CHAPTER THREE

Which way to the #press channel? DDoS as media manipulation

The direct action DDoS provides participants with the theoretical structure and the tactical pathways to directly interact with systems of oppression. But, though disruption may be an effect of a DDoS action, the disruption itself is not always the greater goal of activists. Often, the disruption caused by the DDoS action is used as a tool to direct and manipulate media attention to issues the activists care about. We saw a related example of this in the Lufthansa/Deportation Class Action covered in the last chapter. The challenge for these types of actions, as with public, performative activism on the street, is getting the media to cover the issues that are driving the activist actions, and not merely the spectacle of the activism itself.

In a campaign that primarily seeks to achieve change through the medium of popular attention, activists must enter into an often uneasy symbiotic relationship with the mass media industry. News coverage of an action may result in further coverage of an organization and a cause, which may, in turn, inform a public outcry or directly influence decision makers to initiate desired change. But, as argued by Todd Gitlin, for a

given protest action to attract sympathetic media attention, it must look like what the media expects a protest action to look like: ". . . [protests] become 'newsworthy' only by submitting to the implicit rules of newsmaking (themselves embedded in history) of what a 'story' is, what an 'event' is, what a 'protest' is."[1] The use of innovative tactics and settings presents a challenge as multiple parties (activists, law enforcement, state actors, corporations) attempt to seize the opportunity created by novelty to control the narrative, and define a given action (and subsequent use of the tactic) as legitimate or illegitimate. If a tactic such as DDoS is seen as illegitimate, the media could fail to recognize a given action as "activism" and cover only the novelty, spectacle, and criminality of the tactic being deployed.

This chapter covers some examples of how different DDoS actions and the activists involved with them have interacted with the media. Some were more successful than others. For example, Anonymous is particularly adept at attracting and manipulating the media coverage surrounding its raids, whereas earlier groups like the EDT quickly lost control of the narrative. This chapter also addresses some criticisms specifically directed at media-oriented DDoS actions, including the CAE's principle critique that such acts of "symbolic protest" were, in the online space, fundamentally ineffectual.

Terrorist, hacker, artist, nuisance: The many media reflections of the EDT

One of the first groups to attempt to use DDoS actions as a tool of mass activism was the EDT. Beginning in the late 1990s, the EDT launched a series of "digital storms" supporting the Zapatista struggle in Mexico.[2] The EDT was a quartet of artist-activists, Stefan Wray, Ricardo Dominguez, Carmin Karasic, and Brett Stalbaum. Because of differences in how they believed activism should be practiced online, the four had spun off from an earlier group, the CAE.

Stalbaum and Dominguez developed the tool used to facilitate their DDoS-based actions, a web-based tool called FloodNet. The EDT referred to their actions as "virtual sit-ins," a strategy repeated by subsequent groups such as *the electrohippies*, relying on the historically loaded nature of the term to act as a type of pedagogical shorthand as to the legitimacy and certain formal aspects of the DDoS tactic.[3] They promoted a conceptualization of DDoS as an auxiliary political act, embedded within larger campaigns. While a group using DDoS as a tool of direct action would privilege downtime as a marker of a successful action, this was relatively unimportant to the EDT. Stefan Wray notes that FloodNet, the primary DDoS tool used by the EDT in the 1990s and early 2000s, rarely resulted in actual downtime for the targeted sites.[4] The EDT saw the media attention paid to its actions as a primary goal, taking care to distribute press releases to major media outlets and to announce all actions publicly beforehand.[5]

The EDT did attract news coverage over its active years; however, this coverage did not always cover the deeper political and social issues the group had hoped to draw attention to with their activism. Some articles focused on the spectacle of the EDT and their "virtual sit-ins" in digital culture trend pieces, more interested in performing a roll call of the activist space than in interrogating the motivations and logics behind a specific action. An October 1998 *New York Times* article, headlined "'Hacktivists' of All Persuasions Take Their Struggle to the Web," called the EDT's use of DDoS ". . . computer hacking, so far largely nuisance attacks and the equivalent of electronic graffiti. . . ."[6] Some 14 other individuals and organizations, consistently referred to as "hackers," are mentioned in the 2,025-word article. Stories in the *Ottawa Citizen*,[7] *Computerworld*,[8] and the *Sydney Morning Herald*[9] followed a similar pattern. Other articles grouped the EDT and other activist organizations under the label "cyber-terrorists"[10] or forced their activities into a cyberwar framework, using phrases such as "targeted cyber attacks" and "firing the first shots in a cyber war" to describe protest actions.[11] A June 1999

Christian Science Monitor article quotes a RAND researcher, the director of a social-justice group, and a University of Texas professor as saying that the use of DDoS by the EDT is "idiotic," "not constructive," "not good Internet etiquette," "divisive," and that "the kind of actions espoused by the EDT have been widely shunned by social activists of all stripes."[12] A second *Christian Science Monitor* article, published in July 1999, places the EDT's Zapatista actions exclusively in the company of highly colorful hypotheticals about the dangers of cyberterrorism, while declining to interview any members of the EDT.[13] In 2002, the *Buffalo News* ran a 1,625-word feature article, "Hackers Use Computer Skills to Promote Politically Motivated Mischief, Mayhem," which did not interview any activists, though it did interview multiple academics and computer security researchers. The EDT and *the electrohippies* were grouped together indiscriminately with organizations with significantly different tactics and motivations, such as website defacement and malware distribution, and included theoretical future attacks on infrastructure. All groups, real and imaginary, were referred to as "hackers" or "hacktivists."[14]

While the "cyber-terrorist" label and characterizations of the EDT's activist actions as "attacks" or acts of "cyber war" are clearly prejudicial, it is worth taking a moment or two to unpack how the "hacker" characterization also operates as a prejudicial description, one which has the effect of depoliticizing activist actions and fostering perceptions of such actions as criminal and transgressive. The media's use of the stereotypical hacker figure to promote a social fear of technology and pervasive environment of technoparanoia is deep and complex, and there is not enough space to fully explore it here, but I will attempt a brief sketch. By the late 1990s and early 2000s, the media tropes for the coverage of computer matters had begun to solidify. The word "hacker" was, and is still now, used by the news media as a catchall term to apply to any type of criminal or "bad" computer activity, including those that did not break any laws. The hacker figure himself (media depictions of male hackers outnumber those of female hackers by a wide margin)

became a type of "folk devil," a personification of our anxieties about technology, the technologically mediated society, and our increasingly technologically mediated selves. The hacker, as depicted in film and on the 6 o'clock news, is the central deviant of the information society.[15]

The hacker-as-folk-devil figure has several persistent characteristics. He stands separate from "normal" society; his life is socially, economically, and often physically isolated. See, for example, the stereotypic image of the adolescent hacker living in his parents' basement. Because he is socially alienated, he lacks the normal social checks on his behavior, and is instead engaged in compulsive, competitive cycles with other hackers, who egg on each other's antisocial behavior. He doesn't abide by conventional morality because he is immature or young, and self-importantly believes the rules don't apply to him. His relationship with technology is pathological, and he is sometimes described as being "addicted" to computers or the internet. His abilities are often depicted as far surpassing those of the average person. Paul Ohm described this aspect of the hacker folk devil as the Superuser, someone whose technological skills are so advanced as to be seen as essentially magical to most observers.[16] The hacker is locationless and decentralized, able to cause harm far from his actual location. The hacker folk devil is therefore cast as abnormal, alienated from conventional socials morals, a predictably bad actor, capable and willing to cause great harm to individuals, corporations, and the state. Not only is the hacker tarred with this brush, but anyone who participates in activities or holds views associated with hackers are held guilty by association. In tagging the EDT as "hackers," these news articles characterize digital activists and their activities as antisocial, essentially nonpolitical, and potentially dangerous to the public at large.[17]

The EDT conceived of their FloodNet-powered DDoS actions in the late 1998 and 1999 primarily as media events, meant to direct popular attention to the Zapatista struggle. However, as Graham Meikle argues, because much of the news coverage was either reactionary early-cyberwar rhetoric or

facilely focused on FloodNet's novelty, it would be a stretch to consider the FloodNet actions to be successful on that level.[18] Many of the articles covering the EDT can be seen as attempts on the part of the news media to categorize the activists and their actions into some sort of known quantity, terrorists or hackers or artists. The novelty of the DDoS tactic provided this sorting opportunity, but the coverage did not go so far as to cover the actual story of the politics behind the tactic's use.

The EDT's problems with myopic press coverage highlight the difficulties activists face when attempting to tie their messaging strongly to their disruptive action. The "digital" or "virtual" sit-in nomenclature used by the EDT and other groups is highly evocative, allowing activists to build off the pedagogical and cultural capital of historical physical-world sit-ins.[19] However, the metaphor glosses over many challenges inherent to the digital form, particularly that of proximity to messaging. In a physical-world sit-in, the rhetorical proximity of the protest to the target is central to the disruption. Though this has sometimes been challenged in the United States with the establishment of "protest zones" in locations deemed to be sensitive, the physical closeness of protest actions to direct or symbolic targets is a valuable part of activist messaging, as discussed earlier.

This type of proximal messaging is not natural in the online space. DDoS actions in particular may by invisible to the public. A user attempting to access a targeted site may have no exposure to the protest's messaging at all and may not even register that an action is taking place. All that is apparent to them is that the site they are looking for is operating poorly or not at all. Not only does this represent a failed opportunity for the campaign, but it also shifts blame/credit to the target. Without effective messaging, a given campaign may appear to be incoherent disruption, giving the press an excuse to probe no deeper than chaotic first impressions. We will now move on to some other examples of DDoS campaigns that fared differently in the media sphere than the EDT did.

Allies in the toywar

In December 1999, the EDT, the Swiss art group etoy, and culture jamming group ®™mark (pronounced art-mark) launched "The Twelve Days of Christmas" action using the EDT's FloodNet DDoS tool. Their target was the retail site eToys.com, which had filed a lawsuit against the etoy group over the ownership of the URL etoy.com.[20] As part of the greater "toywar" campaign, which involved physical-world demonstrations, publicity and letter writing campaigns, and a multiplayer online game, the "12 Days of Christmas" DDoS campaign was intended, according to Ricardo Dominguez, to ". . . represent the presence of a global group of people gathered to bear witness to a wrong,"[21] and to disrupt eToys.com's online operations during the critical Christmas shopping season. Some 1,700 individuals participated in the DDoS action. In January 2000, eToys.com dropped its suit and paid the court costs of etoy.

The toywar campaign enjoyed significant coverage in the mainstream news media, mostly due to the ongoing legal drama of the eToys.com lawsuit. The case was seen as a test of the lengths corporations could go to police their trademark online, and was followed closely by the US business press. As the case played out, inside and outside the courtroom, multiple stories appeared in *Wired*, the *New York Times*, the *Washington Post*, the *Guardian*, *USA TODAY*, and other international news outlets. Unlike coverage of the EDT and *the electrohippies*, the toywar coverage, with few exceptions, did not focus on the technical machinations of the protest action or attempt to classify ®™mark, etoy, or the EDT as terrorists, criminal hackers, or even cybersquatters. Rather, news outlets made extensive use of the David and Goliath narrative to describe what was seen as a legal dispute between a large corporate online retailer and a small avant-garde art group.

Of particular interest here is the emergence of vocal third parties advocating for etoy. In coverage of the EDT and

the electrohippies, any third parties quoted who were not also digital activists or hacktivists were predominantly information security professionals or others who condemned the concept of electronic civil disobedience in general. The etoy/toywar coverage, on the other hand, included the voices of John Perry Barlow, attorneys at the Electronic Frontier Foundation, and luminaries from the tech art world, all of whom supported etoy. *Wired*'s 1999 article, "Be Grateful for Etoy," quotes John Perry Barlow extensively, as he calls the etoy/eToys fight "the battle of Bull Run," and invokes the ghost of internet luminary Jon Postel, saying "If Jon Postel were alive, he'd be in tears." The article goes on to quote EFF legal director Shari Steele as saying "Shame on eToys for misusing the law in this way," and characterizing the case as a "clear-cut case of a business bullying a group of artists. . . ."[22] Also in 1999, an article published in the *Washington Post* quotes Karin Spaink, a judge for the 1996 Prix Arts Electronica, which has been awarded to etoy, criticizing the scope of a judicial decision in the case which restricted the ability of etoy to sell "stock" in the United States.[23]

The presence of the solid, easily understood narrative structure of the court case allowed the news media to focus on the nuances of the dispute and the accompanying "12 Days of Christmas" DDoS action. As a result the coverage was much more sympathetic to both etoy's legal claim and the legitimacy of the DDoS action and contained a wider range of voices than coverage of other EDT or *electrohippies*' actions.

Anonymous and the media: Manipulation, entertainment, and readymades

Anonymous, a loose collection of internet denizens that sprang from the unmoderated image board 4chan, has, over

the past few years, rapidly increased their capacity to attract and manipulate mainstream media attention.[24] This ability was on display during the Operation PayBack DDoS campaign in December 2010, also known as Operation Avenge Assange. During this action, the high level of quotable, embed-able graphic and video artifacts produced by the group allowed them a level of control over the media narrative that, for example, the EDT had never enjoyed. Anonymous is, as a group, difficult for the media to cover, but their cultural artifacts are highly accessible online. By pushing the peer production and distribution of these artifacts, which include video manifestos, graphical calls to action, and solidarity images, Anonymous was able, to a certain extent, dictate the visual tools and language used in the media's coverage of Operation Payback.

Operation PayBack was a series of DDoS actions against a variety of entities that Anonymous perceived as taking hostile action toward Wikileaks. Primarily using the LOIC tool (which will be examined in detail in Chapter 6), Anonymous targeted more than ten different sites over the course of 4 days, from December 6 through December 10, 2010, including those of the Swedish Prosecution Authority, EveryDNS, senator Joseph Lieberman, MasterCard, two Swedish politicians, Visa, PayPal, and Amazon.com.[25] Many of the sites targeted experienced at least some amount of downtime.

Unlike the EDT, *the electrohippies*, and other groups discussed in this book, Anonymous had, in 2010, a reputation, in many ways a purposefully cultivated one, for being extremely effective and unpleasant trolls with unpredictable methods of choosing their targets. The majority of the media coverage of Anonymous and Operation Payback was characterized by an unwillingness to critically assess Anonymous as an activist group or Operation Payback as an activist action and a rampant confusion about the facts. There was genuine fear that any organization or individual could be Anonymous' next target, and very few people were willing to hang a bull's-eye on their back by being publicly critical of them,

particularly journalists and news organizations that did not fully understand the technological tactics so freely deployed. Add to this the fact that one of Anonymous' primary methods for spreading information about operations and raids was through the public distribution of slickly produced videos, graphics, and public social media streams, and the result was, in many cases, news organizations embedding Anonymous videos and call-to-action posters directly in news stories. Examples of this could be found in the *Washington Post*[26] and the social media news site *Mashable*.[27] In an article entitled, "'Anonymous' attacks Visa.com, Mastercard.com, in support of WikiLeaks," the *Washington Post* embedded a call-to-action video entitled, "Operation Payback #Anonymous Message RE: ACTA, SOPA, PIPA, Internet Censorship and Copyright," which in turn linked to an Anon-run twitter account. The social networking news site *Mashable,* in a post entitled "Operation Payback Targets Amazon.com," linked to numerous Twitter accounts, which were tweeting scheduling and targeting information, as well as linking to the *Encyclopedia Dramatica* page on the LOIC DDoS tool. They also embedded the same call-to-action video that the *Washington Post* also included in their coverage.

The decentralized, leaderless nature of Anonymous made direct coverage of the group difficult. After all, there were no official spokespeople for the press to rely on, and there was a constant flow of Pastebin statements, videos, and Photoshopped posters popping up in all corners of the internet, all claiming to be from Anonymous. The extreme horizontal nature of Anonymous meant that literally anyone could claim to speak for the group. Anonymous set up a press channel on one of its IRC servers, where members of the press could chat with Anons, but many members of the press were simply not aware of it or lacked the technological skills to access the channel on their own. The combination of the demands of the 24-hour news cycle and an unpredictable, unreliable subject meant that a sizable percentage of the coverage was made up of reprinting Anonymous press releases and posters as journalists

scrambled for new material on an almost hourly basis. Often an Anonymous artifact that had been "legitimated" by one news source would quickly find its way into others, expanding dramatically the range of influence for certain artifacts. For example, the *Washington Post* and *Mashable* article cited earlier both embedded the same call-to-action video, which had originally been linked to by the *New York Times* blog, "The Lede." This pattern of news organizations repeating and homogenizing coverage over the course of an ongoing event fits with the pattern described by Pablo Boczkowski and Martin de Santos in their 2007 examination of homogenization in the Argentine print and online news industries. Boczkowski and de Santos found that online news sites were particularly prone to high levels of "content overlap" on fast moving stories that demanded repeated updates throughout the day. Boczkowski and de Santos ascribe this homogeneity of coverage to "not technology per se, manifested in the emergence of a new medium, but technical practices, or how journalists use the technology to make news."[28] Anonymous' continual furnishing of quotable, embeddable, compelling descriptive content exacerbated an already extant system of aggregating from available information feeds to maintain the constant flow of news content.

This explosion of coverage was a boon to Anonymous in terms of participant population. Anons have subsequently claimed that during Operation Payback, the number of participants active in their IRC channels rose from an average of 70 participants to over 7,000.[29] It is likely that without this influx of new participants, the Operation Payback DDoS actions would not have resulted in the downtime they did.[i] This substantial increase in active participants during Operation Payback can be credited in part to the extensive, relatively uncritical media coverage given to the December stage of Operation Payback.

[i]As addressed in Chapter 6, the use of illicit, nonvolunteer botnets contributed substantially to achieved downtime.

Shadows in the monitor: The CAE's symbolic dissent critique

In the 1996 essay, "Electronic Civil Disobedience,"[30] the CAE posited an evolution on the traditional, physical-world model of civil disobedience. As systems of power migrated from the brick-and-mortar infrastructure of physical buildings to reside primarily as data constructs on the internet, the CAE argued, so too must systems of resistance and protest. ECD as conceived of by the CAE sought to translate the philosophies of disruptive protest from the physical world to the networked world via a system of 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.[31] Central to the CAE's vision was the clandestine and essentially closed nature of the actions, carried out by semiautonomous cells rather than by a large, public, mass demonstration of dissent. The CAE describes this as an "inversion" of traditional civil disobedience.[32] This particular philosophy sprang from a belief that ECD "is an underground activity that should be kept out of the public/popular sphere (as in the hacker tradition) and the eye of the media . . ." because ". . . there is no corporate or government agency that is not fully prepared to do battle in the media."[33] The CAE criticized the actions of groups such as the EDT and others for engaging in public, spectacle-oriented "simulated" actions over "clandestine policy subversion" and direct action.

The CAE felt that the mass-action, media spectacle tactics that the EDT employed, including their use of DDoS actions as attention directors, would ultimately be completely ineffectual at effecting change in corporate and government actors. However, this criticism lifts the tactic out of the context of larger actions or campaigns it might be associated with. The validity of the tactic is equally dependent on the activist structure that surrounds it as any qualities inherent in it.

DDoS actions were not primarily conceived of as stand-alone actions. EDT member Stephen Wray notes that "we are likely to see a proliferation of hybridized actions that involve a multiplicity of tactics, combining actions on the street and actions in cyberspace."[34] To divest DDoS of its "component" nature[35] is to place on its shoulders a weight of ontological justification that no tactic alone could bear.

Similar to the censorship criticism leveled by the hacktivist groups, the CAE's criticism of DDoS as ineffective is as much a description of the different goals and operating philosophies at work between these types of activist organization as it is an autonomous critique.

What does winning look like?

Critics of activist DDoS actions routinely raise the question of measures of success. At a technological level, it is becoming more and more difficult for volunteer-based DDoS action to cause any downtime on major corporate sites. It would be virtually impossible for such an action to crash a modern site without technological augmentation. This is not a new development, even in the early 2000s, the FloodNet powered DDoS actions run by the EDT rarely resulted in downtime.[36] So if an actual denial-of-service caused by server downtime is an unlikely result of an activist DDoS action, what then is an appropriate measure of the success of any given action?

In this, the CAE's criticism of DDoS actions as symbolic and simulated reverses to become its virtue. When used within a broader action to expand opportunities for engagement and participation, DDoS tactics create what Foucault termed a "plurality of resistances," each action being a provocation with not-necessarily-certain desired results.[37] Ricardo Dominguez described this as a "permanent cultural resistance; there is no endgame."[38] The value of this symbolic resistance is not necessarily in its overt effect on the system it ostensibly

targets, but rather in its effects on its participants and on the reflective fields that surround it as it occurs, including media and culture. Particularly in its value as a tool of biographical impact, the subject of the next chapter, DDoS acts as a tool for the revelation of "hidden transcripts" of resistance.[39] This is particularly apparent in the case of the Anonymous Operation Payback, wherein the vast majority of the actions and organization took place online among individuals who had not met in the physical world. As a tactic whose strength is in the digitized power of a crowd, the DDoS serves as an open action wherein individual participants "recognize the full extent to which their claims, their dreams, their anger is shared by other subordinates with whom they have not been in direct touch."[40] This is a quality which will become increasingly valuable as digital activism continues to be unbounded by state borders and moves toward a transnational operational norm.

Notes

1 Todd Gitlin, *The Whole World Is Watching* (Berkeley, CA: University of California Press, 2003), 3.

2 Electronic Disturbance Theater, e-mail sent from the Electronic Disturbance Theater, "24 Hour Digital Storm On the Mexican Government. August 26th 1999," sent on August 25, 1999. Archived at http://www.thing.net/~rdom/ecd/storm99.html. Last accessed February 25, 2014.

3 Brett Rolfe, "Building an electronic repertoire of contention," *Social Movement Studies*, 4 (2005): 65–74.

4 Wray, "Electronic civil disobedience and the World Wide Web of Hacktivism."

5 Dominguez, "Electronic Civil Disobedience," 1809.

6 Amy Harmon, "Hacktivists of All Persuasions Take Their Struggle to the Web," *New York Times*, October 31, 1999.

7 Bob Paquin, "E-Guerillas in the Mist," *Ottawa Citizen*, October 26, 1998.

8 Deborah Radcliff, "Meet the 'Hacktivist'," *Computerworld*, October 16, 2000.

9 Maria Nguyen, "Armchair Activism," *Sydney Morning Herald*, August 17, 2002.

10 Tom Regan, "When terrorists turn to the Internet," *Christian Science Monitor*, July 1, 1999; Editorial, "Cyber-terrorism's threat becoming real," *Hamilton Spectator*, November 10, 1999.

11 John Lasker, "Hackers Use Computer Skills to Promote Politically Motivated Mischief, Mayhem," *Buffalo News*, May 14, 2002.

12 Paul Van Slambrouck, "Newest tool for Social Protest: The Internet," *Christian Science Monitor*, June 18, 1999.

13 Regan, "When terrorists turn to the internet."

14 Lasker, "Hackers Use Computer Skills to Promote Politically Motivated Michief, Mayhem."

15 Molly Sauter, "If Hackers Didn't Exist, Governments Would Have to Invent Them," *The Atlantic*, July 5, 2012. Last accessed February 25, 2014. Retrieved from http://www.theatlantic.com/technology/archive/12/07/if-hackers-didnt-exist-governments-would-have-to-invent-them/259463/.

16 Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," University of Colorado Law Legal Studies Research Paper No. 07–14, *UC David Law Review* 41 (2008): 1327.

17 Molly Sauter, "Policy Effects of the Media Portrayals of Hacktivists," SXSW Interactive, March 2012. Slides available http://prezi.com/waiqewbhgh5q/hackers-in-the-media-sxsw/. Audio available http://schedule.sxsw.com/2012/events/event_IAP12520/.

18 Graham Meikle, *Future Active* (New York, NY: Routledge, 2002), 155.

19 Rolfe, "Building an electronic repertoire of contention."

20 McKenzie Wark, "Toywars: Conceptual art meets conceptual business," *M/C: A Journal of Media and Culture* 6 (2003). Retrieved from http://journal.media-culture.org.au/0306/02-toywars.php/. Last accessed February 25, 2014.

21 Ricardo Dominguez, quoted in Wark, "Toywars."

22 Steve Kettmann, "Be Grateful for Etoy," *WIRED*, December 17, 1999.

23 Richard Leiby, "Etoys vs Etoy: A Clash of Commerce and Art," *Washington Post*, December 10, 1999.

24 Whitney Phillips, "The house that fox built: Anonymous, spectacle and cycles of amplification," *Television and New Media* 14 (2013): 494–509.

25 Sean-Paul Correll (2010), "Tis the season of DDoS: WikiLeaks edition," *PandaLabs Blog*, December 15, 2010. Last accessed February 25, 2014, http://pandalabs.pandasecurity.com/tis-the-season-of-DDoS-wikileaks-editio/.

26 Melissa Bell, "Anonymous attacks Visa.com, Mastercard.com in support of WikiLeaks," *The Washington Post*, December 8, 2010. Last accessed Feburary 25, 2014, http://voices.washingtonpost.com/blog-post/2010/12/mastercardcom_hacked_by_wikile.html.

27 Brenna Erlich (2010), "Operation Payback targets Amazon.com," *Mashable.com*, December 9, 2010. Last accessed February 25, 2014, http://mashable.com/2010/12/09/operation-payback-amazo/.

28 Pablo Boczkowski and Martin de Santos, "When More Media Equals Less News: Patterns of Content Homogenization in Argentina's Leading Print and Online Newspapers," *Political Communication* 24 (2007): 167–80.

29 Gabriella Coleman, "Our weirdness is free," *Triple Canopy* 15 (2012). Retrieved from http://canopycanopy.com/15/our_weirdness_is_free/. Last accessed February 25, 2014.

30 Critical Art Ensemble, *Electronic Civil Disobedience*, 7–32.

31 Ibid., 23.

32 Critical Art Ensemble, *Digital Resistance: Explorations in Tactical Media* (Brooklyn, NY: Autonomedia, 2001), 14.

33 Critical Art Ensemble, *Digital Resistance*, 15.

34 Stefan Wray quoted in Raley, *Tactical Media*, 44.

35 Raley, *Tactical Media*, 44.

36 Wray, "Electronic civil disobedience and the World Wide Web of Hacktivism."

37 Michel Foucault, *A History of Sexuality, Volume One: An Introduction* (New York, NY: Vintage, 1990), 185.

38 Ricardo Dominguez quoted in Raley, *Tactical Media*, 46.

39 James Scott, *Domination and the Arts of Resistance: Hidden Transcripts* (New Haven: Yale University Press, 1990).

40 Scott, *Domination and the Arts of Resistance*, 223.