. All the important networking software was freeware, distributed under a public license system where everyone was allowed to use, copy, and modify it at no charge.
>
> How different the situation now that internetworking is considered a hot global trend. More people want connections than there are connections available, so everyone has to pay….[Your organization] appears to be concerned about commercial exploitation of our natural environment, and about appropriate respect for our indigenous cultures. What about the endangered network environment? What about the first nations of the Net?… I'd urge you, since you no doubt feel you *must* discuss the Internet as a medium for activism, to also discuss responsible use and respect for the Internet's unique culture…. If not, then get off our land, get out of our culture, and go crawl back under a rock, because the last thing the Internet needs is more colonization. (Skala 1996)

The world of artist-activists: an introduction to the postmodern left

The postmodern left is a very loosely bound community that is defined by a combination of political beliefs, theoretical worldviews, and tactical innovations. I use

the term “postmodern” to distinguish this world from the broader progressive scene; this particular segment of the left is more creative in the forms of its activism, and more sophisticated in its understanding and use of communications. While some members identify primarily as artists, and others as activists, these particular artists blur the lines between performance and politics, while these particular activists do their politics in ways that are strongly shaped by a media-savvy artistic aesthetic.

I am not the first to apply the term “postmodern” to this slice of the progressive movement. Best and Kellner describe postmodern politics as

> a politicization of all spheres of social and personal existence. Postmodern models of politics are trying to redefine the "political" based on changes in society, technology, economics, and everyday life. (Best and Kellner)

In her critique of what she also terms the “postmodern left”, Wood describes its themes as:

> a focus on language, culture, and "discourse"…; a rejection of "totalizing" knowledge and of "universalistic" values…in favor of an emphasis on "difference," on varied particular identities such as gender, race, ethnicity, sexuality, on various particular and separate oppressions and struggles; an insistence on the fluid and fragmented nature of the human self…;and a repudiation of "grand narratives"…[I]t should be obvious that the main thread running through all these postmodern principles is an emphasis on the fragmented nature of the world and of human knowledge, and the impossibility of any emancipatory politics based on some kind of "totalizing" vision. (Wood 1995)

Seippel usefully contrasts this postmodern politics with the postmaterialist orientation described by Inglehart:

> While the postmaterialist has a teleological and future-oriented belief in progress, the postmodernist is ultimately keen to cultivate the present, the fragment, the immediate; while the postmaterialist searches out the natural, true and authentic, the postmodernist explores the seductive surface; the postmaterialist is a stable, steady being, whereas the postmodernist is constantly changing, and finally, while the postmaterialist is out to realize himself, the postmodernist is merely out to express himself.

In practice, however, the political agenda espoused by this community is not unlike the agenda of the post-materialist left. The issues of greatest interest are

globalization, corporate power, human rights, civil rights, and the environment. As I will show below, this agenda is reflected in the targets selected by performative hacktivists: targets like Nike, the WTO, and the Mexican government (over the issue of the Zapatistas). Where the postmodern left differs from the broader progressive scene is thus not in its agenda, but in the theoretical lens through which it views that agenda, and thus, the tactics it adopts in that pursuit.

The worldview of these artists and activists is self-consciously shaped by the theoretical works of postmodern and critical theorists such as Baudrillard, Virilio, Foucault and Guattari. Best and Kellner, describing the world of what they call "postmodern politics," note that this world includes "the anti-politics of Baudrillard and his followers, who exhibit a cynical, despairing rejection of the belief in emancipatory social transformation, as well as a variety of efforts to create a new or reconstructed politics."(Best and Kellner) From Virilio, it takes its analysis of globalization as a temporal rather than spatial phenomenon:

> Virilio predicts that the globe will no longer primarily be divided spatially into North and South, but temporally into two forms of speed, absolute and relative. The 'haves' and 'have-nots' are then sorted out between those who live in the hyperreal shrunken world of instant communication, cyberdynamics, and electronic money transactions—and those, more disadvantaged than ever, who live in the real space of local villages, cut off from the temporal forces that drive politics and economics. (Bleiker 2002)

From Foucault it takes the notion of "revolution as spectacle."(Hanninen 2003) And from Guattari, it takes the notion of the body as the site of maximal social regulation, and posits the Internet's capacity for liberating actors from that regulation.(Ensemble. 2000) A final theoretical influence comes from the world of political theater; August Boal, in particular, is cited for his idea of theater as a way "to reinvent the past and to

invent the future." (Boal 1999)

This theoretical lens translates into specific kinds of political strategies and tactics that are much less tedious than the theoretical works that inspire them. The artist-activists of the postmodern left are more likely to bridge art and politics, turning politics into performance and performance into politics. For example, one ascendant tactic is "culture jamming, the practice of parodying advertisements and hijacking billboards in order to drastically alter their messages." (Klein 2000, p. 282.) Culture jamming is "itself a cutting and pasting of graffiti, modern art, do-it-yourself punk philosophy and age-old pranksterism."(Klein 2000, p. 282.) Another characteristic tactic of "carnivalesque resistance" are street protests "that rebelliously reinterpret the experience of consumers putting on garments in acts scripted to raise consciousness." (Boje 2001) A third innovation has been the creation of independent media centers (IndyMedia), whose mission "includes reporting on a wide variety of social injustices, covering social movement mobilizations, engaging in media activism, and embodying participatory democracy in its actions and media policies."(Morris 2002) While participants often describe these tactics with reference to postmodern theory, the practical significance of their innovative activism is that it attracts both more participation and more media attention by making politics look more like play.

While the artist-activist influence on hacktivism is most visible in the explict theorizing of those who come from an art or theater background, there is a growing number of hacktivists whose background has more in common with non-performative progressive activists. In June 2002, the Ruckus Society, which provides training in

disruptive protest techniques, held its first hacktivism training camp; this may well engender more hacktivism from traditional activist groups.

Even though the artist-activist world is truly a postmodern fusion of political art and political activism, people in this world tend to identify themselves as either artists or activists. But whichever label they use – or even if they eschew labels altogether, a not-uncommon postmodern position – they locate themselves within the broader "us" of creative progressives working for social change.

Hacktivist orientations and types of hacktivism

As presented at the beginning of this chapter, the two lines of variation among hacktivists (hacker-programmer vs. artist-activist origins, and transgressive vs. outlaw orientation) divide the world of hacktivism into three distinct types: political cracking, performative hacktivism, and political coding. *Political cracking* is undertaken by hacktivists from hacker-programmer origins, who have an outlaw orientation. *Performative hacktivism* is conducted by hacktivists from artist-activist backgrounds, who have a transgressive orientation. And *political coding* is undertaken by hacktivists with hacker backgrounds, who have the same transgressive orientation as performative hacktivists.

Four interconnected characteristics define the difference between the transgressive orientation of political coders and performative hacktivists and the outlaw orientation of political coders: tolerance for legal risk, naming practices, scale of collective action and propensity for multinational cooperation.

Hacktivists vary significantly in their willingness to engage in illegal or legally ambiguous activities. The outlaw orientation embraces forms of hacktivism that are clearly illegal, like site defacements, redirects, DoS attacks, and sabotage. The transgressive orientation challenges the law, but does not push that challenge to the point of immediate legal jeopardy.

In a related move, the transgressive orientation embraces accountability, while the outlaw orientation avoids it. In practice this means that while some hacktivists conduct their activities under their own names, while others hack anonymously, or using pseudonyms.[11] One hacker convention that has traveled into the hacktivist realm is the use of pseudonyms, or handles, in the execution of hacktions. Hacktivists frequently use handles like mor0n, metac0m, or nathan hactivist. (The use of numerals in place of letters is another hacker convention, dating back to the days when all Internet communication took place in ASCII, a standard set of alphanumeric characters.) Handles are a way for hackers or hacktivists to take credit for an online act, without necessarily being accountable for that act in an offline context. Note that the use of handles does not necessarily prevent the hacktivist from being identified by law enforcement authorities; while some hacktivists take care to keep their real identities secret, others are relatively open about both their handles and their real names.

Another variation is in the presence, absence, or scale of collective action. Individual hacktions may be undertaken by a lone hacktivist, a small group of hacktivists,

---

[11] The significance of anonymous and pseudonymous hacking is discussed in greater detail in Chapter 5.

or a very large number of participants who leverage the work of a smaller core group. The possibility of solo action seems to be one of the attractions of hacking in general, and hacktivism in particular.

The final characteristic that differentiates the transgressive and outlaw orientations is in the propensity for hacktivism across borders. While transnational activism has received some attention in recent years, it is still the exception rather than the rule in political participation. In the case of hacktivism, the reverse is true: hacktivism across borders is at least as common as hacktivism within borders, and it is often difficult to distinguish between the two.

I have found it useful to distinguish between national, multinational, and international hacktivism. National hacktivism occurs when a hacktivist targets a government, business or organization within his or her own country. Multinational hacktivism occurs when hacktivists band together across borders to attack a common target at the subnational, national, or multinational level. And international hacktivism consists of hacktivists in one country targeting a government, business, organization in another country, most often as part of a reciprocal "cyberwar" that parallels an offline international conflict.

We can best understand how these orientations translate into specific practices by looking at each type of hacktivism in greater detail. I begin with an account of political cracking (which comes from an outlaw orientation) before proceeding to performative hacktivism and political coding (which share a transgressive orientation).

Political cracking: an introduction

Political cracking consists of hacktions that are clearly illegal, undertaken by hacker-programmers. This encompasses the largest number of hacktivist incidents to date (though probably not the largest number of participants), and spans a wide range of issues and nations. It also encompasses a wide range of tactics, including site defacements, redirects, denial of service attacks, information theft, and sabotage.

Calling these activities "political cracking" draws on a distinction that is maintained by many members of the hacker community. Among early computer enthusiasts, a "hack" was a technical "feat…imbued with innovation, style, and technical virtuosity" and people "called themselves 'hackers' with great pride."(Levy 1984) Hackers from that generation "prefer to call their progeny 'crackers' in order to differentiate themselves from what they perceive as their younger criminal counterparts."(Thomas 2002). Within the hacker community, hackers who engage in clearly illegal and destructive activity – like web site defacements or information theft – are thus often referred to as "crackers," in order to differentiate this activity from the "leave no footprints" hacking condoned by the hacker ethic. It is in this tradition that I use the term "political cracking" to refer the type of hacktivism that encompasses illegal activities – such as site defacements, redirects, DoS attacks and sabotage – harnessed to political ends.

It should not be surprising that political crackers therefore remain anonymous. The 1996 defacement of the U.S. Department of Justice, for example, left no explicit clue

as to the cracker's identity; the person or people behind the 2000 Nike site redirect likewise remained anonymous.

Political crackers tend to work alone, or in very small groups. A single cracker can experience a high degree of political efficacy by defacing or redirecting a web site, potentially attracting a great deal of media attention. There are none of the coordination or free rider problems of collective action, but the actor is nonetheless able to achieve much of the public recognition that adheres to collective political action.

Small group action is also common. Many political crackers apparently belong to groups that include anywhere from two to perhaps a dozen members; hacktions may be executed by a lone hacker, a couple of hackers, or a larger number of group members. It can be difficult to distinguish solo from small group hacks, since hacktions are so often anonymous or pseudonymous. Where a hack is credited to a specific group, such as the World's Fantabulous Defacers, it may not be clear whether it was executed by one group member or by several hackers working together.

Some ongoing defacement campaigns, like those seen in the transnational conflicts between Israel and Palestine, or India and Pakistan, might also be considered collective action; but in these instances the individual hacks are still conducted by solo or small-group hackers, with little or no apparent coordination of the overall campaign.

Political cracking encompasses national, multinational and international hacktivism, but it is most common in international form. International hacktivism, sometimes called "infowar" or "cyberwar", refers to instances where citizens of one country hack targets in another, usually in a reciprocal conflict between two countries. Examples include the long-running battles between Palestinian and Israeli crackers,

between Chinese and American crackers, and between Pakistani and Indian crackers. We do see some instances of multinational cracking, however, as when milw0rm, a multinational group of hackers, targeted the Indian government to protest its nuclear tests. And particularly in the early days of political cracking, when hacking was just shading into hacktivism, national hacktivism was quite common: the cracker campaigns on behalf of Kevin Mitnick, or against the US Communications Decency Act, both consisted primarily of national cracking.

While the distinction between these three types of hacktivism is theoretically significant, in practice it is often hard to recognize. Because so many hacktivists work anonymously or pseudonymously, their national origin may be impossible to ascertain. Nonetheless there are many instances in which we can distinguish national, transnational and international hacktivism, and in which the distinction usefully informs our understanding of the hacktivists and their actions.

The first quasi-political cracking was focused on hacker-specific issues like the regulation of the Internet or the prosecution of individual crackers. But cracking has since broadened to encompass a much broader range of causes, from gun control (pro and con) to globalization and corporate power. Today the greatest concentration of political cracking incidents occurs in the context of international cyberwars: between Israelis and Palestinians, Indians and Pakistanis, Chinese and Americans. Each of these cyberwars has seen hundreds or even thousands of web sites defaced in a campaign that pits political cracker against political cracker.

While it has been credibly argued that governments have sponsored some of this cyberwar cracking (Borger 1999; Kalathil and Boas 2003; La Canna 2001), the majority

of political cracking activities are illegal in the jurisdiction of the target, the cracker, or both. As a result, political cracking is almost always anonymous, or more often, pseudonymous. Precisely because hacker culture puts so much value on technical prowess, crackers like to build their reputations by taking credit for their hacktions under handles.

The fact that the activities of political crackers are generally illegal does not mean they are necessarily destructive. Indeed, the "hacker ethic" is widely seen as precluding destructive activity:

> It is against hacker ethics to alter any data aside from the logs that are needed to clean their tracks. They have no need or desire to destroy data as the malicious crackers. They are there to explore the system and learn more. The hacker has a constant yearning and thirst for knowledge that increases in intensity as their journey progresses.(Mizrach)

Web site defacements, DoS attacks, and information thefts can adhere to this standard by leaving the sites they deface fundamentally intact.

Unlike other forms of hacktivism, engaging in any form of political cracking requires at least a minimal knowledge of code and/or hacking techniques, which is still almost unheard of outside the hacker community. Political cracking is thus almost entirely confined to hacktivists who come from hacker backgrounds, or who have spent enough time on hacker sites to acquire the necessary skills. These crackers can work alone or in small groups (sometimes called hacker gangs or crews) in undertaking their various hacktions.

Like their non-political counterparts, most political crackers seem to be quite young – if not teenagers, then not far into their twenties. While there are some women involved in political cracking, most of these teenagers are boys. As Douglas Thomas points out, hacking is very much a "boy culture" in its emphasis on notions of mastery,

competition, and subordination. (Thomas 2002) That carries over to the world of political cracking, in which political site defacements will bear comments like "all those wannabe unicode kiddies who are defacing thinking they have joined us can DREAM ON cuz all they are doing is making themselves more GAY"("http://listserv.gao.gov COMPROMISED" 2001).

Comments like this reflect more than adolescent narcissism. The stunt mentality that pervades cracker culture, whereby site defacements and redirects are a way of demonstrating technical prowess and establishing a reputation as a hacker[12], takes on a somewhat different meaning in the hacktivist context. When cracking is politicized, the attention-seeking character of site defacements, etc. is reframed (at least nominally) as the pursuit of attention for worthy and perhaps neglected issues. The implicit logic is that by drawing attention to these issues, political crackers can affect public opinion, and perhaps even public policy.

That logic is the logic of policy change, not policy circumvention. For all that political cracking uses the language of lawlessness, its impact ultimately depends on the rule of law – or at least on some kind of relationship between public opinion and public policy. Political crackers are, in their own way, conscious of maintaining this distinction between rhetoric and direct action; in the words of one cracker group, "[i]t's just a machine we use to do what we do, not a gun or missile or something"("AIC (Anti India Crew) interview").

---

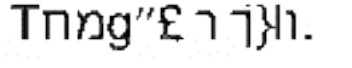
[12] Of course, site defacements, redirects and other forms of cracking only build reputation in the (generally young) segment of the hacker scene that regards cracking as a legitimate or admirable form of hacking. The hacker-programmer "establishment" is not impressed by these kinds of activities – on the contrary, a reputation as a cracker can preclude acceptance into the established hacker-programmer community.

Political cracking: the case of the WFD

The WFD – also known as the World's Fantabulous Defacers – emerged in November 2000, and racked up an extraordinary series of anti-Indian and anti-Israeli defacements over the next two years. The group numbered about a dozen members from five countries ("Interview with World's Fantabulous Defacers"), though reportedly most were from Pakistan (Khan 2001). One defacement lists these members as Nightman, M0r0n, sub-0, Noogie, module, ApocalypseDow and B_Real (B_Real 2001); another lists m0r0n, nightman, Sub-0, Cyberpunk, B_real, laughing3y3s, Sofh, h3ll rais3r, Brake^Off, hid03ous, B1n4ry C0d3 and one additional member whose handle can not be typographically rendered (m0r0n and nightman 2000b)[13].

Estimates of the WFD's total number of attacks vary significantly. The Zone-H defacement mirror lists only 349 defacements (including 26 mass defacements of multiple sites) from November 20 2000 to November 21 2002.("Digital Attacks Archive for WFD" 2004) But Internet security experts mi2g estimated in September 2002 that the WFD had conducted over 400 attacks just in the November 2001-September 2002 period. Since not all WFD attacks are necessarily represented in the Zone-H mirror, this higher estimate is easy to believe. Indeed, the WFD itself claimed that only about 20% of their attacks have been mirrored, since the mirrors are too slow in capturing reported defacements("Interview with World's Fantabulous Defacers").

---

[13] This member's name appears as  .

The majority of these hacks were used to promote "global awareness" (to use the WFD's favorite term) of human rights abuses of Muslim populations in either Palestine or Kashmir, with occasional defacements on other human rights issues affecting Muslims (such as the situations in Chechnya and the former Yugoslavia). WFD members m0r0n and nightman pointed out that the group has a broader agenda:

> We have defaced FOR many issues, if you look at our defacements it says "FREE KASHMIR, PALESTINE, LIFT THE SANCTIONS ON IRAQ, FREE CHECHNIA." So you see we are FOR all those people suffering in the world against atrocities! (m0r0n and nightman 2002)

By the group's own assessment ("Interview with World's Fantabulous Defacers"), its most important hacks have been those against the Bollywood Stock Exchange and Cricketbulls.com, "a site which trades imaginary shares on the popularity of leading Indian players" ("Hackers stump site" 2001). One of the elements that came to distinguish the WFD's defacements was the placement of Flash (Internet-viewable) movies on its web sites. These Flash movies used a sophisticated combination of text, image and sound to create effective messages about human rights issues.

A very typical WFD defacement is the group's February 2001 defacement of an inter-university library network in India, which featured a Flash movie embedded in a very long page of text and images. To illustrate the group's style I am reproducing a series of screen captures from the Flash movie, and a set of screen captures that encompass the complete web page[14] in which it was embedded (see next three pages).

As a group of political crackers, the WFD is both the most transparent and the most opaque of my case studies. On the one hand, everything they have done is online

---

[14] The defacement is archived at http://www.attrition.org/mirror/attrition/2001/02/24/www.inflibnet.ac.in/

and visible: their defacements are archived in the Zone-H and Attrition mirrors, and there is no other WFD activity to be accounted for. On the other hand, because its activities are illegal, the WFD is more elusive than my other subjects. The only source of information about the WFD is the WFD itself. Its web site defacements and online interviews are the ultimate sources of everything that has been written about the group. But m0r0n and nightman's consistent e-mail addresses[15] and ready availability for e-mail interviews makes them one of the few defacement crews for which some (admittedly unverified) biographical details are available. While other WFD members have also conducted interviews, m0r0n and nightman are by far the most frequent and visible interview subjects.

My own e-mail interview with the WFD's m0r0n and nightman has significant overlap with other published e-mail interviews the pair have conducted, since they tend to recycle their answers from one interview to the next. They insisted on being interviewed together, claiming that "[w]e cannot give separate interviews because we don't consider ourselves separate, a team is a team." While that is certainly one credible explanation for their decision to answer collectively, I cannot discount the possibility that this "pair" are actually one person, since I could only find two web pages on which the name of one appears without the name of the other.

Because all information about the WFD flows from the WFD, specifics about the group and its members are very limited – and limited to the areas that group members believe are relevant or desirable to make public. In their e-mailed response to my

[15] When I tried to contact other defacers who had (somewhat unusually) included their e-mail addresses in their defacements, the e-mails bounced, suggesting the accounts had been closed.

questions, m0r0n and nightman declined to share their day-to-day work ("We're all studying. The level does not matter!"); their country of residence[16] ("Dividing people according to country is not our style, as mentioned earlier ``DIVISION`` is not a word in

[16] I later discovered that the pair had identified themselves as Pakistani in some of their pre-WFD hacks.

Figure 2. Stills from WFD Flash Movie "truth9.swf", as seen in a February 2001 defacement

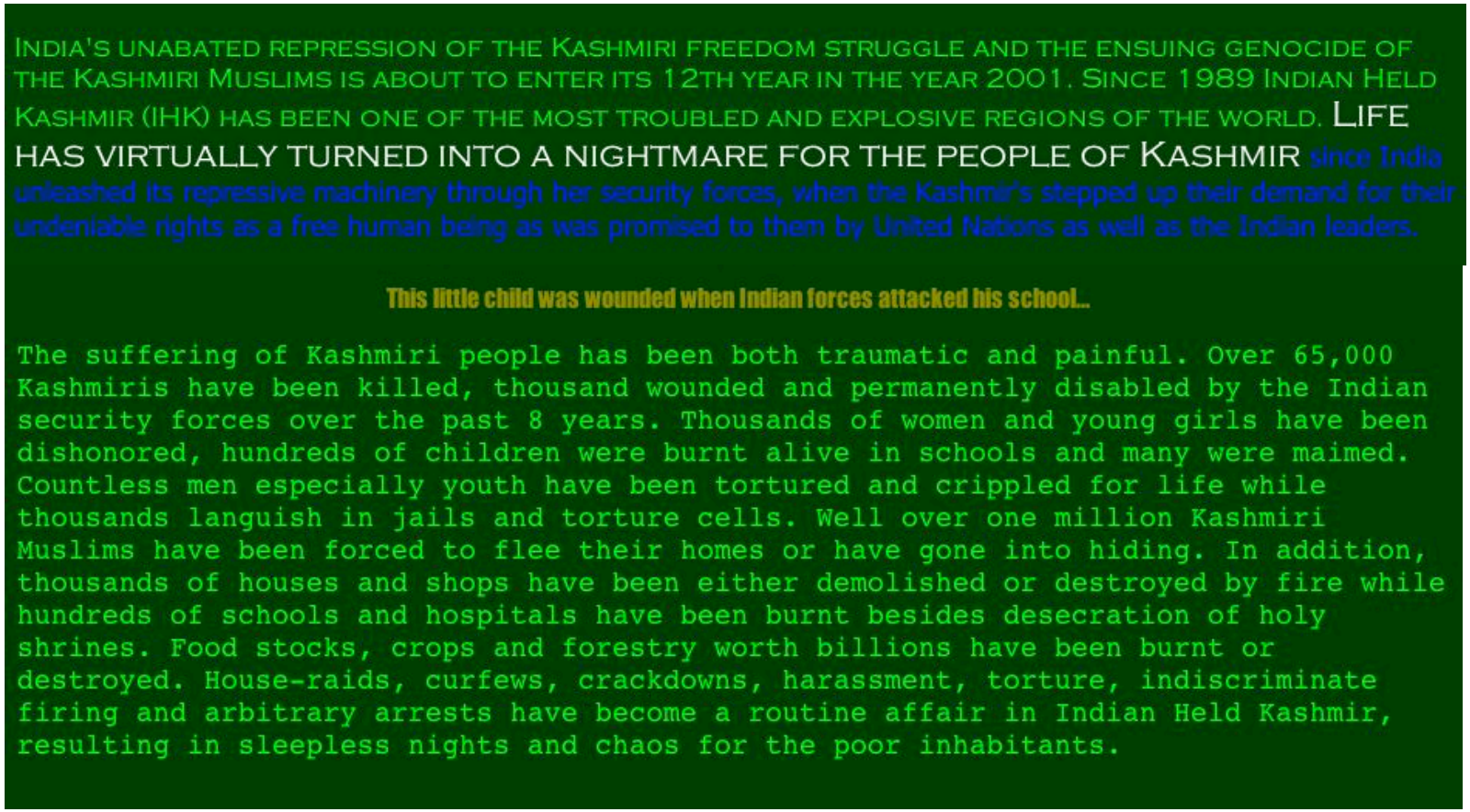


Figure 3. Screen capture of February 2001 web site defacement by WFD (part 1)

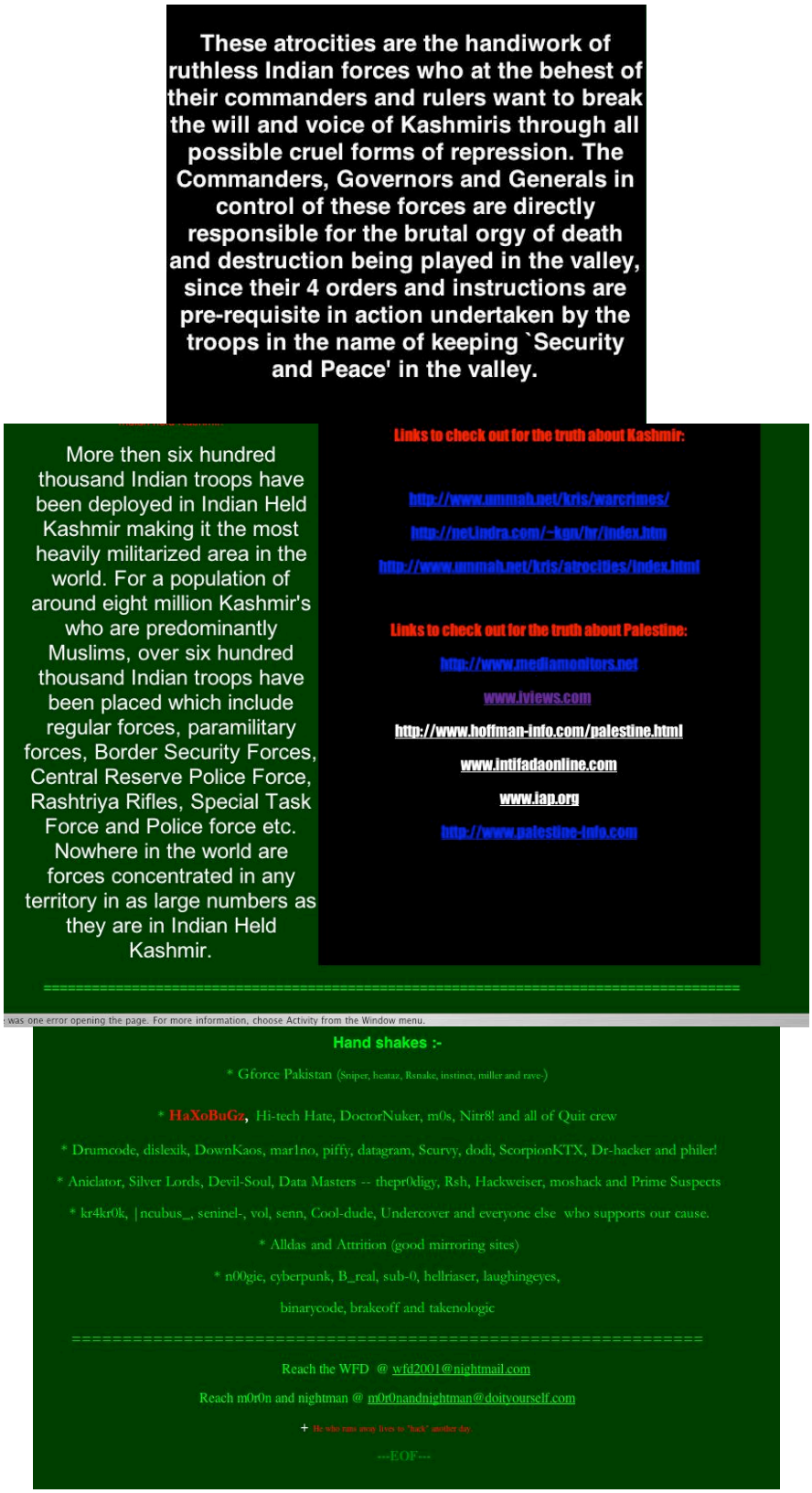


Figure 4. Screen capture of February 2001 web site defacement by WFD (part 2)

our lexicon") and their age ("Old enough to know about the issue we're dealing with inside out.") – although they did state that "We're not old enough to vote yet". And the tone of their answers was further suggestion that they were still teenagers, such as their response to my question, "What hacks do you wish you'd done yourself?": "We'd leave OTHERS to wish they had done what we had done. We do what we wish for!"

Working within these limitations, it is nonetheless possible to construct a basic outline of the WFD's genesis and activities. "We used to hack into systems but for the matter of proving ourselves that we could," m0r0n wrote. "Then one day Nightman & I decided we should do it for a reason!"(m0r0n and nightman 2002)

The pair's initial hacks defaced web sites that seem to have been randomly targeted:

> You are owned by nightman and m0r0n (Pakistan!) We just want to create global awareness so that people might now what Indians are doing to Kashmiris. The members;): m0r0n, NightMan, ftp, code0, laughingeyes, iniquity! (my pal hehe ;), cooldude, pollution, iNfra and Undercover and oh my Computer to ;) Greets: tushay, king, Stargazer, sofh, obi_wan_Kenobi, kitten, pyari, anushah, AlexenderTG, b000m, xpert, Bss (bittersweetsymphony – I did not miss you this time!(m0r0n and nightman 2000c)

The short, plaintext[17] black-on-white defacement was visually different from the rather busy style the pair would later adopt as part of the WFD, and much shorter, but the core message – hacking to promote "global awareness" of Muslim human rights – would remain consistent. The Zone-H archive records 62 hacks under the m0r0n and nightman's handle over the next three months. It is no accident that this defacement was written in English. For the WFD, as with other Islamic hacker groups, "English is currently the lingua franca" and all defacements are posted in English.(Taggart 2001)

---

[17] The term "plaintext" refers to messages constructed strictly in the standard ASCII character set, without the use of images or formatting.

Not long after m0r0n and nightman's hacks first appear in mirror archives, the WFD makes its first appearance. According to the group, its various members came together "sort of haphazardly" ("India Cracked interview with WFD" 2001):

> There is nothing official about the formation of WFD. The first defacement as mirrored by hacking mirror alldas.de is 20th November 2000. At the peak of the Middle East cyberwar that had broken out in late October, m0r0n and nightman were already defacing Israeli websites to spread the truth. CyberPunk & B_Real approached them and joined hands with them on the "global awareness" issue. Then other cyber-warriors like Sub-0 and n00gie shook hands with the truth. We are a team! (m0r0n and nightman 2002)

The first WFD-credited hacks, in November 2000, had no political content – though they bore a closer visual resemblance to the WFD's eventual style. The first WFD defacement that is preserved in the Attrition mirror was an attack on www.oem.com.mx, in which the site was defaced with a simple Flash movie that read, over several screens:

WFD Crew own this
Owned by World Fuck Defacers
members: l^cyBeRpUnK^l, B1n4ry C0d3, Brake^Off,
hid30us, phel0n, Philer, DELAY, Scan_disk&YZT, Module.
wfd@mail.com
weak security means stupidity
(WFD 2000a)

The only elements of this hack that lived on in the style of the hacktivist WFD were the use of Flash, the use of the WFD acronym, and a handful of members: CyberPunk, B1n4ry C0d3, Brake Off, and Module.

m0r0n and nightman were meanwhile continuing their plaintext defacements, expanding the length of their messages as well as the scope of their politics. For example, a November 28 defacement took on human rights in the former Yugoslavia:

> m0r0n and nightman own you. Yugoslavia, which Serbia is a part of started their movement against Kosovah in 1998 in which they conducted a scorched earth policy in Kosova, raising villages to the ground, creating an exodus of over one million refugees and internally displaced persons and committed horrific atrocities against unarmed civilians , including women and children. STOP KILLING INNOCENT CIVILIANS is our message to these people. Stop the violence in Kashmir and Palestine too. The human life is precious and you people donot give a damn about it !!! STOP IT!!! We wish every Muslim a happy Ramadan(or Ramzan). Please remember us in your prayers. All ifs and

> buts to .... m0r0nandnightman@hushmail.com . Greetz to GFORCE Pakistan, DoctorNuker , CyberPunk, B Real and company and all those who support us. Peace @ Kosova , Peace @ Kashmir , Peace @ Palestine and finally Peace @ EARTH! Long Live Pakistan (Pakistan ZIndabad!!!)(m0r0n and nightman 2000c)

We find the WFD's first quasi-political hack on November 28, 2000, in m0r0n and nightman's plaintext style:

> 0wn3d by WFD now were defacing for Global Awareness, ...CyBeRpUnK strikes again(WFD 2000b)

By early December, the group had found its combination of political message and visual style. A December 3 defacement of a a regional government web site in Italy combined images from the Palestinian-Israeli conflict with a lengthy message about Israeli human rights violations in Palestine:

Figure 5. WFD site defacement, December 2000.

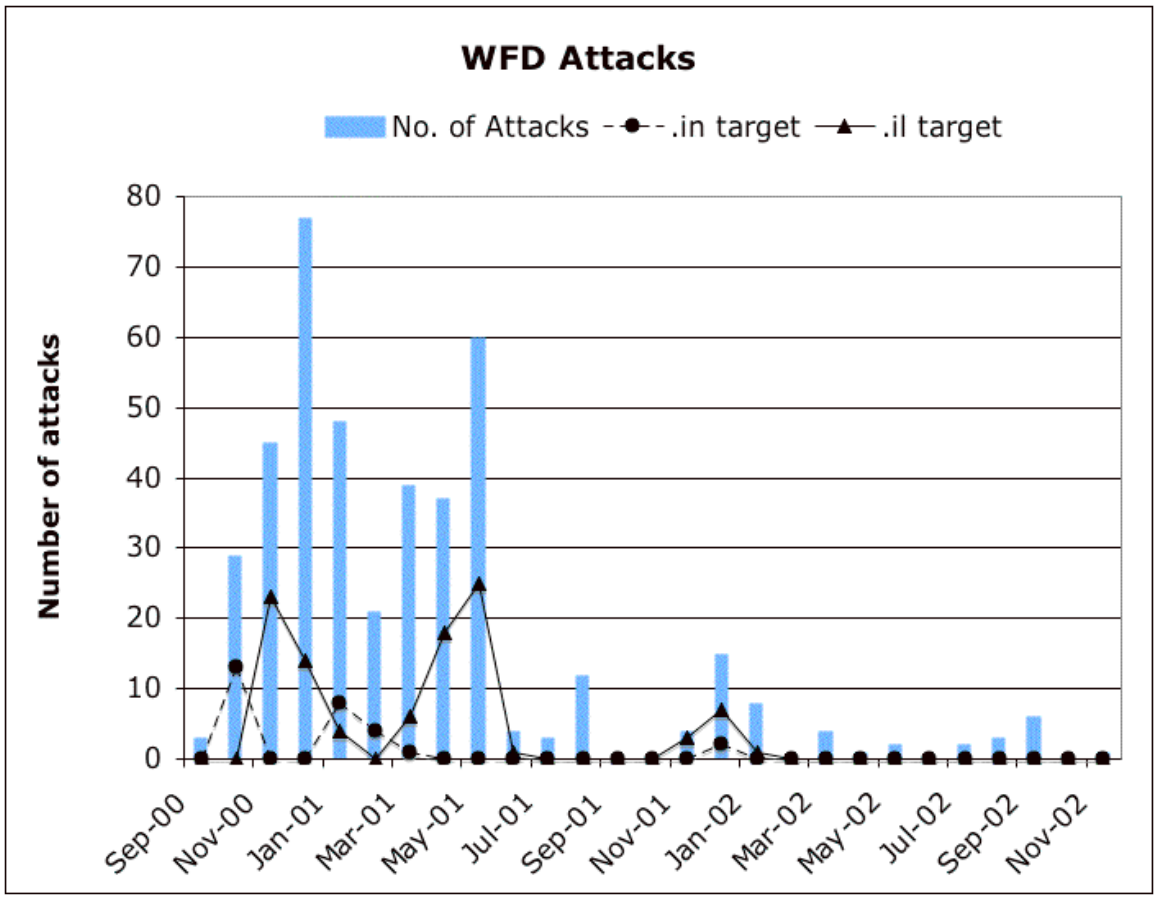


Figure 6. WFD attacks by month and top level domain

An analysis[18] of the defacement statistics archived on http://www.zone-h.org show that December 2000 was the WFD's most active month: Zone-H records 76 defacements that month, out of 424 from September 2000 to September 2002. This analysis further shows that while the group initially focused on Indian web sites in its late 2000 attacks, it quickly shifted to primarily attacking Israeli or Israel-linked sites.

[18] The analysis is based on a list of 424 attacks in the Zone-H archive, including those credited to WFD members m0r0n, CyberPunk and n00gie as well as those credited WFD itself. I used the top level domain of each target (e.g. .com, .il, .in) to indicate the country of target, though this was really only useful in establishing the relative focus on Indian versus Israeli targets, since many targets with other TLDs nonetheless corresponded to Israeli or Indian web sites.

The top level domain (TLD) is only an imperfect measure of the targeted site's nationality, but the peaks in .il (Israel) and .in (Indian) targets do provide a rough indicator of the group's shifts in focus. But .il and .in targets only make up a total of 24% and 6.6% of the WFD's targets, respectively; the group also targeted many.com and .net sites, as well as some .mx (Mexican), .yu (Yugoslavian), .tw (Taiwanese), .au (Australian), .edu, .gov, and assorted other TLDs. Some of these other TLDs still corresponded to Indian and Israeli sites, such as www.semiotica.net (an Israeli site hit in April 2001), www.natyavihar.com and www.bonafidesurgicals.com[19] (two Indian sites hit in January 2001).

Some TLDs correspond to non-Indian, non-Israeli sites that were nonetheless strategic targets, such as the web site of a US Veterans Affairs clinic that was defaced with a message that began, "m0r0n and nightman of WFD (World's fantabulous defacers) own a Government site to spread their message."(m0r0n and nightman 2000a) A similar example was the Navy Marine Corps relief site defaced with the message:

> Site defaced by WFD (World's fantabulous defacers) Free Kashmir and stop the violence in Palestine!! The U.S. Military is giving a helping hand to the corrupt Indians and the Israelis. But they don't know that the truth always previals!! Contact us @ wfd2001@nightmail.com(WFD 2001)

And the web site of the Newspaper Association of America was attacked in January 2001 with a message about US complicity in Israeli actions against Palestinians:

---

[19] As with a number of sites that the WFD targeted, Bona Fide Surgicals is no longer online at this address. Because site identification was often crucial to assessing whether a target was randomly or strategically chosen, I used the waybackmachine to visit web sites that are no longer online. A project of the Internet Archive, the waybackmachine regularly archives cross-sections of the Internet such that at least some pages were archived for each of the sites I needed to identify.

Figure 7. WFD site defacement, January 2001.

The defacement contained a long multi-part message that included discussion of Palestinian feelings about Israeli occupation, details on specific incidents of anti-Palestinian violence, and a description of US assistance for Israel. Its opening words made the choice of target clear:

> The newspapers of America are full everyday with flagrant lies about the events happening in the Middle East. In fact, the entire American media distorts the truth and twists it as to manipulate the minds of the American people. Suffering Palestinian children are portrayed as "terrorists", simply because they fight for their freedom from an oppressor that seeks to destroy their hopes and dreams.

The defacement concluded in similar terms:

> Our message to the newspapers of America
> STOP BLINDLY SUPPORTING ISRAEL WHICH IS, UNDOUBTEDLY, THE LAST THEOCRACY/FASCIST STATE LEFT IN THE WORLD. START TELLING THE TRUTH ABOUT WHAT HAPPENED AND IS HAPPENING IN PALESTINE, as well as the truth about Kashmir and Chechnya.(WFD 2001)

Still other sites, such as trendmicro.com.cn (a Chinese computer company hit in December 2000) and www.vwtrendsweb.com (an automotive magazine) seem to have been randomly chosen. Another apparently random target, a now-defunct US-based

"Midwest Source for Hip-Hop Info and Gear", was defaced with a message that described the attack as retribution for a hack against an English language Muslim web site:

> This is a reply to the Israeli hackers who hacked www.iviews.com. Just to show them that we are not as yet caught or dead! We will always rise when we are needed! -- wfd!

In their interviews –- with me and with others – m0r0n and nightman are less interested in exploring the details of their hacktivism than in recapping the same issues they spotlight in their defacements. In response to the question "what effects do you think your hacktivism has had?" the pair offered a very long history of the Kashmir conflict, detailing Indian human rights violations in the region, before briefly addressing the original question with the comment that "[u]s defacing sites may not bring peace, but it will certainly create global awareness about the suffering of the Muslims of Kashmir, and the righteousness of their cause."

m0r0n and nightman appear to see their hacktivism as a world away from offline political action. When asked "what other kinds of political activity have you been involved with, on or offline?" they responded:

> Haha ... we've helped Osama Bin Laden in doing some stunts & stuffs! Man, we're hacktivists. It's not PHYSICAL WAR! [20]This is the only thing we do. We do what we're best at!(m0r0n and nightman 2002)

---

[20] This argument seems to do justice to the experience of at least one of the WFD's targets. The webmaster of HelpingIsrael.com, an online crisis center that the WFD defaced, wrote of her ultimate reaction to the defacement:

> These digital demons were getting the best of me, and my husband was giving me that "You're a bit touched, aren't you?" look. So I blurted out: "You have no idea what it's like to be a victim of cyberterrorism!"
> I said this to a man who had spent 27 years in the IDF, who had buried comrades, friends and real terror victims.
> Then it dawned on me... it's "virtual," stupid! I'm letting my real world get swept away by some "virtual" goons.
> They can't undo the good that's already been done or break-up the supply lines and connections that have already been established between the donors and the communities (those transactions take place by "snail mail").

This was the only reference I found that provided any thread of connection between the WFD and the events following 9/11. The small spike in WFD activity that is apparent in September 2001 makes eminent sense in the context of the upsurge in both pro- and anti-Islamic web hacking after the September 11 attacks. But it is impossible to evaluate the WFD's response or position in regard to the 9/11 attacks because there are no mirrors available for the period in question.

The group's defacement streak came to a sudden and unexplained end in November 2002. My efforts at contacting m0r0n and nightman for an explanation have gone unanswered. One possibility is that the WFD has been absorbed into a new or different hacker group. Security analysts mi2g reported in June 2002 that the WFD had become part of a larger alliance of Islamic hackers, but their report seems to be at least partially based on the fact that "[I]n a recent anti-Israeli overt digital attack, WFD acknowledged 32 other hacker groups and individuals, many of them with anti-US/UK and anti-India agendas." ("Pro-Islamic Hacker Groups Joining Forces Globally" 2002) As the above examples of WFD hacks should make clear, it is a common hacking practice to send "greetz" to like-minded hackers, and not necessarily a sign of some more organized collaboration. My own research has found no evidence to suggest that WFD members are

---

> Let them waste their time, money and energy on virtual destruction, while I devote my energies to my real family and productive endeavors.
> Real anxiety is when you send your husband and children off in seven different directions in the morning not knowing if Hamas, those only-too-real masterminds of evil, are serious about their top-10 terror countdown.(Horowitz 2001)

now part of another organization; it seems equally likely that they have simply outgrown their hacking phase.

Performative hacktivism: an introduction

Performative hacktivism consists of legally ambiguous hacktions, undertaken by hacktivists with artist-activist backgrounds. It draws heavily on the tradition of political theater in its adaptation of hacking for political purposes. The term "performative" not only captures the broad notion of hacktivism as performance – which these hacktions most certainly are – but also the more particular idea of political protest as a "speech act". The notion of politics as spectacle that has informed performative hacktivism also characterizes a wider array of "carnivalesque" protest tactics popularized by the anti-globalization movement (Boje 2001).

Many performative hacktivists come from theater or art backgrounds, and see hacktivism as a new form of political art. Some of these hacktivists produce other forms of Internet or digital art, in addition to their hacktivism. And even those performative activists who are not artists per se share the aesthetic and theoretical baggage of the postmodern left.

Some examples of art from members of the hacktivist community:
Carnivore (Alex Galloway)
Virtual Quilt (Carmin Karasic)
FadeForward (Ricardo Dominguez)

Since performative hacktivism emerges out of a left political culture, we should not be surprised that it usually focuses on left-wing issues such as globalization, liberation struggles (especially that of Mexico's Zapatistas), and corporate power. Many performative hacktions have been coordinated, or at least timed to coincide, with simultaneous street protests.

The most visible groups of performative hacktivists are the Electronic Disturbance Theater, ®™ark, and the electrohippies. The Electronic Disturbance Theater is a group of four U.S.-based activists who banded together in 1998 to create a digital protest in solidarity with the Zapatistas. ®™ark is a U.S.-based activist "mutual fund" that sponsors acts of "anti-corporate sabotage"—including a number of hacktions. ("®™ark Website", "Bringing it to You" page) It uses its status as a legal corporation to both spoof and (potentially) benefit from limitations on corporate liability(Sebok 2001). The UK-based electrohippies collective was created in July 1999 with the intention of using the Internet to challenge the commercialization of cyberspace; until it disbanded in July 2002, it focused its activities on anti-corporate hacktions like its virtual sit-in against the WTO.

Performative hacktions have encompassed a wide range of issues, but usually focus on offline issues like globalization and human rights. They almost always engage a transnational coalition of activists, even if the sites are assembled by hacktivists in one country who then solicit sit-in participation from a broader cross-national population.

Performative hacktivism mostly takes the form of virtual sit-ins or site parodies – forms of hacktivism with clear precedents in the traditions of street protest and political theater. This area of hacktivism has also made some moves into the field of software development, but only as a way of facilitating the primary tactics of sit-ins and site parodies. The EDT developed an open source version of its sit-in tools, and a group called the Yes Men have created software that automates the creation of web site parodies.

While performative hacktivist tactics are carefully constructed to avoid clear legal jeopardy, they are not without legal risk. The virtual sit-in tactic is essentially a less illegal version of the denial-of-service attack; since actual people are loading the pages that overload a server, it is not clearly illegal. But at least one virtual sit-in (conducted by the EDT in 1998) was counter-attacked by the U.S. military (Schwartau 2000), and a site parody (of the WTO's web site) faced the threat of legal challenge (Ramasastry 2002).

The intensity of the reaction that these hacktivists have provoked attests to the success of their hacktions as performance. Performative hacktivists are very much oriented to the public eye, and see their activities as a way of challenging corporate and media domination of public discourse. Their hacktions are aimed at shifting that discourse by raising awareness and creating public pressure – not at directly affecting outcomes.

As this may suggest, performative hacktivism is more theory-driven than other forms of hacktivism. Performative hacktivists often cite European critical theorists as sources of intellectual inspiration in their efforts to comprehend the political or performative dimensions of cyberspace: Ricardo Dominguez offers a typical voice when he writes that "[r]ecombinant culture, the implosion of genetics and speed, creates a spasm of hypermorphic delusion wherein Sandborn-understands-Virilio-as-Hegel-understands-Napoleon."(Dominguez 1996) Different performative hacktivists offer different theoretical takes on the nature of hacktivism, but a common theme is the way the Internet has changed the relationship between the human body and human identity. Performative hacktivists use the Internet as a way of exploring the new virtual body, and its relationship to the corporeal world; they sometimes argue that power has shifted

altogether into the virtual world, and thus needs to be challenged within cyberspace itself. In the opening words of *The Electronic Disturbance*, a theoretical work that has informed the activities of the EDT in particular:

> The rules of cultural and political resistance have dramatically changed. The revolution in technology brought about by the rapid development of the computer and video has created a new geography of power relations in the first world that could only be imagined as little as twenty years ago: people are reduced to data, surveillance occurs on a global scale, minds are melded to screenal [sic] reality, and an authoritarian power emerges that thrives on absence. The new geography is a virtual geography, and the core of political and cultural resistance must assert itself in this electronic space. (Critical Art Ensemble. 1994, p.3)

Performative hacktivism: The case of the Electronic Disturbance Theater

The Electronic Disturbance Theater was the first performative hacktivist group, and remains an influential leader. The group has four members, all American, although they are geographically scattered and mostly collaborate remotely. Best-known for its invention of the virtual sit-in technique, the group works on a variety of offline progressive issues – most notably, the human rights record of the Mexican government – with projects that are as much art as politics. If performative hacktivism owes a big debt to political theater and digital art, that is partly the influence of the EDT.

The EDT, in turn, owes a debt to the Critical Art Ensemble (CAE), a group that included EDT founder Ricardo Dominguez. A handsome Mexican-American with funky horn-rimmed glasses, Dominguez talks just like he writes: heavy on the critical theory, more like a performance than a conversation. The artists of CAE collectively wrote several books that lay the theoretical foundations for performative hacktivism, including *(Critical Art Ensemble 2001; Critical Art Ensemble. 1994; Critical Art Ensemble. 1996).* In an interview, Dominguez said he left the CAE because he was frustrated that the group was unwilling to put its theories of "electronic civil disobedience" into practice.

Dominguez later made that translation himself, as the founder of the Electronic Disturbance Theater. The EDT was initially geared towards action in solidarity with Mexicon's Zapatista rebels. At the time of the 1994 rebellion, Dominguez was an aspiring digital artist, supporting himself as a network administrator for a progressive computer network in New York City. He was particularly impressed by the Zapatistas' creative use of the Internet, and by their innovative ways of engaging the broader Chiapas community. Take their concept of organizing topical roundtables: setting up discussions around different topics, like music or literature, so that regular people could talk about their ideas and help the Zapatistas brainstorm.

Dominguez decided to adapt the Zapatatistas' tables to an international network setting. He elicited an invitation from MIT as a sort of artist-in-residence, while remaining primarily in New York. But MIT still gave him the resources he needed for his own creation of Digital Zapatismo: a virtual network table, an extension of the Zapatistas' own network table.

He used free audio and video software to run a virtual network table three times a week, for four months. The "table" consisted of inviting various people to talk to him, either by phone or in person; he then broadcast the whole thing over the Internet, and projected it at MIT. Discussions covered a range of issues the Zapatistas had raised, from the future of neoliberalism to the rights of indigenous peoples. These conversations lasted anywhere from two to six hours at a time.

Through his network table, Dominguez came into contact with the other three future members of the EDT. Carmin Karasic was the MIT lab assistant assigned as his technical support. Stefan Wray was living in Austin, Texas when Dominguez

interviewed him about his writings on the US military's role in Mexican drug wars. And Brett Stalbaum was a fellow Internet artist, based in California, who joined Domiguez's mailing list.

The four formed a partnership when the Mexican government returned to Chiapas in full force in December 1997, leaving forty-five unarmed peasants dead in the village of Acteal. The "Acteal Massacre" galvanized the members of Domiguez's incipient network, beginning with Karasic, who e-mailed Dominguez with a request for the names of the Acteal dead. Her intention was to create an electronic monument herself.

Meanwhile Dominguez had been contacted by the Anonymous Digital Coalition, a group of activists based in Italy. The ADC had developed a plan for encouraging people to simultaneously visit a given Mexican government website, constantly reloading a given web site until the server slowed or crashed. Dominguez forwarded the ADC e-mail to his own e-mail list, and immediately heard back from Stalbaum. Stalbaum offered to write a simple program that would make web browsers reload the targeted web page automatically, greatly increasing the effectiveness of the attack. But he was only interested in writing the program, and not in designing its appearance.

Dominguez's solution was to enlist Karasic to design the interface, integrating the net attack into her plan for an Acteal monument. Wray was brought in as a fourth collaborator, to give theoretical depth to their work. Within two weeks, the team had created the first "virtual sit-in" tool, which they named the Zapatista FloodNet. The FloodNet could be used to orchestrate a coordinated attack in which sympathetic computer users could cheaply and easily participate in a protest, from the comfort of their own homes or offices. The EDT would announce a given target and a protest date and

time. All a would-be participant needed to do was download the FloodNet code sometime before the protest was to take place. At the appointed hour, all those participants would activate the code –- itself just a simple script that sent a command to the participant's web browser – and all of their browsers would simultaneously point to the target's web site. The FloodNet code would automate the "refresh" function on the browser, constantly loading and reloading the target's web page on the computers of each and every participant. The flood of simultaneous, constantly re-issued page requests would overload the server. And while the effectiveness of the attack did not depend on the participants having any particular visual experience, the EDT designed the FloodNet code to incorporate a protest message.

The FloodNet sat halfway between a distributed denial of service (DDoS) attack (a longstanding hacker technique) and the kind of manual sit-in envisioned by the Anonymous Digital Coalition. In a DdoS attack, computer hackers infiltrate thousands of private computers in order to direct them to simultaneously target given web sites, so that the targets shut down in the face of overwhelming traffic. The tactic is effective, but lacks public credibility because it can be conducted by a lone hacker, appropriates the computers of innocent bystanders, and is unambiguously illegal. But the ADC's proposed tactic had the opposite problem: its reliance on individual users to target and reload web pages made it inefficient, and unlikely to yield any tangible results without millions of simultaneous participants.

The EDT's FloodNet, in contrast, could hope for some effectiveness – in slowing or even crashing servers – even if participants numbered only in the thousands. But the need for some critical mass allowed it to lay claim to the tradition of "mass" protest, as

did the fact that its effects would be proportional to the number of participants (because more participation translates into more traffic, and more traffic translates into slower and slower servers). The EDT also tried to shore up its legitimacy by departing from usual hacking practices, according to Dominguez:

> I decided that we would become the Electronic Disturbance Theater, and then we made a decision that was very very strange but that seemed on a gut level what we needed to do, but it went against all the usual elements. We decided not to be anonymous. Not to be secret – to be transparent. And this went against hacker culture, which is about anonymity, which is about secrecy. We also pushed open source. That is, all our code had to be very simple, you know, anybody can use it. We would also let people know what we were doing, when we were going to do it, how we were doing it. And I felt this would create a much better drama.(Dominguez 2002a)

EDT's first action was on April 10, 1998: a virtual sit-in targeting the web site of Mexican President Ernesto Zedillo. Stefan Wray later noted that:

> We had 8,141 separate hits on the Zapatista FloodNet browser aimed at Zedillo's web site. We are fairly certain we did not shut down this web site, although we did receive a message that read, 'I think the Mex server just crashed.' We think this message reflects the fact there were sporadic moments when access to the site was slowed down or even blocked.(Wray 1999b)

In what would become characteristic of both the EDT and the larger world of performative hacktivism, the group focused as much on media coverage of their hacktion, as on the hacktion itself. From the beginning, the group measured its success more in terms of press coverage (which drew attention to the Zapatista plight) than in terms of the actual slowing or crashing of servers. By that standard, the EDT could be thrilled with its first FloodNet, which was covered on the web site of the New York Times:

> Don't call them hackers. Ricardo Dominguez and Stefan Wray consider themselves theorists and practitioners of "electronic civil disobedience." …In an early test of their system, Dominguez and Wray posted messages in the Zapatista networks in early April, calling for colleagues to link to FloodNet on April 10. The target that day was the Web site of President Ernesto Zedillo of Mexico. According to Dominguez, 8,141 surfers around the world connected to Flood Net that day, which resulted in some slowing down and interruption of the Zedillo site. Dominguez added that a computer from Mexico tried to hack into Flood Net and disable its program, but was unsuccessful.(Kaplan 1998)

The encouragement came at a crucial time, when the EDT was escalating its FloodNet campaign. Throughout the spring, they kept their sights trained on the Mexican government, organizing actions, giving talks, and publishing articles. In a later speech, Wray described this period as one in which:

> our greatest admirers were among digital artists, while our harshest critics were within the left. Most digital artists were able to see immediately, almost intuitively, the value of our work. But leftists raised age-old questions about effectiveness and responsibility, while hackers thought that we were too soft. Through quite a number of email listservs, we provoked discussion among a range of people. Conversations about what we did and said rippled out way beyond our small group of four.(Wray 1999b)

Thanks to their rising status in the digital art scene, the group received an invitation to the Ars Electronica festival in Linz, Austria, which describes its mandate as

> tracking and nurturing the digital revolution, analyzing the social and cultural effects of digital media and communications technologies from critical as well as utopian, artistic and scientific perspectives, thinking them through and inferring potential developments.("Timeshift: The World in Twenty-Five Years" 2004)

The festival was scheduled for September, 1998. The EDT called its proposal for the festival the SWARM:

> Think of a swarm as an array of Flood Net-like devices, arising, acting, and dispersing simultaneously against an array of cyberspacial political targets. If the electronic pulses generated by our Flood Net actions are represented by a small mountain stream, the electronic pulses generated by a swarm of convergent ECD actions are a raging torrent.(Wray 1998)

The project was described in greater detail in the group's August 25 press release, announcing its planned action during the festival:

> NETSTRIKE AGAINST GOVERNMENT, MILITARY, AND FINANCIAL WEB SITES IN MEXICO, THE UNITED STATES, AND GERMANY: CALL FOR FLOODNET ACTIONS (SWARM) ON SEPTEMBER 9 -- AGAINST PRESIDENT ZEDILLO, PENTAGON, AND FRANKFURT STOCK EXCHANGE
>
> In solidarity with the Zapatistas, indigenous peoples in Chiapas, others resisting the Mexican government, the global pro-Zapatista movement, and people everywhere struggling against neoliberalism and the global economy, the Electronic Disturbance Theater urges SWARM actions, multiple acts of Electronic Civil Disobedience, on Wednesday, September 9, 1998.

To demonstrate our capacity for simultaneous global electronic actions and to emphasize the multiple nature of our opponents, FloodNet will target three web sites in Mexico, the United States, and Europe representing three important sectors: government, military, and financial.

In Mexico, FloodNet will target President Zedillo's web site, (http://www.presidencia.gob.mx/) an obvious choice and one we have made before. In the United States, FloodNet will target the Pentagon, (http://www.defenselink.mil/) also an obvious choice given the level of U.S. military and intelligence involvement in Mexico. And in Germany, FloodNet will target the Frankfurt Stock Exchange, (http://www.exchange.de/) a less obvious choice, but one that makes sense as it is a key European financial site with high symbolic value and as Germany is a major player in the global neoliberal economy.(Electronic Disturbance Theater 1998)

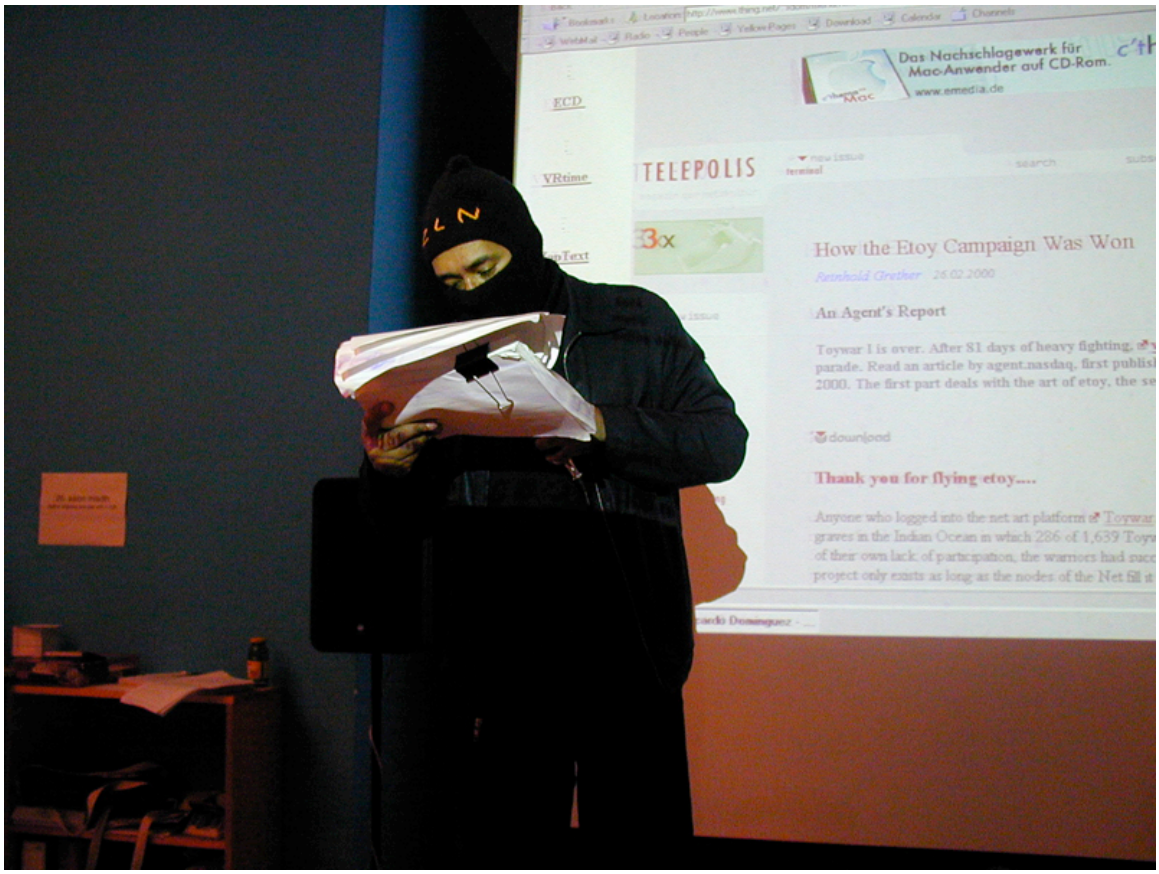


Figure 8. Ricardo Dominguez in performance (occasion unknown).
(Image available at **http://boo.mi2.hr/~zblace/mi2_4promo/**)

At the festival itself, EDT members found fresh fodder for their view that the FloodNet put them on the front line of a battle between digital art and computer hacking.

Festival organizers had convened a hacker gathering in conjunction with the festival, and according to Dominguez, the hackers took a hostile stand towards the EDT's planned installation. "They said, 'Ricardo, Stefan, what you're about to do will destroy infrastructure. And if you guys do it, we will take you down.' It was our first encounter with what I call the 'digitally correct' community. Those who believe that bandwidth is above human lives."(Dominguez 2002a) Also according to Dominguez, the group received its first threat:

> I was getting a lot of calls from the press. So at 7:30 in the morning I wake up haphazardly and they go, is this Ricardo Dominguez? I said, yes. Electronic Disturbance? Yes, yes. Then in very clear, Mexican Spanish, they said, we know who you are, we know where you're at, we know where your family is, do not go downstairs, do not do this performance. You know that this is not a game. You know what will happen to you.(Dominguez 2002a)

The group's immediate reaction was to put out a press release, announcing the threat. But the phone call was quickly eclipsed by the news that the installation itself had crashed.

> According to highly placed Pentagon sources, the Floodnet assault was pre-announced by the EDT so the Pentagon was able to prepare for it. Its response was orchestrated by the Defense Information Systems Agency (DISA), which has experience with both defensive and offensive cyber-tools. Once the attack began, the Pentagon launched a denial of service attack of its own. Requests from the EDT browsers were redirected to a Java applet called 'hostileapplet,' which Dominguez says crashed the browsers. The applet fired a "series of rapidly appearing Java coffee cups across the bottom of the browser screen coupled with the phrase 'ACK.' FloodNet froze," he says. (Schwartau 1999)

The Pentagon's counter-attack had implications that were larger than the EDT could have hoped for. An 1878 law, Posse Comitatus, prohibits the US military from engaging in domestic law enforcement; observers raised the question of whether the response to SWARM was a violation of that law.(Schwartau 1999) The group used the

issue to raise the possibility of a lawsuit – another publicity-generator – but did not pursue it.

A further encounter with the defense community came one year later, in the form of an invitation to speak – or "perform" – for a meeting of National Security Agency. Arranged by Schwartau, the meeting was intended to give NSA officials a chance to assess the EDT for themselves, and to consider whether the group's tactics – which were quickly spreading to a broader community – should be considered cyber-terrorism. While no public verdict was issued, the EDT has not recorded any subsequent counter-attacks from the Pentagon. Dominguez was nonetheless frustrated with what he perceived as his audience's failure to understand the EDT's performance:

> I don't know if you've ever read the very first play written here in the United States, "My Country Cousin," which is kind of a Daniel Boone type character from Kentucky being invited by his city cousins in Philadelphia – remember Philadelphia was the city of cities at that particular time – and they invite him to go to the theater. Well, halfway through the play he gets up, runs onstage, and hits the bad guy. And of course everybody's wondering what's going on. And they have to explain to the country bumpkin that it's a simulation, that the evil guy is not really evil, that he's only pretending. And so basically what the NSA and these information agencies, and hackers, in looking at EDT, are kind of like country bumpkins. They actually believe that Hamlet is killing Claudius. Instead of thinking hey, this is a really good performance, it actually seems real, it's moving, it's bringing me to really think out certain questions. And this is where they haven't read their Baudrillard. And perhaps they did read it, but misunderstood it.

The EDT has retained not only its high-minded theoretical approach, but also its specific dual foci on indigenous rights in Mexico, and distributed denial of service attacks. The group helped to organize a 2002 virtual sit-in against the Mexican supreme court, as well as a 2003 "Operacion Digna" protest against the Mexican government, and the Supreme Court of Chihuahua(fusco 2003)**.** But they have also broadened their activism to encompass issues like globalization and corporate power, collaborating in the

1999 “toywar” protest against the eToys corporation[21] and the 2002 protest against the World Economic Forum (Dominguez 2002b). The individual members of the EDT have also continued to pursue their respective careers as Internet artists and theorists by writing, performing, teaching, and exhibiting their work. The separate accomplishments of each EDT member and the collective reputation of the EDT as a hacktivist leader seem to be mutually reinforcing.

The EDT’s activities have been crucial in defining the activities and culture of the performative hacktivist scene. The group’s November 1998 release of its FloodNet code has allowed other groups to conduct virtual sit-ins for their own purposes: examples include a 1999 protest over arms control issues("Call for Electronic Civil Disobedience" 1999); an October 2000 Italian virtual sit-in over a censorship incident("The Axe of Censorship Falls on the Roman Civic Network" 2000); and a 2001 “living wage” virtual sit-in organized by the EDT on behalf of Harvard’s Progressive Student Labor Movement (Costanza-Chock 2001).

The EDT’s cross-pollination of political theater, digital art, and progressive politics has also been influential. It has extended networks among theater, art, and activist circles, and encouraged members of those circles to upgrade their technical skills. And its application of political hacking to offline issues has helped make hacktivist techniques – especially the virtual sit-in – part of the political repertoire for activists on a number of progressive issues, such as globalization, indigenous rights, and corporate power.

---

[21] See Chapter 4 for details on this case.

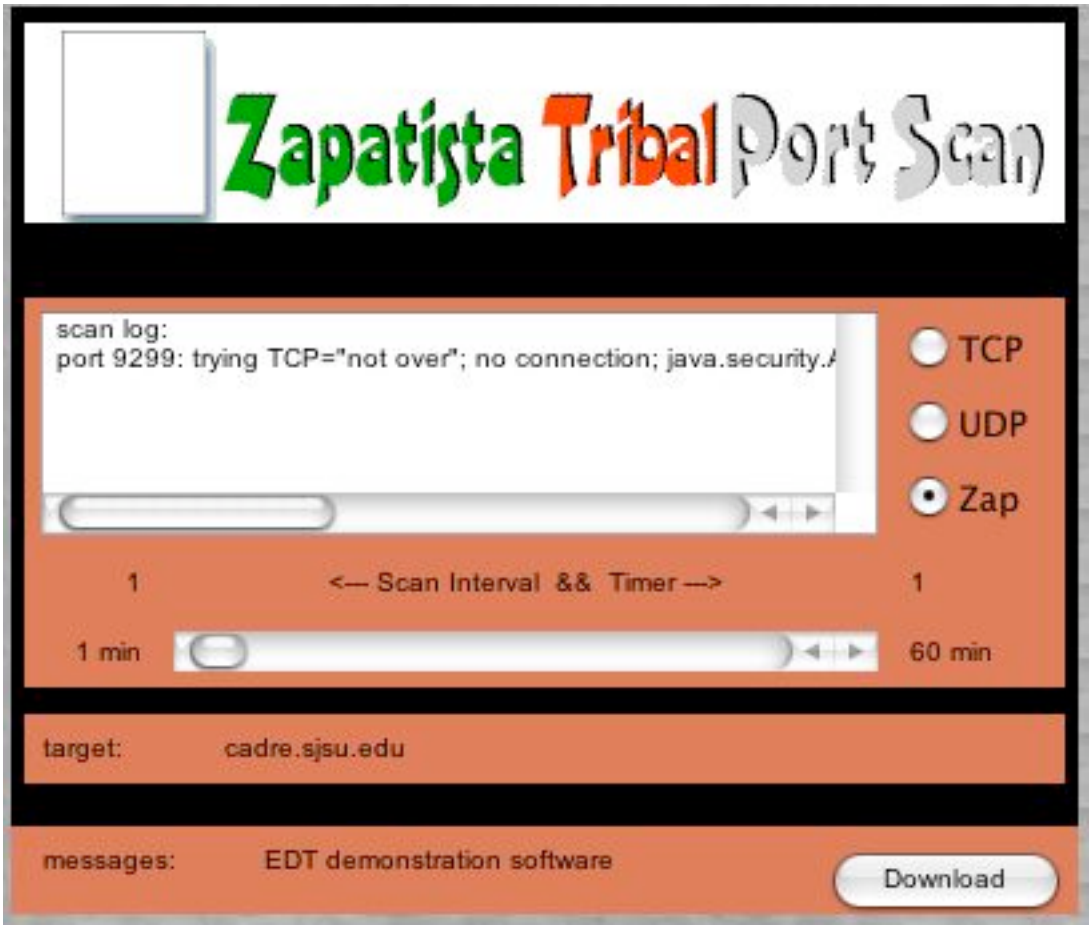


Figure 9. The FloodNet Interface

The EDT members seem to have benefited personally from their involvement in performative hacktivism. The two members I interviewed – Dominguez and Karasic – were basically unknown to the digital art world when they formed the EDT. But in the intervening years, they – along with Stalbaum and Wray – developed a significant profile in the worlds of digital art and progressive activism. Three EDT members (Dominguez, Karasic, and Stalbaum) have been frequent contributors to digital art shows, which have further exposed digital artists to the tactics and potential of performative hacktivism, Two members (Wray and Dominguez) have written and spoken widely on the theory and application of electronic civil disobedience, often drawing linkages to contemporary

critical theorists (such as Baudrillard and Virilio) that have currency with some artists and left-wing activists. Their personal profiles as artists and theorists have been boosted by the notoriety of the EDT, and the EDT's credibility has benefited from the increasing visibility of its members.

Political coding: an introduction

Political coding consists of hackers turning their technical skills into transgressive politics. These hackers are, metaphorically at least, the older brothers of political crackers. Many of the hackers who participate in political coding started out as non-political hackers, programmers or crackers, and came to political coding as an outgrowth of that activity. They typically adhere to the hacker convention of using handles (or pseudonyms), though the real names that correspond to most of these handles are relatively easy to ascertain.

Political coding so far reflects the cyber-libertarian worldview described by Barbrook and Cameron (1995), Katz (1997), Norris (2001) and others in their description of Internet political culture. This cyber-libertarian ideology emphasizes individual rights, especially online rights, as the most important political good. This viewpoint explains why political coding has focused entirely on issues that are directly related to the hacker community. Some hacktivists argue that this focus on Internet-oriented issues is core to the notion of hacktivism – that hacktivism is, by definition, activism related to the Internet. (Ruffin 2002)

Several political coding projects have facilitated the distribution of DeCSS, a piece of software that decrypts DVDs for playback on Linux machines. The software has been banned at the behest of the Motion Picture Association of America (MPAA) which

objected to the cracking of its CSS encryption, meant to prevent copying of DVDs. The DeCSS coding projects have been undertaken by solo or small-group actors, working anonymously or pseudonymously.

Another strand of political coding focuses on Internet censorship, particularly as it affects democracy activists in authoritarian regimes. Internet censorship has been the chief target of the Hacktivismo project, sponsored by the Cult of the Dead Cow (cDc). The Hacktivismo project has rapidly become the center of the political coding scene, and has received a great deal of media attention.

Both of these projects aim not at influence, but at policy circumvention. The various programs aimed at disseminating DeCSS are not trying to change the legal rulings on DeCSS decryption; they are trying to make those rulings unenforceable and meaningless. Hacktivismo doesn't try to directly change the Chinese government's Internet censorship policy; it develops ways of evading that censorship, regardless of the government's policy.

In the process of circumventing policy, these projects may also have some policy impact by raising awareness of the issues they focus on. The Hacktivismo team, in particular, takes care to publicize its activities in order to increase media coverage of the censorship issue. But awareness and influence are useful byproducts, not the primary goal.

The ability to circumvent policy depends on hacktivists committing the time to develop and complete a software product. The software that political coders develop is virtually always open source, which means it can be freely distributed, modified, and improved by other coders. The open source model lessens the burden on any one

developer or team, but software development is still a time-intensive form of hacktivism, compared with defacing a web site.

It is also skill-intensive, since it demands a core team of coders. But not all political coders are programmers: a number of people involved in the Hacktivismo project contribute other kinds of skills, like writing or web design. While this suggests that political coding does not necessarily require a high level of programming knowledge, even non-programmers tend to have some background in Internet-oriented activities. Although they may not be hackers per se, they are certainly conversant in hacker culture.

The legal risks associated with political coding vary from project to project. Jon Johansen, the Norwegian teenager who created the original DeCSS software, was indicted in Norway, and cannot travel to the United States for fear of prosecution there. Hacktivismo's Board of Directors includes Cindy Cohn, the lawyer for the Electronic Frontier Foundation, specifically to guard against the potential legal ramifications of Hacktivismo's various activities. Oxblood Ruffin, the founder of Hacktivismo, regards travel to China as an impossibility in light of his activities (Ruffin 2002).

Ultimately the success of political coding seems to lie in the high perceptions of efficacy among its practitioners. Hacktivists who have started out in other forms of hacktivism may be drawn in by the promise of direct effect. metac0m, creator of thehacktivist.com, comes from an activist background; but he has moved his energies into political coding because it "produces something tangible, rather than just protest" and is "something people can use." (metac0m 2002)

Political coding: the case of Hacktivismo

> Recently members of Legions Of the Underground "attacked" China yet again on their "human rights" condition. China setup firewalls in an effort to detour the people of the Chinese Republic from viewing sites which were found objectional by the Communist rule of China. These firewalls were paralyzed, and reconfigured. The group stands behind these actions 100% although the actions taken were that alone of the of the members who decided to impose action in an conformed fashion towards China. …All in all remember the information is out there, and it belongs to us. Join us in the fight to keep all data free. Keep the government(s) from impertinently tampering with rules, and regulations that go against our rights as inhabitants of this nation, as a society as a PUBLIC of the U.S.A (or whatever other country)... Ban together, and speak out in numbers before your right to speak is contraband entirely.(Optiklenz 1998)

When the Legions of the Underground (LoU) published this item in its December 1998 newsletter, hacker forays into anti-censorship activism were just a footnote in the hacker scene. But the LoU's hacks, led by notorious hacker Bronc Buster, were just the beginning. Anti-censorship hacking – using the tools of political crackers – soon gave birth to the more sophisticated tactic of anti-censorship coding. And at the forefront of this new field of activity was the Cult of the Dead Cow and its offshoot, Hacktivismo.

Hacktivismo initially emerged as a project of the Cult of the Dead Cow, a Texas-based hacker group that has used media savvy to solidify a reputation as a field leader, and "expanded the domain of hacking into the realm of the political" (Thomas 2002). The cDc was the elite of the hacker world, a US-based hacker group that dated back to 1984 (the Internet's equivalent of the Paleolithic era).

The group's founder, who uses the handle Grandmaster Ratte, started the cDc as a fourteen-year-old kid in Lubbock, Texas; eighteen years later he still reigns over the cDc from New York City, where he spends his non-work hours recording hip hop music in his apartment. When we met for an interview his references to his boogie board and his BMX bike reinforced the impression of talking with a teenager; but his aspirations include very middle-aged dreams of an RV, kids, and work as a day trader. His approach

to the cDc was an equal mix of the adolescent and the adult: he talked about making the group "big and popular", but says that goal is driven by the fact that he "wants kids to do something with their skills"(Grandmaster Ratte 2002). Until Hacktivismo, cDc was best known for its "Back Orifice" software program, which revealed some major security problems with the Windows operating system.

Figure 10. An example of the cDc's distinctive visual identity
(designed by Sir Dystic; online at http://www.cultdeadcow.com/large_image.php3?image_id=5)

In 1996, the cDc hacker Omega first used the phrase "hacktivism", inspiring cDc members to start registering domains like hacktivism.net and hacktivism.org (Ruffin 2004b). But nobody was more taken with the concept than the cDc's "Foreign Minister", who uses the handle Oxblood Ruffin. A fifty-two-year-old white man whose buzz-cut and casual clothes are the only mildly offbeat elements of his appearance, he is one of the oldest hacktivists in the sample. His personal demeanor hints at his background in public relations; charming and expansive, he kept up a lively conversation about hacktivism for five hours (my longest interview).

Ruffin's PR background includes ten years' work in the United Nations community in New York, primarily doing media work for UN-related publications. Originally from southern Ontario, Ruffin was living in Toronto at the time of our September 2002 interview. At the time he was working full-time on Hacktivismo; that brief stint of full-time Hacktivsmo work was preceded several months of public relations consulting, which in turn was preceded by a job at Open Cola, a Toronto software company that had some cachet in hacker circles.

Ruffin, by his own admission, is "not in the least technical" (Ruffin 2002)—though his notion of "technical" is clearly influenced by the hacker circles in which he moves. While he is not a full-fledged programmer, he is well-versed in web technologies, able to write computer scripts, and can even claim a youthful career as a "phreaker" – someone who hacks into telephone systems. Ruffin described his relationship to technology in colorful terms: "Did you ever see *Pretty Woman*? There's a scene where Richard Gere is driving a Lotus, but doesn't really know how to drive it. That's how I am with a really sweet computer."(Ruffin 2002)

Despite his technical limitations, Ruffin was invited to join the cDc in 1996. According to Ruffin, cDc membership is by invitation only: "if you ask to join, they'll never let you in." (Ruffin 2002) But Ruffin's online explorations led him into a regular correspondence with Deth Veggie, who forwarded their correspondence to the cDc members' e-mail list; soon, Ruffin received an invitation to join. Six and a half years later, Ruffin was clearly still thrilled by his membership in such a selective group; in the course of our interview, he described the cDc as "like Skull and Bones, but more

exclusive" and "the Beastie Boys of hacking", and noted that when he first saw the cDc web site, he thought it was "insane and brilliant".

When the cDc began playing with the concept of hacktivism, Ruffin had an opportunity to make a major contribution to the group's self-mythologizing. More than any of the cDc members, Ruffin was immediately taken with the concept of hacktivism:

> I always liked hacktivism as a word but thought the definition needed to be tightened up. Cyberwar had a fairly similar connotation; two big brains from RAND Corporation coined that in 1993. No, we needed something unique, something that had never quite existed in quite the same way before. It was Reid Fleming who brought in the hook. Reid set up hacktivism.org that featured a quote from the United Nations Universal Declaration of Human Rights (UNDHR). It was Article 19 and it read, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The first time I read that I felt like my head had gone to heaven. That was it. We would link technology with human rights. (Ruffin 2004b)

Ruffin's efforts at putting meat on the bones of hacktivism started to take shape at the 1999 Defcon hacker convention in Vegas. In conversation with his fellow cDc members, Ruffin arrived at the idea of developing a tool that would take on the large state-sponsored firewalls that limited access to the Internet in countries like Saudi Arabia, Cuba, Tunisia, and China. Firewalls

> act as intermediaries between users and the rest of the Internet. In countries where the Web is censored, the only way to access the Internet is through the firewalls. A user enters a URL - the address of a Web page - into his or her browser. This URL gets passed to the firewall, which checks to see if it is one of those banned by the government. If the URL is not on the list, the firewall forwards the request for the Web page and the contents of the page are relayed back to the user, who can then read it. If the URL is on the banned list the firewall refuses to forward the request and sends a page back to user indicating that the page he or she requested cannot be viewed by order of the government. ("About the Peekabooty Project")

Ruffin began to recruit hackers for his new project, reaching beyond the membership of the cDc itself.

> Bronc Buster and The Pull from the United States, and The Mixter from Germany - who was then working as a security consultant in Israel - jumped on board. All brought different skills to the table and each was highly motivated. What is quite interesting is that we all knew each other by reputation but had never met in person. And over time ideas and code started to flow from one to the other to the point where we had our first

> prototype: a distributed network application called Peekabooty. It would allow users to bypass firewalls, national or corporate, and access the free side of the Web from a host computer. Part of our plan was to publicize state-sponsored censorship of the Internet and raise as much awareness as possible. (Ruffin 2004b)

The project's name was deliberately provocative. Grandmaster Ratte advised Ruffin to make hacktivism

Figure 11. The Hacktivismo logo

> sexy, sweaty, and dangerous. That's what would get hackers interested. They were the ones who were going to sit down and hack the code together for long hours and at no pay; not, with all due respect, the human rights establishment. They were just getting used to Web browsers. I decided to stick hacktivism in everyone's face with a product name that was impossible to ignore. (Ruffin 2004b)

The name might have been playful, but Peekabooty's intentions were serious. As the project's mission statement explains,

> Peekabooty is software that enables people inside countries where the Web is censored to bypass those censorship measures. The theory behind it is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web. …A user in a country that censors the Internet connects to the ad hoc network of computers running Peekabooty. A small number of randomly selected computers in the network retrieves the Web pages and relays them back to the user. As far the censoring firewall is concerned, the user is simply accessing some computer not on its "banned" list. The retrieved Web pages are encrypted using the de facto standard for secure transactions in order to prevent the firewall from examining the Web pages' contents. Since the encryption used is a secure transaction standard, it will look like an ordinary e-business transaction to the firewall. ("About the Peekabooty Project")

As detailed in Chapter 4, Peekabooty became mired in internal conflicts; its chief developer, Drunken Master, left the Hacktivismo team, and took the Peekabooty project with him. In response, Ruffin envisaged a new generation of anti-censorship tools, and recruited a new generation of programmers to complement his existing team. Today, the group claims forty-odd members "from the Americas, Europe, Russia, Israel, Iran, India, Australia, Taiwan, and the Peoples Republic of China." (Ruffin 2004b)

From this diverse group I interviewed a total of seven Hacktivismo members, in addition to cDc guru Grandmaster Ratte and ex-member Drunken Master (now going by his real name, Paul Baranowski). From Hacktivismo's Toronto contingent I interviewed Ruffin, and two members he recruited from Open Cola: Mr. Happy, a 29-year-old programmer; and Ca$h Money, a 32-year-old webmaster. I also interviewed metac0m, who started out as a hacktivist for traditional left-wing causes, got into anti-censorship hacktivism, and was then recruited by Ruffin; he still runs the biggest web site for tracking hacktivist activities world-wide. In Germany I interviewed Mixter, a 23-year-old Arab-German programmer, who remained one of the group's stars: he first popped into international headlines in 2000, when one of his software tools was rumored to be the engine behind a series of high-profile Internet attacks. I also interviewed two of Mixter's recruits: Lisa Thalheim, a nineteen-year-old university student in Berlin whom Mixter knew from the Germany's Chaos Computer Club (CCC), and Jules, another CCC member.

In their physical self-presentation, Hacktivismo members ranged from urban hipsters to stereotypical computer geeks. In their verbal presentation, they were almost universally sophisticated and polished[22], offering clear and often quite original political analyses of hacktivism, computer hacking, and larger social issues. Their idiosyncratic comments included:

---

[22] In view of Hacktivismo's internal struggles it was noteworthy that the one exception was Paul Baronowski, the programmer who split off from Hacktivismo by turning Peekabooty into an independent project. Baranowski lacked the ease that other Hacktivismo members displayed in their discussion of political issues, although he seemed comfortable discussing technical issues around programming Peekabooty. This suggested that the dispute over the relative importance of programming and p.r. contributions may have reflected underlying personality differences.

> "I don't entirely rule out defacements, but the people who do them pick targets that have nothing to do with what they're protesting. I've been tempted, but it's not worth it. I wanted to write an article called 'Why I didn't deface this site.'" (metac0m)
>
> "Everyone here (in Germany) was against the war that Bush wants. No everyone is in favor. It makes me angry that opinions changed without any new argumentation around it." (Jules)
>
> "I'm hoping to get into the question of 'can representative democracy work?'…Everyone is talking about direct democracy, but the problem with direct democracy is that you never get all the facts. Especially in the current system of advertising." (Ca$h Money)
>
> "Politics used to be determined by protests. Before that, guns. Now it's about who controls the technology. A technologically superior force can overcome one that's militarily or financially superior." (Mr. Happy)
>
> "I believe in thinking properly and using the scientific approach. But with such a complex problem (tackling censorship) -- if it doesn't work properly, someone might be killed. You can't just write code. They (Hacktivismo members) are all great coders. But they don't tend to be patient." (Lisa Thalheim)
>
> "Most of the poverty in the third world is not economic or exploitation but due to lack of freedom. In every third world country you have a totalitarian government or overregulation." (Mixter)

Baranowski was a clear outlier in his difficulty in articulating or conceptualizing the social, political and communications aspects of anti-censorship hacktivism; his interest and expertise is in the technical challenges. A former member of the Young Democrats, his most articulate case for Peekabooty was that "censorship rubs me the wrong way". (Baranowski 2002) In our conversation about the Hacktivismo rupture it was clear that he regarded coding as the "real" work of the project, and public relations as irrelevant; speaking of Ruffin, Baranowski said he was "just a PR guy." (Baranowski 2002)

The post-Peekbooty Hacktivismo has launched several projects of its own. Camera/Shy is a steganography program that "enables users to share censored information with their friends by hiding it in plain view as ordinary gif images"(Hacktivismo 2002); according to Ruffin, Hacktivismo "heard from a lot of

expat hackers from Iran, China, and the United Arab Emirates living in the West who were using it with their friends back home." (Ruffin 2004b)

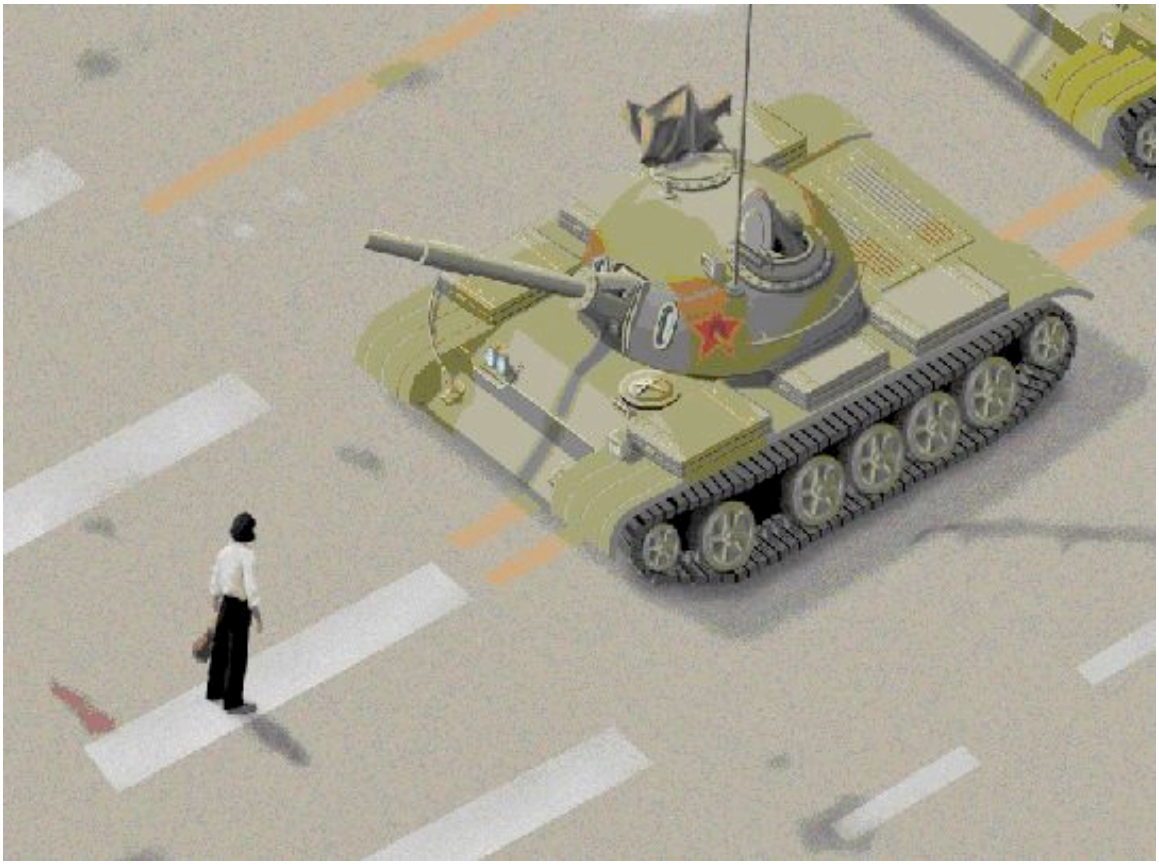


Figure 12. A demonstration of Camera/Shy.
This image hides the text of an article, "Dalai Lama Calls Wang Ruowang a freedom fighter" (stonefisk 2002)**.**

Hacktivismo's other major release was Six/Four, a peer-to-peer protocol for enabling censorship-free Internet traffic that was named for the date of the Tiananmen Square massacre. Six/Four is the closest thing to a new version of Peekabooty, in that it aims at circumventing firewalls. One of the project's biggest hurdles was obtaining US government approval: because the US government regulates cryptographic tools, and Six/Four uses cryptography, Ruffin worried that international distribution of Six/Four

could put US Hacktivismo members in legal jeopardy. So the group went through the US government's formal process for approving cryptography exports, and delayed Six/Four's release for the four months it took to get formal approval.

Arising out of Six/Four was a side project that may prove as significant as Six/Four itself: HESSLA ("The Hacktivismo Enhanced-Source Software License Agreement"), a legal framework that allows software developers to impose political terms of use on their users. HESSLA was inspired by the General Public License (GPL), a software license used by developers who want to make their software freely available and open to modification; but Hacktivismo was concerned that the GPL would allow human rights violators to use its tools, too. Their solution was a legal framework that would make the software available on the condition of human rights compliance:

> The HESSLA explicitly prohibits anybody from introducing spy-ware, surveillance technology, or other undesirable code into modified versions of HESSLA-licensed programs. Additionally, the license prohibits any use of the software by any government that has any policy or practice of violating human rights. The most novel innovation in the license distributes enforcement power instead of concentrating it in Hacktivismo's hands. If it is discovered that any government has violated the terms of the license, the HESSLA then empowers end-users to act as enforcers too. (Ruffin 2004b)

While Ruffin acknowledges that it is unlikely that anyone will use HESSLA as the basis for a human rights lawsuit, he says that Hacktivismo will be satisfied if they "deter at least some of the 'evil-doers' from using our software." (Ruffin 2004b) It is harder to gauge the direct impact of the software itself, for reasons that are intrinsic to the nature of the project. According to Ruffin,

> We've gotten email from people in the PRC and Iran saying that they'd been using Camera/Shy and thanking us, but they didn't say what kind of content they were trading in. We probably got fifty pieces of email when the software was originally released; still get the odd piece here and there. I met a guy [American] at HOPE who said he'd been using Camera/Shy and posting content for some friends in the UAE, but again, just a very quick hello, then he ran away.(Ruffin 2004a)

The Hacktivismo story highlights the extent to which political coding is going mainstream – thanks in no small part to Ruffin and his collaborators. After years of covert hacker wars between the US and China, the US government has now openly embraced Hacktivismo-style activism as a tool of its foreign policy. The Voice of America has launched its own anti-firewall tool, modeled on Peekabooty and Six/Four. And the US Congress recently approved the creation of an "Office of Global Internet Freedom," charged with combating Internet censorship through the use of hacktivist tools; Hacktivismo was consulted during the legislative process.

Hacktivismo's marriage of hacking and activism has helped bring not only hacker tools, but also the hacker agenda, into the political mainstream. While media pundits exclaimed over modest innovations like online petitions and virtual primaries, Hacktivismo insinuated far more confrontational tactics into the political toolbox. Thanks to Hacktivismo, governments are now adopting hacktivist tactics as their own, and Hacktivismo has thrust the Internet itself to the center of the policy stage. Their success makes a compelling case for hacktivism's growing influence on both the means and ends of twenty-first century politics.

Transgressive hacktivism: the commonalities of political coders and performative hacktivists

Reflecting on the three types of hacktivism, we see that it is not merely hacktivist origins that define, unite, or divide different hacktivists. The orientations of different hacktivists – whether outlaw or transgressive – form a second crucial dimension, dividing coders from crackers, and aligning coders and performative hacktivists. A brief review of

the commonalities among political coders and performative hacktivists helps to flesh out the notion of a transgressive orientation, and confirms the line between transgressive and outlaw orientations as a crucial element in modeling hacktivists types.

Both political coders and performative hacktivists try to skirt the boundaries of the law by refraining from activity that is unambiguously illegal, like cracking, instead staging hacktions that may or may not be illegal, but for which they are unlikely to be prosecuted. The virtual sit-in technique, for example, was deliberately designed to circumvent restrictions on denial-of-service attacks; because virtual sit-ins rely on actual human beings rather than "zombie"[23] computers to attack their targets, they are probably legal – or at least, less illegal than distributed denial-of-service attacks. Some hacktivists draw the line at their own national borders; they confine their work to activities that are legal in their own country, but recognize that their hacktivism may preclude traveling to the countries they have targeted.

Political coders and performative hacktivists also share norms of accountability to the liberal democratic legal order. Political coders often use handles, but these pseudonyms are almost always traceable to a real-world identity – more like nicknames than like shields. Performative hacktivists likewise either use traceable pseudonyms, or operate under their everyday legal names.

Political coders and performative hacktivists have the same propensity for collective action. They typically work in medium-size groups, but often aim at mobilizing much larger numbers of participants. Hacktivismo members and DeCSS distributors may

---

[23] When computer hackers surreptitiously take command of other people's personal computers during distributed denial of service attacks, the remotely controlled computers are called "zombies".

number in the dozens – but the impact of their hacktions depends on hundreds or even thousands of people putting the software to use.

Finally, political coders and performative hacktivists share a tendency for multinational engagement, working with hacktivists across national borders. For political coders this fits with the hacker-programmer tradition of discarding superficial or irrelevant information like gender, race, or nationality; for performative hacktivists it fits with postmodern notions about the transcendance of "meatspace"[24].

There are two major ways in which the orientations (as opposed to the origins) of political coders and performative hacktivists diverge. First – as noted in my discussion of hacktivist origins – political coders tend to focus on online issues, while performative hacktivists focus on offline issues. Second, performative hacktivists (like political crackers) tend to focus on policy change, while political coders focus on policy circumvention[25].

Performative hacktivism, like most forms of political participation, is directly or indirectly aimed at influencing the decisions of policymakers – whether those policymakers are businesspeople, government officials, or members of international organizations. Even efforts that seem to focus on galvanizing public support – like creating web site parodies – are pursuing public support as a means of effecting policy change by indirectly influencing policymakers.

The fact that performative hacktivism is aimed at policy or public influence can be obscured by the directly transgressive nature of many performative hacktions.

---

[24] Hacker jargon for real life, as opposed to cyberspace.

[25] This distinction is explored at greater length in Chapter 4, which focuses on the phenomenon of policy circumvention.

Hacktivists may use virtual sit-ins or parodies to directly target the objects of their wrath, but the political significance of those hacktions lies in their ability to command media or public attention. However direct the transgression, it ultimately relies on a policy decision (often, a decision by the hacktion's target or victim) in order to effect any change in political outcomes. Creating a fake WTO web site does not turn the WTO into an anti-globalization organization; it can only hope to embarrass or pressure the WTO into considering the larger issues around trade integration.

Political coding, in contrast, tries to circumvent policymakers by producing software that renders policy ineffective or irrelevant. Software that decodes DVDs circumvents copyright laws; software that reroutes web traffic circumvents censorship laws in authoritarian countries. The kind of hacktions thus present a far more fundamental challenge to our notion of politics and political participation. As long as participation is geared towards policy influence, it corresponds roughly to models of participation as voice; when it is geared towards policy circumvention, it looks more like exit.

Conclusion

The three types of hacktivism not only reflect variation in the political origins and orientations of hacktivists. Each type of hacktivism also has a distinct profile with regard to the other hacktivist and hacktion characteristics I identify earlier in this chapter. The profile of each type of hacktivism can be summarized by those characteristics (see Table 7, below).

These types are more than useful intellectual constructs: they represent meaningful divisions between political crackers, performative hackers, and political

coders. These divisions manifest in tensions and sometimes open conflicts between various groups of hackers. When the political crackers of the Legion of the Underground declared a cyberwar on Iraq and China in 1998, the cDc and other hacker groups issued a joint condemnation of the declaration of war("LoU STRIKE OUT WITH INTERNATIONAL COALITION OF HACKERS: A JOINT STATEMENT BY 2600, THE CHAOS COMPUTER CLUB, THE CULT OF THE DEADCOW, !HISPAHACK, L0PHT HEAVY INDUSTRIES, PHRACK AND PULHA" 1999). Oxblood Ruffin has likewise criticized the virtual sit-in technique of the electrohippies, and EDT member Ricardo Dominguez describes hackers as caring more about computers than about people.

The distinctions between political crackers, performative hackers, and political coders illuminate each of the theoretical problems posed by hacktivism. As the following chapters turn to questions about collective action, policy circumvention, and democratic deliberation, we will see how the differences among hacktivists translate into significant divisions in each of these arenas.

Table 7: Types of hacktivism, summarized by characteristics

	Forms	Origins	Orientation	Issues	When
Political cracking	Defacements Redirects Denial of Service Attacks Sabotage Information Theft	Hacker-programmers	Outlaw	Online issues, gradually encompassing offline issues	Since early 1990s (with earlier antecedents); starts to encompass general issues only since 1997/98
Performative hacktivism	Parodies Sit--ins	Artist-activists	Transgressive	Offline issues	Since 1997
Political coding	Software development	Hacker-programmers	Transgressive	Online issues	Since 1999

Chapter 3

Collective action among virtual selves:

How interaction and identity shape hacktivist participation

Introduction

Why do people engage in collective political action? This is one of the most fundamental questions in political science, and one that has preoccupied scholars of political participation for decades. Framing the problem as a mysterious deviation from rationally self-interested behavior, researchers inquire into the conditions that make some people contribute to the provision of collective goods. Given the ubiquity of political demands and goals, why is it that some people take action to pursue their goals, while others sit on the sidelines?

This chapter uses the case of hacktivism to argue that this formulation of the collective action problem is based on some problematic assumptions. Most crucially, it assumes that political actors – and political action – are essentially purposive. Everyone has an interest in the provision of public goods, so everyone must care about the problem of ensuring these goods are provided. Inquiries into political action are thus inquiries into the mechanisms for dividing up the burden of providing public goods. A variety of selective incentives – like the financial or social benefits of political participation – are invoked in competing explanations.

I use the case of hacktivism to argue that this entire formulation of collective action problems has been assembled upside-down. For perfectly good historical reasons, we have been unable to separate the purposive value of collective action from the

selective benefits it offers. Because hacktivism provides an opportunity for separating political participation from collective action, it allows us to extricate the instrumental goals of collective action from the other rewards it offers. The first part of this chapter is focused on reassessing our picture of collective action as purposive or instrumental, using evidence from the world of hacktivism to rebuff the purposive model.

What results is a picture of political participation in which purposive goals appear to be secondary, rather than essential, in motivating collective action. Once we discard the view of political participation as essentially purposive, we are forced to reevaluate the role of selective incentives – and in particular, the social incentives that have received relatively little attention – as motivations for political participation. The second part of the chapter offers two distinct interpretations of social incentives in the context of the broader literature on selective incentives, while the third part tests each model of social incentives against quantitative and qualitative evidence drawn from fifty-one interviews.

My findings show that social incentives do indeed account for political participation, when they are understood in terms of the benefits of affirming a particular social identity. This notion of social incentives is suggested by previous explorations into "expressive" and "solidary" incentives for participation, but reformulates these as specific identity incentives. In contrast, the notion of social incentives as the demand for interaction is not supported by my evidence; to the extent that hacktivists pursue collective action it seems to be instrumentally driven rather than a pursuit of interaction.

The significance of identity as a driver for political participation is supported by my finding that hacktivists' backgrounds are a good predictor of the type of hacktivism in which they engage. Hacktivists from hacker-programmer backgrounds are

disproportionately likely to engage in political coding (i.e. political software development) or political cracking (e.g. information theft or site defacements) while those from artist-activist backgrounds are disproportionately likely to engage in performative hacktivism (i.e. virtual sit-ins or web site parodies). The correlation between hacktivist origins and type of hacktivism is further supported by a variety of self-categorizing comments, which demonstrate the appetite for identity as label, and a variety of comments about particular forms of hacktivism, which suggest the mechanism whereby hacktivist origins determine the type of hacktivism in which respondents engage. The chapter concludes by reflecting on how this finding helps to resolve the puzzle of hacktivism as a form of activism in which means precede ends.

Collective action and political purpose: Evidence from hacktivism

Political science addresses the purposive dimension of political participation in two ways. The first is to treat political participation as, by definition, purposive. The second is to examine specific purposive motivations as one type of selective benefit. Understanding the limitations of both of these approaches is crucial to appreciating the potential explanatory power of social incentives.

The assumption that political participation is purposive can be found throughout the literature. Verba, Nie and Kim explicitly define participation as "those legal acts by private citizens that are more or less directly aimed at influencing the selection of government personnel and/or the actions that they take" (Verba, Nie, and Kim 1978) – assuming quite specific goals on the part of participants. When White asks "why some citizens choose to act on their political interests and participate in politics, while others

do not," (White 1976) she likewise assumes the a priori existence of political interests. When Chong notes that "political activists, it appears, not only wish to achieve particular political objectives," (Chong 1991) he is looking for variables in addition to the purposive orientation, not in place of it. When Schlozman, Brady and Verba define the problem of participation as "about whose voice is heard"(Schlozman, Verba, and Brady 1995) they assume that citizens have something to say.

There is nothing problematic about treating political participation as, by definition, purposive; the most intuitive way of categorically distinguishing political participation from other forms of social activity is to define it as activity aimed at achieving a specific political outcome. The problem lies in treating the purposive character of participation as a given – an assumption that is belied by the relationship between purpose and participation seen in the hacktivist movement.

An analysis of the hacktivism.ca listserv (Samuel 2001) showed that in many cases, the decision to participate in hacktivism preceded participant commitment to any specific cause or purpose. Instead hacktivists often seem to shop for a political agenda after they have already made the decision to become hacktivists. This is evidenced by the fact that hacktivists define their movement not by its goals, but by its methods:

> [hacktivism is] strategic activism that relies upon intelligence gathering, public opinion swaying, the erosion of confidence in the economy and technology. It's propaganda, disinformation, advertising, education, manipulation, and machiavellian subversion (batz)

Indeed, the emphasis on method seems to have become an article of faith for some hacktivists. One member of the hacktivist list wrote that

> I used to think I was a hacktivist by virtue of being somebody whose activism and use of tech is intrinsically tied. However, if hacktivism is what is happening on this list, I suppose that I'm not a hacktivist, and that the old saying ""Define yourself by your actions, not by your -ism's"" holds very true. (<pete@tao.ca>)

The priority of movement method (i.e. participation in some form of political hacking) over movement purpose (the choice of cause to which that hacking is harnessed) is further evidenced by hacktivists' explicit allegiance to their common form of political participation, rather than to any common purpose. Hacktivists on the hacktivism.ca listserv were very clear about the heterogeneity of their political orientations:

> There is no point in saying such and such a group are not hacktivists simply because we disagree with them. That brings us nowhere. It is about as helpful as the insistence that hackers are "good" and crackers are "evil". So what do you say we simply concur that "hacktivism" covers a very wide range of activities and concentrate on the real discussion: what the results could be, what we can learn from them, and even whether they are "good" or "bad". But not whether they are "hacktivists".(xdaydreamx 30-Aug-99)

At the same time, it was clear that the lack of common purpose was in no way an obstacle to the construction and consolidation of a collective identity. For one participant, this took the form of a direct exhortation to emphasize group commonality:

> The key is to keep positive, keep thinking, and to concentrate on commonality, so sectarianism doesn't incite us to war with each other, rather than the man. :) (Mike 27-Aug-99)

Another list member seemed to share this implicit identification of a hacktivist movement; he wrote that

> Hacktivism is dangerous, and to some extent requries a high degree of proficency in technical skill. Does this make them a high-tech vanguard or a group of activists fighting the best way the know how? I think this is a debate that is yet to be had. (Jones 1999b)

The fact that hacktivists expressed their first allegiance to the form of their participation, and only a secondary allegiance to its end, suggested that a specific political goal or purpose might not always be at the heart of political participation.

This observation challenges the core assumption of studies of political participation: the assumption that participation is inherently purposive. If we problematize this assumption we can ask a series of intriguing questions about the

purposive orientation of participation: How does the purposive character of participation develop? Are purposive orientations a requirement for participation, or do they emerge out of participation? How does the strength of purposive orientations vary across activities, issues, countries, or time?

The literature on purposive incentives starts to get at some of these questions; however even those authors who examine purposive incentives take the purposive character of participation as a given. This limits the explanatory power of their research, since purposive incentives can hardly offer much predictive traction if we assume that purpose is a universal trait of political participation.

The concept of "purposive" incentives traces back to an influential 1961 article by Clark and Wilson on "Incentive Systems". Clark and Wilson constructed a typology of "material," "solidary," and "purposive" incentives which has structured much of the subsequent literature. They define purposive incentives as intangible benefits that "derive in the main from the stated ends of the association rather than from the simple act of associating. These inducements are to be found in the suprapersonal goals of the organization."(Clark and Wilson 1961) Clark and Wilson use their typology to distinguish between organizations that are primarily driven by purposive incentives, and those that are primarily driven by material or solidary incentives. In their view purposive organizations suffer from inflexibility, due to either the vague or sacrosanct quality of those goals.

In the years since Clark and Wilson established the notion of purposive incentives, scholars have come to understand these incentives in two ways. Some scholars focus on the ends-orientation of purposive incentives, and highlight activists'

interest in achieving certain goals. Others have redefined the notion of purposive incentives to encompass the psychological or moral satisfactions of associating oneself with a set of explicitly stated political purposes.

The ends orientation is manifest in Clark and Wilson's original definition of purposive incentives. Bowman, Ippolito and Donaldson (1969) follow Clark and Wilson, and measure purposive incentives as "concern with public issues" and "sense of community obligation" (Bowman, Ippolito, and Donaldson 1969). Knoke and Wood (1981) also stick closely to the Clark and Wilson model, and measure purposive incentives by whether volunteers mention factors like "opportunity to help those in need" "a sense of community responsibility" and "to accomplish the goals and aims of the organization."(Knoke and Wood 1981) The notion here is that purposive incentives capture the extent to which individuals are motivated by the prospect of contributing to the achievement of specific ends.

The "expressive" concept of purposive incentives places more emphasis on the psychological and personal experiences of participation. It speaks to the idea of participation as voice, and indeed, Hirschman himself emphasized the inherent value of participation as an expressive act, describing it as one of those activities that "carry their own reward" (Hirschman 1982). Salisbury (1969) usefully distinguishes the idea of expressive benefits from Clark and Wilson's concept of purposive benefits by separating the pursuit of goals from the expression of values:

> Expressive actions are those where the action involved gives expression to the interests or values of a person or group rather than instrumentally pursuing interests or values…..one can often derive benefits from expressing certain kinds of values….Whether the expression is instrumentally relevant to the achievement of the values in question is, for the moment, not at issue. (Salisbury 1969)

Others have adopted Salisbury's notion of expressive benefits, although these are often referred to as "purposive" incentives. Finkel and Muller (1998) refer to expressive benefits as activists' "psychic reward from 'standing up' for their political beliefs through collective protest" (Finkel and Muller 1998). Chong describes expressive benefits as "the variety of noninstrumental benefits that one might receive from political participation" including "voicing one's opinions" "the feeling that one gets from doing the right thing" and "the important lessons that once learns from taking part in the political process." (Chong 1991)

Some authors incorporate both ends-oriented and expressive notions of purposive benefits. Moe (1981) sees purposive benefits as playing two roles:

> First, they can shape the individual's evaluation of collective goods; the benefits he attaches to the political goals of a consumer group, say, may reflect his broader concern for other citizens, economic justice, or political equality, and may far outweigh any economic gains he expects for himself…Second, when he believes in a group's political goals, he may also gain a purposive sense of satisfaction from the act of contributing itself; he may feel a responsibility to do his part or do what is right, for example, and he may receive satisfaction from following through. These satisfactions are selective incentives; the source of benefits is not the actual provision of collective goods, but the individual's expression of support for them. (Moe 1981)

The first notion advances an ends-oriented view of purposive incentives; the second, an expressive notion.

Seyd and Whiteley (1992) are more explicit in distinguishing between ends-oriented and expressive incentives, although their terminology is different. Their general incentives theory incorporates both "collective incentives" and "altruistic concerns" alongside "selective incentives" and "social norms." "Collective incentives" are ends-oriented motivations, which take the form of policy goals. Their notion of "altruistic concerns" is similar to the idea of expressive incentives; they define altruistic motivations as " a product of affective or expressive motivations." (Seyd and Whiteley 1992)

Schlozman, Brady and Verba also embrace both notions of purposive incentives. They capture the expressive dimension with their definition of "civic gratifications, such as satisfying a sense of duty or a desire to contribute to the welfare of the community" – gratifications that "derive from the act itself" (Schlozman, Verba, and Brady 1995) They explicitly distinguish these gratifications from the motivation to affect "collective outcomes", which amounts to end-oriented motivation.[26] (Verba, Schlozman, and Brady 1995).

An explicit distinction between ends-oriented and expressive notions of purposive incentives proves useful to my later reconceptualization of social incentives. Before developing this reconceptualization, I will first review the current scholarship on social incentives.

Understanding social incentives

Selective incentives and political participation

The literature on purposive incentives does not resolve the challenges that the case of hacktivism poses to the assumed purposive nature of political participation. It merely raises new questions. First, how do political scientists understand the role of purposive goals in motivating participation? Second, how do political scientists understand the role of social or solidary incentives – alongside or in place of purposive

[26] Schlozman, Brady and Verba measure civic gratifications in terms of "my duty as a citizen" and "I am the kind of person who does my share." Their third indicator of civic gratifications blurs the line between expressive and ends-oriented incentives: "The chance to make the community or nation a better place to live." Arguably this speaks more to the desire for an impact on collective outcomes, than to personal psychological gratification.

incentives – in motivating political participation? Third, how do political scientists locate the quest for identity within these notions of participatory incentives?

The first two questions have received some treatment in a common body of political science research on the role of selective incentives in collective action. Collective action theory has primarily emerged in response to Mancur Olson's influential 1965 book, *The Logic of Collective Action*. Olson argued that rational actors would be unlikely to join interest groups in order to pursue public goods, because these goods are non-excludable. As a result, rational actors would be tempted to "free ride" on the efforts of others in creating or protecting public goods, rather than contributing to the effort themselves.

Olson identified two exceptions to this calculus of the costs and benefits of participation: (1) "large members" have an incentive to contribute to interest groups, if their expected share of the public good will be large enough to offset the cost of contributing to the effort, and (2) interest groups can provide "selective incentives" to their members which, unlike public goods, can be limited to actual members of the group. Olson argued that people join interest groups *not* to pursue collective goods, but to receive these selective incentives (Olson 1965).

Olson's model has been widely adopted by scholars of interest group politics, political participation, and new social movements. The idea of modeling interest group participation as a rational cost-benefit decision has become the dominant means of modeling individual participation decisions and organizational dynamics. As part of this burgeoning literature on the political economy of participation, many scholars have sought to broaden Olson's original notion of selective incentives as material rewards for

participation. There is now an established literature that examines not only material incentives but also purposive (or expressive) and social (or solidary) selective incentives.

The results of empirical tests of models that incorporate selective incentives are at best mixed, however. In one of the earliest studies along these lines, Bowman, Ippolito & Donaldson (1969) found that while purposive incentives were very important in motivating party workers, solidary incentives were much less crucial. Hansen (1985) found that as predictors of American interest group membership, selective incentives were less important than perceptions of threat. Chong (1991) found much evidence for the importance of solidary and expressive benefits in his retrospective study of the American civil rights movement. In one of the most methodologically rigorous tests of encompassing selective incentive models, Finkel and Muller (1998) found that selective incentives were a poor predictor of social movement activism in West Germany. On the other hand, Schuessler (2000) finds that expressive benefits are a good explanation for the dynamics of mass political campaigning.

If these mixed results partly reflect the difficulties of fitting "soft" incentives into the hard framework of calculated self-interest, they also suggest that the results might be clearer if we could improve the way non-material incentives are modeled. Seizing on that suggestion, I focus on improving the model of social incentives, and end up building on ideas about purposive and expressive incentives, too.

Social or solidary incentives are motivations that grow out of the social or interactive nature of political participation. Specific incentives include a desire to spend time with interesting or like-minded people, a sense of fun, or the desire to please friends or family. The key distinction here is between a notion of social incentives as the desire

for congenial social interaction, and a notion of social incentives as the pursuit of some sense of belonging (which may emerge out of social norms or pressures.)

In order to satisfy the desire for interaction, participation must necessarily involve some sort of collective action (since it is the collective nature of participation that brings participants into contact with one another). The desire for belonging, in contrast, can be theoretically satisfied by individual (non-collective action) – if that action allows participants to lay claim to a given group membership or identity. It is useful to think of satisfying the desire for interaction through "interactive" incentives, and the desire for belonging through "solidary" incentives, although the literature is equally likely to use the terms "social" or "solidary" in describing either one. Indeed, most authors fail to distinguish between the interactive and solidary motivation types.

Clark and Wilson's original definition of solidary incentives is closer to my concept of interactive incentives. According to Clark and Wilson, solidary benefits

> derive in the main from the acts of associating and include such rewards as socializing, congeniality, the sense of group membership and identification, the status resulting from membership, fun and conviviality, the maintenance of social distinctions, and so on. Their common characteristic is that they tend to be independent of the precise ends of the association. (Clark and Wilson 1961)

Knoke (1988) also uses a strictly interactive notion of social incentives, defining them as "jointly coordinated social and recreational activities whose enjoyment is also restricted to the membership."(Knoke 1988)

Finkel and Muller (1998) focus on solidary incentives. They consider (though ultimately discard) the possibility that "individuals respond to the norms and expectations of other people within their social network and hence derive benefits from adhering to the

behavioral norms of individuals and groups with whom they identify."(Finkel and Muller 1998)

Chong likewise emphasizes the notion of solidary incentives as a desire for belonging. What he terms "social incentives" include the "desire to gain or sustain friendships, to maintain one's social standing, and to avoid ridicule and ostracism." (Chong 1992) While the desire for friendship might be purely social, the broader thrust of his argument emphasizes the solidary dimension of these incentives. Chong is particularly interested in the reputational benefits of participation, which he sees as a sort of social lubricant for the achievement of private benefits from participation. While this sounds like a very instrumental view of the social benefits of participation, it is one that is also grounded in a notion of social benefits as belonging:

> Our social identities are closely tied to the social identities of the people we associate with, because those who witness our associations will use such information to draw inferences about us. Reputation-building is in this respect based on being with the right people rather than doing something in a more active vein. (Chong 1992)

Salisbury's elaboration on the Clark and Wilson definition shows why the conceptual distinction between "social" and "solidary" is so important. Salisbury gives a hypothetical example of a political entrepreneur trying to attract members with social incentives:

> An organizer can build a clubhouse but he cannot easily guarantee it will be worthwhile to go there. The solidary benefits may develop but the entrepreneur is especially dependent on his customer to help him create his product. Furthermore, it is not clear that for most people sociability is valued highly enough to persuade them to join a new group to get it. (Salisbury 1969)

Salisbury's argument speaks to interactive incentives – to their dependence on critical mass in order to have value. Solidary incentives may be rather more robust – though the value of solidary incentives may also depend on how one perceives other

members of the group. But these are very different kinds of problems – the former quantitative, the latter qualitative – and thus lead to very different predictions about membership incentives. This underlines the importance of distinguishing between interactive and solidary incentives.

We are thus left with two very different notions of social incentives, which the literature tends to confuse or conflate: interactive incentives, which necessarily involve collective action; and solidary incentives, which could account for either individual or collective action in pursuit of a given goal. The latter type – the notion of solidary benefits – still suffers from its vagueness about what belonging to a group actually means or entails, however. As I will show, this problem can be addressed by building on more careful treatments of group identity in the literatures on social identity.

Revising the model of selective incentives: incorporating identity

We have already seen that the literature on selective incentives often incorporates a notion of identity as a type of benefit. When we separate the concepts of purposive and expressive benefits, we see that expressive benefits are themselves related to the pursuit of identity: they are statements about the kind of person a participant wants to be. Indeed, investigations into expressive benefits are often operationalized in terms of individuals' desire to project or express a particular self-concept or identity. Investigations into solidary benefits are often operationalized in terms of individuals' desire to subscribe to a particular collective or group identity.

Considering identity as a type of selective incentive is not a simple matter, however; incorporating identity into any causal model demands an explicit and well-

grounded conceptualization of what identity actually means. By referencing the now-established literature on social identity (which arises primarily out of sociology and psychology) we can develop a notion of *identity* incentives. The idea of identity incentives builds on the intuition behind collective action theories of expressive and solidary incentives, but tries to strengthen their theoretical underpinnings.

That effort depends on separating individual identity (which is the most common colloquial use of the term "identity") from group identity: the part of "an individual's self-concept [that] is derived, to some extent and in some sense, from the social relationships and social groups he or she participates in." (Brewer 2001) This is the dimension of identity that is implicitly captured by collective action theory's notions of expressive and solidary incentives; by the notion of participation as a route to belonging, or as a way of confirming that you are a certain *kind* of person. The notion of being a certain kind of person rests on an implicit taxonomy of kinds of people – i.e. a system of groups. An identity incentive is thus the promise of confirming or enhancing a participant's membership in a particular group or groups.

Social identity theory helps us understand the idea of identity incentives by clarifying both the notion of group identity, and the individual drivers for group membership. It posits a notion of group identity that lets us get beyond the narrow definition of group membership as a formal affiliation with a particular interest group, or a demographic affiliation with a particular ethnicity, gender, or sexuality. Instead, group identity is broadly understood as a way of setting boundaries around or between groups; these boundaries become a cognitive tool that shapes how people perceive themselves, their group, and the world around them. People may have multiple overlapping social

identities, which individuals need to mediate or balance (Vescio et al. 1999). The key insight is that individuals assign "value and emotional significance"(Tajfel 1981) to their membership in particular groups – in other words, to their sense of belonging.

Social identity also helps us to understand the micro-level drivers for group identity. It emphasizes "self-evaluation and the need for self-esteem as the principal motivational mechanism" (Hogg and Mullin 1999), suggesting that individuals adopt a social identity in order to "maintain or enhance self-esteem" (Hogg and Mullin 1999). Uncertainty may be an additional motivation for adopting a given social identity; group identification is a way of reducing the discomfort of uncertainty "about beliefs, attitudes, feelings and behaviors that one feels are important to one's sense of who one is." (Hogg and Mullin 1999) Or the pursuit of group identity may be a process of alignment, in which participants endeavour to bring their individual identities in line with that of the group (Snow and McAdam 2000). All of these mechanisms share the notion of group identity as a way for people to feel better about themselves. From there it is a short leap to seeing how "collective identities function as selective incentives motivating participation." (Friedman and McAdam 1992)

We are now ready to integrate identity incentives back into the larger family of selective incentives. Beginning with collective action theory, remember that the broader participation literature has considered five distinctive types of selective incentives. Note that the literature generally uses "incentive," "motivation," and "benefit" interchangeably, to refer to any benefit of participation that a rational actor might anticipate, and which therefore could motivate him/her to participate in collective action.

1. material incentives – incentives that can be assigned a dollar value. These are the only kind of incentives conceived of by Olson in his original *Logic of Collective Action.*
2. ends-oriented incentives – participants' desire to accomplish the anticipated collective or public outcomes of collective action. Usually called "purposive" incentives.
3. expressive incentives – the psychological and/or emotional benefit of expressing one's political or social values through political action that reflects those values. Sometimes called "purposive" incentives.
4. interactive incentives – the enjoyment of participating in an activity that involves interacting with other people. Interchangeably described as "social" or "solidary" incentives.
5. solidary incentives – the psychological and/or emotional benefit of belonging to a group that shares one's political or social values, or of fulfilling the expectations of one's social network. Interchangeably described as "social" or "solidary" incentives.

Material incentives alone cannot explain political participation. As Hansen (1985) points out, private companies can offer material benefits; "only interest groups offer political benefits in addition." (Hansen 1985)

The same argument extends to interactive incentives. There are many ways people can obtain social interaction, from work to bar-hopping to joining churches. Social interaction per se is not a distinctive feature of political participation. (Although

interacting with certain kinds of people may be peculiar to political life…but here we enter the realm of solidary incentives.)

The notion of ends-oriented purposive incentives poses a different kind of problem. As used by Clark and Wilson, Schlozman Brady & Verba, and others, ends-oriented incentives constitute an explanatory variable that helps to predict political participation. Used in this way, ends-oriented incentives are tautological. Explaining participation with reference to ends-oriented purposive incentives is like attributing political participation to "the desire to participate in politics." The idea of ends-oriented purposive incentives is more intriguing when conceived of as a dependent variable. Why do some people feel a sense of concern for public issues, or a sense of community obligation, while others do not? Explaining where purposive orientations come from is a lot more promising than demonstrating why they are politically salient.

Our two remaining types of incentives, expressive and solidary incentives, may help to do just that. These two kinds of incentives capture the psychological or emotional desire for (respectively) value affirmation and a sense of belonging. Both types of incentives closely parallel key concepts that emerge from the literature on group identity.

In the collective action literature, social or solidary incentives speak to an individual's desire for group affiliation. Expressive incentives speak to an individual's desire to express what kind of person he is, or what kind of values she holds. If our goal is to explain patterns of political participation, then we are specifically interested in the desire for affiliation with a group that reflects political values or identities; or in the desire to express the political dimension of one's identity or values. In the identity literature, joining a political group would be described as adopting a specific social

identity – the identity reflected by the political group. This type of motivation can be usefully framed by the social identity literature, allowing us to collapse some illusory distinctions between solidary and expressive incentives, and instead focus on their common ground as identity incentives.

We can begin by revisiting the notion of expressive incentives. In the collective action literature, expressive incentives are conceived of as the psychological and/or emotional benefit of expressing one's political or social values through political action that reflects those values. The expressive benefits of participation lie in "voicing one's opinions" (Chong 1991), "standing up for [one's] political beliefs" (Finkel and Muller 1998), or satifying one's "responsibility to do [one's] part." (Moe 1981)

Like solidary incentives, these expressive incentives seem to be implicitly linked to concepts of identity. The expressive benefits of political participation lie in its ability to define who one is, what one stands for – what *kind* of person one is. This notion of expressive benefits is adequate for explaining relatively solitary forms of participation, like letter-writing or voting. As an explanation for collective action or group membership, however, it is problematic. Why join a group in order to express your individual identity?

The answer lies in the relationship between individual and group identity, as theorized by the social identity literature. Group identity shapes individual identity, and individual identity (or its inadequacies) determines the groups with which one affiliates. Seen in this light, collective action seems to offer two forms of political expression: a declaration of one's identity as a member of the group, and an expression of the group's collective values and identity.

This mirrors the treatment of collective identity in the literature on new social movements, which sees collective identity as a process of meaning construction – in other words, a way of expressing ideas about the world around you. The relationship between the individual and collective levels is addressed in some depth by Snow and McAdam (2000), who argue that much of the "identity work" in social movements lies in the challenge of reconciling individual and collective identity; it is through this process that members are recruited to the movement.

Expressive incentives thus look a lot like solidary incentives: a choice one makes about the kind of group that will reflect your sense of yourself. This brings us back to the challenge of re-theorizing solidary incentives, in order to ground our tests of solidary incentives as predictors of political participation. In political science research, solidary incentives have been defined as the desire to adhere to "norms and expectations of other people within their social network" (Finkel and Muller 1998) or as "reputation building… based on being with the right people rather than doing something in a more active vein." (Chong 1992) This parallels social identity theorists' description of the "need for optimal distinctiveness" (Abrams 1994) or the pursuit of "positive in-group distinctiveness" (Kelly 1988). Social identity theory sees group membership as a function of the "desire for belonging associated with the need for inclusion [which] motivates immersion in social groups." (Brewer and Silver 2000) People join groups as a way obtaining a social identity that is distinct from other social identities.

Because identity theory addresses the roots of this urge for belonging, it helps us to improve our model of solidary incentives. The most significant innovation is the recognition that political science distinctions between expressive and solidary incentives

disguise an underlying commonality: both types of incentives are ultimately about individual cravings for group identity.

We can thus replace the categories of expressive and solidary incentive with the overarching category of *identity* incentives. We can further specify that these identity incentives will reflect individuals' desire to confirm or enhance their sense of belonging to a group, where membership in that group enhances self-image or self-esteem.

Now that we have a detailed theory about what identity incentives might look like, we can ask whether they do indeed motivate political participation. We can also compare the explanatory power of identity incentives with the potential explanatory power of interactive incentives – the more common notion of "social" incentives for political participation. To address these questions, I return to the hacktivist universe, to see how identity and interaction play out as incentives for different kinds of hacktivist participation.

Social incentives for participation: testing the hypotheses

Identity, interaction and the phenomenon of hacktivism

We now turn to the challenge of testing hypotheses about identity and interactive incentives for political participation against patterns of hacktivist participation. These tests focus not on predicting *whether* respondents will engage in hacktivism – in this sample, virtually all of them do – but on predicting *which type or form* of hacktivism respondents will pursue. (The distinction between type and form of hacktivism is summarized in the table below). Because there are significant differences among the

different types of hacktivism, the decision to engage in political cracking, political coding, or performative hacktivist has significant implications for the participant's identity. And because there are significant variations in whether particular forms of hacktivism demand or even allow for collective action, a hacktivist's choice of form – virtual sit-in or web site defacement, site parody or DoS attack – sheds light on the role of interactive incentives.

Table 8. Types vs. forms of hacktivism[27]

Types of hacktivism	Political cracking	Performative hacktivism	Political coding
Forms of hacktivism	Site defacements Site redirects DoS attacks Virtual sabotage	Site parodies Virtual sit-ins	Political software development
	Information theft and distribution		

Before we get to the nuances of particular types or forms of hacktivism, however, we can see why the larger hacktivist universe might provide fertile ground for testing hypotheses about identity and interactive incentives. Its unique value to this theoretical challenge stems from two distinct qualities: first, its characteristics as a form of online participation; and second, its capacity for solo as well as collective action.

As a form of online participation, hacktivism constitutes a tough test for any social account of political participation – whether focused on interactive or identity

[27] The discovery that information theft occurs as part of all three types of hacktivism is a surprise that will be discussed towards the end of this chapter.

incentives. Research on human-computer interaction has already demonstrated that in many ways, the Internet is the *last* place we would expect social incentives to matter. Sproull and Kiesler (1991) found that computer-mediated communication reduced the effect of status differences on interaction. Aspden and Katz (1997) have specifically demonstrated that discrepancies in offline social skills do not affect the capacity to make friends online, noting that

> we found no statistical relationships between propensity to make friends [online] and a wide rage of measures of traditional forms of social connectedness and measures of personality attributes. This perhaps points to the Internet deemphasizing the importance of sociability and personality differences. (Katz and Aspden 1997)

This online quality of "social thinness" has been widely documented. Sproull and Kiesler (1991) note that the dominance of plain text communications greatly reduces social cues. While Internet users compensate for this lack of social cues by using emoticons to represent emotions, such as :) for "happy" and :-(*) for "about to throw up", as well as textual description for physical reactions ("*falls down laughing*") (Reid 1996), these text-based cues are still a far cry from the real thing. While broader bandwidth technologies (like video and audio) increase the transmission of social cues, research suggests that even video communication is a far cry from face-to-face contact in its ability to create interpersonal connectedness.

For my present purpose, the implications of social thinness go far beyond its effective "flattening" of personality differences across groups. The relatively impoverished social environment of the Internet makes it the last place we would expect social incentives to be decisive for political participation. If the desire for interaction or collective belonging is persuasive here – a place where the location, names, and even

gender of fellow group-members are all ultimately unknowable – then we have every reason to expect these incentives to be all the more crucial in an offline context.

The Internet thus offers an excellent testing ground for testing alternative theories about social incentives. But why focus on hacktivism, when there are so many other forms of online activism available to study? Here, the answer hinges on a quality that, while not unique to hacktivism, is exceptionally pronounced in its case: the potential efficacy of solo action.

If theories of collective action have assumed the universality of purposive goals, while puzzling over differences in individuals' willingness to participate in collective action in pursuit of those goals, it is because collective action and political action have only rarely been separable. For most of human history, effective political action has necessarily involved collective organizing; even the efficacy of elite-level actors (like the political entrepreneurs who lead social movements, or the politicians who lead parties and governments) depends on their ability to mobilize mass followings.

In the case of hacktivism, however, individual actors do indeed have a high level of political efficacy. A single hacktivist can unilaterally engage in the political act of defacing a web site or jamming a server. In many cases there is no collective action problem, because hacktivists can engage in uncoordinated unilateral action and still have a visible impact.

The fact that hacktivists nonetheless *choose* to engage in collective forms of action suggests that something other than instrumental goals are pulling them into collective forms of political participation. By testing hypotheses about identity and interactive incentives against this population, we can therefore isolate the demand for

collective action (the demand for "group-ness") from the interest in pursuing specific political ends.

In testing identity versus interactive incentives as predictors of political participation, we must carefully specify the observable differences between the two types of incentive. Happily, the identity literature suggests several aspects of the demand for identity that make it look very different from the demand for interaction. One aspect is the appetite for labeling: the quest for identity often manifests as self-categorization, whereby people explicitly label themselves as members of a particular group (Stryker and Serpe 1994). Second, social identity is a fact of human existence: whereas we can posit potential participants with very limited ex ante social interaction, we cannot imagine a participant with no ex ante group identity – so when we look at the pursuit of identity, we are always looking at that pursuit in relation to participants' ex ante social identities (Stryker and Burke 2000). A final aspect is positive differentiation: most identity theorists argue that people pursue or consolidate group identities in order to reinforce their self-esteem, not undermine it (Huddy 2001; Klandermans and de Weerd 2000). This means that people will seek to align their behaviors with identities to which they assign positive value.

These observations allow us to maintain a theoretical and empirical distinction between the pursuit of identity and pursuit of interaction with other similarly identified individuals. In political contexts, that distinction is often obscured, because participating in a collective action is usually the only way to lay claim to a specific political identity. Even the minimal case – such as the adoption of a specific party label – demands voting or registering as a party member, behaviors that invoke collective action problems. Any

sort of identity-reinforcing or identity-verifying behavior will similarly involve some type of collective action.

In the case of hacktivism, however, individual hacktivists can participate in activities that enhance or confirm identity, without necessarily interacting with other hacktivists. For example, a political cracker might deface a web site with a message that sends "greetz" to fellow hackers, thereby enhancing his identity as a hacker, without actually working with any other hackers on the defacement.

Hacktivism's unsual capacity for solo activism thus allows us to separate and compare the identity and interaction motivations. If interactive incentives drive participation, we would expect a correlation between the propensity for collaboration, and the selection of a collaborative or non-collaborative form of hacktivism. If identity incentives drive participation, we would expect a correlation between a hacktivist's group identity or background, and the particular type of hacktivism in which he or she engages. If neither incentive is operational, we would expect a random pattern of participation in different types and forms of hacktivist activity.

These tests were conducted against the data gathered from the fifty-one interviews described in the introduction to the dissertation. I use three sets of questions, culled from these interviews, to shed light on the role of identity versus interactive incentives:

1. *Would you describe yourself as a hacker? Activist? Hacktivist? What do these labels mean to you?* This question speaks to the issue of identity motivations. I expected hacktivists to self-categorize in ways that would reflect their alignment with different ex ante identities.

2. *Has any of your political hacking involved working with others?* This question assesses the extent to which hacktivists voluntarily collaborate with other hacktivists, even though most hacktivist activities are at least potentially executed on an individual basis. I expected that this question would allow me to reject the hypothesized interactive incentive by showing that collective action was instrumental rather than desirable. That view would be vindicated if hacktivists only work collaboratively on the forms of hacktivism that demand collaboration – namely virtual sit-ins, and to a lesser extent, political software development. I expected that people engaging in other kinds of hacktivist activities would be doing so without working with others, since hacktivism offers little gain in efficacy through collective action, and few apparent interactive benefits.

3. *What is your view of the following activities? Which of them have you engaged in? (If you have engaged in any of the following, please describe the issue or activity, and your role in it, if possible.)*

a. *Virtual sit-ins (e.g. Zapatista FloodNet, anti-WTO sit-in staged by electrohippies)*
b. *Site redirects (e.g. Nike site redirected to S11 anti-sweatship site)*
c. *Site defacements (e.g. India/Pakistan, Israeli/Palestinian, China/US conflicts)*
d. *Site parodies (e.g. WTO parody site at www.gatt.org)*
e. *Denial of Service attacks (solo, not virtual sit-ins)*
f. *Information Theft (e.g. theft of travel info for participants in World Econ Forum at Davos)*
g. *Political software development (e.g. Hacktivismo project to defeat Chinese firewalls)*

I expected people to describe their involvement in and opinion of different forms of hacktivism in ways that were consistent with their prior identities as hacker-programmers or artist-activists.

Interactive incentives: the results

Does interaction also appear to be an incentive for participation? I answer this question by assessing the rate of collaboration among those interview subjects who have participated in different forms of hacktivist activity. Among the 43 participants, 36 reported working with others in their political hacking – 83% of the sample. As predicted, collaborative activity was particularly high among virtual sit-in participants (all of whom had, by definition, participated in collective activity), but it was no higher among political software developers (28 out of 32, or 82%, had worked with others) than among the sample as a whole. If we exclude virtual sit-in participants, but include political software developers, we have 29 participants, 20 (or 69%) of whom report working with others on their hacktivist activities. In other words, the hacktivists interviewed were *much* more likely to work collaboratively than I had predicted, regardless of the type of hacktivism in which they engaged – suggesting that even in the socially thin environment of the Internet, interactive incentives may be a crucial motivation for participation.

There are several possible explanations for the surprise. The most obvious possibility is that my sample was disproportionately likely[28] to include socially networked hacktivists: the use of snowball sampling increased the likelihood that my subjects had social links to other hacktivists. This bias is compounded by the fact that it was easier to find hacktivists who engaged in collaborative activities like political software development and virtual sit-ins – and indeed, 31 of those who had participated in some

[28] Hacktivists engaged in criminal activity like denial-of-service attacks, web site defacements, and virus distribution are much harder to contact.

sort of hacktivist activity had been involved in virtual sit-ins and/or political software development (although not to the exclusion of other hacktivist activities). This leaves only twelve respondents who had been involved in hacktivist activities, without engaging in either virtual sit-ins or political software development. This is a problematically small sample, but it is worth noting that even among these twelve, eight reported working with others on hacktivist activities. While sampling error *may* account for the high number of hacktivists who report collaborative activity, there is no compelling evidence that it is the source of the finding.

Another explanation is that I may have defined collaboration too generously. With the exception of virtual sit-in participants and Hacktivismo members (who together account for 23 of the 43 participants), most of the "working with others" involved working with somewhere between one and four collaborators. Collaboration on this scale might be explained within an Olsonian model as a "small group" case in which sharing the burden of collective action is facilitated by the small number of actors. In Olson's model, however, the small group exception is explained by the small number of actors capturing a disproportionate share of the benefits of action; since the benefits of hacktivist activities remain public and non-excludable, even when the activity is conducted by a small group of actors, the collective action problem can not be resolved by the small group exception.

This is related to the third possible explanation: perhaps that my theoretical model underestimated the instrumental value of collaborative activity. Perhaps hacktivism is not so readily executed by a lone actor, even though lone actors can have some impact. If this

is the case, hacktivists may choose to collaborate in order to achieve certain ends, rather than shoulder the burden of organizing and executing a "hacktion" on an individual basis.

And indeed, hacktivists do describe their collaboration in instrumental terms – and equally telling, rarely attest to its interactive rewards. Interview subjects made remarkably few allusions to the social experience of collaboration – which in itself suggests that social interaction may not be a big incentive for hacktivism, even in its collective forms. One member of Hacktivismo said that the group "just fit" (Mr. Happy 2002); another said that Hacktivismo leader Oxblood Ruffin "put together a really good, bright team" in which "everyone's respected for what you do" (Ca$h Money 2002). A member of the Electronic Disturbance Theater said that "I respect [fellow EDT members]….They have helped me tremendously. I was a baby Internet artist. I learned a lot from them"; at the same time, she acknowledged some tensions within the group by saying that "we all have our own agendas" (Karasic 2002). A pair of political crackers underlined their commitment to collaboration by refusing to be interviewed separately: "We cannot give separate interviews because we don't consider ourselves separate, a team is a team" (m0r0n and nightman 2002). Other than these few comments, however, interview subjects offered little comment on their social relationships with collaborators.

In contrast, many subjects emphasized their instrumental or purposive reasons for engaging in hacktivism, including collaborative forms of hacktivism. These were most often framed in terms of the sense of efficacy derived from hacktivism; the sense that hacktivist participation yielded a measurable political impact. As one political software developer said, "[t]here are things you can accomplish by going to court and meeting with politicians but you have to remember what you can and can't get done that way."

(Haselton 2003) This was echoed by the stress that several Hacktivismo members laid on the sense of efficacy derived from political software development: "I decided I can change something in the world if I participate," said Jules. "Hacktivismo has the manpower to change things." (Jules 2002) "I'm not avenging the world; I am contributing in however small a way." (Ca$h Money 2002) Another Hacktivismo member was drawn towards political software development because it "produces something tangible, rather than just protest. Something people can use." (metac0m 2002)

A theme that was reflected in a number of these comments was the sense that hacktivism offered a form of political engagement in which the impact of activism could be disproportionate to the number of activists. "The idea that it [virtual sit-in participation] should or should not be meaningful because it takes a minute is ridiculous," said EDT member Carmin Karasic. "It's not as simple as number of deaths versus number of clicks." (Karasic 2002) A member of the Space Hijackers wrote that:

> We are always inspired by the ability of people to bend technology to serve a function other that what it was designed for. The internet has been a great leveller of the playing fields as emails and websites cost so little that a 15yr old girl with time on her hands can set up a convincing spoof version of a website that would cost a multinational thousands. Computer programmers can battle the censorship of governments and create political protests out of a company or governments own work. (Priestley 2003)

The lack of reflection on the social rewards of participation, and the regularity of comments on the efficacy of hacktivism, suggests that instrumental rather than social incentives may indeed provide a better account for hacktivists' proclivity for collaboration. But this finding raises the more fundamental question: why are hacktivists so convinced of the instrumental value of collaboration? After all, the same comments that reflect faith in the efficacy of collaborative hacktivism suggest an underlying impatience with the equation of mass action and political impact. Hacktivists are drawn

to hacktivism because it can be executed at the small group level; why not take this dynamic to its logical conclusion, and act alone?

One possible answer is that hacktivists are negotiating a delicate balance between the benefits of collaboration, and the inefficiency of large groups. Cooperation in small groups yields some of the benefits of group action – not only the instrumental benefits underlined by comments about hacktivist efficacy, but also the identity benefits that are suggested by hacktivist preoccupation with self-labeling – while avoiding the collective action problems associated with participation in large groups.

But this kind of small group engagement should not be confused with Olson's own "small group" exception to the logic of collective action. As noted earlier, Olson's prediction of participation in small groups applies to situations in which that group is able to appropriate a disproportionate share of the benefits of collective action. In the case of hacktivism, however, hacktivist groups would receive only a very small share of the public goods that they are pursuing – if that. In the case of Hacktivismo, for example, coders in non-censored countries are doing anti-censorship; these coders expect no personal benefit from the erosion of information controls. Olson's logic of small group participants as the recipients of disproportionate benefit does not hold here.

This returns us to the original formulation of participation as a collective action problem. This collective action problem may be writ small rather than large, with a relatively few participants collaborating in the production of a public good, but it still confounds our expectations of self-interested behavior. If hacktivist collaboration represents an instrumental strategy rather than the pursuit of interactive rewards, we must

still look elsewhere for a notion of social incentives that explain hacktivist participation. Identity incentives provide a promising alternative explanation.

Identity incentives: the results

Identity incentives turn out to be a major determinant of the particular type of hacktivism in which individual hacktivists engage. The group identity that is being pursued, in this instance, is the identity of hacker-programmer (for political coders and crackers) or artist-activist (for performative hacktivists.) People who come from the hacker-programmer world, with its commitment to safeguarding the Internet, pursue forms of hacktivism that reinforce their identities as Internet guardians, and that leverage their particular technological skills. People who come from the postmodern left world, in contrast, pursue forms of hacktivism that reinforce their identities as strategic activists, and that leverage their tactical creativity. This is reflected not only in the relationship between participant identity and *type* of hacktivism engaged in, but also in the dependent relationship[29] between participant activity and the specific *form* of hacktivism pursued.

A tabulation of the relationship between hacktivist background (hacker-programmer vs. artist-activist) and type of hacktivism (performative hacktivism or

---

[29] A reminder: I use "type" of hacktivism to refer to the overarching categories of political cracking, political coding and performative hacktivism; I use "form" of hacktivism to refer to specific activities like virtual sit-ins, site defacements, software development, etc. Note that type and form are related, since different forms of hacktivism are associated with different types (i.e. performative hacktivism focuses on virtual sit-ins and parodies, while political coding encompasses software development) . As a result a relationship between identity and *type* of hacktivism necessarily involves a relationship between identity and *form* of hacktivism. Indeed, when we move from overall patterns in the relationship between identity and type of hacktivism, to specific comments about particular forms of hacktivism, it looks like the selection of particular forms of hacktivism may be the mechanism that produces the overall relationship between identity and type of hacktivism.

political coding/cracking[30]) establishes the relationship between a participant's identity and his or her type of hacktivist participation. A simple chi square test shows that this pattern is statistically significant (see Table 9**).**

[30] Let me emphasize once again that the difference between political cracking and political coding is a significant one – not only in their legality, but in their political effectiveness. But because political crackers are hard to track down, my sample did not include enough crackers to allow for a three-way analysis. While such an analysis might have been enlightening, however, it is not essential to the immediate question of whether ex ante identity (as indicated by the hacktivist's culture of origin) determines the type of hacktivism in which s/he engages. Because both political crackers and political coders come from similar backgrounds of hacking and programming, a binary distinction between performative hacktivism on the one hand, and political coding/cracking on the other, is sufficient to assess the relationship between identity and type of participation.

Table 9.
Relationship between background and type of hacktivism pursued

Type of hacktivism

Background	Performative Hacktivism	Political Cracking and/or Political Coding	Both[31]	Total
Hacker/programmer	0	23	7	30
Artist/activist	10	2	2	14
Hacker/programmer AND artist/activist	0	0	2	2
Neither hacker/programmer NOR artist/activist	1	2	0	3
Total	10	25	11	49

Degrees of freedom: 4
Chi-square = 28.4788199454866
p is less than or equal to 0.001.

The 30 hacker-programmers[32] in the sample all participate in the forms of hacktivism that are encompassed by political coding and political cracking, although a

[31] This category includes hacktivists who have engaged in forms of hacktivism that belong to performative-type hacktivism (such as virtual sit-ins) *and* forms of hacktivism that belong to political coding or cracking-type hacktivism (such as software development or web site defacements). Most of these respondents tend to engage more frequently in one or the other type, however.

[32] This sample includes only those forty-nine respondents who had clearly engaged in at least one activity that qualifies as political cracking, political coding, or performative hacking. The coding of interview subjects as hacker-programmers and artist-activists was based primarily on self-categorization, supplemented by additional information about participants' backgrounds. Most crucially, I categorized participants as hacker-programmers if they had longstanding programming experience, even if they did not self-categorize this way; it was the only way of compensating for respondents' widespread tendency to see their programming skills relative to those of more experienced programmers, such that even people familiar with multiple programming languages would say that they were not "real" programmers because, for example, they had never had formal training.

An additional factor in the categorization process was that a number of participants either fell into multiple categories (most often people with predominantly hacker backgrounds, who nonetheless described themselves as "activists", though not necessarily progressive activists), while several fell into no category at all. In instances where respondents fell into multiple categories, I placed them into the category of their dominant background; in most instances even participants who self-labeled with multiple categories were clearly much more tied to one or the other political culture. In the two instances where participants truly

handful have also done some performative hacktivism. This includes forms of hacktivism like political software development (by far the most common activity among my interview subjects), information theft (more often admitted to than I had anticipated), DoS attacks, web site defacements, and web site redirects.

The fourteen artist-activists were more likely to participate in the forms of hacktivism encompassed by performative hacktivism. This includes organizing or participating in virtual sit-ins, and creating web site parodies. While two people with artist-activist identities had only engaged in the political coding type of hacktivism, each was also extensively involved in non-hacktivist forms of progressive activism online. It is also worth noting that two activists who had engaged in political coding on top of their performative hacktivism were people with significant connections to the hacker community.

The comments of individual interview subjects provide two kinds of support for the finding that participant backgrounds shape the type and form of hacktivism they engage in. First, the way respondents discuss different labels (such as hacker or hacktivist) shows the significance and value that is placed on belonging to particular groups – in other words, to claiming particular identities. Second, the way respondents discuss different forms of hacktivism (such as virtual sit-ins or web site defacements) shows that the form of activism is far from an accidental choice: it is a specific statement of values and identity. By looking closely at the way respondents discuss different forms

---

straddled both backgrounds, they were labeled as such; and in the three cases where neither category was applicable, respondents were counted separately.

of hacktivist participation we can unpack the dynamic whereby identity shapes the form participation (and thus, the type of hacktivism engaged in).

The relationship between participation and ascriptive identity is confirmed by participants' discussion of different labels. Most respondents had strong views about the significance and value of different labels, and about the labels they personally adopted or rejected. The intensity of feeling reinforces the conclusion that labeling does indeed play a role in the dynamic of hacktivist – and perhaps other political – participation.

One interesting pattern was that hacker/programmers had just as many reservations about the hacker label as did artist/activists. Both groups often saw the hacker label as low status, and in need of alternative or improvement:

> I would describe myself as a hacker if there was not possibility of the word being misunderstood and associated with malicious actions. (Hocevar 2003).
>
> I stopped using the term hacker in public, since the meaning 'computer criminal' is to much associated with it. (Dornseif).
>
> I don't use it [hacker] that much because rightly or wrongly hacker still has connotations to a lot of people that it is illegal. (Haselton 2003)

Still others adopted the hacker label, but specifically noted that it had been assigned to them by others – treating it as an honorific:

> I am a hacker. I say that because I have been recognized as a peer by people I regard and respect as hackers, and because I use machines and systems more as instruments instead of interfaces or tools. (Reid 2003)
>
> Hackers consider me a member of their community and I am quite proud of that. (Riemens 2003)
>
> I would be pleased to be called hacker by a hacker I respect. (Jules 2002)

These comments demonstrate the way that hacking and/or hacktivism could be used to reinforce a participant's sense of belonging to a particular group – in other words, to reinforce a particular identity.

Discussion of the hacktivist label often reflected a similar concern with external perceptions of the label's meaning and status. Notably, the hacktivist label was for some respondents linked to an artist/activist identity, while for others, it was associated with hackers/programmers – though the association was not always seen in positive terms:

> When I think about it, I can't make a distinction between Hacktivist and Activist, but I tend to take anyone using the former term less seriously. I don't have a good reason for this, either, except perhaps I see the term used more by people who use "h@X0r" speak, which I guess I find a little silly. (Goldstein 2003)

> I don't really understand the term hactivist[33] properly….in places like australia - people who do stuff become quite cynical if you describe yourself as a hactivist. so, for me, its not a useful term at all... i think a hactivist seems to be someone who may be involved with real or symbolic actions that somehow involve computer technology and data networks. i certainly wouldn't describe myself as a hactivist! (sam)

> When I hear the term hacktivist i first think of silly scriptkiddies looking for a justification for defacements, although I'm aware of the fact that others are called hacktivist, too. (Dornseif 2003).

Even those who engaged in activities that they themselves saw as hacktivism often disdained the hacktivist label. One person who had formerly identified with the hacktivist label gave it up "as soon as it could be seen as military…using military terms, seeing hacktivists as warriors. As a peacenik I don't want to be a warrior." (Hirsh 2002) While another participant was not sorry to hear his work described as hacktivism at a hacker convention, he nonetheless felt "this word is really silly….I won't stand on stage and say I'm a hacktivist." (Paadeluun 2003) One activist carefully distanced himself from others using the hacktivist label: "'Hacktivist' is close to the level we work on, but we certainly don't see ourselves as such. Most hacktivism doesn't really strike us as a

---

[33] Some people assign significance to the spelling of the word "hacktivist". Ruffin (2002) argued that the early tendency to spell hacktivism without the "k" was a sign that people did not understand its inherent relationship to the world of computer hacking.

particularly effective or meaningful method of protest. " (Anonymous 2003) Yet another labeled his activity "electronic civil disobedience" (Dominguez 2002a) specifically to separate himself from those using the hacktivist label, and from the relationship to hacking that the label connotes.

But in some cases, the hacktivist label was seen as desirable:

> "I consider myself a Hacktivist by the classic definition. A hacker who has his own agenda. My agenda is to survive and work up to the top 10%."(Eisley 2003)

> "[I'm not a hacktivist] yet, but I'm moving in this direction. To me true hacktivism is about hacking systems in order to achieve ideological aims. " (Sandberg 2003a)

> Hacktivist – definitely. I am an activist who seeks to use information systems to organise and for action to change social/political perceptions. I know that really annoys a lot of U.S.-based hackers who see 'hacktivism' as action to promote purely computer-based action to promote just computer systems. I see hacktivism as being any type of social or political activism that's enabled by information systems, electronics or mechanics. I see the term as an extension of the MIT 'hacker' idea to activism, not just a subset of the term 'hacker' to describe the promotion of technology. (Mobbs 2003)

> Hacktivist: Well I suppose I can agree to that label. If the term means using hacking skills for activism. (Stevenson 2003)

> I don't really consider myself a "hacktivist" (which to me is a hacker and activist combined), as I'm just simply an activist... Although, I do obviously provide the tools to hack. (Brown 2003)

These latter comments are notable for establishing that participants see a relationship between the kinds of activities they do, and the kind of label they claim. This reinforces the conclusion that the forms of hacktivism participants engage in help to shape or consolidate a particular identity.

That conclusion is reinforced by the way that hacktivists talk about the particular forms of hacktivism in which they do or do not engage. Artist-activists think primarily in terms of how an activity fits with the responsibilities of strategic activism:

> I think a sit-in or defacement could help a campaign. For instance, i've thought about what kind of impact it would have to do something like that to the notre dame site (over their failure to recognize a lgb [lesbian gay bisexual] group), but i generally think that it

> would cause the lgb rights movement to lose a lot of support from moderates.(Kreider 2003)
>
> What is the good of this [defacement] action? It will just hinder a site for some time. Get a web administrator fired or to work more special shifts. People tend to overestimate what they have done there just by crushing it. (Tangens 2003)
>
> i reckon this stuff is really good - but i also think who-ever is developing this stuff really needs to know what they are doing as lives are often at risk (sometimes i am concerned that this stuff with fancy names are being created by rock-and-roll stars) ... i think the leading political software development is the linux project... often when i hear about projects like hacktivismo - i wonder if… how do these projects continue? i mean - its not right to often judge them - but what is the trajectory of these projects? again, you hear sounds about them - but then the trail drops down... i guess lately, personally, i am getting in to sustainability and longevity of projects.(sam)

Hacker-programmers, in contrast, criticize tactics on the basis of their technological merits, and their impact on the health of the Internet:

> I think the Hippies getting hosed down in the streets was more entertaining then anything they did (more like tried to do) on the Internet. A couple modems vs. the latest in network technology, I laugh. (Murphy 2003)
>
> I have never participated in any DOS activities, nor will I. DOS attacks almost always have innocent, unintended victims in addition to the intended. I once worked at a small ISP which hosted several customers who drew DOS attacks. The attacks took the entire ISP offline, affecting not only the intended victim but many others as well.
>
> it would hurt me too because of network-slowdowns (Dietrich 2003)
>
> Never. I firmly oppose the idea of denying access to any service. This, and points B to D are mostly put under the umbrella of a generic term of people called "Script Kiddies". They like to use tools/techniques they find on the internet in a more or less "ready in 10 minutes"-form in a puberal manner. Mostly to make them look tough in front of/impress little groups of these "Script Kiddies". The majority of "regular hackers" thinks of themself not in this way, and hates to be associated with them. (Mildham 2003)
>
> I've never found one of these to be beneficial. I always thought hackers were supposed to free information flow and spread data, not clog up the lines and shut people down. (Eisley 2003)

It is notable that denial of service attacks are rejected here not on grounds of effectiveness, but rather on the grounds of being counter to hackers' interest in and responsibility to Internet health. It suggests that many hacker-programmers reject denial-

of-service attacks because they are counter to the hacker ethic, and counter to hackers' self-image as the guardians of the Internet.

This is confirmed by the way that hacker-programmers talk about their own involvement in political coding, which underlines that way that coding reinforces their positive identification with hacking. The comment that "cypherpunks write code" (Dornseif 2003) exemplifies the view that writing software is what coders are supposed to do. Or as another respondent put it, even more explicitly: "We programmers have to fight on our own terrain. The forces that rule can rule as much as they want as long as we have our censor-resistant p2p-networks."(Dietrich 2003) The self-image of coder-crusaders is also suggested by the way Ruffin framed both Hacktivismo, and political software development more broadly:

> The technology we're developing is really aimed at helping democracy activists. Any technology can be used for negative purposes. Software developers have to ask: does this fundamentally expand or abrogate the democratic experience? (Ruffin 2002)

Artist-activists, in contrast, evaluate the tactics of performative hacktivism by the aesthetic, political, and experiential criteria of the postmodern left:

> All of our technology is only about mass usage. I could sit by myself in my Zapatista Floodnet all day and it's not going to do shit. But if you get a mass, a swarm, it will disturb…I believe the size of the performance means that it's the product of the multitude….that it is only the outcome of a sort of mass agency.(Dominguez 2002a)

> [The eToys virtual sit-in] was important . It showed the synergy of disturbing collective action on the net; and art, and gaming, and politics. People played it because it was fun It felt like it was part of an epic project.(Galloway 2002)

> [Re: parodies] Much more fun! That I am very much in favor. (Riemens 2003)

By embodying postmodern values of artistic creativity, mass legitimacy, and sheer fun participating in performative hacktivism can thus reinforce one's identity as an artist-activist.

The one surprise in both hacker-programmer *and* artist-activist comments was the prevailing attitude towards information theft – which, as a form of political cracking, I expected would be condemned by this sample of coders and performative hacktivists. But only three respondents unambiguously condemned information theft (though many responded with an unelaborated "no" when asked if they had done it) Seven respondents either explicitly admitted to participating in information theft, or answered in a coy but suggestive manner – a surprisingly high number, considering that they were confessing to an illegal activity. Along with several other respondents who avoided answering the question directly, these respondents provided a consistent picture of information theft as an activity that was instrumentally justified in the eyes of many hacker-programmers *and* artist-activists:

> information theft is a fuzzy concept - and generally theft can be only applied to tangible objects. I have retrived information not meant to be viewed by the public - you might call this open source intelligence
>
> if you cant get into the meeting, is there another option? How about full on Identity theft...
>
> My view on information theft is that it is a necessary evil.
>
> Have done this and find it extremely important. Information is a major tool. Like all resources controlled by the powerful, I believe the only way we can beat them is by taking control of it.
>
> I don't have a problem with this where it's done for the purposes of a public campaign. Information theft to support fraud, or some other activity like targeting people for abuse or violence, I don't agree with. On a related topic, I also have no problem with disclosing any that is not *personal* information as a means of exposing the poor security of computer systems, or any form of political/corporate fraud or maladministration.
>
> is it theft if you find it laying out in the open? :>

Ultimately, however, this consensus need not come as much of a surprise, because information theft is consistent with both types of identity. For hacker-programmers, it fits with the view that "information wants to be free", and that it is a hacker's job to break down barriers to that freedom. And for artist-activists it fits with the postmodern analysis of information as power, and with the artist-activist's duty to disrupt power structures.

The way that hacktivists describe their choice of hacktivist activities thus reveals a number of patterns that together help to flesh out the relationship between identity and form of participation. For artist-activists, choice of form seems to be shaped by an assessment of whether a particular tactic fits with their notion of strategic activism. Artist-activists were more likely to assess particular tactics in terms of their longer-term strategic goals, reflecting a worldview that is embedded in a longer tradition of activism. Hacker-programmers, in contrast, made more comments about how particular tactics affected the well-being of the Internet itself, reflecting a worldview in which hacker-programmers are the guardians of the Internet. Interestingly, both sets of respondents made exceptions for political cracking when it took the form of information theft, which intersects with each worldview: for artist-activists, it is consistent with the idea of politics as leveling the playing field, while for hacker-programmers, it is consistent with the idea of hacking as the liberation of information.

We have now reviewed three types of evidence on the relationship between hacktivist identity and both type and form of hacktivism. First, we have uncovered a statistically significant correlation between a hacktivist's background in either the hacker-programmer or artist-activist world, and his or her likelihood of participating in political

coding/cracking or performative hacktivism, respectively. Second, we have seen that hacktivists clearly differentiate between different labels, and that they describe these differentiations in ways that suggest that they place considerable value on their ability to claim different labels – in other words, different identities. Finally, we have seen that hacktivists talk about their choice of particular forms of hacktivism in ways that suggest an assessment of how well an activity fits with one's identity as either a strategic activist (for artist-activists) or an Internet guardian (for hacker-programmers).

The obvious remaining question is whether differences in identity could explain the choice of political coding versus political cracking. Unfortunately, because political crackers are so hard to track down, the sample does not include enough crackers for us to answer this question. But my suspicion is that while political crackers also have hacker-programmer identities, they are from a different slice of the hacker-programmer scene, and thus, have a very different sort of hacker-programmer identity. Interviews with political crackers suggest that they tend to be younger than political coders, and may thus be less steeped in hacker norms of non-destruction and freedom of speech. The preponderance of web site defacements on issues like the Palestinian-Israeli conflict, the Indian-Pakistani conflict, and the China-US conflict further suggests that political crackers may come disproportionately from non-Western countries. That raises the possibility of cultural differences, and in particular, of the possibility that even in the English-dominated Internet language barriers may play a significant role. It may be that the inner circle of hackers communicates fluently in English, while the outer circle knows enough English for technical and instrumental communications, but not enough for

engagement in political debate. In other words, these crackers may be able to soak up hacker techniques, without soaking up the subtleties of hacker politics.

Conclusion

The case of hacktivism provides a provocative counterpoint to the conventional thinking on selective incentives for political participation. By sharpening the distinctions among different selective incentives we are able to focus on the universe of social incentives as uniquely capable of addressing some of the shortcomings of purposive accounts. By further distinguishing between types of social incentives – identity vs. interactive – we are able to test very different notions of what social incentives actually mean. And by grounding the very slippery notion of identity incentives in a properly theorized account of identity-seeking, we are able to discern the role that identity incentives play a significant role in at least this corner of the political universe.

What emerged was a picture of collective action that would confound narrowly constructed notions of self-interested behavior. Yes, participants value collaboration – but not because it provides interactive benefits. Rather, they see collaboration as an instrumentally useful way of pursuing certain political ends. Simply looking at incentives for collaboration still leaves the mystery of why self-interested individuals pursue collective action as a means to those ends.

Identity incentives, on the other hand, help us understand the particular patterns of hacktivist participation. Hacktivists engage in collective action – in very particular forms of collective action – because these forms offer very particular rewards. These are the rewards of confirming and reinforcing a valued group identity. For hacker-programmers,

that is the identity of Internet guardian, reinforced by engaging in forms of hacktivism that express one's technical skill – while avoiding forms that damage the Internet itself. For artist-activists, it is the identity of strategic creative activist, reinforced by engaging in forms of playful, mass hacktivism that meet postmodern aesthetic and political criteria – while avoiding forms that lack offline or mass legitimacy.

These findings help solve the puzzle identified at the beginning of this chapter: the puzzle of hacktivism as a form of participation that places means before ends. For hacktivists, the choice of means – virtual sit-in or web site defacement, political software or denial of service attack – is an end in itself: the end of confirming a very particular kind of social and political identity.

Chapter 4

Hacktivism and State Autonomy:

The Transnational Politics of Policy Circumvention

Introduction

In the bull market of 1999, eToys stood out in the field of favored technology stocks. eToys was one of the hottest properties in online retail at that time, with a market capitalization of $8 billion in September of that year ("Toy retailing -- Trouble in toy town?" 2000). And like any big company, it wanted to protect its brand. Online, nothing is as essential to your brand as your domain name – the web address that lets people find your site (Waxer 2000; Whitman 2000).

So etoys.com was concerned that 20,000 customers a day were mistakenly visiting www.etoy.com (Ziegler). etoy – singular – was the digital home of a group of Zurich-based Internet artists. These artists had been online at etoy.com since 1995 – two years before the advent of eToys the retailer (Dugan 2000).

But that didn't stop eToys from using the usual means of protecting its corporate interests: the courts. On November 29, 1999, an LA court judge issued a judgement against the etoy artists, enjoining them from using the etoy domain or name (Smithers).

For the moment, it appeared that eToys had won. But the victory proved to be short-lived, as is apparent from eToys' share price (see Figure 13: eToys share price). No sooner had eToys won its day in court, then it confronted a new kind of challenge: the challenge of anti-corporate hacktivism.

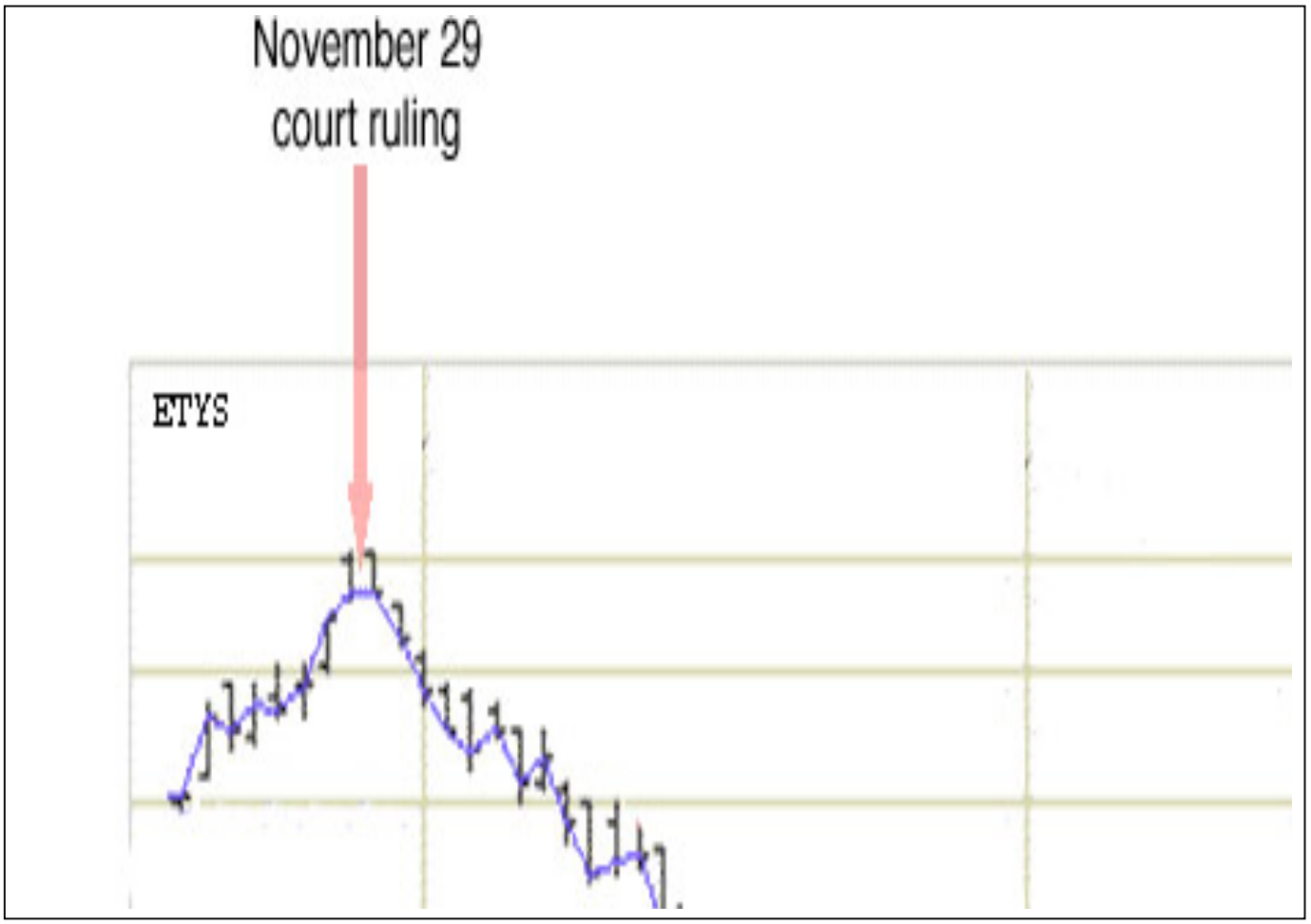


Figure 13: eToys share price
Source: (Grether 2000)

The challenge was mounted by a coalition of performative hackers and political coders, working together to create a variety of tools aimed at hobbling the eToys web site. Like the widely distributed e-mail that challenged etoy supporters to use e-mail, investor web sites, and protest sites to bring down eToys' share price (Grether 1999). Or the online "Toywar" game that inducted players into a community of anti-eToys activists by immersing them in a community of virtual etoy warriors (Kettmann 2000). Or the

little automated shopper who filled a virtual basket with Barbies and Legos, only to abandon its cart…after consuming plenty of server time (Grether 2000).

Within days, the eToys site fell prey to widespread complaints about its slow server and frustrating waits. And all this came during the Christmas shopping season – the season that was supposed to make good on the promise of eToys multi-billion market cap. While the "Toywar" campaign was not solely responsible for eToys' dwindling share price at that time (Leonard 2003), it has been cited as a contributing factor (Abreu 2000; Jones and Smith 2002; Nguyen 2002).

The hacktivist challenge showed that a court decision might *not* be the last word in a corporate dispute. But it is the *way* that this challenge was mounted that should interest scholars of policy, political participation, social movements, and transnational politics. These scholars expect political challenges to focus on efforts at policy influence. In the case of eToys, that might take the form of lobbying for a new system of domain name allocation, so that organizations like etoy would be better protected in the future.

Instead, the Toywar hacktivists pursued a strategy of policy circumvention, a political outcome that poses an as-yet-unrecognized challenge to state autonomy. Policy circumvention is here defined as legal noncompliance that:

a) is a strategic political response to a specific policy, law, regulation or court decision
b) focuses on nullifying the effect of a policy, law, regulation, or court decision, and
c) creates some non-excludable benefits (though there may be additional, excludable benefits of non-compliance).

Strategies of policy circumvention fall outside the models of transnational politics that are emerging from research into the anti-globalization, human rights and environmental movements. These models have successfully directed attention towards transnational civil society actors as a growing source of challenge to nation-states, focusing on challenges that come in the form of efforts at policy change. By focusing instead on efforts at policy circumvention, I hope to build on the transnational politics literature, demonstrating its utility in analyzing policy circumvention as well as policy change.

The promise of the transnational politics literature is clear from the moment we look at the possibility of applying its insights to the burgeoning phenomenon of hacktivism. At first glance, hacktivism would seem to share the four characteristics identified by Keck and Sikkink as typical of transnational advocacy networks: "the centrality of values or principled ideas, the belief that individuals can make a difference, the creative use of information, and the employment by nongovernmental actors of sophisticated political strategies in targeting their campaigns."(Keck and Sikkink 1998)

Hacktivism fits each of these criteria. While the values behind hacktivism vary quite markedly – political coders and crackers are often cyber-libertarians, while performative hackers have more in common with traditional leftists or anarchists – their actions and writings are usually framed in ideological or principled terms. A desire and belief in making a difference as an individual explicitly motivates many hacktivists.[34] Hacktivist activities like online parodies, virtual sit-ins, and information theft epitomize

[34] See, for example, comments from Hacktivismo members on page 189, below.

the very concept of "creative use of information." And hacktivists have demonstrated ever-greater precision and sophistication in targeting their campaigns, which may be aimed at domestic or foreign governments, or at corporations.

Yet Keck and Sikkink, along with other authors who follow them, do not envisage the full range of organizational strategies available to the networks they describe. Instead, they focus on the narrower subset of strategies focused on policy change. And in the case of hacktivism – which frequently aims not at policy change, but at policy circumvention – that means ignoring precisely those strategies and activities that may pose the greatest challenge to nation-states and their governments.

This chapter endeavors to expand the study of transnational politics by directing our attention towards the as-yet unexamined phenomenon of policy circumvention. It begins with an examination of the still-young scholarship on transnational social movements and transnational actors, in order to demonstrate that literature's focus on efforts at policy change. From there, it turns to the challenge of policy circumvention, explaining why it merits study, and positing a model for predicting its emergence and success. Next, it introduces hacktivism as a fruitful field for testing the model of policy circumvention, and tests the model against two cases. Finally, it suggests directions for further research into hacktivist policy circumvention, and into the larger phenomenon of policy circumvention as a form of political action.

Transnational politics and policy change

Any examination of the literature on transnational social movements must begin with Keck and Sikkink's *Activists Beyond Borders*, a volume that has strongly influenced subsequent research into the rise of transnational networks of activists. Keck and Sikkink's object was to show that "advocacy networks are helping to transform the practice of national sovereignty" and are "an important part of an explanation for changes in world politics."(Keck and Sikkink 1998) These networks "try not only to influence policy outcomes, but to transform the terms and nature of the debate."(Keck and Sikkink 1998)

Keck and Sikkink's notion of network influence is explicitly focused on the question of how networks affect state policy-making. While they have an expansive notion of the influence process as one in which networks "must use the power of their information, ideas, an strategies to alter the information and value contexts within which states make policies"(Keck and Sikkink 1998), policy-making remains the central object of interest. This focus reflects the usual priority of network actors themselves; as Keck and Sikkink note, activists' "definition of effectiveness often includes some policy change by 'target actors' such as governments, international financial institutions like the World Bank, or private actors like transnational corporations." (Keck and Sikkink 1998) The successful cases of network advocacy cited by Keck and Sikkink are those that have achieved some sort of measurable policy change, such as the pan-American network of human rights activists who successfully pressured Argentina's military government into ending the kidnappings and disappearances of political prisoners (Keck and Sikkink 1998).

Subsequent scholarship has followed Keck and Sikkink's lead in focusing on how transnational activist networks achieve policy change. In her analysis of the role of transnational social movements in affecting ecological conservation, Lewis (2002) defines these organizations' effectiveness in terms of "the establishment of policies and practices that improve conservation."(Lewis 2002) Schmitz analyzes the impact of transnational activism on human rights in Kenya and Uganda in terms of its "important effects of governmental foreign and domestic policy decisions."(Schmitz 1999) Dalton and Rohrschneider (1999) see transnational activism as the logical means of pursuing an environmentalist policy agenda, since spillover effects mean that "the locus of responsibility for policies designed to redress grievances shifts from the national to the international level."(Dalton and Rohrschneider 1999)

Some of the literature does endeavor to locate the policy-change agenda within a broader set of social movement effects. Sperling et al. note that the political import of social movements may lie in effects that are not conventionally recognized as politics, such as community organizing, "because it occurs outside of formal, male-dominated economic and political institutions."(Sperling, Ferree, and Risman 2001) One widely-examined issue is the impact of transnational politics on political discourse or norms; according to Khagram, Riker and Sikkink, "a significant amount of [transnational network] activity is directed at changing understandings and interpretations of actors or, in other words, the creation, institutionalization, and monitoring of norms."(Khagram, Riker, and Sikkink 2002a)

But these effects remain implicitly – and often explicitly – linked to the goal of policy change. Risse and Sikkink are interested in the moment when governments are

socialized into "talking the human rights talk" (Risse and Sikkink 1999) because they see it as one stage in a five-phase "spiral" of human rights change, culminating in a shift in government policy towards full compliance with international human rights norms. Hawkins traces this kind of process in his examination of changing human rights norms in Chile, crediting changing human rights norms with the emergence of a Chilean human rights network; the successes of this network are seen in how "the military regime altered its agenda, discourse, policies, and practices." (Hawkins 2002)

The consistent return to mechanisms of policy change stems from the broader agenda of the literature on transnational social movements: to demonstrate that transnational advocacy is posing a challenge to state autonomy. As Smith and Johnston (2002) put it, "[m]ost social movement research takes the modern nation-state as the context of contemporary political contention…..Internally, states are increasingly constrained by an expanding web of commitments to other international actors." (Smith and Johnston 2002) Tarrow (2002) critically notes, "much of the early work on 'global civil society' assumed – without a great deal of evidence – a zero-sum relationship between the growth of transnational networks of organization and the decline of state power." (Tarrow 2002) Scholars of transnational social movements are thus trying to substantiate the argument that transnational politics constrains state autonomy; demonstrating the impact of transnational advocacy on domestic (or international) policy is perhaps the clearest way of establishing this claim.

Yet to focus on policy change is to take an unnecessarily narrow view of the ways in which transnational politics impinge on state autonomy. In focusing on policy change, we assume the importance of centralized policy-making bodies, most frequently – though

not always – states. That assumption constrains the transnational politics literature's ability to establish its primary claim: the diminishing of the nation-state.

The phenomenon of hacktivism suggests that the nibbling away at the edges of state authority extends beyond pressures on policy change. The most significant pressure exerted by hacktivism is the sidelining of the state as an arena for effecting political change: rather than pursuing an agenda of policy change, hacktivists often find ways of enabling the circumvention of state policy. By modeling the challenge of policy circumvention, we can see how the phenomenon actually lends greater credence to the core argument of the transnational politics literature: the argument that transnational social movements constrain the autonomy of the state.

Transnational politics and policy circumvention

Policy circumvention is more than just evasion of the law. It is a political strategy that enables resistance to a contentious policy, law, regulation, or court decision. Its effects may ultimately include policy change, but it does not depend on policy change in order to be effective.

But distinguishing policy circumvention from simple law-breaking demands clear criteria for identifying the specifically political dimensions of this form of extra-legal behavior. Let me address each of these criteria in turn:

1. Policy circumvention is a strategic political response to a specific policy, law, regulation or court decision. This criterion captures the deliberately political nature of policy circumvention: it is a protest against a policy, law, regulation or

court decision that is seen as unjust or impractical. The political content of the circumvention is generally conveyed through explicit statements by the entrepreneurs driving the circumvention, who link their actions to a given policy or law, and offer a principled argument about why that policy or law is illegitimate. The policy circumvention is frequently accompanied by other more conventional forms of protest, including those aimed at policy change, such as media outreach, lobbying, or legal action.

2. Policy circumvention focuses on nullifying the effect of a policy, law, regulation, or court decision. Where strategies of policy change focus on combating the root problem – the unjust or impractical policy – strategies of policy circumvention focus on combating the effects of that policy by rendering it moot. Instead of voicing opposition to a given government decision, policy circumventers vote with their feet by finding ways to render a particular policy ineffective or unenforceable.
3. Policy circumvention creates some non-excludable benefits (though there may be additional, excludable benefits of non-compliance). One key distinction between policy circumvention and simple law-breaking is that the consequences go beyond the benefits to the individual participant. While policy circumvention often offers immediate and tangible private benefits, stemming from participants' relief from the law, it also creates larger effects. These effects may include increased issue awareness, declining enforceability of a given policy or law, or even policy change itself. It's important to note that these non-excludable benefits are not necessarily important to all the participants in a given circumvention. While the

entrepreneurs responsible for initiating and facilitating the circumvention may be motivated by the larger political consequences of circumvention, much of the power of the circumvention strategy lies in the fact that many people will be drawn to participate strictly for the immediate tangible benefits of evasion.

Using these criteria, we can distinguish between cases of policy circumvention (some, but not all, of which occurs in the world of hacktivism), and cases of ordinary law-breaking:

Table 10: Policy circumvention vs. law-breaking

Policy circumvention	**Law-breaking**
Hacktivismo (software to circumvent Internet censorship)	Private consumption of child pornography
DeCSS distribution tools (enabling the distribution of DVD-decoding software)	Private copying of DVDs and CDs
Underground currencies, barter systems	Tax evasion
Medical marijuana buyers' clubs	Recreational drug dealing and use
Abortion clinic blockades	Trespassing

In identifying the specifically political phenomenon of policy circumvention, and distinguishing it from ordinary law-breaking, we uncover a world of political activity that has remained outside the scrutiny of the literature on transnational social movements. Yet this activity speaks to that literature's core concerns – and particularly, its interest in establishing the impact of transnational politics on state autonomy. Examining policy circumvention thus promises to advance the transnational politics research agenda in several ways.

First, policy circumvention is a major pressure on state autonomy – perhaps an even more fundamental challenge than pressures for policy change, because it relegates the state to the sidelines. Policy circumvention shunts the state to the status of a side-show whose cooperation is non-essential to obtaining desired political outcomes.

Recognizing and understanding policy circumvention should be part of the agenda for mapping both the challenges to the nation-state, and the consequences of those challenges.

Second, policy circumvention is itself an additional pressure for policy change – making it a crucial missing piece of models that attempt to predict transnationally-driven policy change. Some efforts at policy circumvention act as a public demonstration in support of policy change; others help raise awareness of a key policy issue. The story of policy circumvention is thus not only an important counterweight to arguments about policy change, but must also be incorporated into the arguments and models of those authors who study the role of transnational movements in precipitating domestic policy change.

Third, policy circumvention changes norms about policy compliance, including the norms that govern the relations between states. The transnational social movements literature has widely argued that changing international norms act as the mechanism for translating transnational advocacy into domestic political change. (Hawkins 2002; Keck and Sikkink 1998; Khagram, Riker, and Sikkink 2002b) As we will see from the hacktivist cases below, policy circumvention is an effective pressure on both individual and state norms of behavior. Widespread policy circumvention changes ideas about which laws are legitimate, about the necessity of legal compliance, and about the use of noncompliance as a political tool. These effects can be seen most powerfully in the case of states who themselves adopt policy circumvention as a new tool of international relations.

If the transnational politics literature has something to learn from the study of policy circumvention, it also has much to offer to the project. Building upon the literature on new social movements, the transnational politics literature has underscored the importance of several core concepts for modeling contentious politics: repertoires of contention, mobilizing structures, and political opportunity structures.

Repertoires of contention and cultural framings

The notion of "repertoires of contention" was coined by Charles Tilly, who defined a repertoire as "the whole set of means [a group] has for making claims of different kinds on different individuals or groups." (Tarrow 1994) The related notion of cultural framings is analogous to a set of "discursive repertoires [that] provide contenders with a vocabulary of motives that can be used to legitimate their actions."(Traugott 1995) Keck and Sikkink applied the notion of evolving repertoires to their examination of the transnational slavery campaign, in order to comprehend how "technological and institutional change can alter the 'moral universe' in which action takes place, by changing how people think about responsibility and guilt, and by supplying them with new ways to act." (Keck and Sikkink 1998)

The preoccupation with how repertoires evolve and diffuse suggests the utility of the concept for considering policy circumvention. Since policy circumvention represents an expansion in the repertoire of transnational contention, at least as recognized by scholars of transnational politics, thinking of circumvention in terms of repertoires of contention allows us to usefully frame the phenomenon.

Resource mobilization and mobilizing structures

Resource mobilization theory, led by the work of McCarthy and Zald, has drawn attention to the ways in which mobilizing structures enable or constrain social movement organizing. By looking at mobilizing structures, we are able to examine "how movement organizations are affected by the availability of resources the effectiveness of organizational structures, and the constraints and opportunities provided by their larger environment." (Halcli 1999)

These structures have proven equally significant to the activities of transnational social movement organizations. In her examination of the role of NGOs in addressing violence against women, Joachim emphasizes the importance of "the mobilizing structure which these civil society actors have at their disposal, including the presence of organizational entrepreneurs, an international constituency, and experts."(Joachim 2002) Legler's investigation of transnational opposition to the Free Trade Area of the Americas found that limited mobilizing structures, particularly due to financial disparities among civil society participants, imposed significant constraints on the Hemispheric Social Alliance (Legler 2000).

The transnational politics literature has taken particular note of one emergent mobilizing structure: the Internet. Scholars have moved from seeing the Internet "as a form of communication, one that facilitated the rapid diffusion of information about contentious episodes among chains of movement actors" to "regarding the Internet itself as a form of organization itself." (Tarrow 2002) This has been borne out by specific case studies, such as Smith and Smythe's work on the defeat of the Multilateral Agreement on Investment (MAI); the authors found that "Internet technology contributed to the capacity

of groups to communicate, to quickly mobilize and widely disseminate critical information, outside the control of national elites."(Smith and Smythe 2001) Similarly, Pickerill's study of British environmental movements found that information technology "enables groups to co-ordinate campaigns without the need for a central office, newsletters, or the physical presence of activists" (Pickerill 2001).

The mobilizing structures literature encourages us not only to attend to the technologies of mobilization, but also to organizational resources, such as elite leadership, or movement entrepreneurs. These entrepreneurs prove crucial in understanding the transnational dynamics of policy circumvention.

Political opportunity structures

The notion of political opportunity structures allows us to capture the degree to which a political system is open or vulnerable to political change. McAdam, McCarthy and Zald describe political opportunity structures as encompassing four dimensions:

1. The relative openness or closure of the institutionalized political system
2. The stability of that broad set of elite alignments that typically undergird a polity
3. The presence of elite allies
4. The state's capacity and propensity for repression (McAdam, McCarthy, and Zald 1996)

Recent scholarship suggests that these dimensions can be translated to the transnational level. "Social movement theorists…speak of 'multilayered' opportunity structure, including a 'supranational' layer or a 'multilevel polity,' or they highlight how international pressures influence domestic opportunity structures."(Khagram, Riker, and Sikkink 2002a) As Reimann establishes in the case of Japanese environmental NGOs,

these transnational opportunity structures can sometimes provide a way of escaping from a domestic opportunity structure "highly unfavorable to advocacy NGOs."(Reimann 2002) Transnational pressures can also have dramatic effects on the domestic political opportunity structure, for example by strengthening or limiting the state's capacity for repression. (Maney 2002)

Together, the notions of repertoires of contention, resource mobilization, and political opportunity structures help us conceptualize the phenomenon of policy circumvention. First, we can frame policy circumvention as an extension of the repertoire of contention, beyond the conventionally recognized tactics of policy change. As I will show toward the end of this chapter, this extension represents an innovation in our capacity to recognize policy circumvention, as much it does the popularization of this form of contentious politics.

Next, we can use these notions to help predict the emergence and success of political action that meets the three criteria by which we recognize policy circumvention. Resource mobilization theory helps us understand the emergence of political strategy, such as a strategy of political circumvention. In particular we see that entrepreneurs, organizational capacity, and financial resources are key resources for mobilization. The notion of opportunity structures helps us comprehend the potential costs and benefits of efforts to nullify policy or law. In particular we see that political institutionalization, and the state's capacity for repression, may affect the viability and costs of efforts at nullifying policy. The variables affect the costs of participation in policy circumvention for individual actors, and thus shape the strength and force of the effort at nullification. Finally, the literature on mobilizing structures helps us hypothesize the circumstances

under which law-breaking might generate some non-excludable benefits. Inverting the literature that asserts the role of movement entrepreneurs in creating excludable benefits as an incentive for movement participation, we can imagine that movement entrepreneurs might also facilitate the creation of non-excludable benefits.

Fusing the insights of social movement theory with the main criteria for recognizing policy circumvention, we can thus posit three variables for predicting the emergence and success of policy circumvention:

1. Political entrepreneurs are necessary for the emergence of a policy circumvention effort (though not sufficient to ensure its success). These entrepreneurs frame the circumvention as a strategic response to a particular policy, and design the circumvention in a way that creates non-excludable as well as excludable benefits of participation.
2. Policy circumventions that face a low cost of failure are more likely to succeed. Depending on the policy area, the cost of a failed circumvention may be low or high. Policy areas in which the costs of failure are high will face difficulties in mobilizing participation. Low costs of failure therefore create a more favorable mobilizing structure for policy circumvention.
3. Policy circumvention is more likely to succeed when the state faces political constraints on repression. We can assume that any state would ideally wish to repress law-breaking of all kinds, including policy circumvention. Yet some states face political constraints on their capacity for law enforcement, particularly when dealing with policy circumvention. These constraints create a political opportunity structure that is more favorable to policy circumvention.

Hacktivist policy circumvention offers fertile ground for testing this three-part model of policy circumvention. The desire to circumvent conventional political engagement, and to transcend the limitations of the policy process, is widely described by hacktivists themselves. Furthermore, hacktivism encompasses a range of efforts at policy circumvention, and thus allows us to examine variation in the variables that account for success or failure.

This chapter will focus on two contrasting instances of hacktivist policy circumvention. The first, successful, example of policy circumvention is the case of DeCSS distribution; the distribution of banned code that allows the decoding and viewing of DVDs on Linux machines. (Remember that success here is defined not by the usual standard of policy change, but by the demonstrated incapacity of the state to enforce a given law or policy.) The second, less successful, example of policy circumvention is the case of Hacktivismo, a project designed to evade Internet censorship in China and other non-democratic regimes. Significantly, while Hacktivismo has had only limited success in defeating the effectiveness of censorship policies, there are reasons to think it may be more successful in precipitating policy change.

Policy circumvention: the case of DeCSS

In October 1999, a fifteen-year-old Norwegian named Jon Johansen got frustrated with the fact that he couldn't play his DVDs on his computer. His computer was running the Linux operating system, and the motion picture industry had yet to license software to play DVDs on a Linux machine. So he joined an online group that was working on Linux

DVD software. Ultimately, he successfully reverse engineered the DVD's encryption technology, and came up with a piece of software that would let Linux users watch DVDs. The software was dubbed "DeCSS" – a reference to the "Content Scrambling System" (CSS) encryption that the motion picture industry used to encode DVDs. That software was posted online, and quickly distributed across the Net (Harmon 2000).

But there was one little problem with Jon's program. The CSS encryption technology that Jon cracked didn't just keep DVDs from playing on Linux machines; it prevented DVDs from being copied. In order to play DVDs on his computer, Jon had been forced to crack the encryption system that had been devised as a form of copy protection. So even though Jon's intention was just to watch his own DVDs, his software had much broader implications.

These implications worried the Motion Picture Association of America, which quickly spearheaded a campaign to crack down on DVD cracks. Within a month, Johansen had heard from the MPAA's lawyers. At the MPAA's behest, Johansen was prosecuted under Norwegian law for breaking into his own DVDs ("Norwegian Teenager Jon Johansen Acquitted in DVD Case" 2003). Others who tried to distribute his code – most notably, the hacker magazine 2600 – were prosecuted under US law. While Johansen was acquitted by a Norwegian court in December 2002, an appeals court has subsequently agreed to hear an appeal of the acquittal (Gross 2003a). Meanwhile, in the 2600 case, two US courts have ruled that DeCSS code is not protected by the First Amendment; two other court cases have so far left the First Amendment question unresolved (Gross 2003a).

The motion picture industry's legal actions scarcely put an end to the DeCSS phenomenon, however. CSS descrambling code spread across the Net, distributed by a variety of tactics. Some people embedded the DeCSS code in images – using a technique known as steganography (Touretzky 2000c). Someone else embedded the code in song lyrics, and distributed the song (Touretzky 2000c). You could download a couple of animated characters who would explain the DeCSS code to you(Touretzky 2000c). Or look up a haiku that contained the descrambling algorithm (Touretzky 2000c). All of these approaches exploited the legal distinction between protected forms of speech, like artistic expression, and the unprotected status of executable code.[35]

The proliferation of DeCSS distribution mechanisms – though not DeCSS itself – represents a clear example of policy circumvention. The original DeCSS hack was not, at the time, an explicitly political act; it was a solution to the technical problem of wanting to play a DVD on a Linux machine. The fact that Johansen later became the focal point of

---

[35] For more on this distinction see (Touretzky 2000b) and (McCullagh 2001). As explained by one definition:

> Initially, a programmer writes a program in a particular programming language . This form of the program is called the *source program,* or more generically, *source code*. To execute the program, however, the programmer must translate it into machine language , the language that the computer understands. The first step of this translation process is usually performed by a utility called a compiler . The compiler translates the source code into a form called object code. Sometimes the object code is the same as machine code; sometimes it needs to be translated into machine language by a utility called an assembler.("Source Code" 1996)

The ability to exchange source code is crucial to programmer's abilities to read and improve each other's code(Touretzky 2000a), which makes it crucial to assuring the quality of computer programs, and to the growth of the open source movement (in which programmers constantly exchange and improve code). It is thus only executable code – code that is usable to the *hoi polloi* of computer users who are not themselves programmers -- that one might even consider regulating.

As many analysts have pointed out, however (Felten 2002; Touretzky 2000a) the legally useful distinction between source code and executable code does not always hold up in practice. Some scripting languages allow users to run source code without compiling it, effectively collapsing the distinction between the two; while other languages may create additional forms of code beyond source and executable.

a political and legal battle over DeCSS, and that he became an effective spokesperson for the rights of free software developers, should not lead us to retrospectively interpret his original hack in political terms. The political act that constituted policy circumvention was the outpouring of mechanisms for distributing Johansen's banned algorithm, despite the ban.

This proliferation of DeCSS distributions has successfully circumvented the US and international laws intended to enable the protection of copyrighted material such as DVDs. While some DeCSS authors have been prosecuted under the D.M.C.A. and trade secrets law,[36] the widespread availability of DeCSS code renders the Act largely ineffective in preventing the decoding or duplication of DVDs. Executable DeCSS code has been harder to distribute than the non-executable (but still theoretically usable) code distributed through steganography and other techniques, but even executable code is still available on the Internet.[37]

These distribution mechanisms were most certainly strategic, political responses to the decisions to prosecute Johansen, 2600 magazine, and others; to the American Digital Millennium Copyright Act (D.M.C.A.), which provided the legal basis for US

---

[36] DVD-CCA v. McLaughlin, Bunner et al. (and the related Pavlovich case) were prosecuted in California under trade secrets law; Universal Studios et al. v. Eric Corley was prosecuted under the D.M.C.A.. (Gross 2003b)

[37] As per the executable/source code distinction, the sites distributing executable code face greater legal jeopardy, as reflected in terms of use like:

> By accessing this site, you agree under the penalty of perjury [sic], you are not an agent or representative of any local, state, or federal law enforcement agency. You also agree that you are NOT collecting any evidence of any sort to incriminate this page's author, the [sic] or the authors of any files located on this site. You also agree that you are not accessing this site to collect information which could lead to, but is not limited to, shutting this site down or making its contents unavailable to the general public. ("Terms of Use" 2000)

prosecutions; and to the court decisions that banned 2600 from publishing or linking to DeCSS code. Dave Touretzky, who created the Gallery of CSS Descramblers, was "determined to show these movie industry types that it was a BAD IDEA to try to use trade secret law to interfere with free speech." (Touretzky 2003b) Of ten contributors to the gallery interviewed by this author[38], seven cited an explicitly political motive as the primary or exclusive reason for getting involved in the DeCSS issue. One contributor said that "it gave me an opportunity to talk to [my classmates] about the D.M.C.A., DeCSS, and code as speech"(Michaels-Ober 2003); another became interested in the DecSS issue because"[i]ntellectual freedom, and the ability to record, store and transmit information are dear to me."(Sandberg 2003b)

The fact that DeCSS distributors saw their distribution mechanisms as specific political responses to the D.M.C.A. and court decisions shows that DeCSS distribution meets the first test of a policy circumvention. The distribution schemes displayed in the Gallery of CSS Descramblers are not quite as clearly focused on nullifying these policy and court decisions – making the second test of policy circumvention a little harder. Most contributors to the Gallery expected that their distributions had limited practical impact; of the ten Gallery contributors interviewed, nine described their code as unlikely to be used, and estimated that no more than three people would have downloaded it.

---

[38] The Gallery of CSS Descramblers listed sixty-one unique contributors as of May 12, 2003. Of these, I attempted to contact twenty-two contributors via e-mail. Six e-mails bounced; four contributors did not reply; two more agreed to interviews, but failed to return their answers. Ten interviews were successfully completed, nine via e-mail, and one via online chat. I interviewed an additional five DeCSS distributors (distributors not listed in the gallery) via e-mail, for a total of fifteen interviews.

As Dave Touretzky observed, “If someone just wants to play or copy movies, they can get executables from other sites like doom9.net. I think people visit my site for intellectual stimulation, not to download code they want to use.”(Touretzky 2003b)

And indeed, the Gallery contributors make a point of noting the inevitability of DeCSS distribution. The role of the Gallery distributions is to underscore the fact that DeCSS distribution effectively nullifies the court and policy decisions. “I think my DeCSS webpage caused people to understand how ludicrous it was to try and stop the distribution of decryption code,” said one contributor. (Hocevar 2003) “I expect that the criminalizing of software tools will not remove the software from world wide availability distribution,” said another. (Miller 2003) In slightly grander terms, one Gallery contributor wrote that:

> I am optimistic that in the long-term, a balance will be achieved between "promoting the progress of science and useful arts" and totalitarian digital rights management. This balance will only be achieved once the intellectual property owners concede that hackers will always be one step ahead of them technologically.(Michaels-Ober 2003)

These comments were echoed by the views of the other (non-Gallery) DeCSS distributors, who offered comments like,

> I believe open source CSS code is now available fairily widely, and due to the international and anonymous nature of the internet, I don't believe it is going away anytime soon.(Steve 2003)

and

> There's no way to stop it. The internet is a free society. No content has ever been successfully banned from the internet.(Eisley 2003)

It is also clear that many distributors of executable DeCSS code also see distribution in political terms, and/or as a way of nullifying the court and policy decisions

on DVD encryption.[39] One former distributor[40] (since forced to remove DeCSS from his site) writes:

> this software is simply software to allow linux users to view DVD movies from their hard-drives. Based on all information available to me, I believe it is 100% legal to post this code….I am providing this content because I believe it is legal, and useful information.(Gadd)

A web site linking to a list of DeCSS mirrors (web sites that make DeCSS available for download) describes itself as "[t]he tool that every major film studio in Hollywood doesn't want you to know even exists,"("Humpin.org: King of the Road") and maintains a news page containing criticisms of the court decisions limiting DeCSS distribution. Another web site distributing DeCSS posted a restraining order it had received via e-mail, with the comment, "Note to all 'ye sharks out there: this site is located in Luxembourg. Hence I fail to understand how the rules and opinions of a Californian court (where the hell is that?!) would be relevant to this site or to me. In two words: Shove it."("DeCSS: watch your DVD's on your favorite OS")

The view that DeCSS distribution makes court decisions unenforceable is also widely reflected in discussions of the broader digital community[41]: a 1999 Slashdot discussion of one DeCSS distributor included comments like:

---

[39] The distributors of executable code are harder to track down, however, since their web pages so quickly disappear in the face of legal threats. See, for example, http://home.worldonline.dk/luke_s/

[40] The distributor notes that he was forced to remove DeCSS from his site after the MPAA contacted his Internet service provider. In spite of this, the author clearly believes that distribution has made the DeCSS unenforceable, writing, "If you are looking for DeCSS, be sure to check the DeCSS mirror list. I'm sure there are some sites up that are hosted on servers outside the reach of MPAA's lawyers."(Gadd)

[41] I use this term to distinguish between the "digital community" and the "Internet community." The digital community consists of the online community of Internet and technology professionals, experts, and enthusiasts. The Internet community is the much broader universe that includes all Internet users, many of whom have only limited interest in technology, and use the Internet strictly as a tool for pursuing other

> There's simply no way it can be stopped.
>
> Once the genies [sic] is out of the bottle it's very hard to put it back in.
>
> Well, it happened, The RIAA found out the hard way that you can't bolt the barn door once the Horse has run…The RIAA played rough, they found that netizens can get very rough indeed, and if they want any sympathy from me, Merriam-Webster comes to mind.
>
> Of course there's no way to stop this thing from being widely distributed, just like there is no way to prevent mp3 distribution or commercial software distribution. ("deCSS listed on Download.com" 1999)

The unenforceability of the DeCSS ban is thus widely cited, not only by source code distributors, but also by distributors of executable DeCSS code, and by the larger community. That such comments are common accompaniments to any DeCSS distribution page[42] shows that such distributions are aimed at nullifying court and policy decisions, and as such, meet the second criterion for recognizing policy circumvention.

Finally, we can see that DeCSS meets the third criterion for recognizing policy circumvention in its provision of non-excludable benefits. These include the benefits of raising awareness of the D.M.C.A. and other copyright laws, making it harder to crack down on violations of copyright laws, exposing flaws in DVD encryption technology, undermining public support for copy protection, and promoting awareness and use of open source software[43]. In addition, it provides the excludable benefit of allowing anyone who downloads or accesses the software to watch (or copy) DVDs on a Linux machine.

---

interests and relationships. Slashdot – self-titled as "News for Nerds" – is a major hub for the digital community.

[42] I am distinguishing here between web pages dedicated to DeCSS distribution, and DeCSS files made available on web sites dedicated to distributing pirated software, music, and movies (often known as warez sites). Warez sites are not typically political endeavors, but use the distribution of free software, etc. as the basis for selling advertising and/or pornography.

[43] The Linux operating system, for which DeCSS was designed, is the premiere example of open source software. "Open source" is software for which the source code is made publicly and freely available. This allows other programmers to inspect, improve, and extend the software, and usually allows the end

The DeCSS distribution phenomenon has raised awareness of the D.M.C.A. and other copyright laws by creating a wide range of web sites that draw attention to the problems with enforcing these laws, by precipitating a series of prosecutions under these laws, and by sparking discussion of copyright laws and their consequences. A Google search found more than forty thousand web pages referring to DeCSS in connection with the D.M.C.A. or other copyright issues.[44] There have been at least four court cases precipitated by DeCSS distributions; two in California, one in New York state, and one in Norway(Gross 2003a). A Usenet search for comments on DeCSS and copyright found more than four thousand postings to Internet discussion groups.[45] As previously discussed, many of the DeCSS distribution sites, as well as much online discussion, have drawn attention to the unenforceability of copyright laws in this instance.

DeCSS distribution has drawn attention to the technologies as well as the policies of copy protection. Many observers have noted that the CSS encryption scheme used to prevent DVD copying was relatively weak, since US export restrictions on encryption technologies prevented the industry from using anything stronger than 40-bit encryption.[46] CSS (the Content Scrambling System) has been variously described as

---

user to use the program free of charge. Open source has been praised as an accessible alternative to costly proprietary software (such as Windows), as more robust (because bugs can be identified and fixed more rapidly), and as more secure (because security holes can be identified and fixed).

[44] An April 9, 2003 Google search on *DeCSS (D.M.C.A. OR "intellectual property" OR copyright)* yielded 41,800 results.

[45] An April 9, 2003 search of Google's Groups archive on *DeCSS (D.M.C.A. OR "intellectual property" OR copyright)* yielded 4,060 results.

[46] The strength of different encryption schemes is represented by the number of bits in the encryption key; "[t]he bigger the number, the longer it takes for computer(s) to crack….It is computationally feasible to crack a 40 bit key. For this reason 40 bit encryption is rarely used."("SSL Certificate Encryption Strength" 2003)

"simplistic" (Stevenson 1999), "pathetically weak," (LuNaTiK) and "amazingly weak" (Simons 2000). The inherent weakness of the encryption scheme was compounded by the fact that one licensor of the DVD decryption technology failed to encrypt its key; this provided DeCSS developers with an easy way of cracking the system (Patrizio 1999). By drawing attention to DeCSS, and the encryption flaws that made it possible, DeCSS distribution undermines confidence in the technologies of copy protection.

Finally, DeCSS has served as the latest advertisement for open source software, open source development, and the Linux operating system. DeCSS was necessitated by the fact that Linux lacked a license agreement for the CSS encryption scheme, and "the very philosophy behind the Linux OS [made] it unlikely that such an agreement [would] be reached anytime soon." (Burke 2000) By drawing attention to DeCSS, and through it, to the Linux operating system, DeCSS distributors have expanded awareness of open source software. To many members of the digital community, increasing awareness (and ideally, use) of open source software represents a great leap forward from proprietary software. As one Linux developer writes,

> Open source is a disruptive technology. Disruptive technologies change our relationship to the world—how we travel, communicate, work. The railroad was a disruptive technology to the horse and buggy, the automobile to the railroad. Technologies that don't evolve, disappear. We believe the proprietary software development model is a horse and buggy whose time has come and gone….With open source software development, everybody collaborates, the best software wins. Not just within one company, but among an Internet-connected, worldwide community. ("What is Open Source")

Promoting open source software, exposing flaws in the technologies and policies of copyright protection, and increasing awareness of copyright issues are all non-excludable benefits of DeCSS distribution. These seem to be important benefits to DeCSS distributors, many of whom see copyright laws (as applied to source code) as

infringements of free speech rights. “I was outraged when I first read about the case, and I think I even downloaded the code "just because". Intellectual freedom, and the ability to record, store and transmit information are dear to me,” said one contributor (Sandberg 2003a). “I do believe that DeCSS in all its forms is ‘pure speech,’” said another. (Stevenson 2003) As one distributor described the film industry’s anti-DeCSS lawsuits,

> Say my house is burglarized, and afterwards, one of my neighbors puts up a sign saying "he has no locks on his windows." Yes, I'd conclude he's a asshole. I could say that he's encouraging crime, but he's not actually committing it. He's exercising free speech. And I'd be sure to put locks on my windows (and maybe put up a sign describing his diamond collection). It's not a perfect analogy, but it's a start.(Goldstein 2003)

We thus see that DeCSS distribution schemes meet all three criteria by which we recognize policy circumvention. They are a strategic political response to specific policy and court decisions, specifically, the D.M.C.A. and the court decisions restricting DeCSS distribution. They are attempts to nullify these policy and court decisions by rendering them unenforceable in the face of a flood of different distributions, many of them taking forms that use the shelter of protected speech. And they offer the non-excludable benefits of raising awareness of copyright issues, of flaws in copyright technology and policy, and of open source software. Finally, we can recognize it as a successful instance of policy circumvention because DeCSS remains widely available throughout the Internet.

Establishing that DeCSS is indeed a successful instance of policy circumvention is only the first step, however. The next challenge is to demonstrate that the three-variable model can indeed account for its success.

The first element – political entrepreneurs – clearly played a major role in the emergence of DeCSS distribution. Jon Johansen and other members of the Livid listserv (whose members were searching for a way to decrypt CSS) led the creation of the DeCSS

code. The large number of webmasters who immediately placed DeCSS on their sites got the code into distribution. By writing about the DeCSS phenomenon, and publishing the code, the editors of 2600 Magazine increased the profile and availability of DeCSS. By lending its legal services to the 2600 editors, and other DeCSS defendants, the Electronic Frontier Foundation ensured that the copyright and free speech issues around DeCSS received court, media, and public consideration. Dave Touretzky's Gallery of CSS Descramblers "helped to alert people to the issues raised in the 2600 case…. took some of the wind out of the MPAA's argument …[and] completely destroyed any hope of claiming that CSS is still a trade secret." (Touretzky 2003b) Contributors to the Gallery further muddied the distinction between source and executable code, and made it harder to distinguish between legitimate and illegitimate distributions. Together, these entrepreneurs made it possible for an inestimable number[47] of Internet users to download DeCSS code, despite legal efforts to suppress it.

DeCSS distribution also fits the second element of the model, in that the technical costs of a failed circumvention were and are very low. If a would-be DeCSS user downloaded a version of DeCSS that was incomplete or corrupted, she would simply be unable to watch a DVD on her computer; hardly a matter of life and death. If DeCSS distributors failed to make DeCSS widely available, the aggregate consequences would

[47] The extent and decentralization of DeCSS distribution makes it impossible to tally the number of DeCSS downloads or users. Based on the number of downloads reported by some mirrors, however (in the hundred per month) we can be confident that DeCSS users number in the tens if not hundreds of thousands. One web site reported 26,000 downloads in just five days(Harrison 2000); another small distributor reported a steadily growing pace of downloads from 300 per month in February 2002, to 800 per month as of April 2003.

likewise be minimal: Linux would simply remain a platform that did not support DVD playback.

Note that the costs of failure constitute a separate issue from the legal consequences of distributing the code. The purpose of DeCSS distribution is not to hide the identity of the distributor, but to make the code itself freely available. Indeed, many DeCSS distributors have made no attempt to hide their identities. The legal consequences that some DeCSS distributors have faced do not indicate a failed circumvention; if anything, they testify to the MPAA's perception that DeCSS distribution presents a meaningful threat to DVD encryption.

The low costs of failure have been crucial to the success of the DeCSS distribution phenomenon. Because the consequences of a failed distribution are minimal, anyone can participate in distributing the software. Creating an artistic source code distribution (as per the Gallery contributions) likewise presents no risk greater than leaving a line out of the code. Even the legal consequences of failure have been minimized: with so many DeCSS distributors in the game, the MPAA has been unable to prosecute more than a token handful. Most DeCSS distributors report no legal consequences greater than a "cease and desist" request, often filtered through an Internet service provider. Faced with only minimal costs of failure, many people have joined in distributing DeCSS, ensuring that the software remains widely available despite the legal crackdown.

Finally, DeCSS fits the third element the model: states have faced significant constraints on their efforts to crack down on DeCSS distribution. The two states that have been at the center of the storm – the United States and Norway – are both states with

strong liberal norms, reflected in both law and public opinion. These norms act as legal and political constraints, limiting the extent to which states can identify or prosecute DeCSS distributors.

One such constraint was the scope given to reverse engineering[48] under Norwegian law. The January 2003 acquittal of Jon Johansen specifically noted that Johansen's use of reverse engineering techniques "does not represent a violation of the penal code"("Jon Johansen Court Decision" 2003). Indeed, Norwegian copyright law "expressly permits reverse engineering of computer software."(Stevenson 2000) Reverse engineering has been framed as a freedom of expression issue, since it is sometimes "used by innovators to determine a product's structure in order to develop competing or interoperable products" and "is also an invaluable teaching tool used by researchers, academics and students in many disciplines, who reverse engineer technology to discover, and learn from, its structure and design".("Reverse Engineering") The freedom of information perspective on reverse engineering is reflected in the Norwegian copyright provisions pertaining to reverse engineering, which allows such action if "the information necessary to achieve interoperability has not previously been readily available."(Bing 2000) The liberal norms of freedom of information and freedom of expression are thus directly responsible for the reverse engineering provisions that limited the prosecution of Jon Johansen, and indeed, facilitated the creation of DeCSS in the first place.

The liberal commitment to freedom of expression also acted as a constraint on the repression of DeCSS distribution under American law. DeCSS distributors exploited the

---

[48] Reverse engineering "is taking apart an object to see how it works in order to duplicate or enhance the object." ("Reverse Engineering") Jon Johansen reverse engineered one element of the CSS system in the process of developing DeCSS.

particular protection afforded expressive speech in order to shelter some distributions of DeCSS source code. They then used the widespread availability of DeCSS source code to challenge the distinction between source and executable code, and to underline the difficulty in enforcing restrictions on DeCSS distribution.

By the time Judge Lewis Kaplan issued a ruling on DeCSS in the case of Universal Studios v. Eric Corley (the 2600 Magazine case), at least one US court had already ruled that source code was protected speech. In a case concerning the export of encryption software, the court ruled that

> Software relating to encryption is simply a topic of speech employed by some scientists involved in applied research. Hence, Snuffle [Bernstein's encryption program] is speech afforded the full protection of the First Amendment not because it enables encryption, but because it is itself speech. ("CDT Analysis of Berstein Decision" 1996)

In a different encryption case, the Sixth Circuit Court of Appeals had ruled that "computer source code, whether expressive or functional, is protected by the First Amendment."(Ghosh 2000) The Universal v. Corley ruling stuck a delicate balance between these positions, noting that "this Court assumes for purposes of this motion, although it does not decide, that even the executable code is sufficiently expressive to merit some constitutional protection. That, however, is only the beginning of the analysis."(Kaplan 2000)

The court noted that the DeCSS case demanded some balancing of the free speech principle, along the lines of the "fair use" provisions of copyright law.(Kaplan 2000) The challenge was thus to balance "the public interest in the restriction against the public interest in the kind of speech at issue." Because "DeCSS enabled anyone with even a basic understanding of computer programming to figure out a way around the protections on copyright-protected material…therefore, DeCSS was subject to greater

restrictions."(Morris 2000) In the words of the court, while "DeCSS has at least some expressive content, the expressive aspect appears to be minimal when compared to its functional component."(Kaplan 2000)

By arguing that the protected status of code depended on its expressive value, the court set the stage for the next stage of the DeCSS distribution effort: the Gallery of CSS Descramblers was developed to challenge this distinction. The entries in the Gallery are specifically designed to maximize the expressive value of the code, by embedding the code in recognized forms of expression like music and art. As Dave Touretzky writes in his introduction to the Gallery,

> If code that can be directly compiled and executed may be suppressed under the D.M.C.A., as Judge Kaplan asserts in his preliminary ruling, but a textual description of the same algorithm may not be suppressed, then where exactly should the line be drawn? This web site was created to explore this issue, and point out the absurdity of Judge Kaplan's position that source code can be legally differentiated from other forms of written expression. (Touretzky 2000b)

Because the US courts had acceded to the framing of DeCSS as a free speech issue, the Gallery (along with other forms of DeCSS distribution) collected many contributions from developers who saw the battle as a battle for speech rights. A student who included DeCSS code in his high school yearbook statement said that it "gave me an opportunity to talk to [other students] about the D.M.C.A., DeCSS, and code as speech."(Michaels-Ober 2003) The creator of an animation that embedded DeCSS code said he was motivated by the fact that "[i]ntellectual freedom, and the ability to record, store and transmit information are dear to me." (Sandberg 2003a) Another admitted that his musical contribution had "[a]esthetic value only. Many people had already adequately pointed out that deCSS and source code in general is really a form of speech. Anything beyond that is just for fun."(Schrepfer 2003)

As Touretsky's introduction to the Gallery pointed out, this playfulness had a serious purpose: to underline the difficulty, if not futility, of treating only some forms of software code as protected speech. The fact that US law and public opinion accords so much weight to freedom of expression created a major constraint on the suppression of DeCSS distribution. As long as even some forms of software code were acknowledged as protected speech (a point already conceded in law), the state would be heavily constrained in suppressing the distribution of DeCSS.

Finally, DeCSS distribution benefits from the difficulty the state has in identifying distributors. In the initial case brought by the DVD Copy Control Association (DVD-CCA) against DeCSS, the plaintiff listed five hundred unnamed defendants along with those it was able to identify[49]. As the complaint put it:

> DVD CCA is unaware of the true names and/or capacities of the defendants sued herein under the fictitious names Does 1-500, pursuant to Code of Civil Procedure Section 474, who each were responsible in some way for the acts and omissions complained of herein. DVD CCA will seek leave of court to amend the complaint to allege such names and capacities at such time as they are ascertained. ("DVD CCA Complaint in DVD CCA v. McLaughlin, Bunner, et al." 1999)

The inability to identify many of the DeCSS distributors obviously represented a major limitation in the ability to enforce policy and court decisions pertaining to DeCSS. This difficulty was partly a function of the many tools that Internet authors and users can adopt in order to remain anonymous. But the availability of those tools is itself a function of liberal protections, like freedom of speech, that are enshrined in the constitutions of many Internet-connected countries (Froomkin 1997). The only way of preventing anonymous participation in policy circumvention would thus be to eliminate liberal

---

[49] This case ultimately became three separate cases: Pavlovich v. DVD-CCA, DVD-CCA v. McLaughlin, Bunner, et al., and Universal City Studios et al. v. Eric Corley et al.

protections for anonymous speech, and to disconnect from the Internet (where other countries may still provide digital havens for anonymous activity). Since a liberal state like the United States is unable to take those measures, it is fundamentally constrained in its ability to identify, punish, or discourage anonymous participation in policy circumvention.

The recognition of reverse engineering as an issue of freedom of information, the framing of software code as a form of protected speech, and the inability to prosecute anonymous distributors all demonstrate the constraints that liberal norms impose on state efforts to repress policy circumvention. The case of DeCSS distribution is thus consistent with the third element of the predictive model.

Reviewing the case as a whole, DeCSS distribution appears to meet all the criteria for recognizing a successful policy circumvention. It is a strategic political response to particular policy and court decisions. It attempts to nullify these decisions by creating such a volume of DeCSS distributions that neither plaintiffs nor law enforcement can begin to stem the tide. In addition to offering DeCSS downloaders the excludable benefit of being able to watch DVDs on their Linux computers, it offers non-excludable benefits like raising awareness of copyright issues, of flaws in copyright technology and policy, and of open source software. We can see that DeCSS is not only a policy circumvention, but a successful one, because the software remains widely available online.

Furthermore, this success can be fully accounted for by the predictive model. We have political entrepreneurs, in this case the creators and distributors of DeCSS, who make it possible for many others to participate in the policy circumvention simply by downloading the DeCSS software. We have a policy area in which the costs of failure are

relatively low, in that the consequences amount to whether or not someone is able to watch a movie on his or her Linux-based computer. And finally, we have states that are severely constrained in repressing the policy circumvention, due to liberal norms that limit their law enforcement and prosecution capacity.

Policy circumvention: the case of Hacktivismo

Hacktivismo is a group created to "study ways and means of circumventing state sponsored censorship of the Internet and will implement technologies to challenge information rights violations."(Hacktivismo and Cult of the Dead Cow 2001) An offshoot of the Cult of the Dead Cow, a hacker group that "expanded the domain of hacking into the realm of the political" (Thomas 2002), Hacktivismo became its own group in 2001. Its members are drawn primarily from Canada, the US, and Germany but also reportedly include members in Israel, Korea, Taiwan, and China.

Hacktivismo was conceived by cDc member Oxblood Ruffin as a way to take on the large state-sponsored firewalls that limited access to the Internet in countries like Saudi Arabia, Cuba, Tunisia, and China. Firewalls

> act as intermediaries between users and the rest of the Internet. In countries where the Web is censored, the only way to access the Internet is through the firewalls. A user enters a URL - the address of a Web page - into his or her browser. This URL gets passed to the firewall, which checks to see if it is one of those banned by the government. If the URL is not on the list, the firewall forwards the request for the Web page and the contents of the page are relayed back to the user, who can then read it. If the URL is on the banned list the firewall refuses to forward the request and sends a page back to user indicating that the page he or she requested cannot be viewed by order of the government. ("About the Peekabooty Project")

Hacktivismo's first project, Peekabooty, was a software package that was intended to circumvent these firewalls. As Peekabooty's mission statement explains,

> Peekabooty is software that enables people inside countries where the Web is censored to bypass those censorship measures. The theory behind it is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web. …A user in a country that censors the Internet connects to the ad hoc network of computers running Peekabooty. A small number of randomly selected computers in the network retrieves the Web pages and relays them back to the user. As far the censoring firewall is concerned, the user is simply accessing some computer not on its "banned" list. The retrieved Web pages are encrypted using the de facto standard for secure transactions in order to prevent the firewall from examining the Web pages' contents. Since the encryption used is a secure transaction standard, it will look like an ordinary e-business transaction to the firewall. ("About the Peekabooty Project")

While Peekabooty has since spun off into its own entity, Hacktivismo has continued to create tools aimed at challenging Internet censorship. Its projects to date include Camera/Shy, a steganography program that "enables users to share censored information with their friends by hiding it in plain view as ordinary gif images" (Hacktivismo 2002); HESSLA ("The Hacktivismo Enhanced-Source Software License Agreement"), a legal framework that allows software developers to impose political terms of use on their users; and Six/Four, a peer-to-peer protocol for enabling censorship-free Internet traffic.

Hacktivismo meets each of the three criteria by which we define a policy circumvention. First, it is a strategic political response to policies of Internet censorship in at least twenty countries around the world (Reporters Without Borders 1999). Internet censorship has long been a motherhood issue for members of the digital community, spawning such efforts as the Electronic Frontier Foundation's Blue Ribbon campaign, in which web sites display a blue ribbon in support of free speech, and 1996's Black Thursday, when web sites turned their pages black to protest Bill Clinton's signing of the Communications Decency Act ("Why is this page black?" 1996). Internet censorship by authoritarian regimes has been a hacktivist target since at least 1998, when Bronc Buster,

a member of the Legions of the Underground, defaced China's official human rights web site on the day it was launched, leaving the message:

> China's people have no rights at all, never mind Human Rights. I really can't believe our government deals with them. They censor, murder, torture, maim, and do everything we take for granite [sic] left the earth with the middle ages….The Chinese communist government is made out of a gang of 100+ year old thugs and bullies who hide in seclusion. This pitiful effort of trying to change the hearts and minds of the world is a joke!("Crackers Attack China on Rights" 1998)

Bronc Buster later became one of the founding members of Hacktivismo, conceived by cDc "Foreign Minister" Oxblood Ruffin in the summer of 1999 ("The Hacktivismo FAQ v1.0"). Hacktivismo defined its mission as an explicit response to state policies of censorship:

> we DECLARE:
>
> THAT FULL RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS INCLUDES THE LIBERTY OF FAIR AND REASONABLE ACCESS TO INFORMATION, WHETHER BY SHORTWAVE RADIO, AIR MAIL, SIMPLE TELEPHONY, THE GLOBAL INTERNET, OR OTHER MEDIA.
>
> THAT WE RECOGNIZE THE RIGHT OF GOVERNMENTS TO FORBID THE PUBLICATION OF PROPERLY CATEGORIZED STATE SECRETS, CHILD PORNOGRAPHY, AND MATTERS RELATED TO PERSONAL PRIVACY AND PRIVILEGE, AMONG OTHER ACCEPTED RESTRICTIONS. BUT WE OPPOSE THE USE OF STATE POWER TO CONTROL ACCESS TO THE WORKS OF CRITICS, INTELLECTUALS, ARTISTS, OR RELIGIOUS FIGURES.
>
> THAT STATE SPONSORED CENSORSHIP OF THE INTERNET ERODES PEACEFUL AND CIVILIZED COEXISTENCE, AFFECTS THE EXERCISE OF DEMOCRACY, AND ENDANGERS THE SOCIOECONOMIC DEVELOPMENT OF NATIONS.
>
> THAT STATE-SPONSORED CENSORSHIP OF THE INTERNET IS A SERIOUS FORM OF ORGANIZED AND SYSTEMATIC VIOLENCE AGAINST CITIZENS, IS INTENDED TO GENERATE CONFUSION AND XENOPHOBIA, AND IS A REPREHENSIBLE VIOLATION OF TRUST. (Hacktivismo and Cult of the Dead Cow 2001)

If Hacktivismo was an explicit response to state policies of Internet censorship, it was equally clear about its intentions: to render those policies impotent and ineffective.

> We're hackers, not social justice activists. Let's put it this way. Some groups and individuals are well suited to fight for social and economic progress around the world. If

> as a result of an initiative in Africa, for instance, economic standards were raised and more people could obtain computers -- that would be a good thing. But what kind of Internet would they eventually have access to? One where censorship or the proliferation of vulnerable software left them at risk? We're not willing to sit by and watch that happen. We think of hacktivism and the Internet the same way that homeopathist's think of the body: you have to introduce a little poison to create health. Code has consciousness and healing power whether you like it or not…We are trying to intervene to reverse the tide of state-sponsored censorship of the Internet through the inventive use of code. This is what Oxblood is referring to when he uses the term "disruptive compliance". It's the opposite of "civil disobedience". We favor using disruptive technologies that comply with the spirit and original intent of the Internet. ("The Hacktivismo FAQ v1.0")

Finally, Hacktivismo meets our third criterion: the creation of non-excludable benefits. Indeed, Hacktivismo's mission is such that it primarily creates non-excludable benefits, since it makes its software and tools available not only to its participating coders but to all users of the Internet. In addition to these concrete benefits, Hacktivismo creates larger non-excludable benefits, like greater awareness of Internet censorship, and perhaps, inhibition in the development and maintenance of censorship technologies. While it creates some excludable benefits for members, like the social rewards and prestige of belonging to a high-profile hacker project, these are overshadowed by the non-excludable benefits that constitute its primary focus.

Hacktivismo is thus clearly an effort at policy circumvention: it is a strategic political response to censorship policies; it aims at nullifying the effects of censorship policies; and its primary benefits are non-excludable. But Hacktivismo can not be as clearly defined as a *successful* instance of policy circumvention. It has been bedeviled by internal conflicts, technical challenges and political constraints that have slowed its progress and limited its ability to effect policy circumvention (although it has had some notable successes in promoting policy change). These limitations largely stem from the ambitiousness and significance of the project: taking on the information controls of the

government of China is a much taller order than letting people watch a few DVDs. As a result, Hacktivismo's primary deliverables – the Six/Four system, and its cousin, Peekabooty – remain at the beta stage even after several years of development. The specific ways in which Hacktivismo has been held back, however, clearly support the three-variable model as an explanation for the relative success or failure of policy circumvention.

Hacktivismo certainly possesses the first element of the model: political entrepreneurs have played a major role in its efforts. Oxblood Ruffin[50], the self-styled "Foreign Minister" of the Cult of the Dead Cow, initially conceived of Hacktivismo in 1999, and has continued to drive much of its activities, and particularly, its public profile. At age 53, Ruffin's offline political experience remains relatively limited; he has only voted twice in his life, and has not attended a live political event since his one-time participation in a 1969 antiwar protest, when he was chased down the street after throwing a bucket of red paint. (Ruffin 2002) He worked in the United Nations community for about ten years, first in the media, and later as a political consultant on General Assembly affairs; but his political commitments are now strictly online. For Ruffin, hacktivism is necessarily about Internet freedom: "We're just trying to maintain as much Internet freedom as possible," he said in a September 2002 interview. "One person truly can make a difference. Body mass is not a requirement." (Ruffin 2002)

---

[50] While Ruffin uses his hacker "handle" or nickname in all his activities around cDc and Hacktivismo, and is referred to as "Oxblood Ruffin" in all coverage of Hacktivismo, his real name is essentially an open secret; his handle does not serve to disguise his identity or activities from legal authorities.

Nonetheless, Ruffin has been the nexus for recruiting more bodies to the Hacktivismo team. After founding Hacktivismo with the blessing of his fellow cDc members ("All this hacktivism stuff is cool," Ruffin was told by the cDc's leader, "but don't turn into Joan Baez." (Ruffin 2002)), Ruffin recruited Bronc Buster, known for his attacks on Chinese firewalls, to help in the project. Other early recruits included Mixter, a young German hacker best known for releasing a DDoS tool and related security report[51]; the Pull, who went on to create Hacktivsmo's Camera/Shy tool, and Drunken Master (a.k.a. Paul Baranowski), who became the lead programmer on Peekabooty. Later recruits were drawn from Ruffin's professional colleagues in Toronto, Mixter's hacking colleagues in various chapters of the Chaos Computer Clubs, and other connections forged online, bringing Hacktivismo's current membership to some forty members (Ruffin 2002).

Together, these members constitute a political elite that offers its programming, web design, and other skills to the creation of anti-censorship software tools. Much of its activities are modeled on programming practices in the open source community, in which programmers publish their source code so that others can improve or extend it. Working through a members-only e-mail list, in which all subscribers are expected to tangibly contribute to the work of Hacktivismo (Ruffin 2002), members are able to share their code-in-progress, and exchange ideas about strategy for both individual software tools

---

[51] A DDoS, or Distributed Denial-of-Service attack, is one of the most common methods used for attacking and paralyzing Internet servers. After a large-scale DoS attack in February 2000, Mixter's DDoS tool was briefly suspected of being the tool of the attack. In fact, another tool was used; and as Mixter takes pains to point out, his tool and white paper were released "according to full disclosure security policy", in which hackers publicly release security exploits in order to draw attention to key weaknesses that need to be repaired.(Mixter 2002a)

and the overall project. This working group of entrepreneurs, who are volunteering their own time, effort and knowledge in order to create software for use by a much wider audience, is the core of Hacktivismo's efforts.

Nor are their entrepreneurial efforts limited to software development. Different members bring different skills to the table, such that even non-programmers can be active participants in the project. Ca$h Money worked on the design of the Hacktivismo web site, and maintains its news feeds. (Money 2002) Mr. Happy's role is to maintain the web site, including writing content. (Happy 2002) Oxblood Ruffin admits that he's "not what you'd call a hard-core hacker," but plays a major role "at the strategic level," (Ruffin 2002) using his media skills to commandeer extensive press attention for Hacktivismo's activities. "Everyone's respected for what you do," according to Ca$h Money. "You are respected for how much work you do. What you contribute equals your status or prestige."

Many of Hacktivismo's participants seem drawn to the entrepreneurial role by the belief that here – as compared with offline politics – they can make a difference. "I don't think demonstrations can make a change. You make a change by making something productive….It's more important to have a goal and achieve that goal." (Mixter 2002b) Similarly, metac0m likes the idea that Hacktivismo "produces something tangible, rather than just protest. Something people can use." (metac0m 2002) "I like to concentrate on things that change something," said Jules (Jules 2002). Ca$h Money had a more modest notion of his contribution, comparing himself to the NASA janitor who, when asked what his job is, says it's to send a man to the moon: "I'm not changing the world," he said. "I am contributing in however small a way." (Money 2002)

If Hacktivismo has succeeded in building the corps of political entrepreneurs necessary for policy circumvention, it also illustrates that political entrepreneurs are not sufficient to ensure that circumvention's success. When we come to the second element, the need for low costs of failure, Hacktivismo is crucially lacking. Far from facing low costs of technical failure, the costs of a technical failure by Hacktivismo's tools may be very high indeed. In the words of one of Hacktivismo's early participants, "you need to create plausible deniability" for Hacktivismo users, because in some countries (like China) it is illegal even to request censored content (Baranowski 2002); that means that the software must not only make it possible to access banned content, but to disguise any trace of both the request and the software used to make it. If the software leaves a trail, the user could end up under arrest, or even executed.

These high costs of failure in turn impose a very significant burden on Hacktivismo's programmers, particularly considering that none of them are paid for their Hacktivismo work, Developing code that is robust enough to resist failure is a tall order – one that takes many hours of programming to fill. How those hours are divided up among an all-volunteer work force became a source of contention, and one that has proven very divisive among Hacktivismo volunteers.

Hacktivismo's first undertaking, Peekabooty, split off into its own project after a dispute over relative contributions to the effort. "For one and a half years I did all the work and he got all the credit," Baranowski said of Ruffin. Other Hacktivismo members had a different perspective on Baranowski's role within the project. Ca$h Money criticized Baranowski's attitude as "my way or the highway," and suggested that he was unused to working with an open source model.(Money 2002) Mr. Happy attributed the

break-up to “matters of ego and recognition” and said it had “nothing to do with coding.”(Happy 2002) Ruffin offers his own typically colorful account of the dispute:

> Hacktivismo progressed as a group but encountered a serious hiccup when the lead developer for Peekabooty rewrote the entire code base and decided [to] hijack the project and leave the group. It's amazing what some people will do when they figure they aren't getting enough press. When it was first announced on our listserv there were several days of chaos and rage. Some members wanted to crucify our little fame seeker, but it seemed best to let him go. He had been a disruptive force in Hacktivismo for months and things weren't getting any better. Plus when his code was reviewed it left our security experts dumbfounded. Peekabooty had been rewritten to conform to design specs that been rejected a year before as grossly insecure. You could hear the baby Jesus crying in Shanghai. (Ruffin 2004b)

In this he says-he says dispute, there is no arguing that a demanding coding project is vulnerable to disputes over relative contributions, as members disagree over different styles of coding, and to the value of coding versus other kinds of effort.

It is also clear that these internal disputes, and the ultimate Peekabooty split, have slowed down Hacktivismo’s progress in delivering usable software. “The last year and a half have gone slowly due to Peekabooty,” (Mixter 2002b) said Mixter, the primary coder on Hacktivismo’s Six/Four project. Four years after Hacktivismo was first announced, Peekabooty has only released a developer version[52] of its program; Hacktivismo’s new Peekabooty competitor, the Six/Four tool, has likewise only had a developer release.

Internal disagreements have only been part of the slow-down, however. Another obstacle in Hacktivismo’s development has been the legal hurdles that must be surmounted by software that challenges government authority. The release of the Six/Four developer version was delayed by US government restrictions on encryption

---

[52] A developer release is like a sneak preview of as-yet-unfinished software, intended for other programmers rather than for end users. By releasing a developer version open source software projects can engage other programmers in finding bugs, weaknesses, or areas for improvement, and allow other programmers to begin developing related software that will complement the program once it is released.

technology exports, which had to be negotiated before the software's release. (Mixter 2002b; Ruffin 2003) But encryption technology is not something that a project like Six/Four could easily forego. Precisely because of the high costs of failure, Six/Four needs to use very strong encryption technology in order to protect the identities of its users; and the export of strong encryption is regulated by the US government.

The high costs of failure have thus imposed two significant burdens on the Hacktivismo project. First, by imposing a rigorous standard of quality on the software code, it demands a significant commitment of time by Hacktivismo's programmers. As an all-volunteer project, Hacktivismo is vulnerable to disputes over how that time commitment in shared. Second, by requiring strong encryption to protect users' identities, it subjects Hacktivismo software to US government export regulations. Together, these obstacles have significantly slowed Hacktivismo's progress – although progress is still visible. But this is a game in which pacing matters: as Ruffin himself acknowledges, it is just a matter of time before government authorities figure out how to crack any code that programmers develop to protect people from Internet censorship.(Ruffin 2003) The more slowly Hacktivismo proceeds, the more quickly its target governments catch up.

If Hacktivismo has been slowed by facing high costs of failure, then those costs can be directly attributed to the lack of constraints on Hacktivismo's target governments. As the third variable in our model would predict, tackling non-liberal governments is a much tougher proposition for sponsors of policy circumvention. In the case of Hacktivismo, coders are taking on governments that face negligible political constraints on their ability to identify participants in policy circumvention, or to punish people for using circumvention software. By definition, any country that Hacktivismo targets – any

country that censors the Internet – has a government that is willing to use heavy-handed tactics in controlling information and information technologies.

International observers have amply documented the authoritarian tactics used to control Internet users in censoring regimes. A 2002 Amnesty International report on Chinese control of the Internet documented " prisoners of conscience who have been detained for using the Internet to circulate or download information."("State Control of the Internet in China" 2002) Those who are arrested are not necessarily radical challengers; "many have merely voided a politically sensitive opinion online." (Kalathil and Boas 2003) Online activities have become a central focus and weapon for Chinese state security:

> during searches of any political suspects' home or office, the first thing Chinese security agents seize these days is the computer, hoping to find on the hard drive incriminating evidence such as incoming or outgoing e-mail messages to co-conspirators…..It should also be noted that the authorities appear willing to charge dissidents with 'subversive' uses of the Internet that are inherently nonpolitical in nature, primarily as a tactic to silence them or smear their character…..The authorities searched [dissident writer Wang Yiliang's] home and found pictures of nude women downloaded from the Internet on his computer, which they subsequently used to sentence him to two years of reeducation through labor for 'possessing pornographic articles.'(Chase and Mulvenon 2002)

Using policy circumvention to challenge non-liberal regimes is thus much riskier than using policy circumvention to evade the policies or laws of politically constrained, liberal governments. While policy circumvention efforts may nonetheless emerge under these regimes, as in the case of Hacktivismo, they will be much less likely to succeed in nullifying their target policies.

The case of Hacktivismo shows how policy circumvention may fail, even when political entrepreneurs sponsor its emergence. Hacktivismo has a substantial and dedicated team of entrepreneurs, who together have fostered an ambitious program of

policy circumvention, but its efforts have often been stymied by the combination of high costs of failure and negligible constraints on repression. Despite almost four years of hard work, the project has yet to release end user software[53] that would fulfill its core mission: allowing Internet users in countries that censor the Internet to access the full range of online information and sites.

While Hacktivismo has yet to succeed in sponsoring policy circumvention, however, it has achieved some influence on policy change. Since the emergence of Hacktivismo, the US Congress has begun to consider legislation that would create an "Office of Global Internet Freedom", mandated to "develop and deploy technologies to defeat Internet jamming and censorship."("To develop and deploy technologies to defeat Internet jamming and censorship. 2003) The Congressional Committee considering the bill has contacted Hacktivismo as possible expert witnesses on the project.(metac0m 2002) The International Broadcasting Bureau, which runs the Voice of America, has already commissioned software that would allow people to tunnel through firewalls in Internet-censoring regimes (Festa 2003).

These developments suggest that Hacktivismo's goal, to enable circumvention of Internet censorship, may yet be achieved. But the history of the Hacktivsmo project itself strongly vindicates a model that posits political entrepreneurs, costs of failure and political constraints as crucial ingredients in the success of any given circumvention effort.

---

[53] The currently released version of Six/Four is a developers release.

Conclusion

The cases of DeCSS distribution and Hacktivismo support several facets of the policy circumvention argument. First, they establish that policy circumvention is a distinct and recognizable phenomenon, characterized by the three criteria I have identified: it is a strategic political response to a specific policy, law, regulation or court decision; it focuses on nullifying the effect of a policy, law, regulation or court decision; and it offers at least some non-excludable benefits. Second, these cases support the three-variable model as a predictor of the emergence and relative success of policy circumvention efforts. In both cases, political entrepreneurs played a major role in the emergence of the policy circumvention challenge; but where DeCSS distribution faced low costs of failure, and liberal states constrained in their ability to repress the challenge, Hacktivismo faced the opposite situation. As a result, DeCSS distribution has thrived, while Hacktivismo so far remains stalled at the starting gates.

Most important, however, is that both cases support the larger claim made at the start of this chapter: that policy circumvention, as much as policy change, poses a significant transnational challenge to the authority of the nation-state. In the case of DeCSS, a scrap of code that began its life in Germany and Norway was able to thwart the intellectual property rights of US-based companies, and US law was unable to stem the challenge. In the case of Hacktivismo, a coalition of hackers based primarily in Canada, Germany, and the US has launched a campaign that, while not yet successful in defeating Chinese firewalls, has added to international pressure against censorship practices in China and elsewhere. Together, these cases support the claim made earlier in this chapter: that policy circumvention is itself a major pressure on state autonomy, and one

that must be comprehended by research into the transnational pressures on the nation-state.

These cases also support my other two arguments about the theoretical significance of the policy circumvention phenomenon. First, policy circumvention is itself an additional pressure for policy change. In the case of DeCSS distribution, policy circumvention drew widespread attention to issues around intellectual property law in the digital era, and to the Digital Millennium Copyright Act in particular. While the D.M.C.A. was already law by the time the DeCSS phenomenon emerged, its interpretation in the case of Universal Studios et al. vs. Eric Corley et al. lent fresh credence to the arguments that were earlier voiced by D.M.C.A. opponents. In the ongoing struggle over digital-era revisions to intellectual property laws, the DeCSS case stands as a prominent example of what is at stake in those revisions, and of the difficulty in enforcing their provisions.

Hacktivismo has played an even larger role in promoting debate over Internet censorship. While it has had only limited effectiveness in circumventing firewalls, Hacktivismo has been remarkably effective in drawing attention to the firewall issue. The US government has launched its own Hacktivismo-like initiatives against Internet censorship; and each successive announcement of impending Hacktivismo software draws a major wave of media coverage on the issue of Internet filtering and censorship. While policy change is not the explicit focus of either Hacktivismo or DeCSS, it is nonetheless a potential by-product.

Finally, DeCSS and Hacktivismo illustrate the way in which policy circumvention changes norms about policy compliance. In the case of DeCSS, that takes the form of

widespread law-breaking by individual users of DeCSS, whose contravention of copy protection has been normalized by the widespread availability of contravention tools. In the case of Hacktivismo, the shift in norms is even more institutionalized: the fact that the US government is now adopting Hacktivismo-like tools suggests that even governments may be susceptible to the lure of policy circumvention as a tool of international diplomacy. Rather than pressuring China, Cuba, and other regimes to eliminate their censorship practices, the US will simply throw its resources behind making that censorship ineffective. State-sanctioned policy circumvention represents a significant shift in the norm of respect for the internal jurisdiction of one's fellow nation-states.

Alongside these theoretical issues, the phenomenon of hacktivist policy circumvention raises some crucial problems for policy makers. The first is that in an information economy, policy circumvention will be an expanding sphere of political activity. The domains that are most vulnerable to policy circumvention are domains that are dependent on information: information distribution, and information control. In an information age, more and more economic and social activity unfolds in these domains. That means that more and more of the state's activity, and its policy responsibilities, will unfold in domains that are vulnerable to policy circumvention by hacktivists.

This leads to a second implication for policy-makers: policies must be robust in the face of measurable defection. Policy is about setting rules that *most* people will follow. But policy-makers cannot ensure total compliance – particularly when it comes to policies that affect, or depend on, digital technologies. We can expect that a sizable chunk of the population will have the technological means to "defect" from many policies pertaining to the digital realm; how big a chunk depends on both the risks

associated with defection, and the state's ability to use heavy-handed enforcement. Any digital policy has to be robust in the face of non-compliance; if its fundamental justice or utility would be compromised by a measurable rate of non-compliance – whether 5%, 10%, or 20 – then it's not viable.

Finally, we should note that the threat of policy circumvention is not just a political threat – it's an economic one. States and corporations are partners in the causes and consequences of hacktivist policy circumvention. In the digital era, the infrastructure for policy enforcement is often digital – and the creators of that infrastructure are generally private companies. That makes state security inseparable from corporate security; the ability to enforce policy compliance extends only to the extent that your technology is hack-proof. This creates a complicated relationship of policy interdependence among countries: consider, for example, the fact that China's firewalls – the infrastructure for its information controls, and the target of much hacktivism – run on routers from US-based Cisco. The US is thus in the paradoxical position of fostering technology exports, on the one hand, and fostering circumvention of that technology on the other.

The other side of this coin is that corporations cannot insulate themselves by or from state policy. A court ruling provides no protection from the challenge of hacktivism. So a corporation like Lufthansa may find its web site under attack, as a proxy for a broader challenge to German deportation policy.

Or a company like eToys could find that a court ruling is far from the last word. Etoys certainly learned that policy circumvention can be a powerful counterweight to

state authority. Despite its favorable court ruling, eToys filed for bankruptcy two years ago(Shabelman 2002)[54]. etoy is right where it was: live and online.

[54] The eToys web store has since re-opened, as a division of KB Toys, which purchased the online assets of eToys after its bankruptcy.

Chapter 5

Hacktivism and the Future of Democratic Discourse

Introduction

Can the Internet serve as a new public sphere, a home to democratic discourse? This question frames much of the contemporary research on the prospects for electronic democracy.[55] It captures the widespread hope that online communications can help correct some of the recent injuries to democratic vitality, attributed variously to factors like television(Putnam 2000), excessive emphasis on scientific expertise (Fischer 2001), and the rise in "lifestyle politics" (Bennett 1998).

These aspirations are premised on our ability to create a virtual version of democratic deliberation. That deliberation is sometimes described in terms of a democratic agora, a town hall, a public sphere, or a commons. All of these models share a vision of deliberation in which diverse citizens congregate in order to exchange ideas, discuss issues and perhaps arrive at decisions.

Hacktivism raises a number of challenges for visions of online civic deliberation. In the broadest terms, it draws our attention to the fact that the Internet's political impact may not be neatly contained by tidily structured participatory opportunities. But it also raises more particular challenges to a number of the specific issues surrounding deliberative democracy.

---

[55] See for example, (Dahlberg 2001), (Wilhelm 2000),(Malina 1999).

This chapter will examine two of these challenges: the challenges to deliberative concepts of free speech and accountability. Each of these concepts is to some degree contested, with different deliberative theorists arguing for different formulations. Yet hacktivism challenges the very terms of debate on each issue, encouraging us to reformulate each concept for the purposes of envisioning online deliberation.

Before approaching each of these challenges in turn, I begin with a brief discussion of the notion of online deliberation as others have formulated it. I then use my taxonomy of hacktivism to address each of these problems, demonstrating how the divisions among hacktivists translate into larger problems for conceptualizations of online deliberative discourse. I conclude by suggesting that the problems raised by hacktivism are symptomatic of larger phenomena in the online world, demanding a more fundamental review of our vision for online deliberative discourse.

Envisioning digital deliberation

Much of the debate over the Internet's potential as a home for democratic discourse has been framed by the theories of Jürgen Habermas. Habermas's account of the deterioration of democratic discourse is closely linked to the expansion and deterioration of the public sphere, due in part to the evolution of mass media (Chambers 2000). As a new type of media, the Internet thus presents fresh possibilities for the re-invigoration of that public sphere:

> The age of the public sphere as face-to-face talk is clearly over: the question of democracy must henceforth take into account new forms of electronically mediated discourse. What are the conditions of democratic speech in the mode of information? What kind of "subject" speaks or writes or communicates in these conditions? (Poster 1995)

The Internet's potential for realizing Habermas's vision of deliberative democracy lies in its sheer communicative capacity. As Froomkin frames it, "the Internet draws power back into the public sphere, away from other systems…Could it be that emerging technologies will enable new types of Internet-based discourses that generate the "communicative power" Habermas argues is needed to educate and mobilize citizens to demand that their governments make better and more legitimate decisions?" (Froomkin 2004) Similarly, Thornton argues that

> the Internet does allow people who are taking part to share a basis of understanding as common ground from which to mediate consensus. The Internet allows people to contribute to modifying systems (in the Habermasian sense), using communicative action (Thornton 2002, citing Lamber 1995.)

These authors draw attention to the parallels between the conditions for democratic discourse outlined by Habermas, and the potential conditions of online deliberation. Habermas's vision for deliberative democracy is fundamentally communicative, resting on a notion of deliberation as a perpetual conversation among citizens. The purpose of this conversation is "to generate a 'rationally motivated consensus' on controversial claims."(Benhabib 1986) Habermas specifies the conditions of the "ideal speech situation" necessary to enable this kind of conversation:

1. Participation in such deliberation is governed by the norms of equality and symmetry; all have the same chance to initiate speech acts, to question, interrogate, and to open debate;
2. All have the right to question the assigned topics of conversation;
3. All have the right to initiate reflexive arguments about the very rules of the discourse procedure and the way in which they are applied or carried out. There are no prima facie rules limiting the agenda or the conversation, nor the identity of the participants, as long as each excluded person or group can justifiably show that they are relevantly affected by the proposed norm under question (Mouffe 1999, citing Benhabib 1996.)

Dahlberg discerns the characteristics of the ideal situation in his study of Minnesota E-Democracy, a prominent example of online citizen-to-citizen political debate. Dahlberg describes Minnesota E-Democracy as a successful example of structuring online dialogue "to stimulate reflexivity, foster respectful listening and participant commitment to ongoing dialogue, achieve open and honest exchange, provide equal opportunity for all voices to be heard, and maximize autonomy from state and corporate interests."(Dahlberg 2001)

Despite the theoretical congruity between Habermas's ideal speech situation, and some of the apparent characteristics of online dialogue, there are concerns about whether theory can translate into practice. Dahlberg himself qualifies the longer-term prospects of Minnesota E-Democracy, which he believes "may largely be following the course of what Habermas described as the bourgeois public sphere, a narrowly defined rational-critical public increasingly marginalized by the commercialization of the medium and by more populist forms of political participation."(Dahlberg 2001) Streck raises similar concerns about the WELL, a widely-praised online community that he describes as "a computer-based instance of Jürgen Habermas's bourgeois public sphere, in which the educated and affluent come together outside both home and state for critical discussion of art, literature and politics (Streck 1998).

While Habermas thus provides some useful frameworks for considering the challenge of online deliberation, his work is by no means the solution to questions about how the Internet could house democratic deliberation. Perhaps for that reason, some authors have attempted to go beyond Habermasian models, or to use Habermas's work more loosely in their examinations of online discourse. Hale et al. are among those who

draw on Barber's notion of "strong democracy" to consider possibilities for "more thoughtful, civic-minded and deliberative patterns of communication."(Hale, Musso, and Weare 1999) Coleman and Gøtze frame their examination of policy deliberation with Dewey's vision of "improvement of the methods and conditions of debate, discussion, and persuasion". (Coleman and Gøtze 2001) Witschge (Witschge 2004) synthesizes a range of deliberation theorists (including Dryzek, Bohman, and Cohen) in order to formulate the requirements for online deliberation as "equality in participation, discursive equality, and following from this, diversity of viewpoints and arguments."(Witschge 2004)

Both the Habermasian and non-Habermasian variants share some common preoccupations, however. Each assumes that some sort of free speech principle must be in operation – although the boundaries of legitimate speech may be conceived differently. Each also addresses the problem of anonymity, although there are significant differences as to whether it is seen as constructive or destructive to democratic discourse. The taxonomy of hacktivism introduced earlier (see Chapter 2) helps us understand the internal hacktivist divisions on key questions of free speech and accountability. Both issues are hotly debated in the hacktivist community – as well as among deliberative democrats.

The problem of free speech

Free speech is essential to any model of democratic discourse. Cohen (1998) usefully summarizes the arguments that have been made for the importance of freedom of political expression in a democracy:

1. Democracy is based on the principle of popular sovereignty, which demands "free and open discussion among citizens";

2. Restricting speech creates political inequality between those whose speech is allowed, and those whose speech is restricted;

3. Restricting speech impedes the free flow of information, "perhaps reducing the quality of democratic discussion and decision", and

4. Restricting speech limits the range of ideas or opinions in a political discussion. (Cohen 1998)

As Cohen himself points out, freedom of speech is even more crucial to deliberative democracy. For this reason protection must extend beyond specifically political speech to encompass the full range of "conscientious expression" (Cohen 1998) Some even argue that the very purpose of free speech is "to ensure that it is possible for people to engage in the discussion and deliberation necessary for the successful use of democratic institutions." (Nickel 2000)

But the Internet may make protecting free speech more difficult and more complicated, as the case of hacktivism suggests. Many forms of hacktivism – most notably web site defacements and virtual sit-ins – involve jamming or altering someone else's speech. Web site defacements replace one online message with another. Virtual sit-ins temporarily silence (or muffle) a message as a way of drawing attention to another. Are these actions forms of free speech, or a rebuke to it?

Political coders argue that freedom of speech is absolute, and that any form of hacktivism that interferes with the publishing rights of its target – such as defacements or virtual sit-ins – is thus illegitimate. They argue that freedom of speech is what hacktivism is all about:

> I think hacktivism should be about delivering a message, just like good old grass roots activism. It shouldn't be about doing damage to someone else network, or taking away their right to express their views. We just want to make a fuss so people will pay attention to what the message is we wish to deliver."(27-Aug-99)

Or as Hacktivismo leader Oxblood Ruffin puts it, "don't try to deny anyone the right of speech or the right of publishing" (Ruffin 2002).

This reflects the view, widespread among political coders as well as many other members of the hacker scene, that online freedoms – especially freedom of speech – are core values of Internet culture. Said one coder: "The internet is a free society. No content has ever been successfully banned from the internet." (Eisley 2003) His view is echoed by the comment of a coder who writes that "[f]reedom on the Internet, probably the only medium where censorship and monitoring can be circumvented, is very important." (Prasad 2002) Among the political coders I interviewed, only one took exception to the orthodox position on freedom of speech, saying that "I didn't want to take part in this debate [over code as speech] because the meaning of 'free speech' has a very different (and perverted, in my opinion) meaning in the U.S.A than in European countries." (Hocevar 2003)

The hacker culture's emphasis on freedom of speech leads political coders to put much of their energies into protecting freedom of speech online. The Hacktivismo/Peekabooty projects focus on extending online free speech protections to jurisdictions that have limited speech rights. The DeCSS projects, too, represent a

commitment to free speech rights for code – consistent with coders' view of software as a form of speech. "I believe that code does have consciousness," says Oxblood Ruffin. "Cindy Cohn [a lawyer for the Electronic Frontier Foundation, and a Hacktivismo advisor] has established that code is speech." (Ruffin 2002)

The view that software code is protected speech has spurred much of the activity of DeCSS activists. Dave Touretzky, the founder of the Gallery of CSS Descramblers, wrote that "I was determined to show these movie industry types that it was a BAD IDEA to try to use trade secret law to interfere with free speech." (Touretzky 2003a) He is echoed by the coder who wrote that "It's also important to get every computer professional to understand that this [DeCSS] is a case of freedom of speech." ("Jon Johansen's Answers to Your DeCSS Questions" 2000) As another contributor to the gallery put it:

> I believe that programming code deserves protection under the First Amendment to the United States Constitution and, more generally, that censorship does not benefit society. Publishing a portion of DeCSS in my high school yearbook was a way to ensure that attempts to censor this speech would fail. (Michaels-Ober 2003)

The political coders' emphasis on freedom of speech fits comfortably with utopian visions of the Internet as a forum for unfettered, truly free speech. Their argument for a natural consonance between Internet culture and free speech, resting on the technical difficulty of online censorship, promotes the deliberative democrats' aspirations for democratic discourse online. In this view, the Internet is not only a welcoming forum for the free exchange of views, but it has its own class of warriors dedicated to protecting free speech online.

This sunny picture of the Internet as a natural home to free speech is countered by other members of the hacktivist scene. In sharp contrast to political coders, performative

hacktivists and political crackers argue that freedom of speech is illusory, relative, and less important than political outcomes. Each of these arguments surfaces repeatedly in the writings and comments of performative hacktivists, political crackers and their supporters.

The argument that online freedom of speech is illusory takes several forms. "Arguably," one hacktivist writes, "you cannot effectively implement your right to free speech without stepping on the toes of another....hence, politically motivated hacking."(Me Uh K. 1999) A harder line view is expressed by the electrohippies, who write that

> any claim that you have 'rights' of expression online is clearly wrong. You have only what your service provider gives you. Beyond that, you'd have to challenge them under contract law through the courts - and you'll more than likely lose because in this arena it's contract law that has the primary weight, not civil rights law. (electrohippies 2003)

Other hacktivists seem to hold more respect for the notion of free speech, yet still defend actions that seem to infringe on the speaking rights of others. These are often justified on the grounds that speaking rights are relative, and that inequalities of communications access mean that some have more speech than others. Defacements and sit-ins thus level the playing field. In this view, hacking does not constitute a meaningful assault on speech rights, because

> People who have web sites up can spew whatever it is they want to say 24/7/365. If someone were to change the contents of a web site, and it remained changed for a few hours, how have they _REALLY_ infringed on their freedom of speech? (Buster 1999)

Or as another hacktivist put it, somewhat more dogmatically:

> This 'free flow of information' crap pisses me off. Fascists are fascists, you have to take the fight right up to their faces, to let them KNOW they are irresolutely opposed by members of society and they will not gain power without the cost of CIVIL WAR. fuck it, lets be realistic about who they ARE, what they stand FOR, and what METHODS fascists will use to achieve POWER....LIES and MISINFORMATION are not 'free speech' anyway. (scotartt 1999)

This argument has been used to justify a range of hacktivist projects, most often virtual sit-ins. Writing about the toywar project, one hacktivist observer asks:

> How is the little guy is supposed to fight an injustice against Goliath? A few artists taking on a multibillion dollar dot-com giant doesn't seem like much of a fight. As an example, in order to protect its name, etoy has had to fight eToys in a Los Angeles court. (Dugan 2000)

Similarly, another hacktivist writes:

> Which law are hacktivists to adhere to anyway, when they are trying to support an oppressed group of indigenous peoples in another country? Isn't the law one of the prime obstacles in any activists path? Isn't activism always a way of challenging institutionalised power without going through accepted channels? (xdaydreamx 1999)

Concerns about differences in substantive speaking rights lead to arguments suggesting that the ends justify the means – where the means is performative hacktivism or political cracking. As one member of the hacktivism.ca listserv writes, "[i]f governments are killing people, it seems that almost any action can be morally justified."(Jones 1999a) The ends over means perspective is also reflected in the comment of one of the electrohippies that

> I don't have a problem with this [information theft] where it's done for the purposes of a public campaign. Information theft to support fraud, or some other activity like targeting people for abuse or violence, I don't agree with. (Mobbs 2003)

And in the world of political cracking, the ends-over-means argument is also used as justification for web site defacements:

> We would call ourselves as people who're trying to make a difference and showing the true faces of the countries like Israel, India or any other country doing unjustice. We don't mind what people call us, our work speaks for itself.(m0r0n and nightman 2002)

> i dont have any intention to flame or hurt anyone..if anyone of you get hurt or feel insulted then i am sorry..I dont want to write too much but i will sure use the biggest medium to voice my opinion because its my right and ive been doing this for long. ... This defacing for a cause is to show the people what is going "behind the scenes"..and to make them know about the "real facts" of the respective casue.... I cant go and fight for

> all the nations suffering, but i can do something to make the world know about the injustice going around. Defacing a websites will cost nothing to the target.(Nuker 1999a)

Among performative hacktivists, the ends-over-means argument is explicitly juxtaposed with the hacker/coder preoccupation with protecting the flow of information online. For example, Ricardo Dominguez describes the reaction to one of his virtual sit-ins:

> as we were about to start the action, we were surrounded by a group of hackers called Hart. Dutch hackers. And they said, Ricardo, Stefan, what you're about to do will destroy infrastructure. And if you guys do it, we will take you down. It was our first encounter with what I call the "digitally correct" community. Those who believe that bandwidth is above human lives. (Dominguez 2002a)

Political coders greet this argument with great skepticism, treating the "level playing field" and "ends over means" claims as direct challenges to the hacker emphasis on freedom of speech. Critiquing a virtual sit-in campaign, one political coder wrote that

> I think Electrohippies should just come out and say, "We are not for free speech".Why else allude to it in these kinds of statements? Why admit you are doing Distributed Denial of Service attacks, admit that you are using these attacks to censor, and not just come out and admit you are pro-censorship? (thepull 2002)

The view that virtual sit-ins and other performative techniques are a direct assault on online freedom of speech is widespread among political coders, who worry that such techniques could damage the health of the Internet itself. Writes one hacktivist, "personally, I am against dos attacks even for activism purposes…its counter to the way the net was designed to be used."(sam) Another coder writes that

> I have never participated in any DOS activities, nor will I. DOS attacks almost always have innocent, unintended victims in addition to the intended. I once worked at a small ISP which hosted several customers who drew DOS attacks. The attacks took the entire ISP offline, affecting not only the intended victim but many others as well.

Some argue that performative hacktivist techniques like the virtual sit-in take the hack out of hacktivism:

> I've never found one of these [virtual sit-ins] to be beneficial. I always thought hackers were supposed to free information flow and spread data, not clog up the lines and shut people down.(Eisley 2003)

Not all hacktivists divide neatly on the issue of free speech versus creative action. Some hacktivists struggle with the question of whether certain hacktivist techniques represent intolerable assaults on the Internet and its free speech culture, or whether they are reasonable tactics for action on the part of disadvantaged groups. "I can't take a hard line on the DoS issue," metac0m said. "It's turning tables for a brief period. I'll give them publicity, but I won't organize them."(metac0m 2002) Similarly, another hacktivist said

> I have never taken part in such actions [redirects, defacements, DoS, information theft, or sit-ins]. I have been thinking of it a couple of times, and just could not decide whether it was right or not. For instance when I read about the Nike redirection I thought "haha, in their faces!", but I also thought "hey, that was illegal". Maybe most people do not care, but for me it's a very complex moral and philosophical issue. Will the effects be more important if more risks are taken? Does the righteousness of the political message make it "less" illegal? I just cannot decide yet, so I stick to more secure actions. (Hocevar 2003)

The hacktivist debate over free speech versus tactical effectiveness is an interesting one for deliberative democrats. Whereas much of the discussion over the bounds of legitimate speech focuses on freedom of expression,[56] the hacktivist problem does not derive from limitations on the ability to speak. After all, any hacktivist has the alternative of publishing his or her views on a web page. But that alternative has inherent limitations, as one cracker team notes:

> if we'd build up a site & post our messages on the site, hardly very few people would come & visit us, we've got to make people read the truth; if we post the things on a page already visited by many people for some reason or the other, that's effective. ("Interview with World's Fantabulous Defacers")

The motivation for hacktivism thus lies not in unequal access to speech, but rather, inequality in the ability to be heard.

---

[56] See, for example, (Cohen 1998), (Nickel 2000),(Charney 1998).

The "level playing field" and "ends over means" arguments both amount to claims about speaking rights that are substantive rather than procedural. It is not enough to have networked media that make it possible to speak, goes the level playing field argument: inequalities in access to publicity and mass media mean that the underdog's message may be lost in the shuffle. Hacktivism is a way of ensuring that the underdog's voice may be heard among the louder voices of the more privileged. Similarly, the ends over means argument holds that if your message is really important, it is not enough to simply float it out into the digital abyss; you need to ensure that the message is received. Again, hacktivism is seen as a way of commanding audience.

The problem of pursuing audience, rather than simply speech, stems from the very virtue that so many deliberative theorists see in the advent of the Internet: the universal availability of a platform for self-expression. By providing a very widely accessible tool of mass communication, the Internet has made the ability to communicate much less scarce. Instead, it is the availability of audience that is scarce.

The focus on audience, rather than speech, is clear from the comments of hacktivists themselves, who believe that their tactics translate into audience and awareness. "Sometimes a 'pie in the face' can draw more attention to your cause then putting up a thousand web sites countering their views."(Buster 1999) A member of the Electronic Disturbance Theater said that her group was "forcing people to pay attention" in a climate in which the "attention span is a minute." (Karasic 2002)

Political crackers have made similar claims; for example take the team of crackers who write that, "[u]s defacing sites may not bring peace, but it will certainly create global awareness about the suffering of the Muslims of Kashmir, and the righteousness of their

cause." (m0r0n and nightman 2002) Another cracker claimed victory for his defacement campaign, using one web site defacement to reflect on the media attention he received for his previous defacements:

> At last, Kashmir issue got some attention..
> Thanks to CNN..
> What about a deal now??
> Took more than 40 defacements to get noticed..
> Exactly how many web sites you guys wanna see defaced to solve the problem??
> (Nuker 1999b)

Even those who criticize tactics that infringe on speech rights have sometimes acknowledged that these tactics can be effective attention-getters – if not effective agents of change. As one critic has written:

> The problem with you people (and that applies in equal measure to Paul Mobbs & the 'Electrohippies' EDT/Floodnet epigonism) is that you were for media attention from the very start. And you political ideas never went very much further than to create a cyberspace equivalent of the mass movements of old, with you of course as its avant-garde leaders. … You would do us all a great service if you folks would fold your buffooneries and join the ranks of serious activism. It's less spectacular, and your name will appear less often in the mainstream media. But it's more worthwhile and will get the cause (whatever we believe it to be, justice and peace may be?) more mileage. (Riemens 2001)

All of these comments underline the core problem: audience scarcity. As described by Goldhaber's work on "the attention economy", the problem stems from the fact that "attention…is an intrinsically scarce resource." (Goldhaber 1997) Yet where Goldhaber anticipates that "individual attention getters of all sorts will find it ever easier to get attention directly through the Web," the hacktivist case suggests that even skilled Internet users may find it hard to command an audience in an atmosphere with so many competing for audience. Hacktivism provides a way of addressing inequalities of audience access, even when avenues of expression are widely available.

The challenge for deliberative democrats is that acknowledging audience scarcity (and inequality of access) makes freedom of expression look like a relatively hollow basis for deliberation. If participants cannot be satisfied with the opportunity for speech, but instead demand the opportunity to be heard, how are we to constitute procedural principles for online deliberation?

The problem of anonymity

Perhaps no aspect of online communications poses as great a challenge to our aspirations for meaningful democratic discourse as the ready availability of anonymous speech. Anonymity has been only a rare feature of speech in the "real" world, but in cyberspace, it is routine.

The role of anonymity in public life has been subject to much debate. The debate can be distilled to two contradictory positions. One sees anonymity as a necessary and valuable part of political life. This position ties anonymity closely to free speech, holding that total privacy – anonymity – is sometimes necessary to free speech. Anonymity "encourages the free flow of ideas"(Amis 2001), allowing people to make unpopular statements that nonetheless enrich public debate. Anonymity allows speech in which the focus is on the speech, not the speaker. Anonymity allows people "to avoid persecution" (Marx 2001) even as they speak their conscience freely.

The opposite extreme sees anonymity as a danger to democracy and public life. This position focuses on accountability as the root of responsible behavior and responsible politics. Anonymity brings out the worst in people by allowing them to evade

the consequences of their speech or actions. Anonymity precludes meaningful speech because it makes it impossible to judge the interests or motives of the speaker. Some also argue that "anonymity -- like the myth of Gyges's ring that makes the wearer invisible -- leads inexorably to immoral and even illegal behavior." (Saco 2002)

This debate is crucial to our assessment of the prospects for electronic democracy. If anonymity is congenial to democracy, online deliberation may be if anything more robust than its offline predecessors. If, on the other hand, anonymity is destructive to democracy, our hopes for electronic democracy must be constrained; or our laws and technologies of identity verification must be greatly strengthened.

Yet until now, the debate over anonymity has been largely a theoretical one. The two extreme positions in the anonymity debate represent normative beliefs about anonymous speech, not empirical claims about how anonymity actually works. As long as anonymity was constrained to "bathroom walls and prank calls"(Hilden 2001), this was by necessity a normative debate. But the rapid expansion in anonymous speech facilitated by the Internet allows us to examine these competing principles against a richer field of anonymity practices.

Hacktivism offers a particularly interesting array of anonymity practices. First, it offers three very distinct positions on anonymity, which to a large degree correspond with the three distinct cultures of political crackers, performative hackers, and political coders. Second, the very extremism of hacktivist practices make them appear very similar to the best and worst case scenarios envisaged by anonymity advocates and opponents.

If we fear that anonymity facilitates injurious or even criminal behavior, then hacktivism would seem to be a case in point. Political crackers deface web sites, slow,

block, or damage web servers, distribute viruses, and wreak other kinds of havoc. Their actions seem to typify the kind of antisocial behavior feared by anonymity opponents.

On the other hand, hacktivism also embodies some of the hopes of anonymity proponents. As predicted by anonymity advocates, political crackers use their anonymity to express unpopular or challenging opinions. While they can be destructive, that destruction is usually limited, and is always in service to some form of political communication or action. Both political crackers and political coders detach their message from the identity, nationality or location of the messenger – realizing the vision of anonymous speech as speech in which the focus is on the message, rather than the speaker.

But the actual practices of hacktivists fit neatly with neither the hopes nor the fears expressed in the literature on anonymity. As Gary Marx has observed, anonymity is not a binary phenomenon. Rather, "identifiability at one extreme can be contrasted with anonymity at the other. Describing a variety of kinds of identity knowledge and approaching these as distinct continua brings us closer to the messiness of the empirical world" (Marx 2001).

Some hacktivists, almost always political crackers, usually use what Marx refers to as "pseudonyms that can not be linked to other forms of identity knowledge --the equivalent of "real" anonymity (except that the name chosen may hint at some aspects of "real" identity, as with undercover agents encouraged to take names close to their own)"(Marx 2001). This reflects the fact that crackers are engaged in activities that could entail significant legal consequences if they were caught.

In contrast, political coders most frequently use "pseudonyms that can be linked to legal name and/or locatability --literally a form of pseudo-anonymity." Coders vary somewhat in their use of pseudonymity; the participants in Peekabooty are identified by their legal names on the project's web site. Hacktivismo participants use their pseudonyms in their work with the project, but are mostly forthcoming with their real names in face-to-face interactions. DeCSS authors sometimes use traceable pseudonymns or real names, and sometimes use untraceable pseudonyms or remain anonymous.

Performative hackers – along with some political coders -- are generally known by their real names. The names of the electrohippies, the ®™ark team, and the members of the EDT are all publicly available. The EDT consciously rejected anonymity when it got the hacktivism ball rolling:

> we made a decision that was very very strange but that seemed on a gut level what we needed to do, but it went against all the usual elements. We decided not to be anonymous. Not to be secret – to be transparent. And this went against hacker culture, which is about anonymity, which is about secrecy. (Dominguez 2002a)

The decision to embrace accountability, and reject anonymity, is not always an easy one:

> I worry a lot about what I do online. There are ways to be completely anonymous on the Internet, and if you are very skilled and careful, no one can get back to you, not even the FBI or the NSA or whatever. But I believe that my actions would have less impact if performed anonymously. This is why I do not hide, and why I carefully choose my activities. (Hocevar 2003)

How are we to interpret this variation in nymity practices? Not in the terms afforded by democratic theory's debate over anonymity – with the possible exception of pseudo/anonymity practiced by political crackers. Their use of pseudo/anonymity as a shelter from legal consequences fits the argument that "anonymity supports the

mischievous, the petty vandalisms against each other and authorities that give us room to mock perceived hegemonies and to release 'incorrect' but genuine feelings."(Smith 1997)

But the pseudonymity practiced by political coders is far cry from the kind of anonymity that some fear "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity"(Amis 2001). It is equally ill-described by those proponents of anonymity who see anonymity as a liberating tool in democratic discourse. It is true that deliberative theorists sometimes envision political debate in the public sphere as an "anonymous public conversation"(Benhabib 1996; cited in Charney 1998). But this is not the same type of anonymity as the anonymity practiced by hacktivists and other Internet users, as Bregman points out:

> An anonymous membership is ideal, but not necessarily in the sense of cyberspace anonymity. Anonymity as it is generally conceived of in cyberspace—where persons can communicate without regard for attributes such as race or gender—detracts from the humanity of the discourse. Members should have enough information about one another to gain a universal mutual respect for one another as human beings, but that's not enough. In addition, the discourse benefits from members who appreciate the importance of the recognition of "group-based" identities which can only be gained from knowing something about the specific identity/background of other discourse participants. (Bregman)

Hacktivist nymity practices, like many anonymity practices online, are ultimately ill-described by the scholarship on offline anonymity. They are better understood as decisions about the construction of a digital identity than as statements of offline compliance or subversion. As Diane Saco argues, "electronic pseudonymity -- anonymity through the adoption of an alias -- can have the parallel effect of constructing a kind of public voice even as it protects personal identity." (Saco 2002) This is a function of the exclusivity of usernames on e-mail systems: "Ideally, if someone chooses a pseudonym in one of these systems, no one else can send mail under that name. This allows for the

possibility of a true digital persona -- an 'identity' permanently disembodied from one's physical being." (Saco 2002)

Political coders and political crackers create these digital alter egos through their consistent use of a pseudonym online. If crackers were only interested in escaping the legal consequences of their hacktions, they would be better off leaving their web defacements unsigned. But the use of digital pseudonyms allows the creation of a cumulative body of work – a digital manifesto – for which they are both identifiable and accountable within the virtual community.

Being able to take digital credit for one's hacktivism is only part of the attraction of pseudonymity, however. As the Supreme Court of the U.S. has observed, "anonymity… provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."("McIntyre v. Ohio Campaign Commission 1995) This same benefit is provided by electronic pseudonymity, and is particularly in keeping with the tenet of the hacker ethic that holds that "[h]ackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position." (Levy 1984) This is explicit in political crackers' rejection of questions about their age or nationality: "Dividing people according to country is not our style, as mentioned earlier ``DIVISION`` is not a word in our lexicon."(m0r0n and nightman 2002) Pseudonymous and anonymous hacking is a statement about separating the virtual body from the physical body, and all the criteria (like nationality, race, or gender) that we use to judge physical personae.

Performative hackers' use of real names is an explicit rejection of that separation. Performative hacktivists argue for a reunion of virtual and real politics, and criticize the

hacker fantasy of "having the data body leave the real body, the electronic body uploading itself." (Dominguez 2002a) Using real names in cyberspace is a way of rejecting the hacker separation between the virtual and real, and instead affirming real-world accountability for virtual acts.

These different nymity choices thus translate into different kinds of accountability claims. Political crackers use robust pseudonymity or anonymity to declare that they are accountable to no one (although either coder carelessness or government intelligence work may sometimes put the lie to that claim.) Political coders embrace (generally weak) pseudonymity as a hacker convention. While they thus construct a digital persona that is accountable to the digital community (and also subject to the laws of their physical homeland), it is accountable only in terms that divorce the judgement of the digital body from the characteristics of its fleshy analog. Performative hackers explicitly reject the pseudonymity and anonymity of the hacker world, and embrace accountability to the physical world instead.

These decisions about accountability are partly tied to perceptions of risk, and risk tolerance. Political crackers hack illegally and anonymously because they are confident that their anonymity can protect them from the legal consequences of their actions. As one team of crackers put it: "We don't leave our marks behind for 'anyone' to follow. We're not worried about it. We're outside the jurisdiction of any agency that is hostile to us." (m0r0n and nightman 2002)

Performative hacktivists, on the other hand, tend to be more risk-averse. One performative hacktivist described her boundaries by saying that she "never did anything that I thought would have me arrested."(Karasic 2002) Another said that he was "scared

that taken out of context anything I or my friends are involved in could be considered illegal."(Karasic 2002) A third pointed out the strategic limitations of engaging in illegal activity: "I'm trying to be effective as an activist, and if you want to get the most people involved in movements you generally want to focus on legal activities so that people will participate." (Kreider 2003)

Political coders fall into a middle territory, in which an awareness of legal risks is leavened by confidence in their ability to manage those risks. Sometimes it is a question of picking one's battles: "I wouldn't do anything illegal in North America," says one member of Hacktivismo (metac0m 2002). He is echoed by a Hacktivismo collaborator who doesn't worry about legal issues "at all" because "none of the projects we have underway right now would fall under any [Canadian] laws." (Happy 2002) For others it is a matter of personal ethics happening to coincide with the law: I don't give a fuck about legal issues," said one political coder who had been arrested as a teen hacker. "I do whatever I want. I have my morality that forbids me to do things that are destructive so most times I live within our laws. If there are legal consequences, I was too under-skilled." (Jules 2002) And sometimes an acceptance of a certain degree of legal risk stems from trust in a broader network of support: " I believe I can defend myself, and that an advocacy group, like the EFF [Electronic Frontier Foundation], would help me in any legal battles I would have concerning my online activities." (Brown 2003)

While legal concerns thus factor into nymity decisions, hacktivists can be very explicit about seeing their nymity choices as conscious political statements. As one performative hacktivist put it:

> One main distinction between most Politicized Hacking and the type of Electronic Civil Disobedience just mentioned is that while ECD actors don't hide their names, operating

> freely and above board, most political hacks are done by people who wish to remain anonymous. It is also likely political hacks are done by individuals rather than by specific groups. …This distinction speaks to a different style of organization. Because of the more secret, private, low key, and anonymous nature of the politicized hacks, this type of activity expresses a different kind of politics. It is not the politics of mobilization, nor the politics that requires mass participation. (Wray 1999a)

Another performative hacktivist described the choice of anonymity versus transparency as a strategic choice about what kind of role to play within a broader political movement:

> Where a hardcore hactivist cant talk about what they do because they will go to jail, we court the media, blab about our actions to the press, and try to create the best stories possible. So, it is fundamentally different in that we are like the propaganda wing of a movement, whereas hactivists are the guerrilla fighters who cant show their faces at all. (Guerrero 2003)

All of these conscious nymity choices depart sharply from the theoretical expectations about anonymity in public speech. Hacktivists do not use anonymity as a blanket avoidance of legal consequences; nor do they treat it as a universally ennobling way of liberating message from messenger. Rather, they treat anonymity as a political tool, with different nymity choices conveying different kinds of claims about political strategy, risk, and above all, accountability.

The idea of nymity as a sort of accountability claim is a significant challenge to democratic theories that treat nymity as an issue of principle. Hacktivist practices suggest that rather than framing the question of anonymity as a principled debate over accountability in public speech, nymity should be seen as one of the kinds of claims that speakers make when participating in deliberative discourse.

Conclusion

The challenges that hacktivism has posed to the notions of freedom and accountability in democratic discourse are likely the first wave of a larger transformation. Hacktivist tools are being distributed to a widening audience that will find lower-and-lower barriers to entry. These include the Hacktivismo tools, as well as projects like the Disturbance Developers' Kit and the Yes Men's Reamweaver software. [57]

Meanwhile hacktivists are also publicizing and teaching hacktivist techniques. Several web sites maintain running news files on hacktivist activities and tools. The Ruckus Society, which trains protesters in non-violent resistance techniques, held its first hacktivist training camp in June 2002. These developments promise to expand the ranks of hacktivists, and extend hacktivist-style protest to activists whose primary allegiances lie outside of the hacktivist community.

The challenges to deliberative discourse posed by the digital world are not limited to hacktivists and their disciples. The developments that make hacktivism a challenge to deliberative speech are also visible in other corners of Internet culture. For example, the right to free expression is facing increasing claims of a right to be heard. Advertisers have made legal arguments against technologies that allow consumers to bypass advertising, claiming that what they have purchased is not airtime but eyeballs [58].

---

[57] The Disturbance Developers' Kit was a project of the Electronic Disturbance Theater, and made the EDT's FloodNet code available to any group interested in staging a virtual sit-in. Reamweaver is a program that automates the creation of web site parodies.

[58] Several entertainment companies launched a 2001 lawsuit against SonicBlue, makers of a digital video recorder known as ReplayTV. At the heart of the lawsuit was ReplayTV's ability to automatically skip commercials, which television and media companies (accurately) saw as a threat to their advertising revenue. For a summary of the case see(Isenberg 2001).

The strategic use of anonymity also seems to be a growing phenomenon. People routinely make choices about the degree of identifiability they wish to undertake in any given online context. They may use full names in professional discussion groups, traceable pseudonyms in online support groups or interest discussions, and untraceable anonymizers in discussions about illegal activities, sexuality, or other sensitive areas. These choices reflect decisions about how accountable people want to be, to whom, and under what circumstances.

Can deliberative democracy reformulate the debates over free speech and accountability in order to come to terms with these practices? The question may be moot. Along with the challenges to democratic discourse, hacktivism has significantly compromised the prospects for enforcing any rules of discourse – even if such rules could be agreed upon.

Hacktivists are making the difficult job of policing online speech even harder. And not by accident: many hacktivists are deeply committed to the idea that online speech should be freer than speech in the real world. They are heavily influenced by a kind of hacker romanticism that sees the Internet as the last frontier for truly free speech, and as a kind of generalized libertarian haven.

Both of the challenges previously outlined limit the state's capacity to monitor and regulate speech. Defacements and sit-ins grab opportunities for audience, whether or not they are institutionally or normatively sanctioned. Anonymity and pseudonymity can prevent monitoring and enforcement by the state.

But hacktivists are also consciously use technologies to limit the state's capacity to monitor and regulate speech. Policy circumvention projects like DeCSS and

Hacktivismo aim at crippling government's capacity to restrict online communications. Jam Echelon Day – a stunt that encouraged Internet users to overload government surveillance networks by e-mailing lists of keyword triggers – raised the prospect of stymieing automated monitoring.

The effort to resist regulation of online speech extends far beyond the hacktivist community, however. A variety of privacy tools and organizations are allowing Internet users to elude government regulation of speech. The widespread availability of encryption tools allows people to circulate information beyond the reach of government monitors or censors. Movies that fail government rating standards can be independently distributed online. Organizations like Privaterra[59] use privacy tools to ensure freedom of speech in monitored jurisdictions.

The purpose of these tools is to take the decision to monitor or regulate speech out of the hands of the state. Instead of collective decisions (or authoritarian decisions) about how speech should be regulated, individuals create their own speech regimes by choosing tools that provide them with a greater degree of privacy. By creating these tools, hacktivists and other Internet users preserve the Internet as a space for self-regulating speech.

That may be a challenge for proceduralist visions of deliberative democracy that seek to establish structures for discourse – including ground rules for free expression and accountability. But the impossibility of enforcing rules of discourse may be the ultimate victory for the Habermasian vision of the public sphere as deliberation without coercion,

---

[59] Privaterra works with international human rights workers to ensure that their activities can elude government monitoring and restriction.

its only goal “a consensus brought about by coercion-free communication.” (Habermas 1983)

Chapter 6

Conclusion: The Future of Hacktivism

Introduction

This dissertation started with two goals. First, to establish an empirical picture of hacktivism through the elaboration of a taxonomy of hacktivist practices, characteristics, and cultures. Second, to use the unique qualities of hacktivism to explore three very different questions about political participation. The divergence between these two goals, and among the three central theoretical questions of chapter 3, 4 and 5, took the reader through a variety of political and theoretical landscapes.

The concluding chapter revisits this broad territory in the search for interlinkages among the chapters, looking for larger themes and conclusions. It deliberately pushes the material to its limits, exploring the implications that the chapters have for one another, even where these implications are only elliptically apparent in other chapters.

It begins by reviewing the theoretical agendas of the dissertation, revisiting the issues examined by each of the three central chapters: the incentives for collective political action, the circumstances of successful policy circumvention, and the prospects for online democratic deliberation. It then turns to the empirical picture of hacktivism that was presented in chapters 1 and 2, adding a few more observations to the divisions established in the taxonomy, and describing the ways in which the evidence presented throughout the dissertation bears on the location of hacktivism in relation to civil disobedience and cyberterrorism. It concludes by sketching out some predictions for the future of hacktivism, particularly in light of the events of 9/11.

Hacktivism and theory building

This dissertation took on three very different theoretical agendas in chapters 3, 4, and 5. Chapter 3 suggested that a theoretically grounded notion of identity can provide an account of collective political action as socially-driven, even in the socially thin atmosphere of the Internet. Chapter 4 established a model of hacktivist and offline policy circumvention as a function of political entrepreneurs, costs of failure, and costs of repression. Chapter 5 qualified hopes for deliberative democracy on the Internet with a glimpse at hacktivist approaches to free speech and nymity, both of which challenge proceduralist visions of online deliberation.

The three theoretical issues that are explored in these three chapters can be pushed further, however, when we pursue the interconnections among the themes and evidence that each chapter presents. The three themes of identity, circumvention, and deliberation arise more or less subtly in each chapter of the dissertation, allowing us to draw broader if more tentative conclusions than those reached in each chapter alone.

Identity and collective political action

Chapter 3 argued that political scientists have tended to underestimate the role of social incentives in motivating political participation. By rethinking the notion of social incentives, borrowing from identity theory, and integrating insights from the broader literature on selective incentives, I arrived at the concept of identity incentives: incentives that leverage individual-level aspirations to identifying with a positively valued group. I then compared identity incentives with interactive incentives as predictors of hacktivists'

type and form of participation, and find that hacktivist origins (in the hacker-programmer or artist-activist worlds) do indeed predict the type of hacktivism in which they engage. Combined with the way that hacktivists talk about collaboration, labeling, and specific hacktivist forms, this correlation provides strong evidence for the significance of identity, rather than interaction, as driving hacktivist participation.

In retrospect, this finding was foreshadowed by the picture of hacktivism that emerged in Chapter 2's taxonomy of hacktivists. The most stable distinction among hacktivists rested on their political origins in either the hacker-programmer or artist-activist communities. While hacktivist orientation (either transgressive or outlaw, in my terminology) is crucial in distinguishing between political coders and political crackers, orientations prove to be less tidy than origins. Most notably, even though political coders and performative hacktivists share a transgressive orientation, the former focus on policy circumvention, while the latter aim at policy change.

Later, the chapter on policy circumvention reinforces Chapter 3's findings on collective action dynamics. In a sense, the model of policy circumvention is a narrative of collective action challenges. High costs of failure make it harder to cooperate: thus we see greater tension among anti-censorship coders than among DeCSS coders. This observation anticipates and counters the potential argument that collaboration is simply easier among the small groups and cheap communication of hacktivism. By reminding us that collective political action is a puzzle, even here, it amplifies the significance of the finding that social identity is key to motivating collaboration among hacktivists.

Finally, the consideration of deliberative democracy reflects the identity concerns that emerge in Chapter 3. The discussion of nymity choices highlights the meaningful

distinctions among nymity, pseudonymity, and anonymity; these distinctions correspond to different accountability claims. These are claims of accountability *to particular communities*: the robust pseudonymity of some crackers grounds them in the community of crackers who know their handles; the looser pseudonymity of coders is a statement of dual allegiance to the hacker world, and to the legal polity to which they remain accountable. The performative hacktivists who use their real names are explicitly eschewing membership in an online community in favor of maintaining ties to their offline worlds. Each of these choices serves to declare and reinforce ties to a particular political community, returning us to the idea that political participation is at least partly a choice about social belonging.

Certainly the theme of identity resonates throughout the chapters of the dissertation, and across the three types of hacktivism described therein. Yet my investigation of hacktivist identity was necessarily frustrated by the difficulty in contacting political crackers; that difficulty translated into uncertainty about whether and how identity differences might also predict the choice of political coding versus political cracking. While I have a number of intuitions about identity differences that might indeed account for this variation, it may be virtually impossible to gather the data needed to confirm or disprove these intuitions.

Policy circumvention and policy change

Chapter 4 confronted the literature on transnational social movements, whose growing power has been partially attributed to the Internet. I argued that the social movement literature mistakenly focuses on efforts at policy change, ignoring the more

transformational phenomenon of policy circumvention. I defined policy circumvention as legal noncompliance that is a strategic political response to a specific policy, focuses on nullifying that policy, and creates some non-excludable benefits. I showed that this kind of noncompliance can be found in the worlds of both online and offline politics, but is particularly amenable to hacktivist techniques.

I then used the cases of DeCSS and Hacktivismo to test a three-part model for predicting policy circumvention. I showed that successful policy circumvention depends on political entrepreneurs, low costs of failure, and high political costs of repression. I argued that the growth of policy circumvention constitutes an additional pressure for policy change, and changes norms about policy compliance. The threat of policy circumvention poses major political and economic challenges, demanding policies that will be robust in the face of measurable defection, given the likely expansion of policy circumvention in the context of an information economy.

The significance of the distinction between policy change and policy circumvention is not limited to the social movement literature, however. As Chapter 2 suggests, the choice between policy change and policy circumvention is a crucial question for hacktivists, albeit one that does not map neatly onto either hacktivist orientations or origins. Political crackers and performative hacktivists adopt forms of hacktivism that are geared towards policy change; political coders use a form aimed at policy circumvention. When performative hacktivists turn to policy change, they are explicitly affirming the linkage between on- and offline politics, arguing that the former should serve the latter; and when political crackers set their policy targets, they are

making a similar linkage, although it tends to imply a weakness of offline policy in the face of online power.

When political coders embrace policy change, however, they are making the opposite statement. The decision to focus on policy circumvention is implicated in a larger commitment to hacktivism as a way of insulating the culture and policies of the Internet from the broader politics of the offline world. The legitimacy of political coders' policy circumvention rests on an implicit (and sometimes explicit) claim to self-governance by the Internet community. The intent of a given form of hacktivism (that is, its aim of either policy change or policy circumvention) is constitutive of hacktivist types precisely because it speaks volumes about the political communities in which political coders, crackers, and performative hacktivists variously locate themselves, and about their views of the relationship between on- and offline political orders.

Chapter 3 provides further insights into the dynamics that knit communities of political coders together. The central surprise in its findings was the widespread practice of collaboration among political software developers, who were theoretically capable of effective solo action. The interview data suggested that this collaboration was driven not by a demand for social interaction, but rather, by belief in the efficacy of collective action. This belief largely reflects the rewards of policy circumvention, which offers the immediate gratification of tangible effects in place of the delayed gratifications of indirectly contributing to policy change. Efficacy motivates collaboration, and collaboration reinforces the sense of online political community that coders are driven to protect. Collaboration and efficacy thus form a self-sustaining dynamic of policy circumvention.

Chapter 5 suggests that the dynamics of policy circumvention may not be entirely limited to political coding, however. The pursuit of audience that characterizes the hacktivist model of free speech serves to erode the line between policy change and policy circumvention. The transgressive pursuit of audience is a way of circumventing elite media control: as Vegh's work suggests, challenging elite control of the media is central to the hacktivist project. When crackers redirect a web site, or performative hacktivists draw visitors to a deceptively-addressed spoof, they are wresting audience share away from more established voices.

These acts are in fact circumventing particular legal orders: crackers are circumventing a system of domain name allocation that directs Internet traffic to particular addresses; performative hacktivists are circumventing a system of intellectual property that protects the visual identity and branding of companies and organizations. Like the policy circumvention practiced by political coders, the circumvention of audience control challenges elite power; this type of circumvention thus offers some of the satisfactions (in terms of perceived efficacy) that are available to political coders. But it is ultimately less significant than "pure" policy circumvention, because the circumvention of audience control is a way of pressing for policy change, rather than an end in itself.

Policy circumvention nonetheless emerges as one of the most distinctively characteristic themes of the hacktivist phenomenon. Both the circumvention of audience control and the direct circumvention of policy represent striking departures from the usual dynamics of on- and offline politics.

Deliberative democracy, free speech, and anonymity

Chapter 5 takes a more meditative approach to the hacktivist material. It uses hacktivism as a way of exploring two issues that are crucial to the widely-held aspirations for deliberative democracy online: free speech, and anonymity. Free speech is essential to the principles of popular sovereignty, political equality, free flow of information, and pluralism, all of which are in turn essential to democratic discourse. Anonymity is seen as either threatening or helpful to democratic deliberation, depending on whether you believe that it facilitates irresponsible speech, or constructively separates speech from the identity of the speaker.

Hacktivism challenges expectations for both free speech and anonymity online. In debates over the impact of defacements, redirects and sit-ins on free speech, hacktivists describe the growing significance of the right to be heard – rather than the simpler right to speech itself. In their various approaches to anonymity and pseudonymity, hacktivists' nymity choices constitute different types of accountability claims. A "right to audience", and the strategic use of nymity are both problematic for proceduralist visions of deliberative democracy online, just as the larger phenomenon of hacktivism undermines hopes for enforcing any rules of online debate.

The taxonomy of hacktivism outlined in Chapter 2 thus has practical as well as symbolic significance for deliberative democracy. The ascendance or decay of different types of hacktivism translates into constraints on the viability of online deliberation, or at least, into different kinds of challenges for deliberative democrats. Continued expansion in political cracking would be very problematic, since it undermines online speakers' expectations that their digital voices will be respected, or at least, not violated; crackers'

use of anonymity also represents the worst fears about anonymity as a shield for destructive and irresponsible speech acts. A tide of performative hacktivism would have less dire, but still difficult consequences: virtual sit-ins destabilize the core communication channels of the Internet, even if they are driven by a desire to level the communicative playing field. On the other hand, performative hacktivists' reliance on mass protest at least maintains democratic conventions about the relationship between mass support and political legitimacy, and their use of real names acknowledges accountability to the broader political community.

The ascendance of political coding has more positive consequences for online deliberation. True, the whole notion of policy circumvention undermines the idea of collective decision-making: if people can defect from those decisions by evading enforcement, why engage in collective deliberation? But this abstract irony is less significant than the practical impact of the tide of anti-censorship coding. By dismantling authoritarian controls on the free flow of information and communication, political coders may enable new forms of democratic deliberation within authoritarian regimes, and among the larger world community.

Chapter 3 offers further hope to deliberative democrats. The surprising dominance of collective forms of political action puts the lie to fears about the Internet's atomizing potential. Far from retreating to their separate computers, hacktivists embrace the networking potential of digital tools, forming new political communities among far-flung collaborators. Furthermore, perceptions of hacktivist efficacy suggest a potential for broadening engagement online by expanding the notion of speech to include speech acts: if a model of deliberation could encompass the creative contributions of hacktivists, it

might engage the participation of those who feel alienated from or constricted by conventional models of democratic politics.

We can glean a final, particular insight into the prospects for online deliberation from part of the policy circumvention model presented in Chapter 4. Variation in the costs of failure matters to the success of policy circumvention because people are risk-averse: the prospect of incurring significant legal, financial, or personal consequences from engagement in hacktivist policy circumvention will generally deter participation. This reminds us that the accountability claims implicit in different nymity choices (as discussed in Chapter 5) represent pragmatic, self-interested decisions at least as much as they reflect specific political commitments.

Overall, the inclusion of related material from other chapters tends to leaven Chapter 5's somewhat gloomy conclusions about the prospects for deliberative democracy online. The ascendance of political coding promises to open new avenues of political discussion; the widespread embrace of collaborative approaches to hacktivism underscores the demand for political community; the gratifications of hacktivism may encourage new forms of political engagement. These seedlings of optimism suggest that the problems posed by the demand for audience, as well as by the strategic use of nymity, may amount to design challenges rather than wholesale refutation of aspirations for democratic deliberation online.

* * *

This theoretical cross-pollination fuels two insights. First, it suggests that the three central theoretical questions of the dissertation were appropriate choices, since each one appears as a larger, broadly resonant theme. Second, it reinforces my contention that

hacktivism offers rich territory for exploring different kinds of social science questions: this ramble through the interconnections among the different themes uncovered still more intriguing veins of potential research.

Hacktivism: reviewing the evidence

Chapters 3, 4 and 5 also help to fill out the dissertation's empirical picture of the hacktivist phenomenon. The dissertation's empirical agenda was twofold: first to establish a working taxonomy of hacktivist practices; and second, to bring a new standard of evidence into the debate over whether to construe hacktivism as a form of civil disobedience, rather than as a point on a continuum ending in cyberterrorism.

Illuminating the taxonomy

Chapter 2 of the dissertation established a robust taxonomy of hacktivism. distinguishing three types of hacktivism: political cracking, performative hacktivism, and political coding. These three types of hacktivism represent the intersection of two dimensions of hacktivist variation: hacktivist origins (in the hacker-programmer or artist-activist worlds) and hacktivist orientations (transgressive or outlaw). Based on variations in each of these dimensions, I described three very different types of hacktivism: political cracking, political coding and performative hacktivism. These three categories represent lines of conflict among hacktivists, as well as a theoretically coherent organizational scheme.

Chapter 3 speaks particularly to the significance of hacktivist origins. In this chapter I demonstrate a robust correlation between hacktivists' background in either the hacker-programmer or artist-activist world, and the likelihood of focusing on either political coding/cracking, or performative hacktivism, respectively. This correlation speaks to the significance of both the Internet community (the world of hacker-programmers) and the postmodern left (the world of artist-activists) as influences on hacktivists and hacktivism.

Chapter 4 illuminates one of the more opaque areas of empirical curiosity, which is the relative momentum of different types of hacktivism. Its evidence of the adoption of hacktivist policy circumvention by state and business actors suggests that political coding may be ascendant. The U.S. government's pending creation of a Global Office of Internet Freedom will alone propel anti-censorship coding to an entirely new level; the activities of Voice of America have already legitimated the activities of anti-censorship coders. Particularly when contrasted with the diminishing media attention paid to virtual sit-ins, and the growing (mis)construction of political cracking as cyberterrorism, the gradual institutionalization of hacktivist policy circumvention is indicative of political coding's move to the forefront of the hacktivist scene.

Chapter 5 sees the taxonomy's divisions among hacktivists translated into meaningful conflict over free speech, and meaningful variation in nymity practices. The range of anonymous, pseudonymous, and real-name practices was introduced in Chapter 2 as an issue of principle for at least some hacktivists; Chapter 5 demonstrates that these practices always amount to implicit or explicit statements about political accountability. Even more striking is the intensity of debate over whether cracking and sit-ins amount to

violations of speech rights, or constructive efforts at leveling the playing field. Each of these examples illustrates the utility of the taxonomy in capturing existing lines of conflict, and perhaps in anticipating future debates.

The taxonomy thus serves as an element of continuity throughout all chapters of the dissertation. By organizing hacktivism into meaningfully different subtypes, it identifies lines of variation that prove useful in conducting my inquiries into identity incentives, policy circumvention, and democratic deliberation. Each of these themes provides further insight into the divisions encompassed by the taxonomy itself, reinforcing my contention that the divisions among political crackers, performative hacktivists, and political coders constitute the central fault lines in the hacktivist movement.

Hacktivism as civil disobedience

The introduction to this dissertation showed that the literature on hacktivism falls into two camps. One camp locates hacktivism in the context of civil disobedience, and often focuses on media (mis)portrayal of hacktivism. The other camp locates hacktivism in a continuum of cyberthreats, just a short hop away from cyberterrorism. I professed my own sympathy for the civil disobedience camp, but acknowledged its shortcomings in presenting direct evidence from hacktivists themselves.

The dissertation has sought to remedy this shortcoming by presenting evidence about hacktivist orientations and intentions. To begin with, the taxonomy in Chapter 2 shows that any blanket statement about hacktivism's relationship to civil disobedience and cyberterrorism necessarily obscures the significant distinctions among different types

of hacktivism. While all hacktivist practices fall (by my own definition) between online activism and cyberterrorism, some types of hacktivism are closer than others to offline traditions of civil disobedience. Performative hacktivists explicitly claim links to the civil disobedience tradition: the Electronic Disturbance Theater eschews the term "hacktivism" in favor of the term "electronic civil disobedience," and designed the virtual sit-in technique in order to lay claim to the legitimacy of mass protest. Political coders rarely use the language of civil disobedience, but adhere to norms of political accountability (in their use of traceable pseudonyms), and make some effort to comply with at least their own domestic political order. Political crackers, in contrast, are far less concerned with adhering to legal or political norms; while it is a misnomer to label web site defacements, redirects and information theft as "cyberterrorism," it is not surprising that this clearly criminal form of hacktivism is the type most often confused with cyberterrorism.

The dynamics of collective action among hacktivists outlined in Chapter 3 place hacktivism more squarely on the side of civil disobedience. If clear ethical commitments constitute a criterion for civil disobedience, then hacktivists' concern with the instrumental value of their actions – their ability to effect specific political ends – is evidence that particular commitments guide much hacktivist activity. The further finding that hacktivists value collaboration and a sense of belonging finds precedent in offline civil disobedience: McAdam and Paulsen's study of social ties in the civil rights movement holds that prior social ties encourage activism "when they (a) reinforce the potential recruit's identification with a particular identity and (b) help to establish a

strong linkage between that identity and the movement in question."(McAdam and Paulsen 1993)

Chapter 4 helps to explain why hacktivism is so often mistakenly conflated with cyberterrorism. Precisely because we are used to thinking of political activism as a means of effecting policy change, political activism directed at policy circumvention looks (and for that matter is) threatening – that is what makes it effective. But policy circumvention has been part of some of the most powerful offline examples of civil disobedience: Rosa Parks' refusal to sit at the back of the bus was policy circumvention. Lunch counter sit-ins were likewise direct refusals to adhere to a targeted policy. Today, abortion clinic blockades circumvent laws permitting abortion by attempting to render that legal right meaningless. As much as it fuels the media's conflation of hacktivism with cyberterrorism, policy circumvention is better understood as evidence linking hacktivism to the civil disobedience tradition.

In Chapter 5, the idea of nymity choices as accountability claims speaks to the civil disobedience criteria of openness and accountability. At first glance, the widespread use of pseudonyms and anonymous hacking would appear to contravene the requirement of open, accountable action. But norms of accountability are particular to communities and cultures – and total openness may not be part of every set of norms. Even covert actions may be statements of political accountability – just accountability to a different community. If political crackers were simply concerned with escaping accountability for their actions, they would hack anonymously; the fact that they use consistent pseudonyms amounts to a declaration of accountability to the online political community that registers their activity.

The cumulative evidence presented in the different chapters of the dissertation shows that, first and foremost, hacktivism cannot be uniformly characterized in relation to civil disobedience and cyberterrorism. Performative hacktivists take great pains to establish linkages to civil disobedience traditions, whereas political crackers seem much less concerned with their public image or claims to political legitimacy. But even political cracking is a far cry from cyberterrorism in its steadfast adherence to nonviolence.

When we probe the variation in resistance techniques among different types of hacktivism, hacktivist tactical innovation really does emerge as a process of exploring the meaning and avenues for civil disobedience in the digital age. Are virtual sit-ins a satisfactory translation of offline street protests, or a condemnable violation of Internet infrastructure? Are web site defacements meaningful speech, or free speech infringements? Is political coding a challenge to elite control, or a narcissistic preoccupation of the Internet by the Internet savvy? Different hacktivists come to different conclusions on these kinds of questions, but the fact that they engage in such intense debates over them demonstrates the sincerity of their efforts in pioneering new forms of digital transgression.

The future of hacktivism

What does this synthetic perspective suggest about the future of hacktivism? It certainly indicates that the *study* of hacktivism has a future in political science, and in social science more broadly. That we got traction on a range of issues confirms that

hacktivism's peculiar characteristics make it a useful laboratory for addressing certain kinds of social science questions.

Our conclusions about hacktivism itself are by necessity more speculative. There are two countervailing forces that are interacting to shape hacktivism's future: first, the post 9/11 security environment, and second, the expanding domain of political coding.

The events of 9/11 changed the context for hacktivism in two crucial ways. First, they increased U.S. (and Western) vigilance towards all potential security threats, including cyberterrorism. Second, the immediate and longer-term political consequences of 9/11 have led to the deepening of various international conflicts implicated in international hacktivism (often termed "cyberwar").

Increased vigilance against the prospect of cyberterrorism has had its most tangible impact in the increased penalties for all forms of computer hacking – potentially including much hacktivist activity. The U.S.A PATRIOT Act amended the Computer Fraud and Abuse Act (CFAA) to "lower jurisdictional hurdles relating to protected computers and damages, and increase penalties for violations."(Milone 2002) The scope of the CFAA was expanded to specifically include computers outside the U.S., where they affect U.S. commerce or communications. The threshold of financial damage required for prosecution of computer hacking was revised to allow for aggregating damage caused to multiple computers, and to remove any minimum threshold in the case of damage to systems related to justice, defense, or security. Most significant, the maximum penalty for first-time offenders was raised from five years to ten, and for repeat offenders, from ten years to twenty (Milone 2002).

On the other side of the Atlantic, the European Network and Information Security Agency (ENISA) was created by the European Union in March 2004, headquartered in Heraklion, Greece. While the creation of ENISA was formally proposed in February 2003(Liikanen 2003), its mandate will be significantly influenced by a pending EU "framework decision on attacks against information systems" – i.e. cracking or hacking. (Liikanen 2002). While this decision has yet to be formally adopted, its draft form has already been agreed upon by EU member states (Liikanen 2004), who moved to adopt new standards for information security in April 2002 (Liikanen 2002). The 9/11 attacks were at least part of the context for the new framework, with the announcement explicitly referencing the threat of cyberterrorism:

> Cyberterrorism is a further threat, and must be taken much more seriously following the tragic events of 11 September. There have been a number of occasions where tensions in international relations have led to a spate of attacks against information systems, often involving attacks against web-sites. More serious attacks could not only lead to serious financial damage but, in some cases, could even lead to loss of life, for example an attack against a hospital system or an air traffic control systems…Although this new proposal does not address terrorism specifically, it provides the basic framework for police and judicial co-operation on attacks against information systems. It therefore represents a further important step in dealing with attacks against information systems linked to terrorism. (Vitorino 2002)

The debate over the framework also occasioned what appears to be, to date, the only legislative effort at specifically protecting hacktivism as a form of political protest. Marco Cappato, an Italian Radical Party member of the European Parliament, prepared a draft report on the proposed framework on behalf of the Parliament's Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. In his report, Cappato proposed a number of amendments to the framework proposal, aiming at an

> approach [that] would also make it possible to establish a clear distinction between, on the one hand, forms of 'on-line' political activity, civil disobedience, demonstrations and activities of little or no consequence (some of which might be covered by the term 'hacking') and, on the other hand, 'cracking', violent action directed not only against property, but also against physical persons...It is not acceptable to oblige Member States

> to impose criminal penalties on activities which are already adequately regulated (such as violation of privacy) or which are permissible and tolerated in any democratic country, or indeed which deserved to be recognised as contributing to the public good, even if they involve actions which might be covered by the term 'attacks against information systems'. For example, action to combat censorship and disinformation which involves interference in, or sabotage of, the means used to repress individuals or whole nations.(Cappato 2002a)

As Cappato wrote elsewhere, "[w]e do not want to see a Member State obliged by EU legislation to criminalise harmless demonstrative hackerism or virtual demonstrations, such as those organised by dissidents of totalitarian or dictatorial States."(Cappato 2002b) But Cappato's amendments are not reflected in the latest version of the proposal ("Proposal for a Council Framework Decision on attacks against information systems 2002), making it unlikely that the EU will become the first jurisdiction to explicitly exempt hacktivism from anti-hacking legislation.

If legislators have been reluctant to recognize hacktivism as legitimate, it may be partly because the post-9/11 activity of political crackers tended to reinforce the anxieties of those who worried about the hacktivist threat. The deepening of international "cyberwar" conflicts was apparent within a few days of the September 11 attacks, when several groups of hackers emerged to claim credit for counter-attacks on Arab and Islamic web sites. A group called The Dispatchers claimed to have shut down several Palestinian Internet Service providers, and announced plans to target Afghani web sites (Lemos 2001). An eccentric German millionaire hacker announced the creation of the hacker group Yihat, which he claimed had hacked into the Arab National Bank of Saudi Arabia – a claim that could not be confirmed (McWilliams 2001a). A hacker using the handle "Anonymous Coward" hacked an Islamic web site in Germany, and published the names of subscribers to its e-mail list (Perera 2001). The hacker known as Fluffi Bunni

hacked into a domain registrar, and redirected 10,000 sites to a page with the message "We're Coming for You Oslahmamama".(Murphy 2001)

The threat (and ultimate reality) of a U.S. response prompted hacker activity against the U.S., too. Longtime Pakistani hacker Doctor Nuker defaced the web site of World Trade Services, and replaced the site's content with a message suggesting that the WTC attacks were engineered by the U.S. government (McWilliams 2001c). The web sites of the National Oceanic and Atmospheric Agency and the National Institute of Health were defaced by attackers claiming, "we are not hacker, we are just cyberterrorist," and warning in Urdu, "Americans be prepared to die."(McWilliams 2001b)

The emergent Arab-US hack war was quickly condemned by the Western hacktivist community. The CyberAngels, an Internet safety group, launched an advertising campaign called "Hackers against Terrorism." Their first spot featured Vint Cerf, one of the fathers of the Internet, saying that "[c]omputer attacks and hate speech do not contribute in any constructive way to dealing with the many problems our global civilization faces."(McWilliams 2001d) Germany's Chaos Computer Club issued a condemnation of calls for hacker vengeance, writing that "we believe in the power of communication, a power that has always prevailed in the end and is a more positive force than hatred."("Will hackers keep the cyberpeace?" 2001)

But Western hacktivists' reservations about cyberwarfare have done little to turn back the tide of international hacktivism. In the post-9/11 context, these cyber conflicts have been more often (mis)characterized as cyberterrorism, than described as hacktivism. Sandor Vegh's content analysis of major media in the six months before and after 9/11

concludes that "the media blurs the differences between hacktivism and cyberterrorism"(Vegh 2003); he notes that 97% of the coverage of digitally-enabled terrorism occurred in the time *after* 9/11 (Vegh 2003).

The impact of 9/11 on the cybersecurity environment has certainly sparked discussion and anxiety within the hacker and hacktivist communities. At the same time, political coders have found increasing legitimation in the adoption of political coding techniques in official quarters. As discussed in Chapter 4, hacktivist policy circumvention is emerging as a new method of business and diplomacy: the RIAA has used hacktivist techniques in combating file sharing, and the U.S. government has sponsored projects aimed at circumventing Internet censorship. The ascendance of political coding in elite circles is mirrored by the widespread admiration for projects like Hacktivismo, which receives glowing reviews in many quarters of the hacktivist community.

The temptation is to predict rising fortunes for political coding, and a decline for performative hacktivism and political cracking. The reality is messier and harder to chart. Political crackers have proven remarkably resistant to public opinion: whether cracking is being glamorized or vilified, there will always be teenage kids looking to push their hacks into new political, geographic or technical territory. Likewise, the declining coverage of performative hacktivism could be easily reversed by a clever innovation in its tactical repertoire: virtual sit-ins may have become a little too common to merit coverage, but a new set of tricks could find a new audience. The only clear future is for political coding, which continues to make the technological and political inroads necessary for sustained growth.

Whatever the balance among the three types of hacktivism, the overall evolution of hacktivism will be patterned on the evolution of hacking in general. Hacking techniques evolve through a series of moves and countermoves: hackers figure out a way of getting into systems; systems administrators find a way of closing that door; hackers find a new way in. Hacktivists follow a similar path of continuous innovation, as indeed do the activists honing any tactical repertoire (McAdam 1983). With networks that are always vulnerable to new kinds of hacks, and political structures that are always vulnerable to new forms of challenge, hacktivism will almost certainly maintain a space for digital transgression. This dissertation has endeavored to establish that this should be a hoped-for rather than a dreaded outcome.

Bibliography

27-Aug-99. "Buster: hacktivism.ca listserv.

"About the Peekabooty Project." 2002. [cited October 7 2002]. Available from http://www.peek-a-booty.org/pbhtml/modules.php?name=Content&pa=showpage&pid=1.

Abrams, Dominic. 1994. "Political Distinctiveness: An Identity Optimizing Approach." *European Journal of Social Psychology* 24 (3):357-365.

Abreu, Elinor. 2000. "Business Under Attack." *The Industry Standard*, April 10.

"AIC (Anti India Crew) interview." 2002. *Domina Security*, [cited September 27 2002]. Available from http://www.dominasecurity.com/hackerz/aic.htm.

Amis, Dave. 2002. "Net anonymity: free speech or cheap words?" *spiked-IT*, 2001 [cited November 19 2002]. Available from http://www.spiked-online.com/Articles/0000000054A7.htm.

Anonymous. 2003. *E-mail interview with author*, May 6.

"®™ark Website." Available from http://RTMark.com.

Arquilla, John, and David F. Ronfeldt. 2001a. "The Advent of Netwar (Revisited)." In *Networks and netwars*, edited by J. Arquilla and D. F. Ronfeldt. Santa Monica, CA: Rand.

Arquilla, John, and David F. Ronfeldt. 2001b. "What Next for Networks and Netwars?" In *Networks and netwars*, edited by J. Arquilla and D. F. Ronfeldt. Santa Monica, CA: Rand.

"Attrition: Evolution." 2004. *Attrition*, May 21 2001 [cited July 25 2004]. Available from http://www.attrition.org/mirror/attrition/.

"The Axe of Censorship Falls on the Roman Civic Network." 2004. *The Thing Roma*, October 4 2000 [cited July 15 2004]. Available from http://www.ecn.org/thingnet/reviews/press.html.

Baranowski, Paul. 2002. *Interview with author*.

batz. 2001. "Re: unitedskins.com." *hacktivism.ca listserv*, November 11 1999 [cited July 2001].

Benhabib, Seyla. 1986. *Critique, norm, and utopia : a study of the foundations of critical theory*. New York: Columbia University Press.

Benhabib, Seyla. 1996. "Toward a Deliberative Model of Democratic Legitimacy." In *Democracy and Difference*, edited by S. Benhabib. Princeton: Princeton University Press.

Bennett, W. Lance. 2002. "The UnCivic Culture: Communication, Identity, and the Rise of Lifestyle Politics." 1998 [cited September 7 2002]. Available from http://www.apsanet.org/PS/dec98/bennett.cfm.

Best, Steven, and Douglas Kellner. "Postmodern Politics and the Battle for the Future." Available from http://www.gseis.ucla.edu/faculty/kellner/Illumina%20Folder/kell28.htm.

Bing, Jon. 2003. "Declaration for defendants in DVD CCA v. McLaughlin, Bunner, et al." *Electronic Frontier Foundation*, January 18 2000 [cited April 10 2003]. Available from http://www.eff.org/IP/Video/DVDCCA_case/20000118_bing_norway_law_decl.html.

Bleiker, Roland. 2002. "Activism after Seattle: Dilemmas of the Anti-globalisation Movement." *Pacifica Review* 14 (3):191-207.

Boal, Augusto. 1999. *Legislative theatre : using performance to make politics*. New York: Routledge.

Boje, David M. 2002. "Carnivalesque Resistance to Global Spectacle: A Critical Postmodern Theory of Public Administration." April 30 2001 [cited October 6 2002]. Available from http://cbae.nmsu.edu/~dboje/papers/carnivalesque_resistance_to_glob.htm.

Borger, Julian. 2004. "Cyberwar could spare bombs." *The Guardian*, November 5 1999 [cited April 23 2004]. Available from http://www.guardian.co.uk/Kosovo/Story/0,2763,197390,00.html.

Bowman, Lewis, Dennis Ippolito, and William Donaldson. 1969. "Incentives for the Maintenance of Grassroots Political Activism." *Midwest Journal of Political Science* 13 (1):126-139.

Bregman, Jay. 2002. "Theoretical Frameworks of Deliberative Democracy." 2002 [cited November 22 2002]. Available from http://cyber.law.harvard.edu/projects/deliberation/theory/.

Brewer, M. B. 2001. "The many faces of social identity: Implications for political psychology." *Political Psychology* 22 (1):115-125.

Brewer, Marilynn B., and Michael D. Silver. 2000. "Group Distinctiveness, Social Identification and Collective Mobilization." In *Self, identity, and social movements*, edited by S. Stryker, T. J. Owens and R. W. White. Minneapolis: University of Minnesota Press.

Brown, Tony M. 2003. *E-mail interview with author*, April 9.

Burke, Lynn. 2003. "DVD Case: It's a Linux Thing." *Wired News*, January 28 2000 [cited April 9 2003]. Available from http://www.wired.com/news/politics/0,1283,33925,00.html.

Buster, Bronc. 2001. "Re: unitedskins.com ~ It's about time." *hacktivism.ca listserv*, November 15 1999 [cited July 2001].

B_Real. 2004. "Site Defacement (Schoolnet India Owned!)." 2001 [cited July 23 2004]. Available from http://members.fortunecity.com/feloner/in.html.

Ca$h Money. 2002. *Interview with author*.

"Call for Electronic Civil Disobedience." 2004. *One Global One*, 1999 [cited July 15 2004]. Available from http://members.tripod.com/~oneadvocate/intl.html.

Cappato, Marco. 2002a. "Draft opinion for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on the proposal for a Council Framework Decision on attacks against information systems." In *COM(2002) 173 – C5-0271/2002 – 2002/0086(CNS)*.

Cappato, Marco. 2004. "What is the Borderline Between Criminality and Civil Disobedience in the Net?" September 9 2002b [cited August 1 2004]. Available from http://www.egovmonitor.com/features/cappato01.html.

Castells, Manuel. 2001. *The Internet galaxy : reflections on the Internet, business, and society*. Oxford, UK ; New York: Oxford University Press.

"CDT Analysis of Berstein Decision." 2003. *Center for Democracy & Technology*, December 19 1996 [cited April 11 2003]. Available from http://www.cdt.org/crypto/961219_Bernstein_analys.html.

Chambers, Simone. 2000. "A Culture of Publicity." In *Deliberation, democracy, and the media*, edited by S. Chambers and A. N. Costain. Lanham: Rowman & Littlefield Publishers.

Charney, Evan. 1998. "Political Liberalism, Deliberative Democracy, and the Public Sphere." *The American Political Science Review* 92 (1):98-110.

Chase, Michael, and James C. Mulvenon. 2002. *You've got dissent! : Chinese dissident use of the Internet and Beijing's counter-strategies*. Santa Monica, CA: RAND National Security Research Division Center for Asia Pacific Policy.

Chong, D. 1992. "Social Incentives and the Preservation of Reputation in Public- Spirited Collective Action." *International Political Science Review* 13 (2):171-198.

Chong, Dennis. 1991. *Collective Action and the Civil Rights Movement*. Chicago: University of Chicago Press.

Clark, Peter B., and James Q. Wilson. 1961. "Incentive Systems: A Theory of Organizations." *Administrative Science Quarterly* 6 (2):129-66.

Cohen, Joshua. 1998. "Democracy and Liberty." In *Deliberative democracy*, edited by J. Elster. Cambridge, U.K. ; New York: Cambridge University Press.

Coleman, Biella. 2004. "The (copylefted) Source Code for the Ethical Production of Information Freedom." *Sarai Reader 03*, March 2003 [cited April 22 2004]. Available from http://www.sarai.net/journal/03pdf/297_302_bcoleman.pdf.

Coleman, Stephen, and John Gøtze. 2002. "Bowling Together: Online Public Engagement in Policy Deliberation." *Hansard Society*, 2001 [cited March 1 2002]. Available from http://bowlingtogether.net/bowlingtogether.pdf.

Costanza-Chock, Sasha. 2004. "Mapping the Repertoire of Electronic Convention." 2001 [cited July 15 2004]. Available from http://geneva2003.unige.ch/SP/IMG/doc/doc-24.doc.

"Crackers Attack China on Rights." 2003. *Wired News*, October 27 1998 [cited April 21 2003]. Available from http://www.wired.com/news/politics/0,1283,15857,00.html.

Critical Art Ensemble. 1994. *The Electronic disturbance*. Brooklyn, NY: Autonomedia.

Critical Art Ensemble. 1996. *Electronic civil disobedience and other unpopular ideas*. Brooklyn, New York: Autonomedia.

Critical Art Ensemble. 2000. "Recombinant Theatre and Digital Resistance." *The Drama Review* 44 (4).

Critical Art Ensemble. 2001. *Digital resistance : explorations in tactical media*. Brooklyn: Autonomedia.

Dahlberg, Lincoln. 2001. "The Internet and Democratic Discourse." *Information, Communication & Society* 4 (4):615-633.

Dalton, R. J., and R. Rohrschneider. 2003. "Transnational Environmentalism: Do Environmental Groups Cooperate Globally?" *Center for the Study of Democracy, UC Irvine*, 1999 [cited March 13 2003]. Available from http://www.democ.uci.edu/democ/papers/dalton3.htm.

"deCSS listed on Download.com." 2003. *Slashdot*, 1999 [cited April 8 2003]. Available from http://slashdot.org/articles/99/11/16/0950232.shtml.

"DeCSS: watch your DVD's on your favorite OS." Available from http://www.free-dvd.org.lu/.

Delio, Michelle. 2001. "Is This World Cyber War I?" *Wired News*.

"Denial-of-service attack." 2004. July 30 2004 [cited July 31 2004]. Available from **http://en.wikipedia.org/wiki/DOS_attack** **http://en.wikipedia.org/wiki/DOS_attack**.

Denning, Dorothy E. 1999. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". Paper read at *The Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking*, December 10, at San Francisco.

Denning, Dorothy E. 2002. "Hacktivism and Other Net Crimes." *Ubiquity*, August 2000 [cited August 9 2002]. Available from http://www.acm.org/ubiquity/interviews/d_denning_1.html.

Diani, Mario. 2001. "Social movement networks: Virtual and real." In *Culture and politics in the information age : a new politics?*, edited by F. Webster. London ; New York: Routledge.

Dietrich, Joerg. 2003. *E-mail interview with author, part 1*, March 31.

"Digital Attacks Archive for WFD." 2004. *Zone-H*, 2004 [cited July 20 2004]. Available from http://www.zone-h.org/en/defacements/filter/filter_defacer=WFD/page=1/.

Doctor Nuker. 2004. "Site defacement." December 29 1999 [cited July 30 2004]. Available from **http://www.attrition.org/mirror/attrition/1999/12/29/www.allwithfaith.com**.

Dominguez, Ricardo. 2004. "Interview with Keith Sanborn." November 9 1996 [cited April 23 2004]. Available from http://rdom.thing.net/novrev96.04.html.

Dominguez, Ricardo. 2002a. *Interview with author*, May 28.

Dominguez, Ricardo. 2004. "Netsrike against the World Economic Fools meeting in NYC." January 25 2002b [cited July 15 2004]. Available from http://amsterdam.nettime.org/Lists-Archives/nettime-bold-0201/msg00509.html.

Dornseif, Max. 2003. *E-mail interview with author*, July 9.

Dugan, Sean M. 2003. "The war over a single letter." *InfoWorld*, January 7 2000 [cited May 9 2003]. Available from http://archive.infoworld.com/articles/op/xml/00/01/10/000110opprophet.xml.

"DVD CCA Complaint in DVD CCA v. McLaughlin, Bunner, et al." 2003. *Electronic Frontier Foundation*, 1999 [cited April 11 2003]. Available from http://www.eff.org/IP/Video/DVDCCA_case/19991228-complaint.html.

Eisley, Adam. 2003. *E-mail interview with author*, April 20.

electrohippies, the. 2004. "A response to criticism of dDoS actions online." 2003 [cited February 26 2004]. Available from http://www.thehacktivist.com/modules.php?op=modload&name=News&file=article&sid=174.

Electronic Disturbance Theater. 2004. "TELL THE WORLD: STOP THE WAR IN MEXICO: NETSTRIKE AGAINST GOVERNMENT, MILITARY, AND FINANCIAL WEB SITES IN MEXICO, THE UNITED STATES, AND GERMANY." August 25 1998 [cited July 13 2004]. Available from http://amsterdam.nettime.org/Lists-Archives/nettime-l-9808/msg00093.html.

Felten, Edward W. 2003. "Source Code and Object Code." *Freedom to Tinker*, 2002 [cited April 6 2003]. Available from http://www.freedom-to-tinker.com/archives/000035.html.

Festa, Paul. 2003. "Software rams great firewall of China." *CNET News.com*, April 16 2003 [cited April 23 2003]. Available from http://news.com.com/2100-1028-997101.html.

Finkel, S. E., and E. N. Muller. 1998. "Rational choice and the dynamics of collective political action: Evaluating alternative models with panel data." *American Political Science Review* 92 (1):37-49.

Fischer, Frank. 2001. *Citizens, Experts, and the Environment*. Durham: Duke University Press.

Friedman, Debra, and Doug McAdam. 1992. "Collective Identity and Activism: Networks, Choices, and the Life of a Social Movement." In *Frontiers in social movement theory*, edited by A. D. Morris and C. McClurg Mueller. New Haven: Yale University Press.

Froomkin, A. Michael. 1997. "The Internet As A Source of Regulatory Arbitrage." In *Borders in cyberspace : information policy and the global information infrastructure*, edited by B. Kahin. Cambridge, Mass.: MIT Press.

Froomkin, A. Michael. 2004. "Technologies for Democracy." In *Democracy Online: The Prospects for Democratic Renewal Through the Internet*, edited by P. Shane. London: Routledge.

fusco, coco. 2004. "Operacion Digna." October 31 2003 [cited July 15 2004]. Available from http://www.nettime.org/pipermail/nettime-ann/2003-October/000278.html.

Gadd, Chuck. 2003. "DeCSS Info/download page." [cited April 8 2003]. Available from http://www.csd.net/~cgadd/dvd.htm.

Galloway, Alex. 2002. *Interview with author*, October 16.

Ghosh, Shubha. 2003. "Source Code as Free Speech in Encryption Case." *GigaLaw*, May 2000 [cited April 11 2003]. Available from http://www.gigalaw.com/articles/2000-all/ghosh-2000-05-all.html.

Glave, James. 1999. "Ku Klux Klan Korrected." *Wired News*.

Goldhaber, Michael H. 1997. "The Attention Economy and the Net." *First Monday* 2 (4).

Goldstein, Samuel. 2003. *E-mail interview with author, part 1*, March 18.

Grandmaster Ratte. 2002. *Interview with author*, October.

Grether, Reinhold. 2003. "a new toy for you." December 3 1999 [cited May 12 2003]. Available from http://amsterdam.nettime.org/Lists-Archives/nettime-l-9912/msg00031.html.

Grether, Reinhold. 2003. "How the Etoy Campaign Was Won." *Telepolis*, February 26 2000 [cited May 12 2003]. Available from http://www.heise.de/tp/english/inhalt/te/5843/1.html.

Gross, Robin. 2003. "DeCSS Litigation Timeline." March 2 2003a [cited April 8 2003]. Available from http://ipjustice.org/decsstable.htm.

Gross, Robin. 2003b. *Telephone interview with author*, April 15.

Guerrero, Frank. 2003. *E-mail interview with author*, August 5.

Habermas, Jürgen. 1983. *Philosophical-political profiles*, *Studies in contemporary German social thought*. Cambridge, Mass.: MIT Press.

"Hacker culture." 2004. *Wikipedia*, July 11, 2004 [cited July 29 2004]. Available from http://en.wikipedia.org/wiki/Hacker_culture.

"Hackers stump site." 2001. *Sports Marketing*, April 18.

Hacktivismo. 2003. "Hacktivismo Projects." 2002 [cited April 21 2003]. Available from http://hacktivismo.com/projects/.

Hacktivismo, and Cult of the Dead Cow. 2003. "The Hacktivismo Declaration." July 4 2001 [cited April 21 2003]. Available from http://hacktivismo.com/about/declarations/en.php.

"The Hacktivismo FAQ v1.0." Available from http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html.

Halcli, Abigail. 1999. "AIDS, Anger, and Activism: ACT UP As a Social Movement Organization." In *Waves of protest : social movements since the sixties*, edited by J. Freeman and V. L. Johnson. Lanham, MD: Rowman & Littlefield Publishers.

Hale, Matthew, Juliet Musso, and Christopher Weare. 1999. "Developing digital democracy: evidence from Californian municipal web pages." In *Digital democracy : discourse and decision making in the Information Age*, edited by B. N. Hague and B. Loader. London ; New York: Routledge.

Hanninen, Sakari. 2003. "The Eternal Return of Politics." *Alternatives* 28 (2):287.

Hansen, John Mark. 1985. "The Political Economy of Group Membership." *The American Political Science Review* Vol. 79 (1):79-96.

Happy, Mr. 2002. *Interview with author*.

Harmon, Amy. 2000. "Free Speech Rights for Computer Code." *The New York Times*, July 31, C1.

Harrison, Ann. 2003. "Layers Inadvertently Release DVD Decryption Code." *Industry Standard*, January 27 2000 [cited April 11 2003]. Available from http://www.thestandard.com/article/display/0,1151,9221,00.html.

Haselton, Bennett. 2003. *Interview with author (telephone)*, April 29.

Hauben, Ronda. "From ARPANET to Usenet News: On the Nourishment of the Net Commonwealth." Available from http://neil.franklin.ch/Netizen/ch.4_Arpa2Usenet.

Hawkins, Darren. 2002. "Human Rights Norms and Networks in Authoritarian Chile." In *Restructuring world politics : transnational social movements, networks, and norms*, edited by S. Khagram, J. V. Riker and K. Sikkink. Minneapolis: University of Minnesota Press.

Hilden, Julie. 2002. "The Legal Debate Over Protecting Anonymous Speakers Online." *Gigalaw.com*, 2001 [cited November 19 2002]. Available from http://www.gigalaw.com/articles/2001-all/hilden-2001-02-all.html.

Hirschman, Albert O. 1982. *Shifting involvements : private interest and public action.* Princeton, N.J.: Princeton University Press.

Hirsh, Jesse. 2002. *Interview with author*, September 11.

Hocevar, Sam. 2003. *E-mail interview with author*, March 17.

Hogg, Michael A., and Barbara-A. Mullin. 1999. "Joining Groups to Reduce Uncertainty: Subjective uncertainty reduction and group identification." In *Social identity and social cognition*, edited by D. Abrams and M. A. Hogg. Oxford ; Malden, Mass.: Blackwell.

Horowitz, Ellen. 2001. "Who's afraid of the virtual goons?" March 18.

"http://listserv.gao.gov COMPROMISED." 2002. 2001 [cited July 20 2002]. Available from http://www.safemode.org/mirror/2001/12/09/ftp.gao.gov/mirror.html.

Huddy, L. 2001. "From social to political identity: A critical examination of social identity theory." *Political Psychology* 22 (1):127-156.

"Humpin.org: King of the Road." *Humpin.org*. Available from http://www.humpin.org.

Huschle, Brian J. 2002. "Cyber Disobedience: When is Hacktivism Civil Disobedience?" *International Journal of Applied Philosophy* 16 (1):69-83.

"India Cracked interview with WFD." 2004. May 24 2001 [cited July 20 2004]. Available from http://www.srijith.net/indiacracked/interviews/wfd.shtml.

"Interview with World's Fantabulous Defacers." 2004. *Domina Security*, [cited February 20 2004]. Available from http://www.dominasecurity.com/hackerz/wfd.htm.

Isenberg, Doug. 2004. "High-Tech TV Recording, the Internet and the Law." *GigaLaw.com*, November 2001 [cited March 4 2004]. Available from http://www.gigalaw.com/articles/2001-all/isenberg-2001-11-all.html.

Joachim, Jutta. 2002. "Comparing the Influence of NGOs in Transnational Institutions: the UN, the EU and the Case of Gender Violence". Paper read at *3rd Annual Convention of the International Studies Association*, March 24 – 27, at New Orleans.

"Jon Johansen Court Decision." 2003. January 7 2003 [cited April 10 2003]. Available from http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20030109_johansen_decision.html.

"Jon Johansen's Answers to Your DeCSS Questions." 2004. *slashdot*, February 4 2000 [cited February 20 2004]. Available from http://slashdot.org/interviews/00/02/04/1133241.shtml.

Jones, Flint. 2001. "AKA (Was: Re: Hactivism comments by EFF)." *hacktivism.ca listserv*, October 12 1999a [cited July 2001].

Jones, Flint. 2001. "Archiving..." *hacktivism.ca listserv*, August 27 1999b [cited July 2001].

Jones, Tony, and Suzanne Smith. 2002. "Internet activism changes face of protest movement." *Australian Broadcasting Corporation*.

Jordan, Tim. 2002. *Activism! : direct action, hactivism and the future of society*. London: Reaktion Books.

Jordan, Tim, and Paul A. Taylor. 2004. *Hacktivism: informational politics for informational times*: Routledge.

Jules. 2002. *Interview with author*, December.

Kalathil, Shanthi, and Taylor C. Boas. 2003. *Open networks, closed regimes : the impact of the Internet on authoritarian rule*. Washington, D.C.: Carnegie Endowment for International Peace.

Kaplan, Carl. 2004. "For Their Civil Disobedience, the 'Sit-In' Is Virtual." *The New York Times CyberLaw Journal*, May 1 1998 [cited July 13 2004]. Available from http://www.nytimes.com/library/tech/98/05/cyber/cyberlaw/01law.html.

Kaplan, Lewis A. 2003. "Memorandum Opinion in Universal City Studios et al. v. Shawn C. Reimerdes et al." *Electronic Frontier Foundation*, February 2 2000 [cited April 11 2003].

Karam, William. "Hacktivism: Is Hacktivism Civil Disobedience?"

Karasic, Carmin. 2002. *Interview with author*, October 23.

Katz, J.E., and P. Aspden. 1997. "A nation of strangers?" *Communications of the ACM* 40:81-86.

Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists beyond borders : advocacy networks in international politics*. Ithaca, N.Y.: Cornell University Press.

Kelly, C. 1988. "Intergroup differentiation in a political context." *British Journal of Social Psychology* 27:319-332.

Kettmann, Steve. 2003. "Etoy: 'This Means toywar.com!'" *Wired News*, January 17 2000 [cited May 12 2003]. Available from http://www.wired.com/news/politics/0,1283,33711,00.html.

Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink. 2002a. "From Santiago to Seattle: Transnational Advocacy Groups Restructuring World Politics." In *Restructuring world politics : transnational social movements, networks, and norms*, edited by S. Khagram, J. V. Riker and K. Sikkink. Minneapolis: University of Minnesota Press.

Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink. 2002b. *Restructuring world politics : transnational social movements, networks, and norms*, *Social movements, protest, and contention ; v. 14*. Minneapolis: University of Minnesota Press.

Khan, Ayub. 2004. "Pro-Palestinian Hackers Strike Again." *IslamOnline.net*, May 16 2001 [cited July 22 2004]. Available from http://www.islamonline.net/english/news/2001-05/17/article4.shtml.

Klandermans, Bert, and Marga de Weerd. 2000. "Group Identification and Political Protest." In *Self, identity, and social movements*, edited by S. Stryker, T. J. Owens and R. W. White. Minneapolis: University of Minnesota Press.

Klein, Naomi. 2000. *No Logo*. Toronto: Vintage Canada.

Knoke, David. 1988. "Incentives in Collective Action Organizations." *American Sociological Review* 53 (3):311-329.

Knoke, David, and James R. Wood. 1981. *Organized for action : commitment in voluntary associations*. New Brunswick, N.J.: Rutgers University Press.

Kreider, Aaron. 2003. *IRC Interview with author*, February 13.

La Canna, Xavier. 2004. "The hacker battle for cyberspace." *The Age*, May 8 2001 [cited April 22 2004]. Available from http://www.theage.com.au/news/2001/05/08/FFXM5SNJGMC.html.

Legler, Thomas. 2000. "Transnational Coalition-Building in the Americas: The Case of the Hemispheric Social Alliance". Paper read at *Building the New Agenda: Hemispheric Integration and Social Cohesion*, July, at Robarts Centre for Canadian Studies, York University, Toronto.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. 2004. "A Brief History of the Internet." *Internet Society*, December 10, 2003 2003 [cited July 29 2004]. Available from http://www.isoc.org/internet/history/brief.shtml.

Lemos, Robert. 2002. "Hackers split over vigilante strikes." *ZDNet*, September 14 2001 [cited August 20 2002]. Available from http://news.zdnet.co.uk/story/0,,t269-s2095342,00.html.

Leonard, Andrew. 2003. "Toys were us." *Salon*, March 4 2003 [cited May 12 2003]. Available from http://www.salon.com/tech/feature/2003/03/04/toys/print.html.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Penguin Books.

Lewis, Tammy L. 2002. "Conservation TSMOs: Shaping the Protected Area Systems of Less Developed Countries." In *Globalization and resistance : transnational dimensions of social movements*, edited by H. Johnston. Lanham, Md.: Rowman & Littlefield.

Liikanen, Erkki. 2002. *Attacks against information systems press conference*, April 23.

Liikanen, Erkki. 2003. *The European Network and Information Security Agency Press Conference*, February 10.

Liikanen, Erkki. 2004. *European Network Security*, March 18.

"LoU STRIKE OUT WITH INTERNATIONAL COALITION OF HACKERS: A JOINT STATEMENT BY 2600, THE CHAOS COMPUTER CLUB, THE CULT OF THE DEADCOW, !HISPAHACK, L0PHT HEAVY INDUSTRIES, PHRACK AND PULHA." 2002. 1999 [cited October 7 2002]. Available from http://www.ccc.de/CRD/CRD19990107.html.

LuNaTiK. 2003. "An Open Letter to the DVD Copy Control Association." [cited April 9 2003]. Available from http://members.cox.net/hayai2/rant.html.

m0r0n, and nightman. 2002. *E-mail interview with author*, October 20.

m0r0n and nightman. 2004. "Defacement of www.ann-arbor.med.va.gov." December 16 2000a [cited July 24 2004]. Available from http://www.attrition.org/mirror/attrition/2000/12/16/www.ann-arbor.med.va.gov/.

m0r0n and nightman. 2004. "Mass defacement." December 23, 2000 2000b [cited July 23 2004]. Available from http://www.hagai.com/owned.asp.

m0r0n and nightman. 2004. "Site defacement." September 23 2000c [cited July 25 2004]. Available from http://www.attrition.org/mirror/attrition/2000/09/23/portal.buerger.net/.

MacMillan, Robert. 2002. "Electrohippies Claim Online WTO Protest A Success." *Newsbytes*, December 3 1999 [cited October 5 2002]. Available from http://exn.ca/Stories/1999/12/03/03.asp.

Malina, Anna. 1999. "Perspectives on citizen democratisation and alienation in the virtual public sphere." In *Digital democracy : discourse and decision making in the Information Age*, edited by B. N. Hague and B. Loader. London ; New York: Routledge.

Maney, Gregory M. 2002. "Transnational structures and protest: Linking theories and assessing evidence." In *Globalization and resistance : transnational dimensions of social movements*, edited by J. G. Smith and H. Johnston. Lanham, Md.: Rowman & Littlefield.

Manion, Mark, and Abby Goodrum. 2000. "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." *Computers and Society*.

Marx, Gary T. 2001. "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research." In *Documenting Individual Identity*, edited by J. Caplan and J. Torpey. Princeton: Princeton University Press.

McAdam, D., and R. Paulsen. 1993. "Specifying the Relationship Between Social Ties and Activism." *American Journal of Sociology* 99 (3):640-667.

McAdam, Doug. 1983. "Tactical Innovation and the Pace of Insurgency." *American Sociological Review* 48 (6):735-754.

McAdam, Doug, John D. McCarthy, and Mayer N. Zald. 1996. "Introduction: Opportunities, mobilizing structures, and framing processes - toward a synthetic, comparative perspective on social movements." In *Comparative perspectives on social movements: political opportunities, mobilizing structures, and cultural framings*, edited by D. McAdam, J. D. McCarthy and M. N. Zald.

McAdam, Doug, Sidney Tarrow, and Charles Tilly. 2001. *Dynamics of Contention.* Cambridge: Cambridge University Press.

McCullagh, Declan. 2003. "A Constitutional Right to Decode?" *Wired News*, 2001 [cited April 6 2003]. Available from http://www.wired.com/news/digiwood/0,1412,44183,00.html.

McDonald, Tim. 2001. "Hackers Invade World Economic Forum." *NewsFactor Network*, February 5.

"McIntyre v. Ohio Campaign Commission. 1995. Supreme Court of the United States.

McWilliams, Brian. 2002. "Anti-Terror Hackers Seek Govt Blessing." *Newsbytes*, October 17 2001a [cited August 20 2002]. Available from http://www.infowar.com/hacker/01/hack_101701b_j.shtml.

McWilliams, Brian. 2002. "'Mujihadeen' hackers take out US government sites." *Newsbytes*, 2001b [cited August 20 2002]. Available from http://www.computeruser.com/news/01/12/03/news1.html.

McWilliams, Brian. 2002. "Pro-Bin Laden Pakistani Hacker Defaces World Trade Site." *NewsBytes*, September 19 2001c [cited August 20 2002]. Available from http://www.pcmag.com/article2/0,4149,27903,00.asp.

McWilliams, Brian. 2002. "A TV Plea to Patriot Hackers." *Wired News*, 2001d [cited August 20 2002]. Available from http://www.wired.com/news/print/0,1294,47099,00.html.

Me Uh K. 2001. "Re: unitedskins.com ~ It's about time." *hacktivism.ca listserv*, November 16 1999 [cited July 2001].

metac0m. 2002. *Interview with author*, September.

Michaels-Ober, Erik. 2003. *E-mail interview with author*, March 22.

Mike. 27-Aug-99. "Re: No power without brain.... hacktivism.ca listserv.

Mildham, John. 2003. *E-mail interview with author*, March 20.

Miller, Cameron. 2003. *E-mail interview with author*, April 7.

Milone, Mark G. 2002. "Hacktivism: Securing the National Infrastructure." *The Business Lawyer* 58 (1).

Mixter. 2003. "Facts about the ddos incident." 2002a [cited April 22 2003]. Available from http://mixter.void.ru/about.html.

Mixter. 2002b. *Interview with author*.

Mizrach, Steven. 2002. "Is there a Hacker Ethic for 90s Hackers?" [cited October 7 2002]. Available from http://www.fiu.edu/~mizrachs/hackethic.html.

Mobbs, Paul. 2003. *E-mail interview with author*, July 12.

Moe, Terry M. 1981. "Toward a Broader View of Interest Groups." *The Journal of Politics* 43 (2):531-543.

Money, Ca$h. 2002. *Interview with author*.

Morris, Douglas. 2002. "Globalization and Media Democracy: The Case of Indymedia". Paper read at *Global Congress on Community Networking in the Digital Era*, October 7-12.

Morris, Stan. 2003. "The Tension Between Free Speech and Copyright." *GigaLaw*, November 2000 [cited April 11 2003]. Available from http://www.gigalaw.com/articles/2000-all/morris-2000-11-all.html.

Mouffe, Chantal. 1999. "Deliberative Democracy or Agaonistic Pluralism?" *Social Research* 66 (3):745-758.

Mr. Happy. 2002. *Interview with author*.

Murphy, Kevin. 2001. "Internet Used for Terror Retaliation, but Hackers Disagree." *ComputerWire*.

Murphy, Matthew. 2003. *E-mail interview with author*, July 17, 2003.

National Infrastructure Protection Center. 2001. "Cyber Protests: The Threat to the U.S. Information Infrastructure.

Nguyen, Maria. 2002. "Armchair activism." *Sydney Morning Herald*, August 16.

Nickel, James W. 2000. "Free Speech, Democratic Deliberation, and Valuing Types of Speech." In *Deliberation, democracy, and the media*, edited by S. Chambers and A. N. Costain. Lanham: Rowman & Littlefield Publishers.

Norris, Pippa. 2001. *Digital divide: civic engagement, information poverty, and the Internet worldwide*, *Communication, society, and politics*. Cambridge ; New York: Cambridge University Press.

"Norwegian Teenager Jon Johansen Acquitted in DVD Case." 2003. *Electronic Frontier Foundation*, January 7 2003 [cited May 12 2003]. Available from http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20030107_eff_pr.html.

Nuker, Doctor. 2004. "All With Faith Hacked by Doctor Nuker." 1999a [cited February 21 2004]. Available from http://www.attrition.org/mirror/attrition/1999/12/29/www.allwithfaith.com/.

Nuker, Doctor. 2004. "Vancouver Hospital and Health Sciences Centre Hacked by Doctor Nuker." 1999b [cited February 21 2004]. Available from http://www.attrition.org/mirror/attrition/1999/10/09/www.vanhosp.bc.ca/.

Olson, Mancur, Jr. 1965. *The Logic of Collective Action*. Cambridge: Harvard University Press.

Optiklenz. 1998. "Defunct Internet Protocol." *Keen Veracity*, December.

Paadeluun. 2003. *Interview with author*, January 13.

Patrizio, Andy. 2003. "Why the DVD Hack Was a Cinch." *Wired News*, November 2 1999 [cited April 9 2003]. Available from http://www.wired.com/news/technology/0,1282,32263,00.html.

Perera, Rick. 2002. "Hacker cracks Islamist mailing list." *IDG.Net*, September 18 2001 [cited August 20 2002]. Available from http://www.idg.net/spc_695978_190_9-10025.html.

<pete@tao.ca>, pete. 10/10/99. "Re: Let's get to work: hacktivism.ca listserv.

Pickerill, Jenny. 2001. "Weaving a Green Web: Environmentla protest and computer-mediated communication in Britain." In *Culture and politics in the information age : a new politics?*, edited by F. Webster. London ; New York: Routledge.

Poster, Mark. 2002. "CyberDemocracy: Internet and the Public Sphere." 1995 [cited November 22 2002]. Available from http://www.hnet.uci.edu/mposter/writings/democ.html.

Prasad, Srinivasa. 2002. "We are the United Nations of Hacking." *Hindustani Times*, November 10.

Priestley, Robin. 2003. *E-mail interview with author*, July 12.

"Pro-Islamic Hacker Groups Joining Forces Globally." 2004. *Content-Wire*, June 18 2002 [cited July 25 2004]. Available from http://www.content-wire.com/FreshPicks/Index.cfm?ccs=86&cs=1946.

"Proposal for a Council Framework Decision on attacks against information systems. 2002.

Putnam, Robert D. 2000. *Bowling alone : the collapse and revival of American community*. New York: Simon & Schuster.

Ramasastry, Anita. 2004. "The Law and Politics of Internet Activism." *FindLaw*, June 5 2002 [cited April 22 2004]. Available from http://writ.news.findlaw.com/ramasastry/20020605.html.

Raymond, Eric Steven. 2004. "A Brief History of Hackerdom." August 25 2000 [cited July 29 2004]. Available from http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/.

Reid, Elizabeth. 1996. "Communication and Community on Internet Relay Chat: Constructing Conmmunities." In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by P. Ludlow. Cambridge: MIT Press.

Reid, Jamie. 2003. *E-mail interview with author*, July 10.

Reimann, Kim D. 2002. "Building networks from the outside in: Japanese NGOs and the Kyoto Climate Change Conference." In *Globalization and resistance : transnational dimensions of social movements*, edited by H. Johnston. Lanham, Md.: Rowman & Littlefield.

Reporters Without Borders. 2003. "The Enemies of the Internet." 1999 [cited April 21 2003]. Available from http://www.rsf.org/rsf/uk/html/internet/ennemis.html.

"Reverse Engineering." 2003. *Chilling Effects*, [cited April 10 2003]. Available from http://www.chillingeffects.org/reverse/.

Riemens, Patrice. 2004. "Re: <nettime> Hackers: the political heroes of cyberspace + URL target for NeTstrike." 2001 [cited February 26 2004]. Available from http://amsterdam.nettime.org/Lists-Archives/nettime-l-0103/msg00074.html.

Riemens, Patrice. 2003. *E-mail/mail interview with author*, April 18.

Risse, Thomas, and Kathryn Sikkink. 1999. "The socialization of international human rights norms into domestic practices: introduction." In *The power of human rights : international norms and domestic change*, edited by K. Sikkink. Cambridge: Cambridge University Press.

Ronfeldt, David, John Arguilla, Graham E. Fuller, and Melissa Fuller. 1998. "The Zapatista Social Netwar in Mexico: Rand Arroyo Center.

Ruffin, Oxblood. 2002. *Interview with author*, September 4.

Ruffin, Oxblood. 2003. "Telephone conversation with author." 2003 [cited April 2003].

Ruffin, Oxblood. 2004a. *E-mail to author*, July 26.

Ruffin, Oxblood. 2004. "Hacktivism, From Here to There." March 28 2004b [cited July 16 2004]. Available from http://islandia.law.yale.edu/isp/digital%20cops/papers/ruffin_hacktivism.pdf.

Saco, Diana. 2002. *Cybering Democracy: Public Space and the Internet*. Minneapolis: University of Minnesota Press.

Salisbury, Robert H. 1969. "An Exchange Theory of Interest Groups." *Midwest Journal of Political Science* 13 (1):1-32.

sam. 2001. "successfully echelonised." *hacktivism.ca listserv*, September 27 1999 [cited July 2001].

Samuel, Alexandra. 2001. "Digital Disobedience: Hacktivism in Political Context". Paper read at *American Political Science Association Annual Meetings*, at San Francisco.

Sandberg, Anders. 2003a. *E-mail interview with author, part 1*, March 21.

Sandberg, Anders. 2003b. *E-mail interview with author, part 2*, April 7.

Schlozman, K. L., S. Verba, and H. E. Brady. 1995. "Participation is Not a Paradox - the View From American Activists." *British Journal of Political Science* 25:1-36.

Schmitz, Hans Peter. 1999. "Transnational activism and political change in Kenya and Uganda." In *The power of human rights : international norms and domestic change*, edited by T. Risse, S. C. Ropp and K. Sikkink. Cambridge: Cambridge University Press.

Schrepfer, Jeff. 2003. *E-mail interview with author, part 1*, March 17.

Schuessler, Alexander A. 2000. *A logic of expressive choice*. Princeton, N.J.: Princeton University Press.

Schwartau, Winn. 2002. "Cyber-civil disobedience." 01/11/99 1999 [cited 5/24 2002]. Available from http://www.nwfusion.com/news/0111vigcyber.html.

Schwartau, Winn. 2004. "Can you counter-attack hackers?" *CNN.com*, April 7 2000 [cited April 22 2004]. Available from http://www.cnn.com/2000/TECH/computing/04/07/self-defense.idg/.

scotartt. 2001. "Re: unitedskins.com ~ It's about time." *hacktivism.ca listserv*, November 16 1999 [cited July 2001].

Sebok, Anthony J. 2004. "The Strange Paradox of RTMark." *FindLaw*, November 19 2001 [cited April 22 2004]. Available from http://writ.news.findlaw.com/sebok/20011119.html.

Seyd, Patrick, and Paul Whiteley. 1992. *Labour's grassroots : the politics of party membership*. Oxford; New York: Clarendon Press ; Oxford University Press.

Shabelman, David. 2002. "eToys details liquidation plan." *The Daily Deal*, August 27.

Simons, Barbara. 2000. "To DVD or Not to DVD." *Communications of the ACM* 43 (5).

"Site defacement, US Dept. of Justice." 2004. August 18 1996 [cited July 30 2004]. Available from http://www.attrition.org/mirror/attrition/1996/08/18/www.doj.gov.

Skala, Matthew. 2004. "First Nations of the Internet." August 1, 1996 [cited July 29 2004]. Available from http://ansuz.sooke.bc.ca/vipirg.html.

Smith, Jackie G., and Hank Johnston. 2002. "Globalization and resistance : An Introduction." In *Globalization and resistance : transnational dimensions of social movements*, edited by J. G. Smith and H. Johnston. Lanham, Md.: Rowman & Littlefield.

Smith, Janna Malamud. 1997. *Private matters : in defense of the personal life*. Reading, Mass.: Addison-Wesley Pub.

Smith, Peter Jay, and Elizabeth Smythe. 2001. "Globalization, citizenship and technology: The Multilateral Agreement on Investment (MAI) meets the Internet." In *Culture and politics in the information age : a new politics?*, edited by F. Webster. London ; New York: Routledge.

Smithers, Captain. 2003. "Toywar Story." [cited May 9 2003]. Available from http://www.toywar.co.uk/.

Snow, David A., and Doug McAdam. 2000. "Identity Work Processes in the Context of Social Movements: Clarifying the Identity/Movement Nexus." In *Self, identity, and social movements*, edited by S. Stryker, T. J. Owens and R. W. White. Minneapolis: University of Minnesota Press.

"Source Code." 2003. *Webpedia*, 1996 [cited April 6 2003]. Available from http://www.webopedia.com/TERM/S/source_code.html.

Sperling, Valerie, Myra Marx Ferree, and Barbara Risman. 2001. "Constructing Global Feminism: Transnational Advocacy Networks and Russian Women's Activism." *Signs: Journal of Women in Culture and Society* 26 (4):1155-86.

Sproull, Lee, and Sara B. Kiesler. 1991. *Connections : new ways of working in the networked organization*. Cambridge, Mass.: MIT Press.

"SSL Certificate Encryption Strength." 2003. *WhichSSL.org*, 2003 [cited May 12 2003]. Available from http://www.whichssl.org/content/strength.html.

"State Control of the Internet in China." 2003. *Amnesty International*, November 26 2002 [cited April 22 2003]. Available from

http://web.amnesty.org/library/Index/engasa170072002?OpenDocument&of=COUNTRIES\CHINA?OpenDocument&of=COUNTRIES\CHINA.

Sterling, Bruce. 1993. "A Short History of the Internet." *The Magazine of Fantasy and Science Fiction*, February.

Steve. 2003. *E-mail interview with author*, April 18.

Stevenson, Frank. 2003. *E-mail interview with author, part 1*, March 20.

Stevenson, Frank A. 2003. "Cryptanalysis of Contents Scrambling System." November 13 1999 [cited April 9 2003]. Available from http://freedom.gmsociety.org/extra/decss/.

Stevenson, Frank A. 2003. "Declaration in DVD CCA v. McLaughlin, Bunner, et al." *Electronic Frontier Foundation*, January 7 2000 [cited April 10 2003]. Available from http://www.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-stevensondec.html.

stonefisk. 2004. "Camera/Shy demo." July 7 2002 [cited August 1 2004]. Available from http://www.houseofdotcommons.com/~zardi/test3.html.

Streck, John M. 1998. "Pulling the Plug on Electronic Town Meetings: Participatory Democracy and the Reality of the Usenet." In *The Politics of Cyberspace*, edited by C. Toulouse and T. W. Luke. London: Routledge.

Stryker, S., and P. J. Burke. 2000. "The past, present, and future of an identity theory." *Social Psychology Quarterly* 63 (4):284-297.

Stryker, Sheldon, and R. Serpe. 1994. "Identity salience and psychological centrality: Equivalent, overlapping, or complementary concepts?" *Social Psychology Quarterly* 57:16-35.

Taggart, Will. 2004. "The Digital Revolt: Resistance & Agency on the Net." *Working Papers on New Media and Information Technology in the Middle East (NMIT)*, June 2001 [cited July 20 2004]. Available from http://nmit.georgetown.edu/papers/wtaggert.htm.

Tajfel, Henri. 1981. *Human groups and social categories : studies in social psychology*. Cambridge; New York: Cambridge University Press.

Tangens, Rena. 2003. *Interview with author*, January 13.

Tarrow, Didney. 1994. *Power in Movement: Social Movements, Collective Action and Mass Politics in the Modern State*. Cambridge: Cambridge University Press.

Tarrow, S. 2002. "The New Transnational Contention: Organizations, Coalitions, Mechanisms". Paper read at *American Political Science Assoication Annual Meeting*, September 1, at Boston, MA.

Taylor, Paul A. 2001. "Editorial: Hacktivism." *The Semiotic Review of Books* 12 (1).

"Terms of Use." 2003. *The Mr. Brown Network*, 2000 [cited April 6 2003]. Available from http://www.mrbrown.net/decss/.

thepull. 2004. "In Condemnation of Electrohippies Defense of DDoS'n for Censorship." *Hacktivismo*, April 2 2002 [cited February 20 2004]. Available from http://hacktivismo.com/news/modules.php?name=News&file=article&sid=1152.

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

Thornton, Alinta. 2002. "Does Internet Create Democracy." 2002 [cited November 21 2002]. Available from http://www.zip.com.au/~athornto//thesis_2002_alinta_thornton.doc.

Tilly, Charles. 1978. *From Mobilization to Revolution*. Reading, MA: Addison-Wesley Publishing Co.

"Timeshift: The World in Twenty-Five Years." 2004. *Ars Electronica*, 2004 [cited July 13 2004]. Available from http://www.aec.at/en/festival/first_statement_2004.asp.

"To develop and deploy technologies to defeat Internet jamming and censorship. 2003." IU.S. Congress. *HR 48 IH*.

Touretzky, Dave. 2003. "Declaration in Universal et al. v. Reimerdes et al." 2000a [cited April 6 2003]. Available from http://www-2.cs.cmu.edu/~dst/DeCSS/touretzky-decl.html.

Touretzky, Dave. 2003. "Gallery of CSS Descramblers." April 3 2000b [cited April 6 2003]. Available from http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/index.html.

Touretzky, Dave. 2003. "Steganography Wing of the Gallery of CSS Descramblers." September 6 2000c [cited April 6 2003]. Available from http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html.

Touretzky, Dave. 2003a. *E-mail interview with author, part 2*, March 18.

Touretzky, Dave. 2003b. *E-mail interview with author, part 3*, March 20.

"Toy retailing -- Trouble in toy town?" 2000. *Retail Week*, February 18, 12.

Traugott, Mark. 1995. "Recurrent Patterns of Collective Action." In *Repertoires and Cycles of Collective Action*, edited by M. Traugott. Durham, NC: Duke University Press.

Vegh, Sandor. 2003. "Hacking for Democracy: A Study of the Internet as a Political Force and Its Representation in the Mainstream Media, American Studies, University of Maryland, College Park.

Verba, Sidney, Norman H. Nie, and Jae-on Kim. 1978. *Participation and political equality : a seven-nation comparison*. Cambridge, Eng. ; New York: Cambridge University Press.

Verba, Sidney, Kay Lehman Schlozman, and Henry E. Brady. 1995. *Voice and equality : civic voluntarism in American politics*. Cambridge, Mass.: Harvard University Press.

Vescio, Theresa K., Miles Hewstone, Richard J. Crisp, and J. Mark Rubin. 1999. "Perceiving and Responding to Multiply Categorizable Individuals: Cognitive Processes and Affective Intergroup Bias." In *Social identity and social cognition*, edited by D. Abrams and M. A. Hogg. Oxford ; Malden, Mass.: Blackwell.

Vitorino, António. 2002. *Speaking points by European Commissioner for Justice and Home Affairs Commission proposal for a framework decision on attacks against information systems Press conference*, April 23.

Waxer, Cindy. 2000. "First.com, First Served?" *Business 2.0*, March.

Weisman, Robyn. 2001. "Palestinian Hacktivism and Viruses Collide." *NewsFactor Network*, March 20.

WFD. 2004. "Site defacement." November 19 2000a [cited July 25 2004]. Available from http://www.attrition.org/mirror/attrition/2000/11/19/www.oem.com.mx/.

WFD. 2004. "Site defacement." November 28, 2000 2000b [cited July 24 2004]. Available from http://www.attrition.org/mirror/attrition/2000/11/28/oxygen.mse.arizona.edu/.

WFD. 2004. "Site defacement." February 23, 2001 2001 [cited July 25 2004]. Available from http://www.attrition.org/mirror/attrition/2001/02/23/wwwnt.cnet.navy.mil/mirror.html.

"What is Open Source." 2003. *redhat*, [cited April 9 2003]. Available from http://www.redhat.com/about/mission/opensource/whatis_os/.

White, Louise G. 1976. "Rational Theories of Participation: An Exercise in Definitions." *The Journal of Conflict Resolution* 20 (2):255-278.

Whitman, Jason. 2003. "Protecting your online brand." *bigfatsite.com*, August 7 2000 [cited May 9 2003]. Available from http://www.bigfatsite.com/_articles_/2000-08-07-1.html.

"Why is this page black?" 2003. *Yahoo*, 1996 [cited April 21 2003]. Available from http://xarch.tu-graz.ac.at/speech.html.

Wilhelm, Anthony G. 2000. *Democracy in the Digital Age : challenges to political life in cyberspace*. New York: Routledge.

"Will hackers keep the cyberpeace?" 2001. *Reuters*, November 16 2001 [cited November 20 2001]. Available from http://www.zdnet.com/ndnn/stories/news/0,4586,2825353,00.html?chkpt=zdnnp1tp02.

Witschge, Tamara. 2004. "Online Deliberation: Possibilities of the Internet for Deliberative Democracy." In *Democracy Online: The Prospects for Democratic Renewal Through the Internet*, edited by P. Shane. London: Routledge.

Wood, Ellen Meiksins. 1995. "What is the `postmodern' agenda? An introduction." 47 (3):1.

Wray, Stefan. 2004. "The Electronic Disturbance Theater and Electronic Civil Disobedience." June 17 1998 [cited April 23 2004]. Available from http://www.thing.net/~rdom/ecd/EDTECD.html.

Wray, Stefan. 1999a. "Electronic Civil Disobedience and the World Wide Web of Hactivism." *SWITCH* 4 (2).

Wray, Stefan. 2004. "floodnet: the NSA show." 1999b [cited July 8 2004]. Available from http://www.thing.net/~rdom/ecd/nsa_show1.html.

xdaydreamx. 30-Aug-99. "Re: Re: Timorese 'hacktivists' warn of revenge: hacktivism.ca listserv.

xdaydreamx. 2001. *hacktivism.ca listserv*, August 27 1999 [cited July 2001].

Ziegler, Henning. 2003. "Etoy: Playing with the Corporate Giant." [cited May 9 2003]. Available from http://www.netzwissenschaft.de/media/ziegler.rtf.