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.

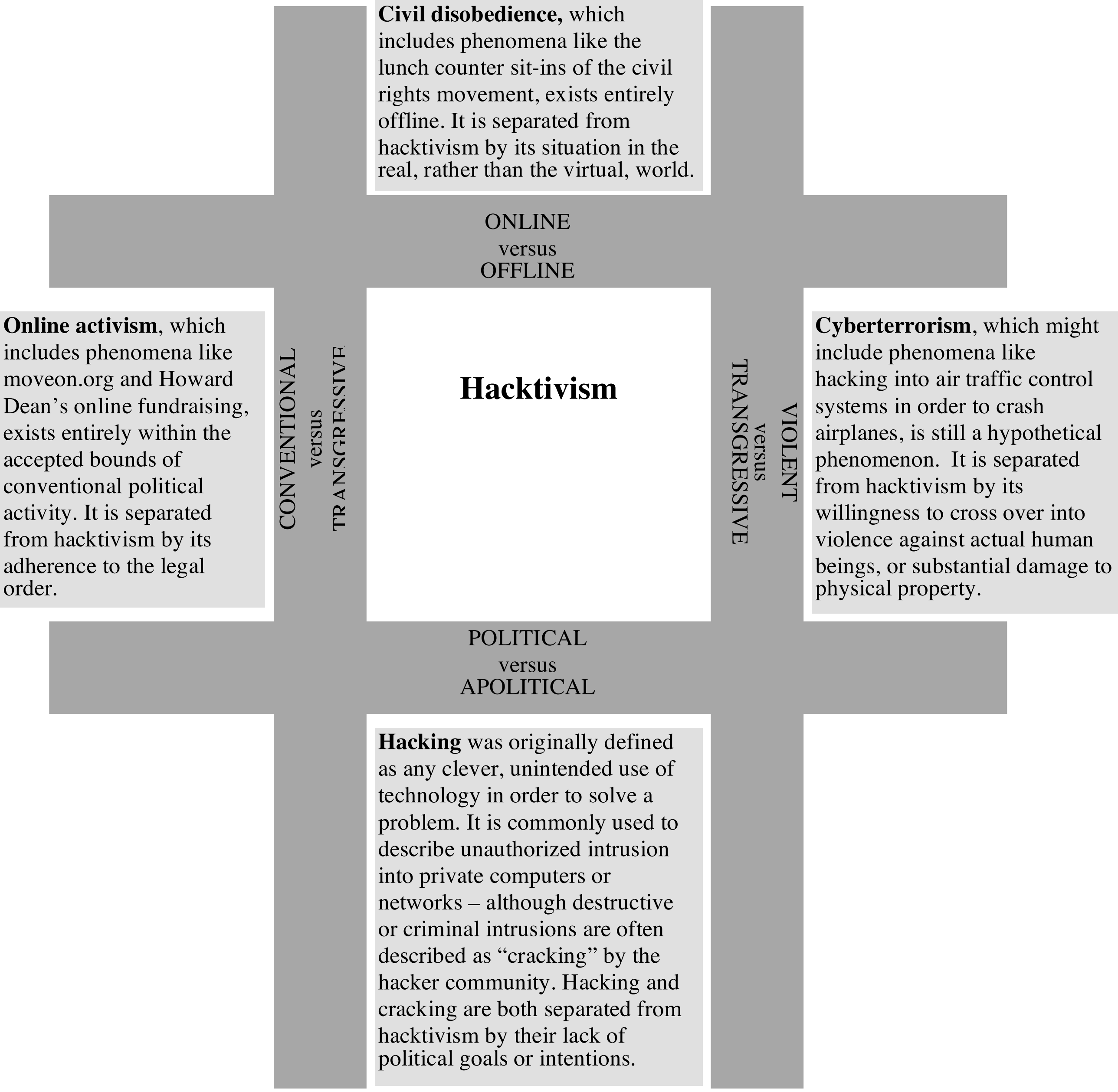
This dissertation is the first empirical study of hacktivism and the people who engage in it. It is based on three years of research, including online and face-to-face interviews with more than fifty people who are directly or indirectly involved in hacktivist activities. While not all of these interview 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.



Civil disobedience, which includes phenomena like the lunch counter sit-ins of the civil rights movement, exists entirely offline. It is separated from hacktivism by its situation in the real, rather than the virtual, world.

Online activism, which includes phenomena like moveon.org and Howard Dean's online fundraising, exists entirely within the accepted bounds of conventional political activity. It is separated from hacktivism by its adherence to the legal order.

Cyberterrorism, which might include phenomena like hacking into air traffic control systems in order to crash airplanes, is still a hypothetical phenomenon. It is separated from hacktivism by its willingness to cross over into violence against actual human beings, or substantial damage to physical property.

Hacking was originally defined as any clever, unintended use of technology in order to solve a problem. It is commonly used to describe unauthorized intrusion into private computers or networks – although destructive or criminal intrusions are often described as "cracking" by the hacker community. Hacking and cracking are both separated from hacktivism by their lack of political goals or intentions.

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			
		Ch. 2: Taxonomy	Ch. 3: Identity incentives	Ch. 4: Policy circumvention	Ch. 5 Deliberative Democracy
Interconnecting Themes	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.**