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.