Sauter, Molly. "Blockades and blockages: DDoS as direct action." *The Coming Swarm: DDoS Actions, Hactivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic, 2014. 39–57. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781628926705.0008>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 11:19 UTC.

Copyright © Molly Sauter 2014. You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

CHAPTER TWO

Blockades and blockages: DDoS as direct action

In late November 1999, the World Trade Organization (WTO) held its Ministerial Conference in Seattle, Washington. The city streets were filled with protesters opposed to the WTO's procorporate globalization agenda. A number of different activist organizations were involved, and a variety of tactics were employed, running the gamut from peaceful permitted street marches, puppets and colorful costumes (including a plethora of activists dressed up as sea turtles) to the Black Bloc's highly confrontational campaign of corporate property destruction. Popularly known as the Battle for Seattle, the coming together of so many different activist groups coupled with the aggressive response of police and city officials helped make the 1999 WTO protests into a defining moment for the anticorporate globalization movement.

While the sea turtles were marching in the streets of Seattle, a British organization called *the electrohippies* waged a simultaneous online action against the WTO. From November 30 through December 4, *the electrohippies* organized and staged a combination DDoS/e-mail bombing campaign targeting the WTO's main conference servers, public-facing websites, as well as various individuals associated with the WTO, including PR and operations staff, and various state representatives.

The DDoS section of the action used a Javascript tool, based on an open source tool developed by the EDT in 1998. Technological limitations required that participants be connected to the internet with the tool, available at *the electrohippies* webpage, downloaded and running for the duration of their participation. Representatives of the group claimed that over the course of the action, over 450,000 people participated in the action, with the targeted sites experiencing sporadic downtime and service slowdowns. The extent to which the DDoS action affected the functioning of the WTO websites and conference network is disputed. The goal of the DDoS action, stated in the calls to action distributed on various mailing lists and on its website, was to hamper the PR efforts of the conference:

[T]he electrohippies are organising a “virtual sit-in” of the WTO’s special conference website. It is intended that this website will be the main conduit for accessing information about the conference, and the events taking place. By taking action against the conference server and the main WTO server, we restrict the PR staff at the WTO from spreading their global corporate agenda.¹

After the DDoS campaign ended on December 4, *the electrohippies* began a 2-day e-mail bombing campaign. The group directed their supporters to e-mail large, uncompressed picture and document files (some suggested documents were the Kyoto Protocol on Climate Change, and several Environmental Protection Agency (EPA) and WHO reports) along with personal messages, to a list of WTO affiliated addresses. The goal was to overwhelm the internal e-mail systems of the organization and hamper internal communications.

So far we’ve demonstrated that the WTO’s public information system is not immune from public pressure. Now we move to their private information system—their email. What we would like people to do is email the WTO with personal

meepassages expressing your own reasons why you object to them and the Seattle conference. Of course, sending a short types [sic] message will not be that effective—so you'll also need to attach a large file to send with it.²

Four years before *the electrohippies action*, in 1994, CAE published an essay called, "Electronic Civil Disobedience" (ECD). The essay served as a call for activists to move the locus of their activism from the streets to the digital, online space: "The CAE has said it before, and we will say it again: as far as power is concerned, the streets are dead capital!"³ Organizations and systems of power had moved from the physical world to take up residence in the networks of "cyberspace" (a term which dates the essay rather sharply), and if activists and agitators wanted to have any impact at all, they had no choice but to follow them there.

The CAE advocated directly importing "traditional" civil disobedience to the digital space. "Blocking information conduits is analogous to blocking physical locations: however, electronic blockage can cause financial stress that physical blockage cannot and it can be used beyond the local level. [Electronic civil disobedience] is [civil disobedience] invigorated. What CD once was, ECD is now."⁴ They advocated direct engagement with institutions over individuals, encouraging activists to exploit the affordances of the network to make possible a direct confrontation between the activist-as-individual and the structural manifestations of power that were moving into the online space.

What tactics could be deployed, and how, became a point of contention within the CAE. Eventually, a small group of activists split from the larger organization to form the EDT, a group that will play a large role in our analysis. Right now, though, it is important to note that the CAE was advocating a type of digital direct action. Direct action, as an ideologically grounded set of tactics, values direct confrontation with oppressive structures of power. These could be state or corporate structures. The goal is to both disrupt the prevailing structure that is seen

to be causing harm, and thus hopefully lessening its impact, and to provoke a response, usually unduly punitive or violent, which is then allowed to stand on its own as an illustration of the reality of the challenged institution,⁵ similar to Thoreau's goal of performing the state's unjust nature by provoking his own arrest. Direct action as a motivating ideology assigns to individuals the power and the responsibility to confront and interrupt harmful systems and structures without requiring that those actions be sublimated through those systems and structures, which could imply tacit approval.

Direct action is often highly performative, engaging in both an illustration of alternative modes of political engagement, what has been referred to as "propaganda by deed"⁶ and a deliberate provocation to the target. The spectacle of an unreasonable response can add resonance to the original issues the activists meant to highlight.

This chapter looks at several DDoS actions that can be categorized as direct action DDoSes. Like other direct action tactics, these DDoS actions seek first, to disrupt a process for the purpose of disrupting that process, and secondarily, to trigger a cascade of responses on technological, political, media, and social levels. The direct action DDoS most clearly highlights the importance of "place" and proximity within digital activism, a concept that this chapter will explore through the theory of "contested space." Like street direct action, direct action DDoS actions are vulnerable to charges of censorship or harassment or simply disrupting democratic conversation with meaningless noise. This chapter will also examine the merits of those critiques.

Functional metaphors of geography and physicality

The electrohippies were interested in creating models of online activism that were functionally and philosophically equivalent

to physical practices already in existence. In this they weren't alone; the EDT had been running what they referred to as "virtual sit-ins" beginning in 1998. Both *the electrohippies* and the EDT were interested in establishing the online space as an arena of activism socially, culturally, and legally equivalent to the physical world. They made heavy use of the "virtual sit-in" metaphor and used "popular legitimacy" as a marker of success:

The structure of client-side distributed actions developed by *the electrohippies* means that there must be widespread support across a country or continent in order to make the system work. Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure.ⁱ

The "client-side" terminology used here differentiated *the electrohippies'* action from other types of DDoS actions that did not require the conscious, active commitment of a large number of participants to be successful. The "client-side" approach was philosophically conceived of as opposed to exploit-based and application layer "server-side" actions, which could amplify the flow of traffic from individual participants or use means which did not rely on the active presence of thousands of

ⁱ"Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act?" is collectively credited to "DJNZ and the action tool development group of *the electrohippies collective*" This is further explained:

"*the electrohippies collective* are a 'virtual group' in the sense that their activities are organised and carried out solely on the Internet *they do not meet*. The aim of the group is to extend the philosophy of activism and direct action into the 'virtual' world of electronic information exchange and communications. Why use the name 'electrohippies'? It's based upon a situationist paradox that seeks to promote a positive message by exploiting it's negative connotations. But it's also a nicely comical label, with plenty of stereotypical overtones that we can exploit as a means to make our point about the position of ordinary people within the global 'new world order.'" (DJNZ 2000)

participants to bring down a site. *The electrohippies*, and the EDT before them, purposefully hamstringing the technological tools they used in order to maintain a one-to-one participant to signal ratio.⁷

The desire to remain in functional lockstep with existing forms of on-the-street activism (the refusal to augment activist traffic, the strict reliance on popular participation for judgments of success) also provides a basis for the use of DDoS as a tool of direct action. *The electrohippies* viewed the internet as a public space whose ability to function as such was being compromised by the overwhelming presence of corporate and commercial interests. The WTO action was intended to hamper the public and private operation of the WTO, but also to be a forceful, public-facing statement in support of the right of the public to use the internet as a public, activist space.

In the United States, “public” space is not always necessarily public, and “private” space is, likewise, not always wholly private. Rather, the Supreme Court has repeatedly described a “continuum” of public fora, which has been aptly described by several scholarsⁱⁱ of free speech and public activism. The continuum roughly articulates four types of public fora, “the ‘traditional public forum,’ the ‘limited’ or ‘designated’ public forum, the ‘nonpublic forum,’ and private property.” These distinct fora are differentiated by the different obligations the state holds toward the practice of free speech within the fora. The “traditional public forum,” made up of public streets, sidewalks, and parks is the most free of these, where the state is forbidden from regulating speech based on content, and only permitted to regulated the “time, place, and manner” of speech acts.⁸ “Private property” is the most restrictive, wherein the owner of the property has extensive license to regulate speech as it occurs on her property.⁹ *The electrohippies’* action can be

ⁱⁱIn particular, the work of McPhail, Schweingruber, and McCarthy in “Policing Protests in the United States: 1960-1995,” and by Timothy Zick in *Speech Out of Doors* has influenced my thinking in this section.

seen as an attempt to assert a fundamental view of the internet as a “public forum” in the face of its attempted designation as “private property.”¹⁰ This assertion comes, by design, into direct confrontation with the WTO’s attempt to establish and occupy private and ideologically controlled spaces on the internet, in addition to its function as a force for corporate globalization. This struggle for the definition of online space mirrored the struggle on the streets of Seattle, where protesters clashed with police in an attempted assertion of “public space,” and where the anarchistic Black Bloc engaged with physical, spatial representations of globalized corporate capitalism in an attempt to forcefully interpolate the “public space” into the “private space.”

The strict physical-world parallelism sought by digitally enabled activists such as the EDT and *the electrohippies* necessitates a physicalized view of the internet itself: the internet itself must be seen as a physical place, albeit one with special attributes. Websites become representative static containers, which maintain an occupying presence on the network even as their content and functionality is pushed off-line by the force of the DDoS. That presence remains in the nonresponsive yet still labeled and branded blankness of the downed website. Conspicuous in its lack of expected messaging and voice, this “presence” is still very much an occupying, informatic structure online. A direct action DDoS seeks to strip away the attractive, humanized facade to reveal a corporate target’s reality as black boxed and monolithic, fundamentally unresponsive (metaphorically and actually) to human concerns. This is a paraphrase of the goals of street-level direct action, which seeks to lay bare the true nature of things through unvarnished confrontation with state and corporate structures of power.

As discussed in the first chapter, the signal disruption caused by the activist DDoS can constitute a unit of meaning in and of itself, despite its lack of overt “content.” It is a contribution to the larger spectacle of alterity being produced by the acts of direct action. The responsive-made-unresponsive, the available-

made-unavailable. The actions themselves produce the reality of alternatives, which are then incorporated into the ensuing media coverage, statements of corporate spokespeople, and reactions of law enforcement, including those present at the scene. As the public consumes the spectacle of destruction/disruption, the manifestation of alternatives, and responses to it, the hope is that they will be drawn out of passive consumption and into action.

Direct action DDoS actions also emphasize the value of “place” in online activism. Some critics of direct action acts of digital activism, such as DDoS actions or website defacements, ask why the activist actions can’t be moved off-site, perhaps to a reserved “activist domain,” where they would not be so disruptive. This is similar to the “demonstration zones” and “free speech zones” often set up around political party conventions or meetings of international governmental organizations, like the WTO or the G8. In 2004, a federal judge described one such “demonstration zone” to be used at the Democratic National Convention in Boston as a “symbolic affront to the First Amendment.”¹¹ There is critical value in being physically or conceptually proximate to locations that are symbolic of or central to a specific activist cause. Timothy Zick calls these “contested places,” which serve to “facilitate, amplify, and convey particular messages.”¹² In addition to adding symbolic value to an activist action, contested places offer access to specific audiences who are often connected to the activists’ message.¹³ Sequestering physical-world activists in an isolated “demonstration zone” or digital activists in a perhaps even more isolated “activist domain” severely hampers their ability to get their message out to individuals to whom it would be the most relevant. The open airing, reception, and discussion of dissenting views are a vital part of democracy. To deny activists access to contested places because of their potential for disruption cripples the public debate. Direct action DDoS aims to engage through temporary disruption, a goal which would be impossible if they were not allowed some access to the contested place of a specific website.

Shouting down your opponent: The censorship critique

The direct action DDoS, focused on interrupting a given signal stream, is vulnerable to the critique of censorship. This criticism has been most aggressively voiced by hacktivist groups such as Cult of the Dead Cow and Hacktivism. Jordan and Taylor classified this as the “digitally correct” view, wherein the integrity of the network and the right of individuals to an unfettered flow of information take precedence over the political ideals of activism and civil disobedience present in activist DDoS actions.¹⁴ Hacktivists considered the primary goal of hacktivism, or technologically based activism, to be defeating state censorship and the disruption of online communications via the creation and distribution of tools to evade censorious regimes.¹⁵ Writing in response to various *electrohippies* DDoS actions, Oxblood Ruffin, a prominent member of the Cult of the Dead Cow, wrote, “No rationale, even in the service of the highest ideals, makes [DDoS actions] anything other than what they are—illegal, unethical, and uncivil. One does not make a better point in a public forum by shouting down one’s opponent.”¹⁶

This criticism highlights a difference between hacktivist groups, made up of hackers who became politically active through writing and distributing code and tools beginning in the 1990s,¹⁷ and digitally empowered activists like the EDT and *the electrohippies*, who were more often than not experienced activists who subsequently began using internet tools and capabilities to supplement more traditional, physical-world actions.¹⁸ Hacktivists, coming from a culture that values personal autonomy and the freedom of information,¹⁹ are often strongly opposed to the use of DDoS, viewing it as an abridgment of free speech. Operating mostly in an environment made up of digital code and bits, the acceptance of the silencing of bits as a reasonable tactic of dissent was, and remains, unpalatable to most “old-school” hacktivists.²⁰

Ruffin was very clear that he did not consider digitally empowered activist groups like *the electrohippies* to be operating at the same level or with the same clarity of logic as his group: “One does not become a hacktivist merely by inserting an ‘h’ in front of the word activist or by looking backward to paradigm associated with industrial organization.”²¹ And it is true, these groups were not operating along the same lines of philosophy and practice. Groups such as Cult of the Dead Cow and, later, Hacktivism were often engaged in building tools of dubious legality, tools that enabled users to encrypt their communications, evade firewalls and censors, and mask their internet traffic.²² As a result, the security of the project was paramount. Groups tended to be small and secretive, with definite members rather than a large amorphous pool of participants. In many jurisdictions, the tools that these groups were developing were illegal, and using them exposed the user to legal and sometimes physical risks. It was vital that developers be experienced, skilled coders, and the ranks of serious hacktivists were closed until one could show he or she had the necessary skills.²³ Interestingly, these groups operated in a fashion that more closely resembled what the CAE, the primogenitor to the EDT, had envisioned as the operating model for ECD than how the EDT operated. The CAE envisioned practitioners of “electronic civil disobedience” operating as small, semiautonomous cells of specialized practitioners, each performing a specific action or role within a larger organization while simultaneously maintaining individual identities within the larger group.²⁴

The EDT and *the electrohippies* were proponents of legitimacy through mass action. Physical-world parallels were central to their philosophy of practice in the online space. Meaning and vitality was drawn from the simultaneous presence and action of thousands of people, not necessarily any actual or extended effect that action may have on the targeted site. In this sense, it was relatively unimportant to groups like the EDT whether a given action was “successful,” that is, whether it brought down a site. Stefan Wray notes that

FloodNet, the DDoS tool designed and used by the EDT in the 1990s and early 2000s, rarely resulted in actual downtime for the targeted sites, and as such, its value lay mostly in the “symbolic gesture” of the “simulated threat.”²⁵ The number of participants and the amount of media coverage the action attracted were most relevant to a judgment of “success” or “failure.”

The censorship criticism of activist DDoS actions is sometimes valid, as when the tactic is used against organizations that operate primarily online, such as stand-alone blogs, file-sharing sites, or ISPs, such as the IGC/*Euskal Herria Journal* case, which is explored in the next section. In other instances, the criticism fails to recognize unequal power dynamics between targets and activists, such as when a group of individual activists DDoSes a multinational corporation, the presence of alternative outlets of communication, or the intrinsic value of the DDoSed website to the target. The criticism in many cases also fails to interrogate how censorship could be practiced, if at all, by entities not occupying a dominant position in the current power hierarchy. Drawing an equivalency between the actions of private, nonstate actors and censorship, traditionally conceived of as a state-mediated action or at least an action performed by the more powerful party in a conflict, opens up questions about what entities are capable of performing censorship, particularly in the online space. While DDoS is undoubtedly a “disruptive” tactic,²⁶ disruption does not always equal a denial of speech rights. For example, in the WTO action described earlier in this chapter, though the central website was disrupted, the abilities of the delegates and the WTO as an organization to communicate their particular agenda to the greater public was not stymied. That the website was slowed down or made more difficult to access did not stop the conference from taking place or prevent the press from covering it. Though certain aspects of the WTO’s telecommunications infrastructure were negatively effected, the activists engaged in the DDoS and e-mailing bombing actions cannot be said to be “censoring” the speech of the

WTO. Later in this chapter we will examine a case in which, again, while certain aspects of an organization's data presence were disrupted, their ability to engage in public speech was not disrupted, causing the censorship conception to fall flat.

As has been documented by Ethan Zuckerman and others, there are many nonactivist DDoS actions that do readily fit the state-actor censorship model. Zuckerman catalogued instances where independent media and human rights sites were targeted by government actors with the goal of driving those sites off-line entirely. Due to the high cost of defending against large scale DDoS actions, and the propensity for ISPs in certain jurisdictions to view independent media and human rights sites as potential liabilities, these smaller sites can sometimes be driven off-line completely by a DDoS of relatively short duration.²⁷ State-sponsored or state-directed DDoS actions are not considered to be activist actions in this analysis, and a DDoS waged to effect the permanent removal of content is not considered to be a proper use of the tactic.

An analysis of extant power dynamics between the organizers, participants, and targets of activist DDoS actions can help address concerns of bullying or censorship that can arise regarding the use of the tactic. As the internet lowers barriers to individual connections across a variety of physical-world borders and barriers, it also enables activism to occur at scales of distance previously unheard of, fostering interactions between individuals and entities that may have been previously impossible, such as allowing individuals to enter into direct confrontation with the fully realized entity of a corporation or state.

Several activist DDoS actions have occurred over international borders, where activists from one country targeted the government websites of another country. An early example of this is the 1995 Strano Netstrike, which was organized by activists in Italy, but targeted the web presence of the French government in order to protest that government's policies. Similarly, the EDT's Zapatista actions were organized in the United States, but targeted the websites of the Mexican

president Ernesto Zedillo, and the Frankfurt Stock Exchange, among others, in order to protest the Mexican government's treatment of the Zapatistas. In addition, participants may be drawn from a grab bag of countries and jurisdictions. This practice of "transnational activism"²⁸ has transformed traditional understandings of state/activist relations.

In these cases, there are several different dynamics to be picked apart. The initial, assumed power struggle between activists and state entities is complicated when those activists are not citizens of the targeted states. The interaction raises questions as to a given state's responsibility for the concerns of foreign civilians and to the global activist public. There is the added power relationship between the state(s) from which the organizers and the bulk of the DDoS action originates and the targeted state. This is a particularly important consideration when allegations of cyberwar are or could be at play. Given the current uncertainty regarding the rules of engagement in international conflicts, organizers engaging in transnational activist actions should take care that they do not inadvertently set off an international incident.

Beyond transnational activism, DDoS actions expand potential modes of interaction between individuals or groups of individuals, and corporations. An important consideration for actions targeting corporate entities is the potential for unintended, adverse effects on the public. As more companies move primary aspects of their public-facing business online, it is important to consider the importance of constant uptime to users for reasons beyond convenience. For example, a temporary disruption in the online presence of a retail service or professional association could be substantially different in scope and effect from a disruption in medical or financial services. Disruption is a highly valuable tool of activism, drawing attention via the spectacle of novelty to issues activists want to highlight. However, in planning actions that aim to disrupt essential services in the medical, financial, or utility spheres, organizers should take into account the potential for unintended damage caused by disruptions in these services.

The *Euskal Herria Journal* and the IGC

Oxblood Ruffin's accusation that DDoS actions are nothing more than "illegal, unethical, and uncivil"²⁹ censorship is correct when the goal of a DDoS action is to permanently render inaccessible speech on the internet that has no other outlet. One such example is the popular DDoS action launched in Spain against the internet service provider IGC in 1997. The stated goal of the action, initiated and led by persons at this point unknown to this author, was to force IGC to stop hosting the Basque publication *Euskal Herria Journal*.³⁰ The campaign included network level actions and an e-mail campaign, eventually rendering inaccessible the websites and e-mail of IGC's over 13,000 subscribers. This was a populist-minded action; at one point, the major Spanish newspaper *El Pais* threw its support behind the e-mail bombing campaign and published target e-mail addresses for the IGC, though it later retracted its support and removed the addresses from its website.³¹ In the interest of continuing to provide service to its other subscribers, many of which were also minority political publications, IGC was forced to stop hosting *Euskal Herria Journal*, though it did so under protest.³²

As an ISP, IGC exists primarily, if not entirely, online. Removing IGC's ability to be present online removes its *raison d'être* and its ability to function as a corporation. A DDoS action against IGC strikes a blow to the core of the organization directly. The stress placed on the IGC network crippled the entire IGC apparatus. System outages affected more than just the *Euskal Herria Journal's* site, and the e-mail bombing campaign hampered the communications of all who used the IGC's mailservers. The levels of collateral damage at the level of basic communications were high.³³

The goal of the action against IGC was to force the removal of the *Euskal Herria Journal* website from its servers and by

doing so deny *Euskal Herria Journal* access to its *only* outlet for speech. This was an objection to content being available on the internet. For as long as it was successfully running, the DDoS action rendered that content unavailable. The goal of the DDoS action, and the surrounding campaign was the permanent imposition of its immediate effects.

The “Deportation class” action

Not all disruptions of content are equivalent to the silencing of speech, however. This is particularly true when the intent of an action is to change something not wholly present on the internet, such as the behavior of a large, multinational corporation. Here I would like to offer a contrasting example to the Euskal Herria/IGC case. In 2001, two German activist organizations, Kein Mensch ist illegal (No man is illegal) and Libertad! launched the “Deportation Class” action against Lufthansa airlines. This was a coordinated, multipronged protest against the German government’s use of the airlines’ flights to deport immigrants. Using an adapted version of the EDT’s FloodNet tool, some 13,000 people participated in a DDoS action against the airline’s homepage, which did experience some downtime over the course of the action.³⁴ Shortly after the action, which included press releases and physical-world actions at stockholder meetings, Lufthansa stopped allowing the German government to use its flights to deport immigrants.

The Deportation Class action targeted the website of a major airline. While the site itself was rendered briefly inaccessible, the actual corporation, its ability to fly planes, maintain normal operations, and communicate internally and with the media remained for practical purposes unaffected. Unlike the IGC action, which effectively prevented the basic functions of business for the organization, this action neither sought nor achieved a fatal disruption in either the airline’s normal operations or modes of communicating internally or

externally. This type of action, which only affects the homepage of an organization that does not primarily exist online, has been described as “[tearing] down a poster hung up by the CIA,”³⁵ with the implication that the action is technologically simplistic and has little practical impact on the organization targeted. It is a symbolic action, performed for the benefit of those participating and those watching.

The stated goal of the Lufthansa action was to disrupt ticket sales, draw public attention to a specific aspect of the airline’s business model, and through the focused attention change the corporation’s behavior. Though the DDoS action took place on the internet, the effect it sought was not limited, was not even present in the online space. In and of itself, this DDoS action could not have achieved what the EDT set out to accomplish. It took positive behavior on the part of Lufthansa for the “Deportation class” action to achieve its goals, as opposed to the IGC action, which was designed to accomplish its intended effect by the force of the DDoS itself.

Direct action is an ideological mode of activism that encourages activists to disrupt harmful processes and systems at the same time as they attempt to provoke a dramatic, illustrative reaction from their target. It doesn’t force activists to channel their dissent through ombudsmen or PR departments, or to curtail their political behavior to that recognized by their targets as “valid.” Protesters aren’t required to tacitly supply their consent before being permitted to express their dissent. Direct action DDoSes aim to disrupt the functioning of a harmful system or process and provoke a performative reaction and attract attention. These actions give us a lens with which to draw a sharp focus on the importance of relative place in online activism, and to address those critics who would tar all activist DDoS actions with the brush of censorship.

Though all DDoS actions, if they are technologically successful, disrupt computer processes, that is not always their primary goal as political activities. The next chapter will look at those DDoS actions that valued marshaling the attention of the media and the public over any actual services that were interrupted.

Notes

- 1 ehippies@tesco.net, message posted to diggers350 yahoo group. "WTO Sit-in open!—enter the virtual protest now!" November 29, 1999. Archived at groups.yahoo.com/group/Diggers350/message/236. Last accessed on February 25, 2014.
- 2 ehippies@tesco.net, email message from *the electrohippies*. "THE WTO SIT-IN: PHASE 2 STARTS NOW!" December 2, 1999. Message released by *the electrohippies*. Archived at www.thing.net/~rdom/ecd/phasetwo.html. Last accessed on February 25, 2014.
- 3 Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Brooklyn, NY: Autonomedia, 1996), 10–11.
- 4 Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas*, 18.
- 5 A. K. Thompson, *Black Bloc, White Riot: Antiglobalization and the Genealogy of Dissent* (Oakland, CA: AK Press, 2010), 59–80.
- 6 Laura Portwood-Stacer, *Lifestyle Politics and Radical Activism* (New York, NY: Bloomsbury Academic, 2013), 19.
- 7 Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwar: Rebels with a Cause* (New York, NY: Routledge, 2004), 167.
- 8 Timothy Zick, *Speech Out of Doors: Preserving First Amendment Liberties in Public Places* (Cambridge: Cambridge University Press, 2009), 7.
- 9 Clark McPhail, David Schweingruber, and John McCarthy, "Policing Protest in the United States: 1960–1995," in *Policing Protest*, edited by Donatella della Porta, and Herbert Reiter (Minneapolis, MN: University of Minnesota Press, 1998), 49–69.
- 10 McPhail, Schweingruber, and McCarthy, "Policing Protest," 49–69.
- 11 Zick, *Speech Out of Doors*, 230.
- 12 *Ibid.*, 105.
- 13 *Ibid.*, 231.
- 14 Jordan and Taylor, *Hacktivism and Cyberwar*, 114.
- 15 *Ibid.*, 90; Rita Raley, *Tactical Media* (Minneapolis, MN: University of Minnesota Press, 2009), 41

- 16 Oxblood Ruffin, "Hacktivism," (July 17, 2000), *Cult of the Dead Cow Blog*. Retrieved from <http://w3.cultdeadcow.com/cms/2000/07/hacktivism.html>. Last accessed February 25, 2014.
- 17 Oxblood Ruffin, "cDc, show and prove," Paper presented at the Yale Law School Cybercrime and Digital Law Enforcement Conference (New Haven, CT: March, 2004). Retrieved from http://www.cultdeadcow.com/cDc_files/cDc-0384.html. Last accessed February 2014.
- 18 Ricardo Dominguez, "Electronic civil disobedience: Inventing the future of online agitprop theater," *Proceedings of the Modern Language Association of America: Theories and Methodologies* 124 (2009): 1806–12.
- 19 Stefan Wray, "Electronic civil disobedience and the World Wide Web of hacktivism: A mapping of extraparliamentarian direct action net politics," *Switch* 4 (1998). Retrieved from <http://switch.sjsu.edu/web/v4n2/stefan/>. Last accessed February 25, 2014.
- 20 Wray, "Electronic civil disobedience and the World Wide Web of Hacktivism."
- 21 Ruffin, "Hacktivism."
- 22 Ruffin, "cDc: show and prove."
- 23 Ibid.
- 24 Critical Art Ensemble, *Electronic Civil Disobedience*, 23.
- 25 Wray, "Electronic civil disobedience and the World Wide Web of Hacktivism."
- 26 Sasha Costanza-Chock, (2003). "Mapping the repertoire of electronic contention," in *Representing resistance: Media, civil disobedience and the global justice movement*, edited by Andrew Opel and Donnaly Pompper (Greenwood, NJ: Praeger, 2003), 173–91.
- 27 Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey, *2010 Report on Distributed Denial of Service (DDoS) Attacks* (Berkman Center for Internet and Society Research Publication No. 2010–16) (Cambridge, MA: Berkman Center for Internet and Society, 2010).
- 28 Sidney Tarrow, *The New Transnational Activism* (Cambridge: Cambridge University Press, 2005).

- 29 Ruffin, "Hacktivism."
- 30 Chris Nicol, "Internet censorship case study: *Euskal Herria Journal*," Melville, South Africa: Association for Progressive Communications. Last accessed February 25, 2014. Retrieved from <http://europe.rights.apc.org/cases/ehj.html>.
- 31 Francisco Gor, "Internet y ETA," *El Pais*, September 14, 1997. Last accessed February 25, 2014, http://elpais.com/diario/1997/09/14/opinion/874188011_850215.html.
- 32 Institute for Global Communications, "Statement on the suspension of the Euskal Herria Journal website." July 18, 1997. Last accessed February 25, 2014. Originally published at <http://www.igc.org/ehj/>. Retrieved from <http://www.elmundo.es/navegante/97/julio/18/igc-ehj-en.html>.
- 33 Institute for Global Communications, "Statement on the suspension of the EKJ website."
- 34 Dominguez, "Electronic Civil Disobedience," 1809.
- 35 Randall Munroe, "CIA," *XKCD*, August 1, 2011. Last accessed February 25, 2014. Retrieved from <http://xkcd.com/932/>.