Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet

By

Molly Sauter

B.A. History and Philosophy of Science, University of Pittsburgh 2010

SUBMITTED TO THE PROGRAM IN COMPARATIVE MEDIA STUDIES/WRITING IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN COMPARATIVE MEDIA STUDIES
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2013

Signature of Author: ______________________________
Program in Comparative Media Studies/Writing
May 17, 2013

Certified by: ______________________________
Ethan Zuckerman
Principal Research Scientist, MIT Media Lab
Director, Center for Civic Media, MIT
Thesis Supervisor

Accepted by: ______________________________
James Paradis
Head, Comparative Media Studies/Writing

Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet

By

Molly Sauter

Submitted to the Program in Comparative Media Studies/Writing
on May 17, 2013 in Partial Fulfillment of the
Requirements for the Degree of Master of Science in
Comparative Media Studies

ABSTRACT

This thesis examines the history, development, theory, and practice of distributed denial of service actions as a tactic of political activism. DDOS actions have been used in online political activism since the early 1990s, though the tactic has recently attracted significant public attention with the actions of Anonymous and Operation Payback in December 2010. Guiding this work is the overarching question of how civil disobedience and disruptive activism can be practiced in the current online space. The internet acts as a vital arena of communication, self expression, and interpersonal organizing. When there is a message to convey, words to get out, people to organize, many will turn to the internet as the zone of that activity. Online, people sign petitions, investigate stories and rumors, amplify links and videos, donate money, and show their support for causes in a variety of ways. But as familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, is there also room for the tactics of disruption and civil disobedience that are equally familiar from the realm of street marches, occupations, and sit-ins? This thesis grounds activist DDOS historically, focusing on early deployments of the tactic as well as modern instances to trace its development over time, both in theory and in practice. Through that examination, as well as tool design and development, participant identity, and state and corporate responses, this thesis presents an account of the development and current state of activist DDOS actions. It ends by presenting an analytical framework for the analysis of activist DDOS actions.

Thesis Supervisor: Ethan Zuckerman
Title: Principal Research Scientist, MIT Media Lab
Director, Center for Civic Media, MIT

PREVIOUS PUBLICATION NOTE

Sections of this work were originally published in the *American Behavioral Scientist*, under the title, " 'LOIC Will Tear Us Apart': The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks," and the blog *HiLoBrow*, under the title, "Guy Fawkes Mask-ology."

BIOGRAPHICAL NOTE

Molly Sauter attended St John's College and graduated from the University of Pittsburgh with a B.A. in the History and Philosophy of Science in 2010. Before attending MIT, she worked at the Berkman Center for Internet and Society at Harvard University, researching distributed work, digital activism, information security, and internet regulation. At MIT, she has worked as a research assistant at the Center for Civic Media, researching digital activism, social movement theory, civic engagement, hacker culture, and co-design practices. She spent the summer of 2012 interning with the activism team at the Electronic Frontier Foundation, and is a fellow at the Berkman Center for 2012-2013.

She will be starting the PhD program in Communication Studies at McGill University in the fall of 2013.

Molly can be reached at molly.sauter@gmail.com.

TABLE OF CONTENTS

INTRODUCTION: Working Back from Wikileaks........9
- Technical Note........18
- Legal Note........21

CHAPTER ONE: Theories and Models of Practice........26
- DDOS as direct action........27
- DDOS as media manipulation........35
- DDOS as tool of biographical impact........44
- Critical models of DDDOS actions........51
- Conclusions........58

CHAPTER TWO: A Comparative Analysis of DDOS Tool Design........60
- The Electronic Disturbance Theater and FloodNet........61
- Anonymous, Operation Payback, and LOIC........64
- Conclusions........78

CHAPTER THREE: Participant Identity in Context........80
- Identity, anonymity, and responsibility within protest........81
- Identity within distributed actions: Anonymous and the hacker identity........90
- Accessibility within technologically defined tactical spaces........93
- DDOS and "impure dissent"........95
- Conclusions........100

CHAPTER FOUR: State and Corporate Responses........102
- State responses: terrorism and sentencing recommendations........102
- Corporate responses: the avatar nature of online brand presence........108
- Conclusions........111

CHAPTER FIVE: Ethical DDOS Actions: An Ethical Framework........112
- The value of disruption and the right to be heard........113
- Intended effects and actual effects........116
- Technology utilized........122
- Context within a greater campaign........125
- Power relations between organizers, participants, and targets........126
- Conclusions........128

CONCLUSION: The Future of DDOS........130

ACKNOWLEDGEMENTS........135

REFERENCES........137

INTRODUCTION

Working Back from Wikileaks

On November 28, 2010, Wikileaks, along with the *New York Times*, *Der Spiegel*, *El Pais*, *Le Monde*, and *The Guardian* began releasing documents from a leaked cache of 251, 287 unclassified and classified US diplomatic cables, copied from the closed Department of Defense network SIPRnet (Borger and Leigh, 2010). In the days that followed, different organizations and corporations began distancing themselves from Wikileaks. Amazon WebServices declined to continue hosting Wikileaks's website, and on the first of December removed its content from its servers (Pelofsky, 2010). The next day, the public could no longer reach the Wikileaks website at wikileaks.org; Wikileaks' DNS[1] provider, EveryDNS, had dropped the site from its entries on the second of December, temporarily making the site inaccessible through its URL (Associated Press, 2010). Shortly thereafter, what would be known as the "Banking Blockade" began, with PayPal, PostFinance, MasterCard, Visa, and Bank of America refusing to process online donations to Wikileaks, essentially halting the flow of monetary donations to the organization (Hope, 2010).

Wikilieak's troubles attracted the attention of Anonymous, a loose group of internet denizens, and in particular a smaller subgroup known as AnonOps, who had

[1] DNS, or Domain Name System, is a hierarchical distributed naming system used to identify and locate computers connected to the Internet or any networked system. One of its primary functions is to translate human-friendly URLs (like www.wikileaks.org) into numerical IP addresses (like 108.162.233.13). Without a DNS provider, such translations would not occur, and a website would only be accessibly via the numerical IP address.

been engaged in a retaliatory distributed denial of service (or DDOS) campaign called Operation Payback, targeting the Motion Picture Association of America and other pro-copyright, anti-piracy groups since September 2010 (Anderson, 2010). A DDOS action is, simply, when a large number of computers attempt to access one website over and over again in a short amount of time, in the hopes of overwhelming the server, rendering it incapable of responding to legitimate requests. Anons, as members of the Anonymous subculture are known, were happy to extend Operation Payback's range of targets to include the forces arrayed against Wikileaks and its public face, Julian Assange. On December 6, they launched their first DDOS action against the website of the Swiss banking service, PostFinance. Over the course of the next four days, Anonymous and AnonOps would launch DDOS attacks against the websites of the Swedish Prosecution Authority, EveryDNS, Senator Joseph Lieberman, MasterCard, two Swedish politicians, Visa, PayPal, and Amazon.com, and others, forcing many of the sites to experience at least some amount of downtime (Correll, 2010).

For many in the media and public at large, Anonymous's December 2010 DDOS campaign was their first exposure to the use of this tactic by activists, and the exact nature of the action was unclear. Was it an activist action, a legitimate act of protest, an act of terrorism, or a criminal act? These DDOS actions—concerted efforts by many individuals to bring down websites by making repeated requests of the websites' servers in a short amount of time—were covered extensively by the media. In the eyes of the media and public, Operation Payback opened the door to the potential for civil disobedience and disruptive activism on the internet. But Operation Payback was far from the first use of DDOS as a tool of activism. Rather, DDOS actions have been in use for over two decades, in support of activist campaigns ranging from pro-Zapatistas actions to protests against German immigration policy and trademark enforcement disputes.

The aim of this work is to place DDOS actions, including Operation Payback, in a historical and theoretical context, covering the use of the tactic, its development over time, and its potential for ethical practice. Guiding this work is the overarching question of how civil disobedience and disruptive activism can be practiced in the current online space. The internet acts as a vital arena of communication, self expression, and interpersonal organizing. When there is a message to convey, words to get out, people to organize, many will turn to the internet as the zone of that activity. Online, people sign petitions, investigate stories and rumors, amplify links and videos, donate money, and show their support for causes in a variety of ways. But as familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, is there also room for the tactics of disruption and civil disobedience that are equally familiar from the realm of street marches, occupations, and sit-ins?

The overwhelmingly privatized nature of the internet is a challenge to the practice of activism online, on the levels of large scale, peaceable assembly, free of expression, and civil disobedience. Early practitioners of distributed denial of service actions recognized this, and staged their actions, in part, with the goal of legitimating through practice civil disobedience online. However, their actions did not stop continued, successful efforts by corporate, state, and regulatory powers to render the internet a privately controlled space, similar to the "privately-controlled public spaces" that pepper our physical world cities today, such as Zucotti Park, the home of the original Occupy Wall Street encampment.[2] This forces disruptive activism into conflict with the rights of private property holders, the rights and philosophies of free speech fighting with deeply engrained property rights of individuals and companies. In the physical world, activists can take their actions to the street, a culturally respected, and legally protected, avenue for the outpouring of civic sentiment of all kinds, be it the 1963 March on Washington or the Nationalist Socialist Party of America on the streets of Skokie. There is no "street" on the internet.

Because of this rampant privatization and other reasons to be explored in this work, the theoretical and practical challenges faced by those seeking to engage in collective action, civil disobedience or disruptive activism online are different from those faced by activists organizing similarly motivated actions in the physical world. However, the two domains are often treated as though they were the same. Infringement on the property rights of private actors is often brought up as a criticism of DDOS actions, as if there was a space online that wasn't controlled by one private entity or another. Charges of censorship are usually thrown into the mix as well, because (ironically) of the internet's overwhelming use as an outlet for speech, by individuals, corporations, states, and everyone else. "Why," the critique goes, "can't you come up with a way to

[2] Foderaro, L. (2011, October 13) Privately Owned Park, Open to the Public, May Make Its Own Rules. *New York Times*

protest that doesn't step on somebody else's toes?" But the internet, as it were, is all somebody else's toes.

Collectively, we have allowed the construction of an entire public sphere, the internet, which by accidental design, has none of the inherent free speech guarantees we have come to expect. Dissenting voices are pushed out of the paths of potential audiences, effectively removing them from the public discourse. There is nowhere online for an activist to stand with her friends and her sign. She might set up a dedicated blog—which may or may not ever be read— but it is much harder for her to stand collectively with others against a corporate giant in the online space. Because of the densely intertwined nature of property and speech in the online space, unwelcome acts of collective protest become also acts of trespass.

While disruptive activism like distributed denial of service actions are condemned for being an unreasonable violation of others' rights, they are also derided as being too easy. This "slacktivism" critique posits that most tools of digital activism, from disruptive tactics like distributed denial of service actions to changing your Twitter or Facebook profile picture to proclaim your support of a cause, are lazy, simplistic modes of engagement which have little real effect on activist causes, and as such have no value. As Malcolm Gladwell articulates it in his critique of "slacktivism," which he refers to as internet based, "weak-ties" activism:

> In other words, Facebook activism succeeds not by motivating people to make a real sacrifice but by motivating them to do the things that people do when they are not motivated enough to make a real sacrifice. We are a long way from the lunch counters of Greensboro [North Carolina, 1960].
>
> (Gladwell, 2010)

Oxblood Ruffin, one of the founding members of the influential hacktivist organization Cult of the Dead Cow, made a similar critique of Anonymous's use of DDOS:

> I've heard DDoSing referred to as the digital equivalent of a lunch counter sit-in, and quite frankly I find that offensive. It's like a cat burglar comparing himself to Rosa Parks. Implicit in the notion of civil disobedience is a willful violation of the law; deliberate arrest; and having one's day in court. There is none of that in DDoSing. By comparison to the heroes of the civil rights movement DDoSing tactics are craven.
>
> (Ruffin, 2013)

These critiques makes a series of assumptions about the purpose and practice of activism and often ground themselves historically in the Civil Rights Movement and anti-Vietnam War protests. In this model, worthwhile activism is performed on the streets, where the activist puts himself in physical and legal peril to support his ideals. Activism is "hard," not just *anyone* can do it. Activism has a strong, discernible effect on its target. If the activist is not placing herself in physical danger to express her views, then it is not valid activism.

The "slacktivism" critique achieves its rhetorical purpose by holding a developing, theoretically-juvenile body of activist practices in comparison with the exceptional activist movements of the past. But, it fails to consider that activism can have many divergent goals beyond direct influence on power structures. It explicitly denies that impact on individuals and personal performative identification with communities of interest can be valid activist outcomes. It demands a theoretical and practical maturity from a sphere of activism (that is, online activism) that has not been around long enough to either adapt existing theory and practice to the online environment or generate its own. It casts as a failure the fact that the simpler modes of digitally-based activism allow more people to engage. As the cost of entry-level engagement goes down, more people will engage. Some of those people will continue to stay involved with activist causes and will continue to scale the ladder of engagement to more advanced and involved forms of activism. Others won't. But there must be a bottom rung to step on, and so-called "slacktivism" can serve as that in the online activist space.

Activist DDOS actions are easy to criminalize in the eye of the public. In fact, the overwhelming majority of DDOS actions reported in the news media *are* criminal actions. DDOS is a popular tactic of extortion, harassment, and silencing. Here is another challenge faced by practitioners of activist DDOS actions not faced by individuals participating in other types of disruptive actions: a sit-in is perceived as activist in nature, a DDOS action is perceived as criminal. Sit-ins are overwhelmingly used in activist situations. DDOS is deployed as a tactic of criminality much more than it is as a tactic of activism. This means that each use of DDOS as an activist tactic must first prove that it is not criminal before it can be accepted as activism. This raises vexing questions about the use of multi-purpose tactics in activism when they are also effective criminal tactics. Is it possible for DDOS to be taken seriously as a tool of activism when it must first overcome such a strong association with criminality?

These negative associations and assumptions are further entrenched by the terminology commonly used to refer to DDOS actions of all stripes: DDOS *attacks*. By referring to all DDOS actions, regardless of motivation as "attacks," the public, law enforcement, even practitioners, are primed to think of DDOS actions in terms of violence, malice, and damage. In order to conduct and present this analysis without this bias towards an interpretation of violence and harm, I do not use the term "DDOS attacks" throughout this thesis, but rather refer to all uses of DDOS as "DDOS actions."

Today's distributed denial of service actions are part of a history of denial of service actions. Actions like strikes, work slowdowns, blockades, occupations, and sit-ins all serve as ideological and theoretical antecedents to the digitally-based distributed denial of service action. Activist DDOS actions have undergone basic shifts in practice, purpose, and philosophy over the past two decades. Beginning as an exercise by experienced activists looking to stake out the internet as a new zone of activism, it is now mainly practiced by transgressive, technologically-mediated subcultures, often focused on internet-centered issues, who consider the online space to be a primary zone of socialization, communication, and activism. This has had implications for the basic sets of motives behind actions, the technological affordances present in the tools used, and the specific contexts of the tactics' deployment.

The structure of this work

This thesis will situate distributed denial of service actions within the spheres of both online and offline activism, addressing its development over the past two decades, and the particular aspects and challenges that separate it from similar types of disruptive activism in the physical world. Through this analysis of distributed denial of service actions, I address the broader issue of civil disobedience and the practice of disruptive activism in the online space. The internet is a vital outlet for innovative political speech, and civil disobedience is a valuable and well-respected tool of activism. This work attempts to put forward an analysis that will aide in the practice of civil disobedience on the internet, its perception as a valid form of contemporary political activism, and the online space as an appropriate zone for disruptive political speech and action.

I'll begin with two brief notes, which will explain some of the technical and legal aspects of distributed denial of service actions, as well as a timeline, which gives some brief background on the different DDOS actions examined in this work.

Chapter One looks at the different theories and models of practice that can motivate the use of DDOS as an activist tactic. These different models of practice each encompass a set of goals and rationale that in turn adapt the use of the tactic to a particular context. This chapter examines direct action, media manipulation, and biographical impact as models of practice that can animate a DDOS action. The chapter also considers several critical models: DDOS as censorship, DDOS as ineffective activism, and DDOS's unclear criteria for success.

Chapter Two examines the role of tool design and development in activist DDOS actions. For DDOS actions, the tool used is often serves a central, unifying function. It represents a shared jumping off point for the action. The design and affordances of the tool used can define a variety of aspects of the actions, including the level of engagement expected from participants, as well as indicating, after the fact, the types of individuals who were recruited and active, and the amount of political "seriousness" indicated by the action. This chapter looks at the design and development of the

Electronic Disturbance Theater's FloodNet tool, and two versions of Anonymous's Low Orbit Ion Cannon tool, paying particular attention to the changing functionality and interfaces of the tools.

Chapter Three examines several aspects of participant identity within the context of a DDOS action. A variety of identity constructions, revelations, and concealments come into play with DDOS actions. The anonymity that can be part of a DDOS action has become a particularly contentious issue among critics of DDOS actions, and is examined in this chapter. The construction of collective, performative identities within activist groups, especially with Anonymous is also examined, along with issues of gender, race, and class as played out in a technologically defined activist space. Finally this chapter explores how the concept of unsympathetic actors and "impure dissent," as defined by Tommie Shelby, applies to modern DDOS actions.

Chapter Four looks at state and corporate responses to activist DDOS actions. These reactions typically deny or belittle the activist nature of these actions, instead defining them as criminal or acts of terrorism or cyberwar. This strategy further diminishes attempts to keep the internet available as a public space, as it elevates the interests of security and stability over First Amendment issues. This chapter looks at how those interests are played out in the legal reactions to DDOS actions, the consignment of DDOS actions to the realm of terrorism and cyberwar, and in the structure of corporate internet presences and reactions to online protest.

Chapter Five provides an analytical ethical framework for the analysis of activism DDOS actions. The framework considers the use of the tactic within broader campaigns;

activists' motivations for using the tactic; the intended and actual effects achieved; the technological capacities used; power relations between organizers, participants and targets; and the role of state, state-related, and semi-state actors. Taken together, these factors create a holistic, qualitative system for evaluating the ethical validity of a given DDOS action, and can be used to create models to guide the use of the tactic, and similarly disruptive tools of digital activism in the future.

Technical Note

At its most basic level, a denial-of-service action seeks to render a server unusable to anyone looking to communicate with it for legitimate purposes. When this action comes from one source, it is called a denial-of-service, or DOS, action. When it comes from multiple sources, it is called a *distributed* denial-of-service, or DDOS, action. Complex or sophisticated tools are not necessary to launch a DDOS action. A group of people reloading the same website again and again at the same time could constitute a manual DDOS action if they intend to bring that site down. However, automated tools and methods are much more effective against websites that rely on today's web infrastructure.

One such automated method is to flood the target machine with "pings" from active machines. A ping is a request for availability, one computer asking another, "Are you there?" However, when employed as part of a DDOS action, the humble ping is transformed into a "ping flood," wherein thousands of ping requests a second can be transmitted to the target server. These requests quickly overwhelm the server's limited resources, and the server is unable to effectively respond to legitimate traffic requests. This is one of the goals of the action: “downtime” on the targeted server.

A DDOS action can exploit different processes to achieve its goal, monopolizing the lines that connect the server to the outside world or taxing the target’s processing and memory resources (Eddy, 2007). A mail bomb drops an enormous amount of e-mail messages onto a server, crashing it under the load. Making repeated process intensive requests, such as searches, can also cripple a website (Zuckerman, Roberts, McGrady, York, & Palfrey, 2010).

As mentioned above, a few dozen people clicking “Refresh” at the same site at the same time could constitute a DDOS action. Other, far less labor-intensive ways of waging such an action exist. One method is to employ a “botnet,” a collection of computers acting under the control of a central machine. Often these machines are innocents, having been illicitly infected with a program that renders them susceptible to the commands of the central machine (Zuckerman et al., 2010). Sometimes these are voluntary botnets, where users have volunteered their computing power by downloading and running a program. It is important to distinguish among actions carried out with botnets comprising compromised machines, voluntary botnets, and individuals operating autonomous machines. The use of nonvolunteer botnets has a significant affect on the ethical and political validity of an activist DDOS action. This will be examined in detail in a later section.

To defend against a DDOS action is difficult and expensive. One can attempt to block the individual IP addresses the noxious traffic appears to hail from, but it is possible for a participant to spoof an endless series of IP addresses, turning simple blocking into an endless game of Whack-A-Mole. If the action is distributed across a sufficiently large number of machines, the number of packets sent by each machine need not be particularly large, making it difficult to tell legitimate traffic from illegitimate. One could acquire the servers and processing power necessary to absorb the additional traffic until it abates. This avenue is generally available only to large corporations able to handle its high costs. As a result, smaller sites can sometimes be driven offline completely by a DDOS action of relatively short duration, not through the direct process of the DDOS itself but through the reactions of support services, like ISPs (Zuckerman et al., 2010).

Legal Note

DDOS actions are considered illegal in most jurisdictions. In the United States of America, DDOS actions are prosecuted under Title 18, Section 1030 (a)(5) of the U.S. Code.[3] The crime described by the statute is the "intentional . . . damage" of "protected

[3] This section, known colloquially as the Computer Fraud and Abuse Act (1984), forbids any action that
"(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."

A "protected computer" is defined in Title 18, Section 1030 (e)(2) as

"a computer—(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by computers," broadly defined as computers used, in whole or in part, by financial institutions or the U.S. government. However, as will be discussed later, confusion persists about the legal status of activist DDOS actions, something that presents serious challenges to the organizers of these actions.

There are many confluences of computational circumstances that appear identical in form to a DOS or DDOS action but that are not DDOS actions. For example, a website operator may use an automated "stress-testing" tool to generate an exceptional amount of traffic directed at a particular server to see how the machine reacts, essentially launching a DOS action against his or her own machine for research purposes. There is no difference between the basic functionality of a stress-testing tool and an automated DDOS tool, and most automated DDOS tools are usually distributed as stress-testing tools.[4] Another example of a "DDOS that is not a DDOS" would be the crash that sometimes occurs when a popular blog links to a site whose server buckles under the unexpected crush of attention. The linker did not direct his or her followers to click the link with the intention of crashing the site, as with a manual DDOS, but the

or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

[4] As noted by havonsmacker (2010) at the "loiq" distributed denial-of-service (DDOS) tool download page:
"LOIQ stands for LOIC [Low Orbit Ion Cannon] in Qt4. It is an attempt to re-create the LOIC server stress-test tool using Qt4/C++ instead of original C#/.Net to make it available under *NIX OSes (primarily under Linux). It is released under the terms of GNU GPL 3 or later."
It is worth noting that this "a-wink-and-a-nod" method of distribution has a physical-world analog in the sale of glass pipes "for use with tobacco only." This is seldom their ultimate use case. Thanks to Ethan Zuckerman for pointing out this parallel.

effect is the same. This makes the stipulations that crimes under the Computer Fraud and Abuse Act (1984) be "intentional" an important one.

Similarly, identical actions that intend to knock a site offline could be undertaken for significantly different motivations. A DDOS action may be launched against a site in an attempt to force it to remove a specific piece of content or in an effort to drive a vulnerable site offline entirely, by making it impossible for an ISP to host the content. Online publications and small ISPs are particularly vulnerable to this type of action. An example of this occurred in 1997, when a large, popularly supported DDOS campaign was launched against the ISP Institute for Global Communications (IGC, 1997) in an effort to force it to stop hosting a Basque web publication, *Euskal Herria Journal* (Nicol, n.d.). The IGC's servers were knocked offline, rendering inaccessible the websites and e-mail of more than 13,000 subscribers. Although the IGC did eventually remove the *Euskal Herria Journal*'s content from its servers, it replaced it with a statement decrying what it saw as vigilante censorship on the Internet and was supported in its arguments by groups such as NetAction, Computer Professionals for Social Responsibility, and the Association for Progressive Communications (IGC, 1997). When classifying these types of actions, it is useful to consider the centrality of an online presence to the target's mission. To take an ISP or a small blog offline can effectively destroy that organization or individual's ability to fulfill its professional purpose and communicate with the public. These cases might be viewed as instances of cybercrime, cyberterrorism, or censorship, and will be discussed in detail later.

Alternatively, a DDOS may be launched against a large, well-defended corporate or government site, one unlikely to fall under the pressures of a DDOS action, for the purpose of drawing attention to an issue. Such corporate or governmental homepages rarely serve a vital role in the operations of those organizations. One does not go to www.starbucks.com to get one's morning latte. Furthermore, such organizations use established press channels to communicate with the public, not poorly trafficked homepages that more often than not serve a placeholder or trademark defense purpose. To briefly tear down the online poster of these organizations (Munroe, 2011) may serve a symbolic purpose and be a good way to attract attention, but it often has little effect on their practical, day-to-day operations. Actions aimed against such sites can be seen as an example of "electronic civil disobedience" or valid online protest (Auty, 2004; Critical Art Ensemble, 1996). The U.S. statute, however, contains no provisions acknowledging that such an action could constitute political speech.

The technological simplicity behind a DDOS action has contributed to its attractiveness as an activist tactic. One does not need advanced technical skills to construct a simple automated DDOS tool and virtually no skills to participate in a manual DDOS. A DDOS action also lends itself conceptually to metaphors and comparisons to physical-world activism. Activists have often called DDOS actions "virtual sit-ins." By invoking this metaphor, they seek to take advantage of the cultural capital and symbolism of historical sit-in campaigns (Rolfe, 2005). This comparison is imperfect yet commonly invoked. The virtual sit-in metaphor is just one of a number of models and metaphors used by the tactics proponents and critics to conceptualize DDOS within existing activist practice. The use of DDOS as a protest tactic has evolved as the political identity of the Internet has grown more complex. Before the use of this tactic can be understood, the tactic's place in the overall culture of digital activism must be understood.

CHAPTER 1

Theories and Models of Practice

Activist actions, be they street marches, petition drives, or DDOS actions, are each individually driven by particular theories of change and models of practice. Theories of change set out hypotheses of how change may be effected within a given system, while a model of practice is an attempt to codify a given theory of change into an example that may be followed. An analysis of these theories and models as they apply to specific actions can illuminate the motivations of the organizers and participants and their histories and political philosophies, as well as serving as benchmarks in the evolution of DDOS as an activist tactic itself. Such an analysis can also provide a space where we can evaluate the expected value of DDOS as an activist tactic and its perceived shortcomings in concert with case studies; we can set theoretical expectations against actual events, and thus judge the usefulness of different theories and models as they are used in activist DDOS actions. Although there are numerous possibilities, this section will focus on direct action, media manipulation, and biographical impact, along with historical examples to highlight the interpreted strengths, weakness, affordances, and controversy points of each of these models. I will follow by examining several critical models.

DDOS actions are rarely driven by a single theoretical or practical motivation. Often there are a number of overlapping goals and justifications, added on as the action is developed in the context of a larger campaign. The examples presented below, though used to illustrate definitional norms of activist DDOS practice, should not be taken to mean that the theories and models described were the only ones present in a given action. While the examples were chosen because they allow certain details and questions central to the different models to be brought more clearly to light, they often contain aspects of other models in practice and a plethora of motivations.

DDOS as direct action

Direct action in activism is an embodiment of an inherently confrontational philosophy of action. Direct action tactics value direct confrontations with structures of power, often state or corporate in nature. The tactics aim to both disrupt through action a prevailing structure viewed by the activists as causing harm, and to, by challenging that structure, provoke a response which is then allowed to stand on its own as an illustration of the reality of the challenged institution (Thompson 2010). Drawn from anarchist and Situationist philosophy, direct action tactics aim to inject direct, actualized democracy into the activist process (Graeber, 2007). In so much as it relies on the revelatory spectacle of the provoked response, direct action communicates more to spectators and participants than to targets, though an exchange with the target is necessary to provoke the spectacle of response. When the on-the-street tactics involve physical disruption of property, such as the destruction of corporate property as often practiced by Black Bloc anarchists, or violent confrontations with law enforcement, this model is the most vulnerable to accusations of hooliganism and terrorism in the media and by law enforcement (Thompson, 2010).

In the case of DDOS actions, those pursuing the direct action model are motivated by a desire to disrupt a process for the purpose of disrupting that process and potentially provoking a cascade of responses, on technological, political, media, and social levels. Direct action DDOS also highlights the importance of "place" within digital activism, which is here explored through Timothy Zick's concept of "contested place."

The Electrohippies vs the WTO, 1999

In late November, 1999, the World Trade Organization held its Ministerial Conference in Seattle, Washington. The city streets were filled with protesters opposed to the WTO's pro-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. After the aggressive reactions of police and city officials to the activist activities, the events surrounding the WTO Ministerial Conference become popularly known as the Battle for Seattle. It is seen as an important moment in the development of the anti-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 though December 4, *the electrohippies* organized and staged a combination DDOS/e-mail bombing campaign targeting the WTO's main conference servers, public-facing websites, and 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 the Electronic Disturbance Theater's Zapatista FloodNet tool, which was developed in 1998 and released to the public in 1999. The limitations of the tool 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. *the electrohippies* 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 (DJNZ, 2000). The goal of the DDOS action, stated in the calls to action *the electrohippies* distributed on various mailing lists and on its website, was to hamper the PR efforts of the conference:

> *the 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.
>
> (Ehippies@tesco.net,1999))[5]

After the DDOS campaign ended on December 4, *the electrohippies* began a two-day email bombing campaign, the group directed their supporters to email large, uncompressed picture and document files (some suggested documents were the Kyoto

[5] ehippies@tesco.net (November 29, 1999) WTO Sit-in open! - enter the virtual protest now! Message posted to diggers350 yahoo group, archived at groups.yahoo.com/group/Diggers350/message/236

Protocol on Climate Change, and several EPA and WHO reports) along with personal messages, to a list of WTO affiliated addresses. The goal was to overwhelm the internal email 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 messages 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.
>
> (Ehippies@tesco.net,1999))[6]

The Battle in Seattle, online and on the ground

As with other early proponents of online-based activism, *the electrohippies* were interested in creating models of online activism that were functionally and philosophically equivalent to physical practices already in existence. They were particularly interested in establishing the online space as an arena of activism socially, culturally, and legally equivalent to the physical world. Like the Electronic Disturbance Theater, *the electrohippies* drew heavily on 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

[6] ehippies@tesco.net (December 2, 1999) THE WTO SIT-IN: PHASE 2 STARTS NOW! Message released by *the electrohippies*, archived at www.thing.net/~rdom/ecd/phasetwo.html

> accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure.
>
> -DJNZ, (2000)[7]

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 electrohippies* referred to this approach as "server side" DDOS actions, 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 participants to bring down a site. *The electrohippies*, and the EDT before them, purposefully hamstrung the technological tools they used in order to maintain a one to one participant to signal ratio.

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

[7] "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. They 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 its 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)

commercial interests. The WTO action was intended to hamper the public and private operation of the WTO, but was also intended to be a forceful, public-facing statement in support of the right of the public to use the internet as an activist space. The Supreme Court articulated a continuum of public fora, adeptly described by McPhail, Schweingruber, and McCarthy in "Policing Protests in the United States: 1960-1995," and by Timothy Zick in *Speech Out of Doors*. 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 towards 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, wherein the state is forbidden from regulating speech based on content, and only permitted to regulated the "time, place, and manner" of speech acts (Zick, 2009). "Private property" is the most restrictive, wherein the owner of the property has extensive license to regulate speech as it occurs on her property (McPhail, 1998). *the electrohippies'* action can be seen as an attempt to re-assert the fundamental reality of the internet as a "public forum" in the face of its attempted re-designation as "private property" (McPhail, 1998). 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 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 like the Electronic Disturbance Theater 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 offline by the force of the DDOS. That presence remains in the non-responsive 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 has a transitory equivalence in 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.

Destruction, in the case of physical world altercations with corporate facades, and disruption, in the case of DDOS actions, is part of the sought after spectacle: the responsive-made-unresponsive, the available-made-unavailable. Ensuing media coverage, statements of corporate spokespeople, and reactions of law enforcement, including those present at the scene, all add to the spectacle being produced. As the public consumes the spectacle of destruction/disruption and response, the hope is that they will be drawn out of passive consumption and to action.

Direct action DDOS actions also emphasize the value of "place" in online activism. Some critics of direct action acts of digital activism, like DDOS actions or website defacements, ask why the activist actions can't be moved offsite, 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" (Zick, 2009). 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." Contested places serve to "facilitate, amplify, and convey particular messages" (Zick, 2009, p 105). 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 (Zick, 2009). Sequestering physical world activists in an isolated "demonstration zone" or digital activists in an perhaps even more isolated "activist domain" severely hampers activists ability to get their message out to individuals to whom it would be the most relevant. As will be discussed in Chapter Five, the open airing, reception, and discussion of dissenting views is a vital part of democracy. To deny activists access to contested places because of their potential for disruption hamstrings 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.

DDOS as media manipulation

A second model for DDOS in activism is as a tool of media manipulation and popular attention direction. In this instance, the DDOS action is primarily used to focus attention on an event or issue external to the DDOS itself. The challenge, as is the case with public, performative activism in the physical world, is getting media outlets to cover the issues that drive the activism, and not merely the spectacle of the activism itself or tactics used.

The Electronic Disturbance Theater: no such thing as bad press?

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" (Gitlin, 2003). The use of innovative tactics and settings present a challenge as multiple parties (activists, law enforcement, state actors, corporations) 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 defined 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.

The Electronic Disturbance Theater pioneered the use of DDOS actions as a tool of popular activism, beginning in 1998 with a series of pro-Zapatista actions targeting a number of sites, using a specially developed tool called FloodNet. The EDT referred to their actions as "virtual sit-ins," a strategy picked up by subsequent groups like *the electrohippies*, relying on the historically-loaded nature of the term to act as a type of pedagogical short hand as to the legitimacy and certain formal aspects of the DDOS tactic (Rolfe, 2005). The EDT 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 DDOS tool designed and used by the EDT in the 1990s and early 2000s and which will be examined in detail in a later chapter, rarely resulted in actual downtime for the targeted sites (Wray, 1998). 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 (Dominguez, 2009).

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 the EDT and their "virtual sit-ins" in digital activism trend pieces, more interested in performing a roll call of the activist space than 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..." (Harmon, 1998). Some 14 other individuals and organizations, consistently referred to as "hackers," are mentioned in the 2,025 word article. Stories in the *Ottawa Citizen*[8], *Computerworld*[9], and the *Sydney Morning Herald*[10] followed a similar pattern. Other articles grouped the EDT and other activist organizations under the label "cyber-terrorists"[11] or force these activities into a cyberwar framework, using phrases like "targeted cyber attacks" and "firing the first shots in a cyber war" to describe protest actions.[12]

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

[8] Paquin, B. (1998, October 26) E-Guerillas in the Mist. *Ottawa Citizen*

[9] Radcliff, D. (2000, October 16) Meet the Hacktivist. *Computerworld*

[10] Nguyen, M. (2002, August 17) Armchair Activism. *Sydney Morning Herald*

[11] Regan, T. (1999, July 1) When terrorists turn to the Internet. *Christian Science Monitor*

Editorial (1999, November 10) Cyber-terrorism's threat becoming real. *Hamilton Spectator*

[12] Lasker, J. (2002, May 14) Hackers Use Computer Skills to Promote Politically Motivated Mischief, Mayhem. *Buffalo News*

would be a stretch to consider the FloodNet actions to be successful on that level (Meikle, 2002). 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 what was not required was the actual story of the activism behind the tactic's use.

Toywar allies: third party advocacy and packaged narratives

In December of 1999, the EDT, the Swiss art group etoy, and RTmark 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 (Wark, 2003). 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" (Dominguez quoted in Wark, 2003), as well as hamper 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 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 national 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 RTmark, etoy, or the EDT as terrorists, criminal hackers, or even cybersquatters. Rather, news outlets made extensive use of the David and Goliath narrative of 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[13]. The etoy/toywar coverage, on the other hand, included the voices of John

[13] A June, 1999 *Christian Science Monitor* article, "Newest tool for social protest: the Internet," quotes a RAND researcher, the director of a social-justice group, and a University of Texas professor as saying 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." (Van Slambrouck, 1999)

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. (Regan, 1999)

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

Perry Barlow and attorneys at the Electronic Frontier Foundation[14] and a judge for the 1996 Prix Arts Electronica[15].

The presence of the solid, easily understandable 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: a study in manipulation

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 (Phillips, 2012). This ability was on display during the Operation PayBack DDOS campaign in December 2010, sometimes known as Operation Avenge Assange. During this action, the high

defacement, malware, and included theoretical future attacks on infrastructure. All groups, real and imaginary, were referred to as "hackers" or "hacktivists." (Lasker, 2002)

In 1998, the *New York Times* called the EDT's 'virtual sit-in' "largely nuisance attacks and the equivalent of electronic graffiti…" (Harmon, 1998)

[14] *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 Electronic Frontier Foundation 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..." (Kettmann, 1999)

[15] 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 that restricted the ability of etoy to sell "stock" in the United States. (Leiby, 1999)

level of quotable, embed-able graphic and video artifacts produced by the group allowed them a level of control over the media narrative that the EDT did not enjoy. Anonymous is, as a group, difficult for the media to cover, but their cultural artifacts are highly accessible online. By pushing the production and peer 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 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 Low Orbit Ion Cannon tool (which will be examined in detail in a later chapter), Anonymous targeted more than ten different sites over the course of four 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 (Correll, 2010). Many of the sites targeted experienced at least some amount of downtime.

Unlike the EDT, *the electrohippies*, and other groups discussed in this thesis, 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 rampant confusion about the facts. There was genuine fear that any organization or individual could be Anonymous's 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 being so freely deployed. Add to this the fact that one of Anonymous's 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*[16] (Bell, 2010) and the social media news site *Mashable*[17] (Erlich, 2010).

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, and who was anyone to say it was not true? 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

[16] 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 & Copyright," which in turn linked to a Anon-run twitter account.

[17] In a post entitled "Operation Payback Targets Amazon.com," *Mashable* linked to numerous Twitter accounts which were tweeting scheduling and targeting information, as well as linking to the *Encyclopedia Dramatica* page on the Low Orbit Ion Cannon DDOS tool, in addition to embedded the same call-to-action video that the *Washington Post* also embedded.

technological skills to access the channel on their own. The combination of the demands of the 24-hr 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 which 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 above both embedded the same call-to-action video, which had originally been linked to by the *New York Times* blog, "The Lede" (Bell, 2010). 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" (Boczkowski & de Santos, 2007). Anonymous's continual furnishing of quotable, embeddable, compelling descriptive content exacerbated an already present 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 (Coleman, 2012). It is likely that without this influx of new participants, the Operation Payback DDOS actions would not have resulted in the downtime they did.[18] This substantial increase in active participants during Operation Payback was, in large part, attributable to the extensive, relatively uncritical media coverage given to the December stage of Operation Payback.

DDOS as a tool of biographical impact

We've looked at direct action and media manipulation through their specific theories of change, models of practice, and historical case studies. Another model for the use of DDOS in activism under consideration is as a tool of "biographical impact." This is the impact the experience of participation has on the individual activist. Doug McAdam differentiates between two varieties of biographical impact: conversion and alternation. He defines "conversion" as "a radical transformation of a person's life, including their self-conception, network of associations and larger worldview...[which] tends to occur in groups that demand the exclusive loyalties of its members and maintain a hostile stance toward mainstream society." The milder "alternation" consists of "identity changes that are not as drastic as conversion...which are part of or grow out of existing programs of behavior." Alternation can take place in groups that are "relatively more inclusive and tolerant of the other attachment of its members" but which "...can be very demanding of a person's time, energy, and loyalties." The more

[18] As addressed in a later chapter, the use of illicit, non-volunteer botnets contributed substantially to achieved downtime.

culturally immersive an activist experience is, in terms of exposure to like-minded peers, the creation of social and technical structures of support and interaction, and the furnishing of a vocabulary to articulate the experience, the more likely it is to result in alternation on the part of the individual.

Here is it particularly useful to remember that DDOS is often most effectively used within the context of a larger campaign, wherein multiple tactics are utilized. Ideally, these tactics each reinforce a certain ideological stance of the group and provide opportunities to lead participants from one tactical action to another.

The Culture of Anonymous: biographical impact in Operation Payback

The precise nature of Anonymous is a difficult thing to pin down, but it is best described as a "culture" (Norton, 2011a, Auerbach, 2012). Quinn Norton articulates the characterization of Anonymous-as-culture this way:

> It takes cultures to have albums, idioms, and iconography, and I was swimming in these and more. Anonymous is a nascent and small culture, but one with its own aesthetics and values, art and literature, social norms and ways of production, and even its own dialectic language.
>
> (Norton 2011a)

Auerbach identifies what he call "A-culture," which broadly encompasses the trolling, anonymous, internet-based sub-altern counter public of which Anonymous is a part. A-culture is strongly defined by the online communications technologies on which it was originally reliant. These technologies were text and static-image based, fundamentally anonymous in their attribution structure, and "evanescent," containing no archive of interactions or communications. Core to A-culture, Auerbach observes, are the practices of ironizing, recreational offense, self-documentation, elitism, and heightened meta-awareness, coupled with persistent economies of suspicion and unreality (Auerbach, 2012). I would add to this highly democratized modes of appropriation-based production, which while being extremely social and open, operates as an effective shibboleth into the active culture. Knowledge of and competencies with certain suites of cultural reference are expected of participants. The ability to actively participate in the production of cultural artifacts, using a practice-vocabulary based in the appropriation and remix of images from popular culture and A-culture itself, is also expected.

The evolution of Anonymous from an inward-facing group concerned with its own amusement often at the expense of outsiders to an open activist culture adept at attention-building and attractive to the uninitiated occurred over time, though several trigger events hastened developments significantly. Prior to the WikiLeaks-related actions of 2010, Anonymous was known in part for the internet memes that spilled forth from the board (some examples are rickrolling[19] and lolcats)[20], and in part for intensely personal harassment campaigns and aggressive "raids" it conducted across the Internet (Coleman, 2012). Sometimes these raids were DDOS actions; other times they were site invasions, wherein massive numbers of Anons would converge on a site to monopolize comment threads or occupy a location in massively multiplayer online games (Coleman, 2011b). A key factor was the aesthetic of "doing it for the lulz," an

[19] "Rickrolling" is a "bait and switch" meme, wherein a person is tricked into clicking on a link leading to Rick Astley's 1987 "Never Gonna Give You Up" music video.
[20] Lolcats are pictures of cats with humorous text inscribed on them.

agenda of having fun at the expense of another (Coleman, 2012). Like many active in hacker and Internet culture, Anons valued free speech and the autonomy of the Internet, although their early raids were more often than not focused on showing up their target and generally causing hilarious (to them) chaos.

Beginning in 2008 with Operation Chanology, the actions of Anonymous began to take on a more overtly political tone. Operation Chanology targeted the Church of Scientology, initially for attempting to legally force the takedown of a video featuring Tom Cruise talking about the church, but it later expanded to more general objections to the church itself (Coleman, 2012; Vichot, 2009). The operation involved DDOS actions and other digital tactics as well as physical-world street protests. It marked the first occasion Anonymous raids crossed over into the physical world, with masked Anons gathering outside Church of Scientology locations in various cities and countries, holding signs and protesting the church's policies. This was a controversial step among Anons. Some objected to taking Anon actions to the streets, arguing that Anonymous should restrict its actions to the online space.[21] Others felt that the political tone of Operation Chanology was in opposition to the "spirit of the lulz" that had previously defined Anonymous (Coleman, 2011a). Operation Chanology represented a shift in the makeup and tenor of Anonymous. The "lulz" lost its purity, and raids began to represent a developing political sensibility, one heavily influenced by net libertarianism, free-

[21] Previous to this, the Electronic Disturbance Theater, *the electrohippies*, etoy, and other groups had used DDOS as a tactic within larger campaigns, often in coordination with other organizations. Anonymous's internal dispute about coupling street protests with DDOS actions and other digital tactics is special to Anonymous, and arose in part because of the "internet-native" nature of the group, which had previously been active only in the online space.

speech absolutism, moderate levels of anarchy (Coleman, 2011a), and a strongly held belief in the ethical treatment of cats ("Dusty the Cat," 2011).

Anonymous's activist incarnation is primarily represented by two visual icons: the Guy Fawkes mask, and an empty black suit. Of these, the Guy Fawkes mask has proven the more durable, and more effective representation. It is also an efficient metaphor for the identity subsumation that occurs as individuals become involved in Anonymous actions. Anonymous's conception of identity within the culture is at base a pluralistic one. The power and attraction of Anonymous is built out of the concept of the hoard, the mass, the unstoppable wave. "We are legion. We do not forgive. We do not forget. Expect us," is the unofficial motto of Anonymous. It appears in videos, image macros, and all manner of viral media produced by and around Anonymous. The phrase "We are legion" comes from the Gospel of Mark, from the story where Jesus exorcises a demon from a possessed man. When asked for its name, the demon replies, "αὐτῷ Λεγιὼν ὄνομά μοι, ὅτι πολλοί ἐσμεν:" meaning, "I am [called] legion, for we are many." The original phrase, perhaps better than the Anonymous adaptation, captures the peculiar nature of the Anonymous identity meme, wherein many different identities are drawn up and into a single identity. One central source is made more powerful by the participation of many individuals. But those individual identities move in and out of different states of participation. Individuals join in under the banner of Anonymous, temporarily subsuming their personalities under the larger, meta-personality of the Anonymous hoard.

A technological parallel for this, which will be examined in detail in a later chapter, is the “Hive Mind” mode built into a version of the LOIC DDOS tool, which was popular during the Operation Payback DDOS actions. When running in Hive Mind mode, rather than independently targeting and deploying the tool, a participant choreography familiar from the EDT and *the electrohippies* use of the independently controlled FloodNet tool, you could instead place your computer under the control of a central IRC server. By joining this voluntary botnet, you were able to add your individual digital voice to the stream of other voices being controlled by an overarching persona: “I am legion, for we are many."

Three aspects of Anonymous culture and activist practice make it more likely that individuals who participate in the Operation Payback DDOS actions would experience alternation or conversion as a result. First, the communications channels used for planning, publicity, and in-group socializing were often open and public. These included many IRC channels and various social media accounts. Through IRC and social media channels, participants were immersed in a like-minded peer community, one in the throes of an intensely active period whose energy persisted after the end of the Operation Payback actions. Very shortly after the end of Operation Payback, the Arab Spring, the HBGary hack, Occupy Wall Street, and other events repeatedly triggered and reinforced the activist instincts of the Anonymous population, who continued to use the communications practices used in Operation Payback.

Second, Anonymous visual culture relies on appropriation and remix practices, liberally quoting from pop culture and from itself in persistent, borderline repetitive cycles of production. This means the ability to quickly produce highly relevant cultural products is easily available to members of the in-group, already privy to the layers of meaning and reference contained within the symbols. For outsiders, particularly outsiders in the media, the opaque, hieroglyphic nature of Anonymous visual culture, which during Operation Payback and its aftermath were experiencing a super-proliferation online, made the images and videos highly useful for their reductive, symbolic value. The use by the media of these artifacts of Anonymous visual culture to represent Anonymous further reinforced their value as meta-symbolic objects within the culture and made their production a more experientially valuable enterprise. As the visual culture spread, the ability to repeatedly produce culturally-consistent artifacts became a more important marker of insider status than simply recognizing or correctly interpreting specific cultural tropes.

Third, the "hive" model of action valued by Anonymous activists, which requires a merging of personal agency and identity with a overarching supra-identity structure, assigns all participants the activist identity, regardless of experience or participation level. Even "passive" participants whose favored mode of participation was turning on Hive Mind and walking away were just as important to the success of the action as those who man their terminals for the duration. Those who had considered themselves to be an audience in the world of politics and industry could become actors, strengthened by the invisible yet palpable presence of thousands of their new comrades-in-arms.

Each of these factors reinforce each other and channel participants from one impactful activity to the next. An individual may initially encounter a call-to-action on Twitter, participate in a DDOS action, and subsequently contribute to planning chats, collaborative manifesto writing, or video production. Each draws the participant deeper into the culture and creates more opportunities for biographical impact. Participants may also dip into one or two activities, or participate once and never return to the culture. However, the cultural nature of Anonymous actions fosters many opportunities for participation for those who are interested.

Critical models of DDOS actions

There are also a number of critical models used to describe the use of DDOS in activism. These models highlight ways in which the use of the tactic can go awry or become incompatible with other modes of activism. Though most of these criticisms will be addressed in detail in the ethical framework section, I will briefly describe them here.

The Digitally Correct model: DDOS as censorship

The "censorship" model is a common critical model of DDOS in activism. Most vocally put forward by hacktivist groups such as Cult of the Dead Cow and Hacktivismo, Jordan and Taylor (2004) have 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. Hacktivists considered the primary goal of hacktivsm to be defeating state censorship and the disruption of online communications via the creation and distribution of tools to evade censorious regimes (Jordan and Taylor, 2004; Raley, 2009). 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 an public forum by shouting down one's opponent" (Ruffin, 2000).

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 (Ruffin, 2004), and digitally empowered activists like the EDT and *the electrohippies*, who were more often than not experienced activists using Internet tools and capabilities to supplement more traditional, physical-world actions (Dominguez, 2009). Hacktivists, coming from a culture that values personal autonomy and the freedom of information (Wray, 1998), 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 (Wray, 1998).

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." (Ruffin, 2000) 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, Hacktivismo were often engaged in building tools of dubious legality, tools that enabled users to encrypt their communications, evade fire-walls and censors, and mask their Internet traffic (Ruffin, 2004). 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 (Ruffin, 2004). Interestingly, these groups operated in a fashion that more closely resembled what the Critical Art Ensemble, the primogenitor to the EDT, had envisioned as the operating model for electronic civil disobedience than what the EDT did. The Critical Art Ensemble envisioned practitioners of what they termed "electronic civil disobedience" to operate 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 (Critical Art Ensemble, 1996).

The EDT and *the electrohippies* were strict 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 such as 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" (Wray, 1998). 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, wherein a large DDOS action was held in order to force an ISP to stop hosting a particular website. In other instances, the criticism fails to recognize unequal power dynamics between targets and activists (as when a group of individual activists DDOSes a multi-national 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, non-state actors and censorship, traditionally conceived of as a state-mediated action, opens up questions about what entities are capable of performing censorship, particularly in the online space. While DDOS is undoubtedly a "disruptive" tactic (Costanza-Chock, 2001), disruption does not always equal a denial of speech rights. Later we will examine examples of DDOS actions where I argue that though 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 non-activist 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 offline 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 offline completely by a DDOS of relatively short duration (Zuckerman et al., 2010). State-sponsored or state-directed DDOS actions are not considered to be activist actions in this analysis, and as will be shown later, a DDOS waged to effect the permanent removal of content is not considered to be an ethical use of the tactic. But the tactic does have the propensity to be misused in this fashion.

The Critical Art Ensemble: symbolic dissent is ineffectual

In the 1996 essay, "Electronic Civil Disobedience" (Critical Art Ensemble, 1996), the Critical Art Ensemble, a performance art and activist group active in the United States and Europe, 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. Electronic civil disobedience 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, semi autonomous cells of specialized practitioners, each performing a specific action or role within a larger organization, while simultaneously maintaining individual identities within the larger group (Critical Art Ensemble, 1996). Central to the CAE's vision was the clandestine and essentially closed nature of the actions, an aspect the CAE terms an "inversion" of traditional civil disobedience (CAE, 2001). This sprang from a belief that electronic civil disobedience "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 of government agency that is not fully prepared to do battle in the media" (CAE, 2001). The CAE criticized the actions of groups like the Electronic Disturbance Theater (a spin-off from the CAE) 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. As I argue later in this paper, it is important to consider the tactic in context. The validity of the tactic is equally dependent on the activist structure that surrounds it as any qualities inherent in itself. Moreover, DDOS actions were not primarily conceived of as stand-alone actions. EDT member Stephen Wray notes “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" (Wray quoted in Raley, 2009). To divest DDOS of its "component" nature (Raley, 2009) 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.

How will we know when we've won?

Critics of DDOS activist 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 (Wray, 1998). So if 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 result

(Foucault, 1990). Ricardo Dominguez termed this phenomenon "permanent cultural resistance; there is no endgame" (Dominguez quoted in Raley, 2009). 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 tool of biographical impact, DDOS acts tool for the revelation of "hidden transcripts" of resistance (Scott, 1990). As previously described, 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" (Scott, 1990). This is a quality which will become increasingly valuable as digital activism continues to be unbounded by state borders and moves towards a transnational operational norm.

Conclusions

Direct action, media manipulation, and biographical impact are three major theories behind the use of DDOS as an activist tactic. Though technologically undifferentiated, activist DDOS actions can be strikingly different from each other depending on the theories and practice models used to animate them. While a direct action DDOS aims to disrupt and provoke a response spectacle, a media manipulation

DDOS looks to direct media coverage away from the novelty of the activist action and towards a larger issue. When used as a tool of biographical impact, DDOS actions serve to draw participants deeper into a particular activist culture, where different modes of participation can be introduced. As each of these theories and models positions DDOS differently within activism, they also embrace different assumptions about the best activist use of the online space, as do the critical models I described. These models are not mutually exclusive, though some critics of activist DDOS actions may describe them that way. It's true that DDOS can and repeatedly has been used in extortionist, repressive, and censorious ways by criminals, state governments, and other bad actors. However, the potential for misuse should not preemptively condemn all potential uses of the tactic. As the first three sections of this chapter have shown, motivating theories for DDOS actions exist beyond the simple extortion-censorship-harassment continuum. In the next chapter, I'll look at how the design of tools used in an activist DDOS action can impact their form, function, as well as who participates and how.

CHAPTER 2

A Comparative Analysis of DDOS Tool Design

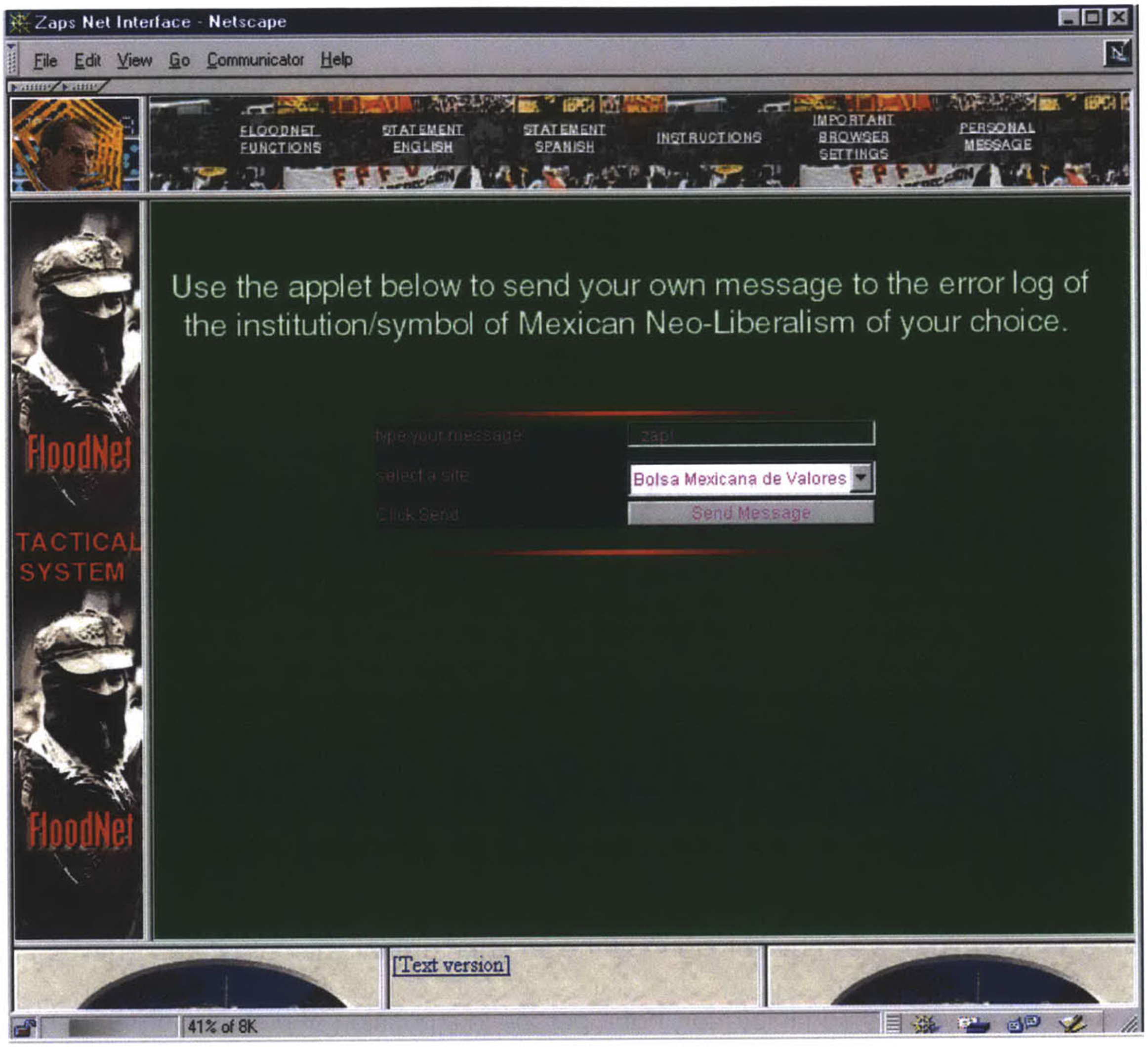
In this section, I will be tracing the development of the Electronic Disturbance Theater's FloodNet DDOS tool and Anonymous's family of LOIC DDOS tools, highlighting where their functionalities overlap and diverge. The language and memes used in the tool interfaces are of particular interest here, as they can be analyzed to show the lineage and intended audience for the tool. I will be analyzing FloodNet and two iterations of the LOIC tool, one developed contemporaneously with Operation Chanology and a later version used during Operation Payback. Much of the functionality present in LOIC was present in FloodNet.

As activist events, DDOS actions tend to be undertheorized by organizers, participants, and academics. Though the previous chapter was an attempt to address that at the level of social movement theory, this chapter uses the technological tools used during these actions as an additional point for the analysis of these actions. Rather than looking at them on a purely technological level, this chapter examines these tools in the context of activist actions and communities, at how their existence impacts campaigns. For DDOS actions, the tool used is often serves a central, unifying function. It represents a shared jumping off point for the action. The design and affordances of the tool used can define a variety of aspects of the actions, including the level of engagement expected from participants, as well as indicating, after the fact, the types of individuals who were recruited and active, and the amount of political "seriousness" indicated by the action.

The Electronic Disturbance Theater and FloodNet

The FloodNet tool was created in 1998 by the EDT and operated by exploiting the Java applet reload function. Participants ran FloodNet from a browser window by navigating to a specific page and allowing the tool to run in the background (Wray, 1998). "Messages" could also be sent to a target website by using FloodNet to insert "404_file not found" messages into the target server's error logs. A participant would choose a target from a list of preselected options, type a short message, and hit "Send." FloodNet would request a file from the target server that corresponded to the message text, causing a 404 error log to be generated.[22] For example, the message "human rights" would generate the error message "human_rights not found on this server" (Jordan & Taylor, 2004). This performative "messaging" functionality would also appear in Anonymous's LOIC DDOS tool. Although it was possible that these generated messages could be seen by someone at the targeted organization, that person was likely to be a systems administrator, not a person in a position of power. Consequently, these messages serve primarily as an one-way outlet for the participant rather than a tool of communication. This was replicated during the Operation Payback action as well.

[22] A "404 error" is the hypertext transfer protocol response code generated by a server when the file being searched for cannot be located. Such an error would be logged by the server in logs that could be accessed by a systems administrator later.



Use the applet below to send your own message to the error log of the institution/symbol of Mexican Neo-Liberalism of your choice.

type your message: zap!

select a site: Bolsa Mexicana de Valores

Click Send

Figure 1: A screenshot of the web based version of the EDT's FloodNet DDOS tool.

The EDT held thirteen pro-Zapatista actions in 1998 using FloodNet, targeting websites ranging from those of the Clinton White House and the Pentagon to those of Mexican president Ernesto Zedillo and the Frankfurt Stock Exchange, with mixed success. These actions attracted up to 18,000 participants but did not generate much focused media attention (Dominguez, 2009). On the 1st of January 1999, the source code for the FloodNet tool was released, allowing other groups to use the tool in their own actions.[23] Its design was simple and for the most part undifferentiated version to version. The language used in the interface clearly marked the tool as belonging to a particular population of activists and artists who were familiar with the language and practices of street and media activism (see Figure 1).

The version used in the pro-Zapatista actions of 1998 invited users to "send your own message to the error log of the institution/symbol of Mexican Neo-Liberalism of your choice," specialized language that creates a gulf between those who already understand it and those who do not. The tool does not appear to have been designed to appeal to users who were not already interested in and informed about the issue at hand. This impression is underscored by the methods by which the EDT publicized its actions: through mailing lists and message boards frequented by media activists and special interest lists devoted to South America, the Zapatistas, and other related topics. Similarly, as previously addressed, in its attempt to translate the physical world sit-in to the online space, FloodNet clings to a one-person/one-computer operations model, refusing to augment the resulting flow of traffic with tools such as botnets (volunteer or otherwise) or other traffic amplification exploits (Jordan & Taylor, 2004). This tied the ethical validity of their actions, and eventually of DDOS itself as a tactic, to how closely they could be compared to physical-world actions. As I will show, the Anonymous tool was unconstrained by these technical limitations, which complicates any comparisons made between its actions and physical sit-ins.

[23] It was this version that *the electrohippies* later adapted for their WTO action.

Anonymous, Operation Payback, and LOIC

Operation Payback and the events that precipitated it highlight the differences in motivation and effects of DDOS actions with regard to the active removal of content versus an attempt to attract attention to an issue. The action began in September of 2010 as what Anonymous claimed was a retaliatory DDOS campaign targeting the MPAA, the Recording Industry Association of America (RIAA), and other targets after those organizations had taken the legally dubious step of hiring an Indian firm to DDOS the Pirate Bay, a file-sharing website (Anderson, 2010).[24] Anonymous viewed the DDOS actions by the RIAA and the MPAA as a threat to file sharing and torrenting and as a further example of the abuses perpetrated by the corporate content and IP industries.[25] Specifically, the use of DDOS tactics by the RIAA in an attempt to completely disable the Pirate Bay, which only existed in its online state, while Anons had been imprisoned for launching DDOS actions against the websites of the Church of Scientology, which existed primarily in the physical world as a complex organization, seemed breathtakingly hypocritical. A group of Anons called AnonOps led the DDOS actions against the RIAA, MPAA, and Aiplex, which continued for more than a month. All three targets reported downtime (Anderson, 2010).

The Pirate Bay action and the Anonymous action against the websites of the MPAA and the RIAA had strikingly different motivations and actual effects. The

[24] The Motion Picture Association of America and the Recording Industry Association of America are the major lobbying groups for the content industry and have a history of litigiously opposing what they consider to be the theft of their content via peer-to-peer file- sharing sites, such as the Pirate Bay.

[25] Torrenting is a method of peer-to-peer file sharing that allows individuals to download large files, broken up into pieces, from several different servers at the same time.

motivation behind the attack-for-hire on the Pirate Bay was to remove content from the Internet, in this case, torrent files available on the Pirate Bay's servers (Anderson, 2010). The Pirate Bay exists as an online resource. It has no public presence beyond its Internet presence and serves no function beyond making certain files available online. The motivation of the DDOS actions was not to call attention to the issue of online file sharing but to obliterate the organizational entity known as the Pirate Bay. Alternatively, the RIAA and the MPAA do not exist primarily online. Their websites are little more than informational homepages. No business is conducted there, and the hearts of the organizations do not reside online. The stated motivation for the Anonymous actions on the MPAA and the RIAA was to disrupt their operations and cause the organizations to spend money and resources fending off the actions (Anderson, 2010), but the primary benefit of the actions lay in the media attention and new participants it attracted, who sympathized with Anonymous's views and could participate in future actions. It functioned, in part because of media coverage as a recruiting drive.

December 6, 2010, marked the beginning second stage of Operation Payback, sometimes known as Operation Avenge Assange. This second wave of DDOS actions targeted organizations and individuals Anonymous believed were acting against the interests of WikiLeaks, either by cutting off its channels of financial support, by refusing to provide hosting to the website and its domain name, or by speaking out against the organization publicly. Over the course of four days, Anonymous's DDOS actions against over a dozen sites, causing downtime and service outages at several (Correll, 2010).

These actions were powered by volunteers using the LOIC DDOS tool and were augmented by nonvolunteer botnets (Coleman, 2012; Olson, 2012).

The program used during the Anonymous DDOS action, LOIC, is similar to FloodNet but differs in significant ways. By the time LOIC was developed, the basic functionality of automated DDOS programs had evolved to match improvements in website infrastructure. Beyond that, more important shifts had been made in the areas of community development and open-source coding projects and platforms. LOIC was "forked" several times, allowing the creation of different versions of the tool adapted to the needs and preferences of different user groups.[26] Not only did LOIC represent an evolutionary step in the development of activist-oriented DDOS tools overall, but it continued to evolve within the context of Anonymous during the course of Operation Chanology and Operation Payback.

LOIC was originally developed and distributed by a developer known as praetox (Norton, 2011b) as a server "stress-testing"[27] tool. A number of different versions of the tool based on praetox's original code were developed, some of which added new functionalities to the tool or adapted it to run in different environments. I group those projects that are based on praetox's original code and that retain the LOIC name and the core functionality with the name LOIC, although I will be examining some of the forks individually, as they reflect the previously examined shifts in the Anonymous

[26] To "fork" an open-source software project is to take the source code from one project and independently develop it, thus creating a separate piece of software. The LOIC forks reflect distinct differences in affordances and design.

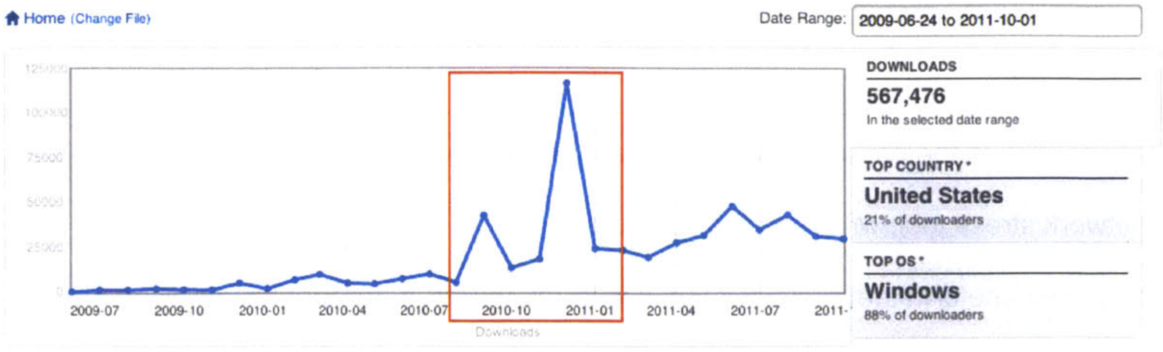
[27] As mentioned in the introduction, it's likely that this tool was never strictly intended to be used as a legitimate stress-testing tool, and the classification is instead a useful cover for the tool actual purpose: to disrupt the websites of others.

population, strategy, and political goals. The evolution of this particular tool further serves as a case study in the mainstreaming of DDOS as a tool of political protest.

A Forked Comparison: abatishchev and NewEraCracker

When the first version of LOIC was made available on the Internet is difficult to determine, but it was in use in 2008, during Operation Chanology (Coleman, 2011b). In the next 2 years, different versions of the project began popping up on open-source software development sites. Versions of LOIC could be downloaded from SourceForge and GitHub, popular open-source software repositories. Individuals could also add code to LOIC projects on these sites (a practice known as “committing code” or “code commits”), leave comments for the developers, request features, and report bugs. As such, they were far more social in their development and distribution than FloodNet. Use of those development community websites meant that more people con-currently participated in the development of LOIC, making it possible for the tools to more accurately reflect the needs, whims, and tastes of the target audience. By December of 2010, versions of LOIC could be run on Windows, Mac, and Linux PCs as well as Android phones and jail-broken iPhones. A version called JS LOIC, or JavaScript LOIC, ran, like the EDT’s FloodNet application, from within a web browser; the user was not required to download or install anything (Warren, 2010).

The most widely downloaded versions of LOIC in December of 2010 were posted to SourceForge and GitHub by abatishchev and NewEraCracker, respectively. These two versions will be examined because they represent a particular line of evolution for the tool, were very often linked in media coverage and LOIC tutorials, and were extremely popular, if one counts by download numbers. Both hewed closely to praetox's original code while updating the graphical user interface (GUI) and adding features. The version from abatishchev is the older of the two, initially uploaded to SourceForge in June of 2009 (abatishchev, SourceForge Stats, n.d.). This version of LOIC was downloaded 116,988 times in December, 2010, up from 61,936 times in at the beginning of Operation Payback in September (abatishchev, SourceForge Stats, n.d.; see Figures 2 and 3). To compare, in August of 2010, before the launch of the first wave of Operation Payback, this version of LOIC was downloaded 5,318 times (abatishchev, SourceForge Stats, n.d.). Together, the September 2010 (when Operation Payback initially began) through December 2010 (when the Avenge Assange portion of Operation Payback took place) downloads make up nearly a third of the 567,476 downloads abatishchev's version of LOIC racked up from June of 2009 to October of 20011 (abatishchev, SourceForge stats, n.d.; see Figure 2). Just under a third of those downloads occurred during the week of Operation Payback's Avenge Assange campaign. It is impossible to tell from SourceForge records how many of those downloading the tool actually used it during the course of Operation Payback, but it is an impressive and telling spike.


Home (Change File)

Date Range: 2009-06-24 to 2011-10-01

DOWNLOADS

567,476

In the selected date range

TOP COUNTRY *

United States

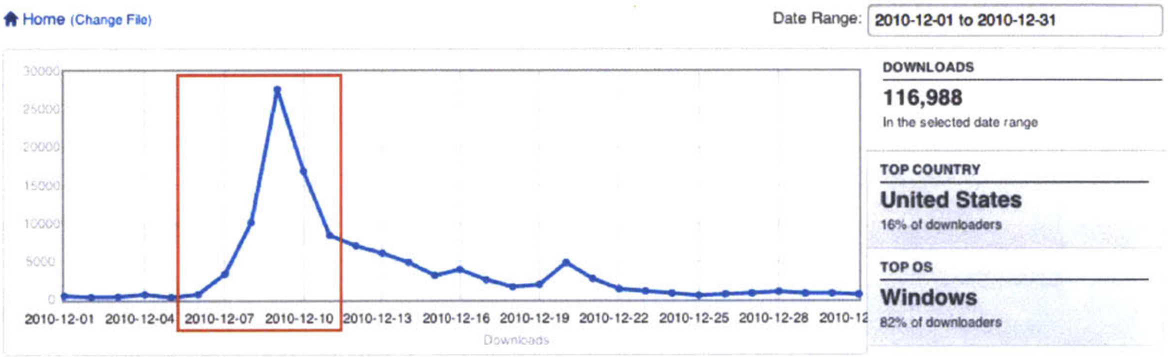
21% of downloaders

TOP OS *

Windows

88% of downloaders

Figure 2. This SourceForge chart shows downloads of the abatishchev LOIC from June 2009 through October 1, 2011. The first spike in the highlighted portion is September 2010, at the start of the Operation Payback. The second, larger spike is December 2010. From September through December, 2010, abatishchev's LOIC was downloaded 191,781 times. Retrieved from http://sourceforge.net/projects/loic/files/stats/timeline


Home (Change File)

Date Range: 2010-12-01 to 2010-12-31

DOWNLOADS

116,988

In the selected date range

TOP COUNTRY

United States

16% of downloaders

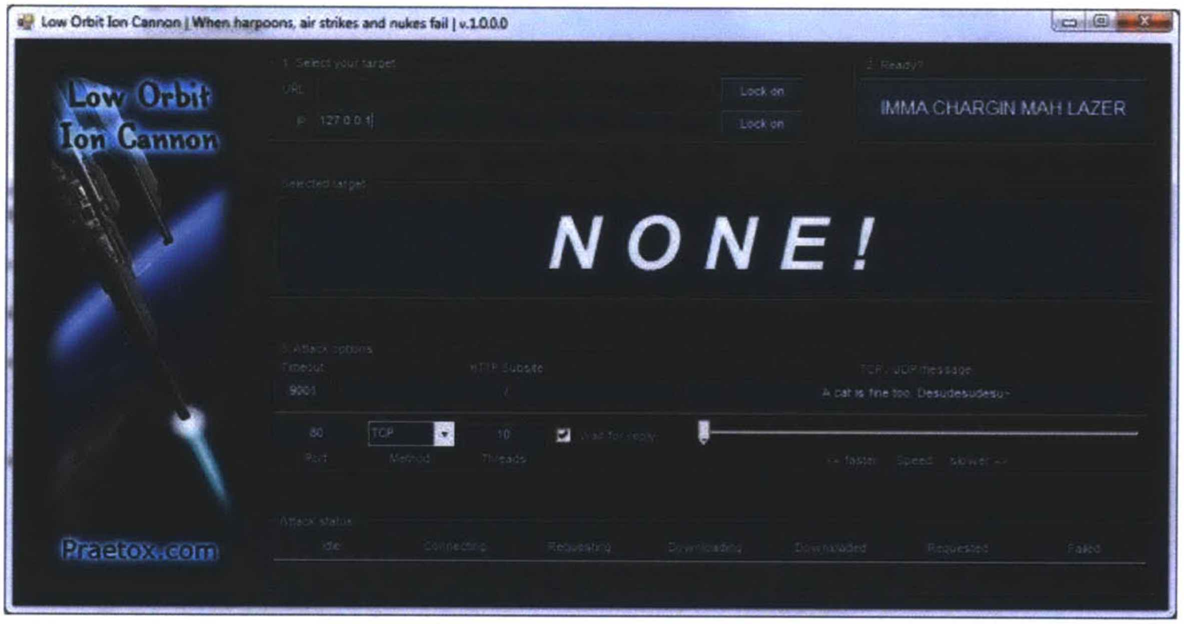
TOP OS

Windows

82% of downloaders

Figure 3. This SourceForge chart shows the December 2010 downloads of abatishchev's LOIC program. The highlighted portion shows the duration of Operation Payback's Avenge Assange actions, starting with an action against the Swedish banking website postfinance.ch on December 6 and ending with an action against conservatives4palin.com on December 10. During the campaign's weeklong run in December, 2010, abatishchev's LOIC was downloaded 58,795 times, accounting for half the total downloads for the month, and just under a third of the total downloads from the September through December 2010 period. Retrieved from http://sourceforge.net/projects/loic/files/stats/timeline

NewEraCracker uploaded his version of LOIC to GitHub in late September 2010, stating clearly that his work was based on abatishchev's version of the original praetox tool, as was written in the project's README file:[28] "Low Orbit Ion Cannon—An open source network stress tool, written in C#. Based on Praetox's loic project at https://sourceforge.net/projects/loic/" (NewEraCracker, n.d.). From its creation in September 2010 to December 2011, NewEraCracker's version of the tool was downloaded 80,660 times (unfortunately, GitHub does not currently offer finer-grain analytics on projects) (NewEraCracker, n.d.).



IP: 127.0.0.1

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

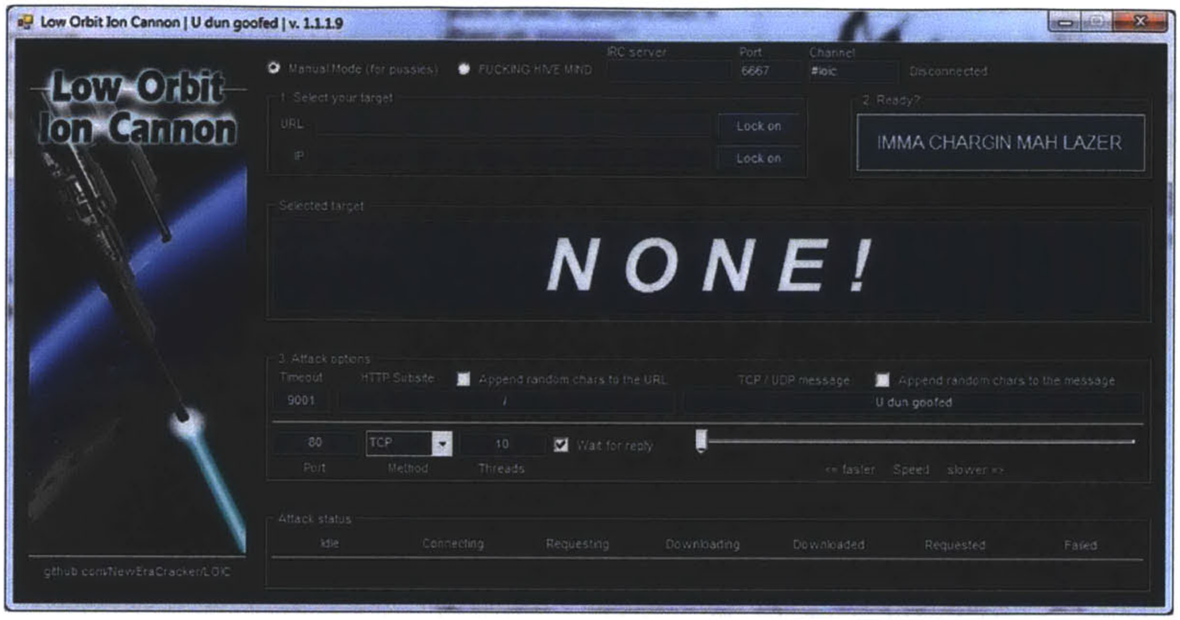
Method: TCP

Threads: 10

☑ Wait for reply

Figure 4. A screenshot of abatishchev's version of LOIC. Retrieved from http://sourceforge.net/projects/loic/

[28] The README file for NewEraCracker's version of LOIC is available at https://github.com/NewEraCracker/LOIC#readme Note that NewEraCracker credits Praetox but links to abatishchev's SourceForge project.


Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.9

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

IRC server:

Port: 6667

Channel: #loic

Disconnected

1. Select your target

URL

IP

2. Ready?

Selected target: NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

■ Append random chars to the URL

TCP / UDP message: U dun goofed

■ Append random chars to the message

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

Attack status

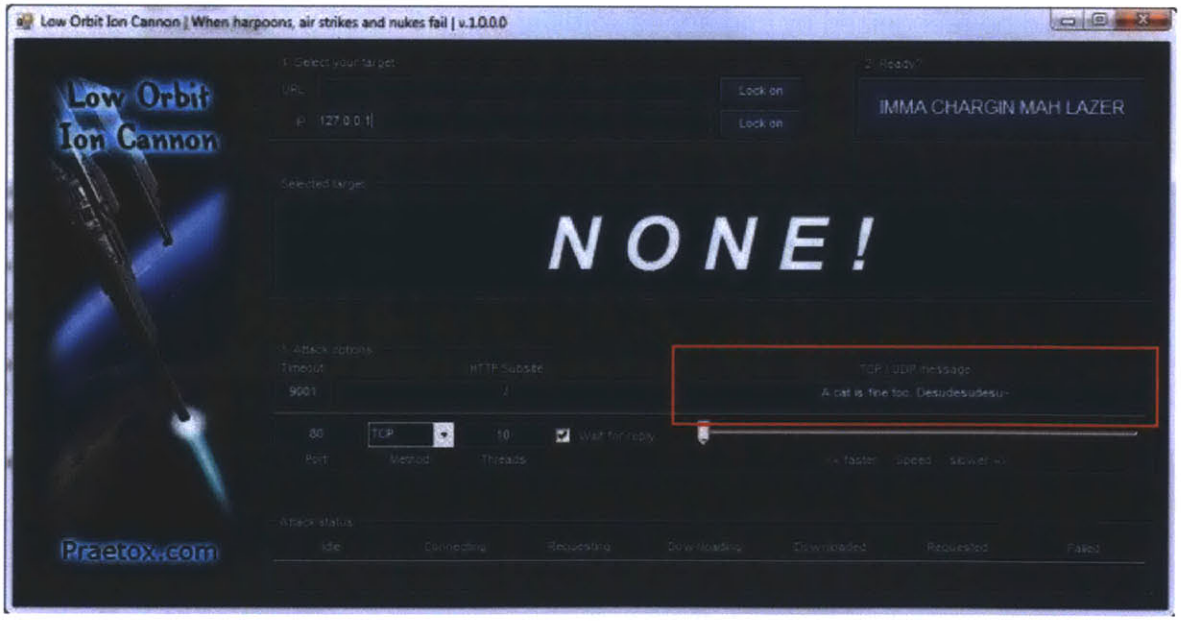
Idle | Connecting | Requesting | Downloading | Downloaded | Requested | Failed

Figure 5. A screenshot of NewEraCracker's version of LOIC. Retrieved from https://github.com/NewEraCracker/LOIC/

Although NewEraCracker's and abatishchev's tools share virtually identical GUIs and core functionalities, there are differences in the design and functionality of each tool that would be recognized by and appeal to different participant groups. Both employ the same color scheme, dark blue on black with white text, and use the same image of a futuristic laser weapon firing at a planet, although different fonts are used for the Low Orbit Ion Cannon moniker. Both GUIs are peppered with references to memes and video games that would be instantly recognizable to individuals associated with Anonymous or familiar with Internet meme culture, although the references differ between the two versions in ways that make the tools temporally and politically distinct.[29] These differences can be used to position the different versions of the tool in

[29] A meme is an idea, phrase, image, or other concept that spreads virally over the Internet and is adopted, repeated, and remixed by people. In Anonymous culture, many

time and how DDOS was being used by Anonymous in terms of its activist strategy. For instance, the phrase "A cat is fine, too," which appears as the default message in the transmission-control protocol/user datagram protocol (TCP/UDP) message field in the abatishchev version (see Figure 6), began appearing on 4chan and /b/ in 2006 ("A Cat is Fine Too," 2009). "Desudesudesu," also included in the TCP/UDP message field, references a separate meme, also popular on 4chan in 2006 ("Desu," 2009). NewEraCracker replaces that message with "U dun goofed," a reference to the Jessi Slaughter meme, which became widespread during the summer of 2010 ("Jessi Slaughter," 2010) (see Figure 7). The abatishchev version also includes the subtitle "When harpoons, air strikes and nukes fail," a reference to the video game series *Command and Conquer*, from which the name "Low Orbit Ion Cannon" is taken.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

IP: 127.0.0.1

Selected target: NONE!

3. Attack options

Timeout: 9001

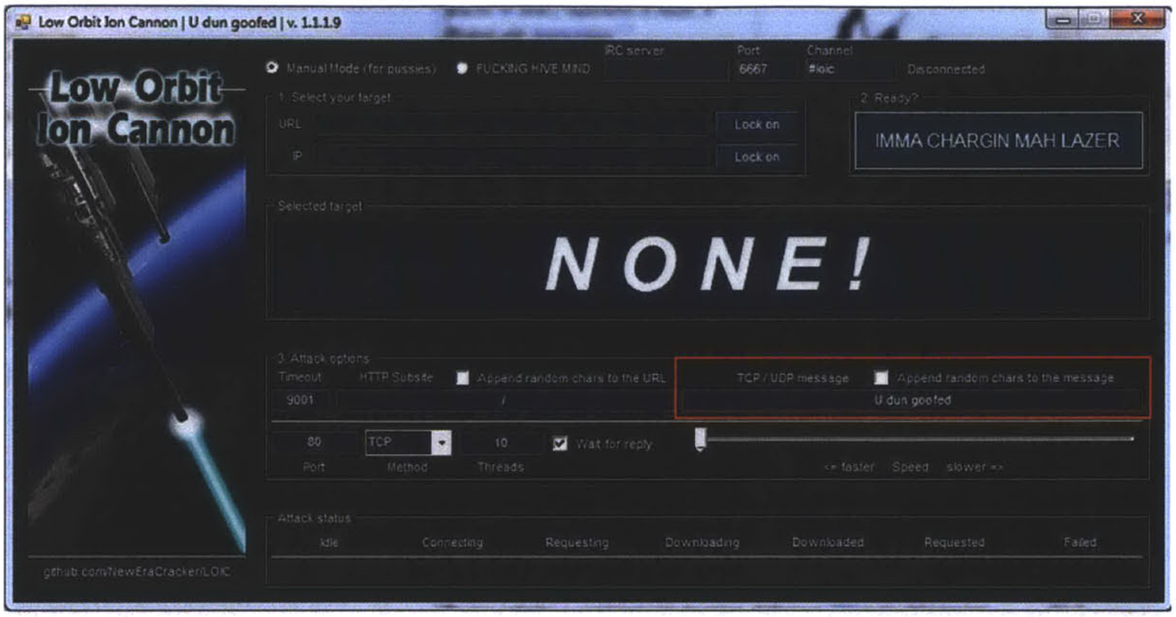
HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80 Method: TCP Threads: 10 ☑ Wait for reply

Figure 6. In this screenshot of abatishchev's LOIC, the TCP/UDP messaging field is highlighted, with the default message, "A cat is fine too. Desudesudesu."

memes serve as markers of community involvement, shibboleths to differentiate those who are part of the community from those who are not.


Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.9

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

IRC server

Port: 6667

Channel: #loic

Disconnected

1. Select your target

URL

IP

2. Ready?

Selected target

NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

□ Append random chars to the URL

TCP / UDP message: U dun goofed

□ Append random chars to the message

Port: 80

Method: TCP

Threads: 10

☑ Wait for reply

<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

github.com/NewEraCracker/LOIC

Figure 7. In this screenshot of NewEraCracker's LOIC, note the highlighted change in the TCP/UDP's default message, from "A cat is fine too" to "U dun goofed."

One reference the abatishchev and NewEraCracker versions share in common is the "IMMA CHARGIN MAH LAZER" phrase, splashed across the button one presses to launch the attack. This references the Shoop Da Whoop meme, which also originated on the 4chan /b/ board in 2006 ("Shoop da Whoop," 2009). Whereas "IMMA CHARGIN MAH LAZER" and "U dun goofed" enjoyed widespread popularity beyond 4chan, "A cat is fine, too" references an obscure bestiality meme derived from Japanese manga. It did not achieve recognition or popularity beyond 4chan and similar image boards, such as SomethingAwful and YTMND. Given the proliferation of 2006 Internet memes in the older versions of LOIC, and given that 2006 predates any significant media coverage of Anonymous or 4chan, it is reasonable to assume that the original developer of LOIC was most likely active on /b/ and with Anonymous, saw the target audience as members of the same community, and developed the tool sometime during 2006.

These two versions of LOIC are semiotically tagged with memes popular within different populations at the time of development. The abatishchev and, theoretically, original praetox versions reflect memes that occurred predominantly within the community of /b/ and 4chan and did not leak out into the wider Internet culture. The NewEraCracker version replaced those more obscure references, either because the developer did not recognize them or because he wanted to explicitly realign the cultural references of the tool with memes that had attracted the attention of the more mainstream Internet culture. At the time, the Jessi Slaughter "U dun goofed" meme had attracted the attention of popular Internet culture blogs, such as Gawker, and the mainstream news media ("Jessi Slaughter," 2010). So marked, NewEraCracker's version of LOIC can be seen as appealing more to individuals who had relatively little interest in the more recreationally offensive aspects of /b/'s culture but were drawn to Anonymous for other, perhaps predominantly political, reasons.[30]

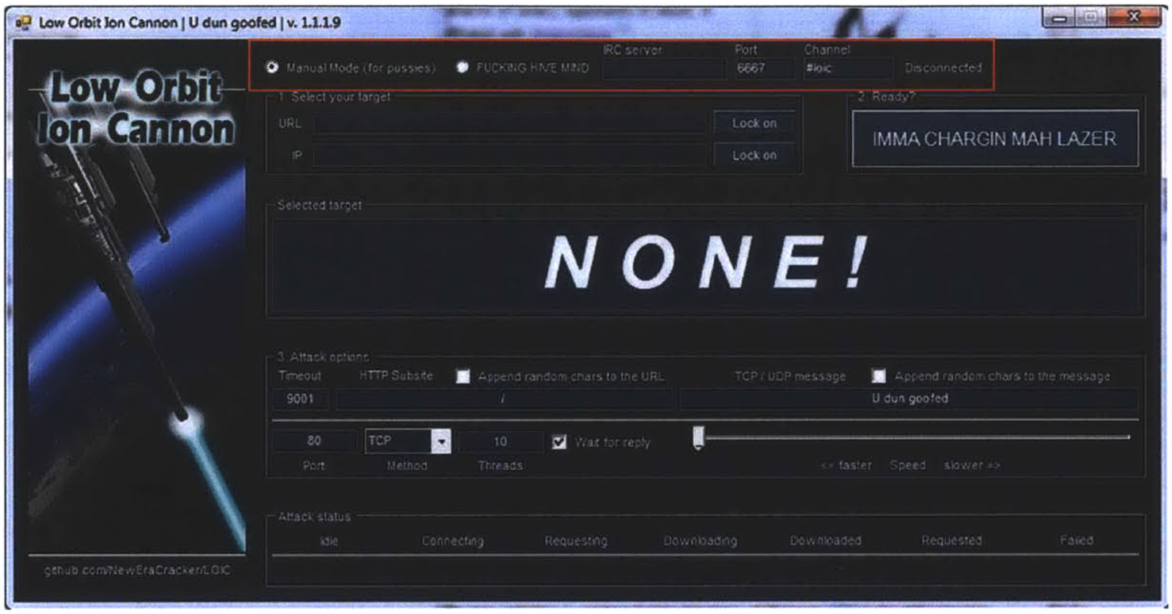
The changes made by NewEraCracker also heighten the explicit and overt political value of the tool. Whereas "A cat is fine, too" and "Desudesudesu" are relatively nonsensical in the context of an adversarial DDOS attack, "U dun goofed" is explicitly confrontational. It accuses the target of making a grave error and implies that he or she is now, or shortly will be, suffering the consequences of his or her actions. In the original viral video from which the meme sprang, "U dun goofed" is followed shortly by the line

[30] This shift in rhetorical tone can also be interpreted as a reflection of Anonymous's overall move away from its 4chan roots, towards a new activist identity.

"The consequences will never be the same" ("Jessi Slaughter," 2010). So whereas the praetox and abatishchev LOIC can be seen as calling out to a specific, rather limited group of like-minded individuals, the NewEraCracker LOIC throws its net much more broadly and advertises its vengeful motives much more overtly. This messaging functionality is identical to the one found in the original FloodNet tool. The message many never be seen by the target and, as such, serves more as a rhetorical flourish for the benefit of the sender, adding a weight that might not be carried by the hurling of bits alone, and augments the sense of communal participation.

The design of the interface makes the operation of the tool relatively simple, even for someone with little experience participating in DDOS actions, but it also contains features for more advanced users to "personalize" their actions. The required steps (target, attack mode, and some customizable options) are numbered 1 to 3. A website can be targeted by entering either its URL or its IP address. A more advanced user can also set the port destination, the number of simultaneously open threads, request timeout, and the relative speed with which packets are hurled at the target. Most of these options have a default setting, so all an inexperienced user has to do is enter a target URL, click "IMMA CHARGIN MAH LAZER," and sit back. However, if a user were still confused, there are a myriad of tutorials and FAQs available online, posted on webpages and as video tutorials on YouTube. Information on how to operate LOIC is, and in December of 2010 was, extremely easy to find. In fact, much of the news coverage of Operation Payback and Operation Avenge Assange contained enough information to constitute a tutorial on the use of LOIC in and of itself.

A significant difference between the abatishchev and NewEraCracker versions of LOIC is NewEraCracker's addition of the Hive Mind automated attack mode (see Figure 8).



Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.9

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

IRC server:
Port: 6667
Channel: #loic
Disconnected

Timeout: 9001
HTTP Subsite: /
□ Append random chars to the URL
TCP / UDP message: U dun goofed
□ Append random chars to the message

Port: 80
Method: TCP
Threads: 10
☑ Wait for reply

Figure 8. In this screenshot of NewEraCracker's LOIC, note the addition of "FUCKING HIVE MIND" and attendant options at the top of the interface.

This added functionality also represents a important advancement from FloodNet, which, like abatishchev's LOIC, operated in only one "manual" mode. Although the tool automated the process of sending packets, a user still had to target and engage the tool manually. Hive Mind mode allowed the tool be controlled remotely, through the IRC[31] protocol. During Hive Mind mode, the user was essentially volunteering his or her machine to be part of a botnet. To operate in this mode, the user simply selected "Hive

[31] IRC, or Internet Relay Chat, is an internet protocol to support instant messaging, chat, and synchronous conferencing. IRC channels are be hosted on a central server and joined by individuals via clients or an online interface. Hive Mind exploited the IRC protocol to control an instance of LOIC on a given machine.

Mind" at the top of the interface and entered the IP address of the IRC server, the port number, and the channel name. These were also set to defaults during installation, further simplifying the process. Moreover, nearly all of Anonymous's internal communications during the December stage of Operation Payback took place in IRC channels, so it is very likely that even a relatively new participant would be passingly familiar with its protocols (Norton, 2011b). But again, if a user were confused, there were, and still are, many tutorials to be had just a Google search away.

The Hive Mind feature represents a significant break with the one-person/one-computer protocol practice exemplified by FloodNet. Although an original goal of the FloodNet project might have been to "leave one's computer protesting at home and then hit the streets to do the same" (Dominguez, 2009, p. 1810), it was Anonymous that actually took advantage of the protocol's physics-defying potential. Hive Mind mode enabled Anonymous to engage with participants who did not, for whatever reason, follow the targeting and scheduling information that Anonymous was constantly releasing and updating. A lower level of commitment was required. Although Anons may not have "hit the streets" as EDT envisioned, Hive Mind mode did enable them to go to school, work, sleep, or anywhere while still participating in DDOS actions as they arose.[32]

By updating and making more accessible the memes in the tool's interface, and by adding functionality that allowed less technically able individuals to participate in the

[32] This functionality was anticipated during the Help Israel Win campaign, a DDOS action launched in late 2008 that featured a voluntary botnet similar to LOIC's Hive Mind. The Help Israel Win campaign will be examined in Chapter 5.

actions, Anonymous was able to expand its participant community dramatically. Coleman (2012) quotes one Anon as saying that the number of participants on the Operation Payback IRC servers rose from an average of 70 participants to over 1000. The ease with which one could participate in the Operation Payback actions was rivaled only by the ease with which one could take on the identity of an Anon. As noted previously, the Anonymous identity meme is based on the strengthening of a central core via the participation of many individuals who move in and out of different active or passive states. This subsumption of personal agency has the potential for a strong biographical impact on the participants, particularly, those who had not previously considered themselves political actors, by merging their agency with other active participants. This merging allows for the temporary sharing of an activist identity, which subsequently becomes more easily adopted by those participants who opt to remain involved.

Conclusions

The choices made in the design and distribution of the tools used for activist DDOS actions have a strong impact on various aspects of the campaigns. Who participates and how, the political engagement of the action, and the likelihood that participants will stay involved can all be affected by these decisions. Close analysis of these tools after the fact can also provide indications as to the political philosophies and theories animating these protests. Any attempt to examine political and social movements within the online space should make room for the analysis of the tools and other technological artifacts, such as meeting places and communication protocols, used in these movements. In this analysis, I've shown how the actions of Anonymous do not constitute the breaking of some new political ground, but rather represent the continued evolution of political activism in the digital space, specifically in the realm of tool design. In the movement from the Electronic Disturbance Theater's FloodNet to Anonymous's LOIC, we have seen how this realm of online activism expanded from one dominated by experienced activists organizing relatively small populations of like-minded individuals to a horizontal structure that opens the tools and mechanisms of protest to anyone with an internet connection. In the next chapter, I'll examine how participant identity functions within activist DDOS actions.

CHAPTER 3

Participant Identity in Context

Crowd based actions, like DDOSes, blockades, and public marches, are not based on the discreet identities of individual participants to be successful. Rather, the visual spectacle of the mass (or, in the case of DDOS, the imagined spectacle) is more valuable than the individual as a self-contained entity in the greater campaign. That said, a variety of identity constructions, revelations, and concealments come into play with DDOS actions. A highly debated aspect of DDOS actions is their propensity to enable anonymous action, wherein people take active steps to conceal their identity over the course of their participation. This can be compared to the wearing of masks during a street protest. Other identity performances beyond anonymity have historically come into play with regard to DDOS actions, such as Anonymous's highly theatrical adoption of a stereotyped "hacker" identity in its actions. This section will examine practices of overt identification and anonymization; the construction of collective, performative identities within activist groups; issues of gender, race, and class as played out in a technologically defined activist space; and how the concept of unsympathetic actors and "impure dissent," as defined by Tommie Shelby, applies to modern DDOS actions as they are practiced in the contemporary, privatized online space.

Identity, anonymity, and responsibility within protest

Early groups, like the Electronic Disturbance Theater and *the electrohippies* explicitly revealed and advertised the identity of the organizers of DDOS actions. They did this in support of their explicit modeling of their DDOS action on physical world sit-ins, which contain within their operational logic a give-and-take with the state. This is in contrast to more recent DDOS actions, particularly those of the group Anonymous, who maintain anonymity as a aspect of their culture. The anonymity of Anonymous actions is also a reflection of their refusal to engage with the mechanisms of the government on government's terms. Anonymous refuses to buy that the government is engaging with digital activism in good faith, and moreover denies that the current form of the state has any legitimate role in governing the net at all.

Both the EDT and *the electrohippies* explicitly revealed and advertised their identities as organizers of DDOS actions. This tactic of preemptive identification was yet another aspect of their adaptation of physical world protest tactics for the online space. As articulated by *the electrohippies*:

> We have nothing to hide, as we believe that our purpose is valid, and so we do not seek to hide it from any authorities who seek to surveil us. Likewise, we do not try to bury our identities from law enforcement authorities, any authority could, if it chose to, track us down in a few hours...The right to take action against another entity on the 'Net must be balanced with the principle of accountability."
>
> (DJNZ, 2000)

the electrohippies claimed that by openly revealing their identities as organizers, they could be held accountable by the public whose participation they were seeking. Further, they claimed that such accountability ensured that the tactic would only be used in "justifiable" situations: "If the group using the tool do not feel they can be open about its use then we consider that their action cannot be considered justifiable. A justifiable action cannot be mounted from behind the mask of anonymity." (DJNZ, 2000). They also viewed the practice as a hedge against accusations of terrorism or criminality by the state or press.

In their essay analyzing their use of what they termed "client-side distributed denial of service" and in other writings, *the electrohippies* repeatedly frame their use of DDOS as a natural continuation of existing constitutional rights. Like the EDT, the activists saw the online space as a complementary, equally valid theater of activism to the physical world, and approached it as such with the assumption that if previously accepted activist practices, like sit-ins, were symmetrically adapted to the online space, the reactions of the state could be predicted.

These groups did not require participants to publicly identify themselves to the same degree as organizers; *the electrohippies* recommended the use of anonymous, throw-away email addresses for their WTO email-bombing campaign. However, the groups did acknowledge the likelihood and potential consequences of being identified as a participants in these actions, as stated on the EDT's website:

> WARNING: This is a Protest, it is not a game, it may have personal consequences as in any off-line political manifestation on the street:
> Based on critiques from the Heart Hackers and other individuals about FloodNet:
>
> 1. Your IP address will be harvested by the government during any FloodNet action. When you click and enter FloodNet your name and political position will be made known to the authorities.

> (Similar to having your picture taking during a protest action on the street.)
>
> 2. Possible damage to your machine may occur because of your participation in the FloodNet action.
> (Just as in a street action -the police may come and hurt you.)
>
> 3. FloodNet clogs bandwidth and may make it difficult for many individuals using small pipelines around the world to get information. FloodNet may not impact the targeted website specifically as much as it disrupts traffic going to the targeted website, i.e. problems for Internet routes to the site.
>
> (This also happens when people take to the streets. Individuals may find themselves unable to get to work or buy a newspaper because of the action. FloodNet actions are short term and only disturb bandwidth during the time of the manifestation. The Electronic Disturbance Theater feels that even if FloodNet only functions as a symbolic action, that is enough to make the collective presence of activists felt beyond the electronic networks.)
>
> We hope that when you join our Virtual Sit-in's in support of global communities of resistance, you will take the above information to heart.
>
> (Electronic Disturbance Theater, 1998[33])

The EDT and the electrohippies's reliance on physical world structures of accountability indicate a belief that the assumptions of physical world activism hold true for activism in the online space as well, particularly assumptions around interactions with the state and its agents. The EDT's warning acknowledges the expected role law enforcement typically plays in street activism. In this conception, the state serves as a theatrical antagonist and legitimater of dissent by virtue of their reaction: as stated by

[33] The FloodNet warning page was posted in September, 1998, and developed by Carmin Karasic and Brett Stalbaum. It is archived at http://www.thing.net/~rdom/zapsTactical/warning.htm and was last accessed on April 13, 2013.

Jerry Rubin in 1969, "The cops are a necessary part of any demonstration theater. When you are planning a demonstration, always include a role for the cops. Cops legitimize demonstrations." (Rubin, 1969) Similarly, in his original conception of civil disobedience, when Thoreau says, "Under a government which imprisons any unjustly, the true place for a just man is also a prison," (Thoreau, 1849) he values the spectacle of the state imprisoning a just man for its value as an illustration of the injustice of the state, to which others may react. Encounters with law enforcement of a certain type are seen as a necessary and sometimes useful part of activist actions.

Symbolic activism of the type practiced by the EDT and other co-temporaneous groups requires a dialog with the state to be effective. The state is assumed to be able to respond to the activist action in good faith, as it is understood to be activism. The state is seen as having an interest in engaging with activists productively, and moreover is seen as a useful actor in the process that activists are trying to impact.[34]

Contrary to this, Anonymous holds anonymity to be a core aspect of its culture. Individuals who out themselves are derisively referred to as "name-fags" and can sometimes be reacted to quite aggressively (Coleman, 2012). Auerbach, as previously noted, lays the credit for this cultural development at the feet of the technological systems upon which the Anonymous culture was built, fast-moving message boards which were ephemeral and unsigned by nature. While this explains where the value

[34] In this vein, the EDT's Zapatista actions provoked aggressive counter-measures from the Pentagon, in the form of a "counter-hack" which redirected and tied up the EDT's systems (Denning, 2000) Later, in early 2010, EDT member Ricardo Dominguez was investigated for leading a "virtual sit-in" action against the official website of the University of California Office of the President.

originated, it does not explain why it has penetrated so deeply into the culture's activist activities, nor why it has persisted at the levels of both technological systems and cultural practice.

Anonymous's maintenance of anonymity in the face of established activist practice in part indicates a refusal to accept the assumptions of earlier groups. While the EDT and *the electrohippies* inherently granted the rights of states to govern the online as they govern the physical world, Anonymous does not. Anonymous's political conception of the internet, in so much as it coherently stands, is more akin to that articulated by John Perry Barlow in his 1996 "A Declaration of the Independence of Cyberspace":

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.
>
> (Barlow, 1996)

Anonymity, in this context, becomes a political response to the perceived illegitimacy of state governance online. During the Operation Chanology street protests against the Church of Scientology, Anonymous encouraged participants to wear masks to protect themselves against later harassment by the Church. During Operation Payback and later actions, the use of anonymity during a DDOS action incorporates within it a refusal to engage with traditional scripts of activism that inherently legitimize the role of the state and of law enforcement within the action.

In addition to simply denying the legitimacy of the state in governing dissent online, anonymity as an online activist practice contains within it a belief that the state and corporate actors targeted by the activists will not respond in good faith (Shelby, 2012). Earlier groups drew on the history and scripts of street activism to anticipate interactions with states and law enforcement. Anonymous, operating some ten years later, draws on a much different history of state antagonism of hackers, DRM battles, and post-9/11 War on Terror surveillance and policing of dissent. Given the history in the US of frankly ridiculous and over-reaching CFAA-enabled computer crime prosecutions, this assumption of bad faith is not unreasonable. This is similar to the rationale behind the use of masks by Black Bloc actors during street actions. Thompson quotes Black Bloc activists citing "protect[ing] ourselves from illegal police surveillance" and "provid[ing] cover for activists engaged in illegal actions during the demo" (Thompson, 2010 p. 57) as reasons for the use of masks during street protests. The logic is clear: if you aim is to commit a political act not recognized as a privileged political act by the state, then taking actions to prevent yourself as a political actor from being assigned the role of criminal actor by the state is reasonable.

Anonymity as an outward-facing cultural practice strengthens the "relational equality" between the individual participant and the greater cultural movement (Ollman quoted in Thompson, 2010 p. 56). As mentioned before, Anonymous relies on the perception of an inexhaustible mass for much of its rhetorical bite. Similar to stereotypes of hacker culture, which will be explored later, Anonymous relies on the identical-ness of its masked, technologically anonymized participants to foster a sense of omnipresence. Outward-facing anonymity prevents outside actors, like the media, from focusing on and privileging charismatic actors. Anonymous values the optics of the mass, the "hive," while simultaneously continuing to value internally individuality and individual initiative (Coleman, 2012).

That said, though anonymity is sought by Anonymous during these actions, it is not always achieved. Neither the abatishchev nor the NewEraCracker versions of LOIC tried to cover the user's tracks. More sophisticated DDOS tools will "spoof" IP addresses, generating a fake IP to assign to the packets the program sends out, or take other steps to prevent the target of an action from tracing the packets back home. However, all packets sent with LOIC are tagged with the IP address of the sender. ISPs maintain records of the IP addresses of computers on their network and can match those IP records to the real names and addresses of their subscribers. Law enforcement can and often does subpoena those records when pursuing computer crime prosecutions. It was possible for an individual using LOIC, without taking additional security measures, to be identified on the basis of information contained in the packets he or she sent.[35]

For a sophisticated user, this security flaw is relatively easy to detect by glancing at the tool's source code or by testing the tool against a known machine (such as one's own server). However, most of those participating in the December 2010 DDOS campaign were not sophisticated users. They were recent additions to the Anonymous DDOS army, "n00bs" or "newfags" in Anonymous parlance. Whereas an experienced user may have been aware that running LOIC through a proxy or a spoofed IP address would provide some measure of protection from the security flaws in the tool, it is unlikely that someone new to digital activism would be aware those tools existed or would understand how to operate them. Very few of the tutorials available online made mention of any of these options. In fact, many of the FAQs and tutorials reassured users that they were unlikely to be caught using the tool as is, or if they were caught, they were unlikely to face any serious trouble. These statements were often factually inaccurate and based on a faulty understanding of how servers operated. One FAQ reads, in part:

> **Q:** Will I get caught/arrested for using it?
> **A:** *Chances are next to zero* [italics added]. Just blame [*sic*] you have a virus, or simply deny any knowledge of it.
> (Operation Payback Setup Guide, n.d.)

[35] The EDT's FloodNet tool, as well as the adapted version used by *the electrohippies*, also did not utilize any measures to mask the identity of participants. However, this should be seen as an extension of those groups' integration of physical world/legal identity into their actions. Given Anonymous's history of anonymous action and the emphasis placed on anonymity within Anonymous culture, that LOIC does not conceal users' identities is more likely to be a mistake or hallmark of an inexperienced developer rather than an intentional decision.

The media also picked up this line, and repeated it extensively, as in this article by Joel Johnson (2010) of Gizmodo:

> What is LOIC? It's a pushbutton application that can be controlled by a central user to launch a flood of killer internet packets with *little risk to the user* [italics added]. Because a DDoS knocks everything offline—at least when it works as intended—*the log files that would normally record each incoming connection typically just don't work* [italics added]. And even if they do, many LOIC users claim that another user was on their network or that their machine was part of a bot net—a DDoS client delivered by virus that performs like a hivemind LOIC, minus the computer owner actually knowing they are participating.
>
> (J. Johnson, 2010)

In this article, Johnson mistakenly states that a server targeted by a DDOS action would not log the IP addresses on the incoming packets, a statement that is simply inaccurate. In fact, PayPal and other Operation Payback targets kept extensive logs of traffic to their websites, logs that law enforcement used to target participants for searches and arrests.

As a result, it is probable that many newly recruited Anons used LOIC to join in on large-scale DDOS actions against financial institutions, such as PayPal, Visa, and MasterCard, without taking any security precautions whatsoever. In the coming months, dozens of those individuals would be arrested and charged under the Computer Fraud and Abuse Act (Zetter, 2011). It was later revealed that those arrests were based on a master list of IP addresses collected by PayPal as its servers were struck by a massive wave of DDOS actions on December 9th and 10th, 2010 (Poulsen, 2011), something sites such as Gizmodo had previously claimed was impossible. Despite criticism that activist DDOS actions are cheaper or easier or “less risky” than other forms of activism, these actions can be extremely legally risky, due to an insistence on the part of the judicial system that activist DDOS actions be treated as criminal, not political, acts.

Identity within distributed actions: Anonymous and the hacker identity

Although early practitioners of mass DDOS actions sought to create an overarching collective identity for their actions, it usually extended only to vaguely defined "witnessing" crowd, similar to how Ricardo Dominguez described the participants in the etoy/toywar DDOS action: "...a global group of people gathered to bear witness to a wrong" (Dominguez quoted in Wark, 2003). This is in keeping with the underlying conceit of DDOS as "virtual sit-in." The internet-based nature of the DDOS releases the participant from the challenges of distance and physical space, but she is still valued as a far-flung, unaffiliated individual. She does not participate because she is culturally obligated, but because the networked nature of the DDOS allows her to add her presence to whatever cause she feels drawn to. A unified, restrictive cultural identity would have undercut the 'global' mass action aesthetic sought (but not always achieved) by the organizers, particularly in actions that purposefully crossed national borders, such as the EDT's Zapatista actions or the Strano Netstrikes[36]. As explored earlier, however, the EDT’s reliance on very specific socio-political and linguistic frames

[36] The Strano Netstrikes were a series of DDOS actions in December of 1995 targeting the websites of various French government offices in protest against their nuclear policies. The actions were organized by an Italian group called the Strano Network, led by Tommaso Tozzi. (Ludovico, n.d.) (Thomas 2001)

within their actions, though not an overt cultural identity, served to restrict the global distribution of their actions.

While the Electronic Disturbance Theater and other groups based their political philosophies and group cultures within wide frames of anti-capitalist/anti-globalization activist culture, Anonymous actions are strongly embedded within the restricted, bounded, cultural frame of A-culture. As previously explored, this allowed participants to immerse themselves in a pervasive activist setting, and added to the biographical impact value of participating in the action. This culture also contains a deeply performative aspect. Drawing on media tropes of hackers and technology, as well as internet meme culture, Anonymous culture plays with stereotypes to create a public identity which is anarchic, humorous, and trollish, feeding off the fearful or angry reactions of the uninformed[37].

The hacker figure featured prominently in news media and film is a type of modern folk devil. Based in a deeply seeded apocalyptic techno-paranoia, popular media more often than not serves to stoke fears that armies of basement-dwelling adolescents males are eager to dish out vindictive mayhem to a society so tied to technology that it would be unable to adequately defend itself. The hacker in this story

[37] This is generally known as "for the lulz." As explained by Gabriella Coleman: “Trolling on 4chan often consists of an unpredictable combination of the following: telephone pranking, having many unpaid pizzas sent to the target's home, DDoSing, and most especially, splattering personal information, preferably humiliating, all over the Internet. Since at least 2006, “Anonymous” has conducted many such trolling campaigns. The motivating force and emotional consequence for the instigators of many acts of trolling, including those on 4chan, are cited as the "lulz," a pluralization and bastardization of laugh out loud (lol). Lulz denotes the pleasures of trolling, but the lulz is not exclusive to trolling. The lulz can also refer more generally to lighthearted and amusing jokes, images, and pranks." (Coleman 2011a)

is a dark, unseen force in the network, decentralized and able to cause havoc far from his physical location. Socially alienated and cut off from normal moral checks, he engages in pathological, compulsive behaviors with other hackers.[38]. His nights are spent trying to outdo other hackers in technological feats of mayhem and disruption, and his skillz are beyond the ken of any 'normal' person (Sauter, 2012).

Anonymous has seized delightedly upon this mythological figure, further reveling in epithets attached to them by the news media, like "Internet Hate Machine"[39]. Their slogan, "We are Anonymous. We do not forgive. We do not forget. Expect us," evokes the omnipresent threat of the locationless hacker. Though their methods, DDOS in particular, may be fairly simplistic in reality, they are advanced enough to confuse the majority of the public, including law enforcement and the news media, who are happy to assign the "hacker" moniker to any non-mainstream technological practice deemed newsworthy. The Anonymous-as-hacker cultural image is a collaboration of sorts between Anonymous and the media, with Anonymous culture happily playing to type as the news media repeats and reinforces the stereotype. Anonymous's adoption of the hacker-figure, a figure generally interpreted as criminal in the media and popular culture, further reinforces the widely perceived nature of DDOS actions as inherently criminal. This complicates Anonymous's attempts to use DDOS as a form of political activism.

[38] The characterization of such a pathological cycle of behavior is cited by James Aho as critical to the demonizing of the social enemy, a role the hacker figure occupies in our modern technology-reliant society. (Aho 1994)

[39] This reference originally appeared in a televised investigative report by Phil Shuman, an investigative reporter for *MyFOX Los Angeles*, which aired July 26, 2007. The segment can be viewed here: https://www.youtube.com/watch?feature=player_embedded&v=DNO6G4ApJQY

This embrace of the media's anti-social hacker figure is also another performance of dissent on the part of Anonymous. By embodying the ultimate boogeyman of the modern technological age, Anonymous rejects the social order as undesirable and irredeemable. By performing the empowered outcast[40], they also perform *symbolic exit* (Shelby, 2012). Anonymous as a culture symbolically exits the mainstream, commercialized internet, overrun with private interests and attempts at state governance, and sets itself up as the theatrical embodiment of the internet as it could to be: anarchic, absurdist, free of outside interference.[41]

Accessibility within technologically defined tactical spaces

DDOS actions were taken up by digitally enabled activists to be a more accessible, less geographically bounded tactic for activist expression than physical world actions. While the Critical Art Ensemble saw the move to the online space as tracking the movements of structures of power to their new abode (Critical Art Ensemble, 1996), later groups saw it as a way to lower the barriers to entry. As mass DDOS actions have continued to develop tactically over the years, different groups have

[40] Though the hacker folk devil is a thoroughly othered outcast, he is also seen as being a techno-wizard, capable and willing of upsetting the entirety of modern society with a few keystrokes. (Sauter 2012)

[41] Gabriella Coleman pointed out in response to an early draft of this section that Anonymous's use of the hacker image is not universal, and has in several instances been rejected by various participants in the culture. This brings to the fore the question of how much of Anonymous's use of the "hacker" identity is reaction to the media's use of the characterization, and how much is internally developed. It is my view that Anonymous trollishly exploits the media's overuse of the "hacker" image primarily to manipulate the culture's perceived "mystique" by outsiders, and secondarily to maintain an internal, tongue-in-cheek reflection of their own A-culture. But, as with most aspects of Anonymous, these uses of the "hacker" image are not universally accepted.

continued to adapt it so that it is easier for individuals to participate. This adaptation occurs both on the level of tool design and information distribution, but also at a community level. During Operation Payback, for example, LOIC tutorials began popping up on YouTube and other locations around the web. Though it would be impossible to get an exact figure, YouTube search for "LOIC tutorial" yields thousands of results. One video, "How to Use LOIC (Low Orbit Ion Cannon)", uploaded in mid November 2010, had been viewed over 80,000 times by December 12, 2010, and had been viewed over 250,000 by April 2013.[42]

However, any efforts to further spread the tactic will be hampered by its very nature as a high bandwidth digital tactic. Its use is restricted to relatively affluent populations with unrestricted access to digital technology and high quality, predictable internet connectivity. Most DDOS tools in use from 2010 on must be downloaded and run from a computer, though other, less widespread versions exists which can be run from a website or a smart phone. This automatically excludes potential participants in areas with poor internet connectivity, or those who don't own their own computers and must rely on machines at schools, libraries, or cyber cafes where they aren't allowed to download and install new programs.

In some ways, the earlier, webpage based tools like the EDT's FloodNet may have been more diversely accessible than tools like LOIC or its successors. The early actions were also strictly scheduled to last for only short amounts of time, at most an hour or two, to accommodate the restrictions and expense of participating in an action

[42] This video and its metrics can be viewed at https://www.youtube.com/watch?v=sQRu-J3f_Kw and was last accessed on April 23 2013.

over a dial-up connection. The "occupation"-style DDOS actions organized by Anonymous, conversely, have run for days through DSL or fiber connections. So though connectivity and computing power advances have made it possible for actions to last longer, taking advantage of those advancements can severely limit the potential participant pool.

This has resulted in natural narrowing of trigger events for activist DDOS actions to mostly internet or technology oriented events. While the EDT, *the electrohippies* and others targeted the online representations of state governments and multi-national organizations, responding to cross-border issues of policy and globalization, Anonymous and its kin most frequently respond to events that occur in the online space itself. Operation Chanology was triggered by the Church of Scientology's attempts to remove a video of Tom Cruise from various websites. Operation Payback, both in its initial and Avenge Assange segments, was provoked by actions taken online which affected "internet native" entities, like the Pirate Bay or Wikileaks. This focus results in a further narrowing of the potentially interested participant pool. So while DDOS actions were and are often now deployed with intentions of dramatically expanding the activist population, accessibility and cultural issues often create severe barriers to that goal.

DDOS and "impure dissent"

Tommie Shelby notes that dissent, when it does not take the form of traditional, morally exemplary civil disobedience or other anticipated forms of protest, can be regarded as "impure dissent." Shelby analyzes hip hop and rap as forms of impure dissent, but his analysis leaves room for confrontational tactics like DDOS as well. Shelby defines impure dissent this way:

> ...while it contains valid political content, it also includes other elements that sharply diverge from conventional or widely held normative standards, and these deviant elements may seem to undermine its political aims. Impure dissent is meaningful political dissent that is mixed with, for example:....relentless use of profanity, epithets, and other offensive language; enactment of negative group stereotypes; violent and pornographic images; romantic narratives about outlaw figures and street crime;....xenophobia, homophobia, and misogyny; devaluation of education and other conventional paths to upward mobility....
> (Shelby, 2012, pp. 8-9)

Activist DDOS actions enter into the realm of impure dissent in two areas: DDOS actions bring activists into direct conflict with the privatized nature of the online space, with the actions themselves diverging from normative standards of speech and property; and modern practitioners, particularly Anonymous, whose actions are without questions the most widely known activist DDOS actions to date, are indelibly linked to anti-social hacker and criminal personas.

The use of the stereotyped hacker persona by Anonymous has a number of uses within the culture, including creating greater community cohesion through performance, aligning the group with a romantic and compelling history, and providing a ready-made hook for the media to latch on to in their reporting of Anonymous actions. However, by taking on the outlaw persona, Anonymous also recuses itself from the pantheon of traditional civic actors. The hacker outlaw is a politically impure actor, a potential threat who lives on the fringes of respectable society. By taking on that character's mantle, Anonymous renders their dissent both politically and morally impure. The "inflection" or tone of their outward messaging is also seen as deeply problematic, as it often incorporates cursing, vulgar humor, epithets, and a host of content unsuitable to polite conversation. Anonymous's status as impure dissenters make it difficult for them to communicate their political message to those outside the culture, but it does not in and of itself invalidate their dissent.

As previously mentioned, a primary motivation for the EDT and *the electrohippies* during the DDOS actions of the late 1990s was to establish the internet as a viable space for civil disobedience and dissent. As stated by *the electrohippies* in one of their initial papers defending the use of DDOS actions:

> Whilst the Internet was originally a place of discussion and networking, the invasion of corporate interests into this space has changed the perceptions of what the purpose of the Internet is. Some believe that the Internet is no longer a 'public' space – it has become a domain for the large corporations to peddle their particular brand of unsustainable consumerism. For many this is unacceptable....Whatever the views of particular people about the development of e-commerce on the 'Net, we must not ignore the fact that as another part of society's public space the Internet will be used by groups and individuals as a means of protests. There is no practical difference between cyberspace and the street in terms of how people use the 'Net.
>
> (DJNZ, 2000)

However, despite their aspirations, the commercialization and privatization of the internet continued. As of early 2013, the online space is, as it stands, thoroughly privatized. Public spaces, as they are understood to exist in the physical world under the guise of parks, sidewalks and roadways, do not exist online. As such, the expectations of speech rights online follow, not the norms of public fora, but the norms of private property.

The Supreme Court has laid out a "public forum doctrine" which guides the regulation of speech acts in public spaces. It identifies three, sometimes four broad categories: “the ‘traditional public forum,’ the ‘limited’ or ‘designated’ public forum,’ the ‘nonpublic forum,’ and private property (McPhail, 1998). The most permissive of these is the traditional public forum, streets, parks, sidewalks, town commons, and other areas traditionally recognized as being held in common for the public good. Limitations of speech and protest actions in these spaces, can be subject to only limited “time, place, and manner restrictions,” which cannot be based on the message of the protesters themselves (Zick, 2009).

The next two categories on the continuum, the limited/designated public forum and the nonpublic forum which “includes governmental property that is not a public for ‘by tradition or designation’–such as a post office or jail,” (McPhail, 2009 p. 58), are subject to the same criteria as the traditional public forum. That is, speech acts at these locations cannot be restricted based on the content of the speech, and such restrictions must be “reasonable.” However, the Court has noted that the government is under no Constitutional obligation to proactively protect free speech rights within limited/designated public fora and nonpublic fora (Zick, 2009). The only property category that is not limited in its possibly restrictions is private property. The owners of private property are relatively free in the restrictions they can place on the speech of others when it takes place on their property. (McPhail, 1998)

The internet has essentially developed into a entire zone of modern life lacking some crucial First Amendment protections. While the freedom of the press is relatively well protected in the online space, the rights of assembly and speech of the average individual remains unprotected. Given the internet's current role as a basic outlet of personal expression, association, and communication, this is deeply troubling. While protest taking place in the various public fora in the physical world have a foundation of history and legal doctrine to support their legitimacy as valid and protected political speech, actions that take place in the online sphere can only ever infringe on privately held property. The architecture of the network does not, as of yet, support spaces held in common.

As a privately-held public sphere,[43] disruptive acts of civil disobedience online will always be in conflict with dearly held doctrines of private property. Without substantial legal precedent supporting the rights of the political action to take place, the use of DDOS as a tactic in and of itself has the potential to render the activist action impure by coming into conflict with private property rights without the established cultural and legal protections that have developed around physical world civil disobedience. This is disastrous for the development of civil disobedience online. By being continually compared with activism in a sphere with substantially different norms of property and speech (i.e.: the physical world), civil disobedience online consistently comes out tainted

[43] This conflict has a physical world parallel. The initial Occupy Wall Street camp was established at Zucotti Park, a "privately-held public space" ostensibly available for public use but still subject to the potential restrictions of private property. The free speech obligations/protections provided by such spaces are legally murky.

by perceived criminality or bullying behavior. In this case, it is primarily the evolved constraints of the network itself that render DDOS activist actions impure.

Conclusions

Activist identity within movements and actions, a complex idea in the physical world, is further complicated by the highly distributed, mediated nature of online activism, particularly in the case of activist DDOS actions. In this chapter, I've looked at how identification and anonymity can each represent specific, intentional political stances on the role of the state in activism and online. I've further examined Anonymous's adoption of the exaggerated anti-social "hacker" figure as a cultural identity, and how this both aids cultural cohesion and complicated their efforts to engage in popularly legitimated political activism. It's also clear that popular claims that the internet has opened new doors to political participation and activism are substantially complicated by the inherently elitist nature of networked technology itself, which in turn has a direct effect on the types of issues activist DDOS actions are brought to bear on. Finally, the widespread privatization of the online space, something early practitioners of activist DDOS actions specifically sought to array themselves against, presents significant issues to the use of activist DDOS and its practitioners as they attempt to gain recognition as legitimate political actors. Rather, those who use activist DDOS as part of their repertoire of protest are likely to be seen as "impure dissenters." Though they can often reach populations not sympathetic to mainstream political discourse, "impure dissenters" often cut themselves off from popular legitimation, thus opening themselves up to a variety of criticisms and censures that traditional political actors would not have to face.

CHAPTER 4

State and Corporate Responses

The reaction of state, corporate and media actors has not been overly sympathetic to the activist use of DDOS, preferring to interpret uses as criminal or even acts of "cyberwar." This stunts the potential for not only the evolution of activist DDOS, but also for civil disobedience online in general. As we saw in Chapter One, early media coverage of DDOS actions tended to focus on the spectacle of the incident rather than the reality of the activism. Media reactions were, and have continued to be, predominantly colored by attempts to associate digital activists and their actions with the anti-social hacker persona, and acts of criminality or cyberwar. Coverage of the Electronic Disturbance Theater and *the electrohippies* typified this pattern of categorizing activist actions with criminal actions, while Anonymous's self-promoted association with anti-social hacker stereotypes supported the negative public image of DDOS as a tactic of civil disobedience. This chapter will look at how the responses of states and corporate targets of DDOS actions push the criminal perception of activist DDOS actions on the one hand, and on the other how these reactions fit into the practice of activist DDOS actions..

State responses: terrorism and sentencing recommendations

In their DDOS action against the WTO in 1999, *the electrohippies* were, in many ways, operating within a self-generated frame of digital activism. Though they were attempting to adapt the accepted frame of civil disobedience from physical world activism, the ways in which they were attempting to apply that frame to their disruptive, direct action campaign against the WTO were novel. This framing, that disruptive, distributed dissent, which occurred at a distance[44], was necessary for the validation of distributed activism which occurred primarily in the online space. Recognition of this frame was necessary for *the electrohippies*'s actions to be viewed as legitimate activism. Unfortunately, as was noted earlier, this was often not the case, as *the electrohippies* themselves note:

> As a result of the WTO action *the electrohippies collective* were labeled as terrorists...The problem with the knee jerk response of politicians and e-commerce gurus is that we run the risk of losing legitimate electronic action as governments use the excuse of 'hackers' to criminalize certain activities. We must make sure that both the positive and negative aspects of internet activism are clearly debated, and that cyberspace is not excised from the everyday realm of constitutional rights and freedoms.
>
> (DJNZ, 2000)

This classification mostly took place in the media, as was shown in Chapter 1. Other analysts paid greater attention to groups' self characterization, as noted by Dorothy Denning in her testimony before the House Armed Services Committee in 2000:

> While the above incidents were motivated by political and social reasons, whether they were sufficiently harmful or frightening to be classified as cyberterrorism is a judgment call. To the best of my knowledge, no attack so far has led to violence or injury to persons, although some may have intimidated their victims. Both the EDT and *the electrohippies* view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction. Most activists, whether participating in the Million Mom's March or a Web sit-in, are not terrorists. My

[44] Most of the organizers and activists in *the electrohippies* were British and operated from the UK. (electrohippies collective, 2000)

> personal view is that the threat of cyberterrorism has been mainly theoretical, but it is something to watch and take reasonable precautions against.
>
> (D. Denning, 2000)

Denning's testimony, combined with *the electrohippies*' statement, brings to the fore a number of issues pertinent to the influence and roles of states in digital protests. While Denning acknowledges the role of self-identification in judging the activist value of an action, *the electrohippies* point out that if the online space as a zone is judged to be unavailable for activist action, then the self-identification matters little. As the Internet developed from a pseudo-public academic intra-net into a vital part of everyday life for many people, it was inevitable that those who opposed the privatization of a perceived commons would be systematically marginalized by both the corporate and state interests that stood to benefit financially and politically from stabilization of the network. So although Denning hangs her definition of terrorism on the hook of personal harm and violence, she also acknowledges that a "judgment call" is required when classifying new disruptive behaviors. When the relevant "judge" is also the target of the disruptive protest, it is in their interests to reclassify legitimate protest as ideological violence.

As of this writing, there have been a several cases of activist DDOS actions which have gone to trial or been pleaded out, in the US and internationally. A significant case is that of Andreas-Thomas Vogel, a German national who ran the libertad.de website during the 2001 Deportation Class action against Lufthansa Airlines. Vogel had posted a call to action on libertad.de and was arrested on charges on coercion. Initially in 2005, a lower court in Frankfurt found Vogel guilty of using force against Lufthansa, based predominantly on the economic losses the airline had suffered during the campaign, both in terms of lost sales and the costs of acquiring additional bandwidth to soak the protesters' traffic. Vogel was sentenced to either pay a fine or serve 90 days in jail. However, the next year, a higher court overturned the verdict, finding, "...the online demonstration did not constitute a show of force but was intended to influence public opinion" (Post at thing.net, 2006). Libertad responded to the ruling with a statement that echoed those we have seen from *the electrohippies* and the EDT: "Although it is virtual in nature, the Internet is still a real public space. Wherever dirty deals go down, protests also have to be possible" (Hans-Peter Kartenberg quoted in thing.net post, 2006).

The Vogel case was the first international precedent to recognize the legal and philosophical arguments put forth by supporters of DDOS activist actions. The high court decision pivots on the point that these actions were oriented to influence the public, and through that avenue, influence the actions of the Lufthansa corporation, rather than badgering the airline into conceding to a set of demands. Specifically, the judge ruled that the protest was not an action of force intended to compel an action from Lufthansa; the action's intention was to impact public opinion first.

There has been no such precedent-setting case thus far in the US courts. This is in part due to the limited number of arrests resulting from DDOS actions until recently. Two individuals were arrested in connection with Anonymous's Operation Chanology DDOS actions against the Church of Scientology in 2007 and 2008. Both cases resulted in guilty pleas. (Goodin, 2008; Leyden, 2010). The Operation Payback DDOS actions resulted in fourteen individuals (including one minor) being charged under the CFAA with participating in the DDOS action against PayPal. Each defendant is being charged with two felony counts, which could result in up to 15 years in prison and fines of up to $500,0000 dollars (Hopkins, 2013). Others have been convicted in connection with the action internationally (Albanesius 2013). As of April 2013, a verdict had not yet been reached in the PayPal 14 case.

Potential sentences for DDOS actions in the US are high compared to other crimes and especially compared to other types of traditionally recognized activist activities. For example, in the US a sit-in would typically result in a charges of trespass, if anything. In state of Massachusetts, the punishment for criminal trespass is "a fine of not more than one hundred dollars or imprisonment for not more than thirty days or both such fine and imprisonment."[45] Resisting arrest, another typical charge, results in a term of imprisonment of "two and one-half years or a fine of not more than five hundred dollars, or both."[46] DDOS actions are prosecuted under Title 18, Section 1030 (a)(5) of the U.S Code, otherwise known as the Computer Fraud and Abuse Act, DDOS actions, along with other computer crimes, and are classified as fraud. US sentencing guidelines, laid out in a yearly United States Sentencing Commission Guidelines Manual, which are used as recommendations regarding federal cases within the US legal system, contain a series of adjustments that can be applied to "base offense level" according to a number of factors. The resultant "offense level" is then used to

[45] Massachusetts General Laws, Part IV, Title 1, Chapter 266, Section 120: "Entry upon private property after being forbidden as trespass; prima facie evidence; penalties; arrests; tenants or occupants excepted. Retrieved from http://www.malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter266/Section120

[46] Massachusetts General Laws, Part IV, Title 1, Chapter 268, Section 32B: "Resisting arrest." Retrieved from http://www.malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter268/Section32b

determine the recommended sentence. Particularly relevant to the case of DDOS actions are those adjustments that involve the amount of financial losses suffered[47]; and the number of victims[48]. PayPal claimed in a British court that the Operation Payback action cost them £3.5 million in losses, or roughly $5.5 million. That loss figure adds 18 levels to the base offense level for fraud of 7. PayPal did not disclose in court the number of victims it believes was impacted by Operation Payback, but we can assume it was probably higher than 250, which is the maximum listed in the US Sentencing Guidelines, for an additional 6 offense levels, giving us a total offense level of 31. For an individual with no previous criminal record, the recommended sentence for an offense level of 31 is 135 months, or more than 11 years. This is without the "special skills" or "sophisticated means" adjustments, both of which would add several more offense levels.

There are no established requirements for determining the figures for losses or number of victims in these cases. PayPal and the prosecution stated during the UK trial of Christopher Weatherhead that they included the "considerable damage to its reputation and loss of trade" that resulted from the actions in their calculations[49] (Williams, 2013). The lack of oversight in the calculation of damages and the low maximum number of victims mean that the judicial system is predisposed to come down hard on the participants and organizers of these actions. Threats of long prison terms may lead to more individuals pleading out before trial, which could delay a precedent-

[47] United States Sentencing Commission Guidelines Manual, 2B1.1.b.1
[48] United States Sentencing Commission Guidelines Manual, 2B1.1.b.2 A-C
[49] Weatherhead was sentenced to 18 months jail time for his role in the action.

setting court decision like the Vogel decision in Germany, legitimating disruptive civil disobedience online.

Corporate responses: the avatar nature of online brand presence

DDOS actions expand potential modes of interaction between individuals or groups of individuals, and corporations. Corporate websites allow for a symbolic and actual centralizing of the normally distributed brand reality of a corporate entity. Just as a corporate headquarters acts as the physical world manifestation of a corporation's brand identity, and individual products as distributed, appendage-like instances of the same, a company's website functions as a digital, responsive brand model, but as a cohesive whole. In physical world activism, the activist is restricted to confrontations with the physical manifestations of corporate brands, which, especially in the case of national or multinational entities, are often only a part or appendage of the whole corporate entity. Instances of activism are limited in their scope and impact: a defaced billboard is still just one among many; an action at a factory or headquarters does not distribute itself across multiple brand enactments. But because a corporate brand website is meant to represent a sprawling corporate entity as a coherent, comprehensible whole, a confrontation with that digital entity is effectively symbolic of a confrontation with the corporation as a whole. The bounded nature of the website allows a new, more symmetric manner of confrontation with individual activists, bounded individual to bounded individual. The vulnerability of the single instantiation empowers the activist for the duration of the confrontation, rather than the corporation.

As holistic representations of corporate entities, websites are high value brand manifestations. As such, interference or disruption of predictable continuity can provoke a response that other activist tactics are unlikely to elicit. By imbuing corporate websites and digital, branded storefronts with the symbolic selfhood of avatars, corporations have effectively reduced their public resilience to be equal only to the resilience of that website.[50] Any crack in that digital facade requires immediate attention, as it has the potential to reflect on the entire corporation, not just one part. In its pre-internet, distributed incarnation, any number of slights, insults, or disruptions could have gone unremarked upon. But as a website now can be the manifestation of an entire corporate entity or brand, continuity disruptions cannot be disregarded. Again, this necessity-of-response empowers activists by acting as a forcing function with regard to the responses of corporations. Rather than having to wait and hope that corporations will respond to an activist action, with the very likely result that the action will simply be ignored, offenses to the sanctity of the digital brand representation come too close to disrupting the image of corporate continuity and stability to be ignored. By virtue of the symbolic value they have invested in the digital brand representation, corporate entities have obligated themselves to engage with the public disruption, thus providing activists with a trigger point, provoking a public response.

[50] The symbolic investment of corporate selfhood in these online presences should not be interpreted as either reducing the ability of the corporation exploit other lines of public communication (through spokespeople, press conferences, etc) or as permission to reduce the actual and legal vulnerability of such corporate avatars to disruption and disparagement, either through DDOS actions, parody, satire, or appropriation. Mickey Mouse may be precious to Disney, but (for now, at least) he can still be used as a tool of derision against his parent company.

Like states, these responses are often an attempt to push an interpretation of the actions as criminal or anti-social rather than activist in nature. As stated above, it is relatively easy for corporations to claim large damage and victim totals, thus making it appear that these actions are more disruptive and destructive than they may actually be. By over-estimating their potential for damage, corporations can promote the perspective that DDOS actions are incompatible with the continued presence of legitimate business on the internet.

In this face of this, the question arises: why go for the symbolic disruption of a corporate homepage when core systems, such as PayPal's payment processing systems might have been disrupted instead? This response echoes the critiques of the Critical Art Ensemble referred to in Chapter One, namely that attention-oriented activism, or activism which aims to influence media and public opinion first, is not as effective as direct action models. This criticism, however, does not consider that there may be multiple, equally viable goals to an activist DDOS campaign, and that not all goals are equally served by simple, covert disruption. If the goal is to publicize, say, Paypal's participation in Wikileaks Banking Blockade, disrupting their payment processing system does little to further that goal. This goal is markedly different than attempting to disrupt the internal operations of an already high-profile event like the WTO. Within an analysis of a disruptive action, the nuances of what is disrupted and how are relevant. In some cases, it is more useful to disrupt an image, while in others it is more useful to disrupt a process.

Conclusions

Because of its relative novelty, activist DDOS actions are vulnerable to classifications of criminality and cyberterrorism. Fundamentally, activist actions need to be recognized as acts of political speech by the state, their participants, law enforcement, bystanders, and their targets to be effective means of political dissent. Without that recognition, activist actions can be rendered impotent or counter-productive. Thus, the responses of states and corporations to the activist DDOS actions is highly relevant to this analysis. The United State government's pattern of using cyberwar rhetoric and heavy punishments for so-called "hacking" crimes do not bode well for its acceptance of activist DDOS actions as a legitimate form of civil disobedience or disruptive protest. While corporations may perhaps wish that activist DDOS actions could be ignored, the symbolic importance often invested in the stability of a corporation's online presence, which is read as a reflection of the stability of the corporation as a whole, makes this impossible. In this way, corporations have obligated themselves to respond quickly to activist DDOS actions, ironically making them an attractive mode of activism for individuals and groups who see disruption as an effective model of political action.

CHAPTER 5

Ethical DDOS Actions: An Analytical Framework

Though DDOS actions have been used as a tool of digital activism for the past two decades, the past few years have seen an explosion in the popularization of the tactic and a sharp increase in the attention its use attracts from the media and state actors. This attention has brought with it loud criticism from various stakeholders in the digital space, including other digital activists. However, both the tactic's critics and defenders seek to declare the tactic as a whole good or bad, without a nuanced understanding of the variety of circumstances and contexts that can render the tactic's use ethical or unethical. In this chapter, I aim to lay down the preliminaries for a framework by which to perform an ethical analysis of activist DDOS actions in individual use contexts.

The purpose of this ethical framework is to provide a basis for the analysis of DDOS actions that have already occurred. The framework considers the use of the tactic within broader campaigns; activists' motivations for using the tactic; the intended and actual effects achieved; the technological capacities used; power relations between organizers, participants and targets; and the role of state, state-related, and semi-state actors. Taken together, these factors create a holistic, qualitative system for evaluating the ethical validity of a given DDOS action, and can be used to create models to guide the use of the tactic, and similarly disruptive tools of digital activism in the future.

The value of disruption and the right to be heard

The disruptive nature of activist DDOS action does not, in and of itself, invalidate it as a tactic of activism. Particularly in so much as the technologically bounded nature of the tactic enables it to confront the changing nature of the online environment, the disruptive use of DDOS constitutes a form of Pfaffenberger's "technological reconstitution," wherein

> ...impact constituencies actively reshape technological production processes or artifacts guided by a self-consciously 'revolutionary' ideology, producing what I call *counterartifiacts.* This ideology is produced by means of a symbolic inversion called *antisignification.*
>
> (B. Pfaffenberger, 1992)

The "counterartifact" produced here is the disruption itself. By replacing continuity with disruption, activists attempt to create a rhetorical cavity in the digitized structure of capitalism wherein activism can take place. This break in "business as usual" makes room for counter-actions of activism. It is the creation of excavated, disrupted space that is valuable in these contexts, sometimes even more valuable than the specific instances of activist/target engagement. In this way, environments are created for the revelation of "hidden transcripts" of resistance (Scott, 1990). 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" (Scott, 1990). While hidden transcripts are valuable independently, they are most effective when performed by a group or crowd, a concerted action that allows the participants to recognize that they are a connected, though not necessarily in constant contact. The disruption, i.e. the creation of the counterartifact allows for the establishment of this meeting space, which is in its turn a type of antisignification.

This is to say that the disruption inherent in DDOS actions is not empty of meaning. The targeted content is not supplanted by a void. Rather, it is exchanged for the fact of action. A conversation occurs, though the parties are speaking with different vocabularies.

It is often the case with unpopular, dissenting, or poorly funded causes that disruption is one of the only avenues to public attention. As covered in Chapter One, the news media is the modern arbiter of popular attention, deciding which activist causes are worth space on the front page or time on the 11 o'clock news. If the actions taken by activists don't "look like" activism, or the views presented are too outside the mainstream to appeal to viewers—and advertisers—it is likely that these actions will not be covered at all (Barron, 1967). However it is vital to a democracy that unpopular and dissenting ideas be aired, discussed, and debated in the open. As Justice William O. Douglas wrote in his 1951 dissent to *Dennis v. United States*:

> Full and free discussion even of ideas we hate encourages the testing of our own prejudices and preconceptions. Full and free discussion keeps a society from becoming stagnant and unprepared for the stresses and strains that work to tear all

> civilizations apart. Full and free discussion has indeed been the first article of our faith.
>
> (W. Douglas, 1951)

An unbroken broadcasting of the status quo impoverishes our democracy. In order to avoid such a situation, dissenting views much not only be *spoken* but also *heard.* Owen Fiss (1996), Jerome Barron (1967), and others have presented interpretations of the First Amendment which encompasses a “right to be heard” and a “right to hear” as well as a “right to speak.” Though it may be argued that the internet has substantially increased the number of soap boxes available, it has not increased the availability of the audience. Rather, as individuals become more adept at filtering their information taps, and as the infrastructure of the internet and the physical world around them makes it easier to avoid unwanted encounters with unpopular or simply different viewpoints, the ability of dissenters to truly have a voice in the national debate is being steadily diminished (Zick, 2009).

For unpopular and dissenting causes to attract the attention of a news media industry that, for economic reasons, is often uninterested in covering them, disruption of some kind is often necessary. Attention is attracted via the fact of the disruption, and the dissenting view is covered. As discussed in Chapter One, this is often a complicated process as activists attempt to engage the attention of the mainstream through the use innovative and disruptive tactics, always running a risk that their activism will not be recognized as such or dismissed as a novelty. However, in an information landscape where corporate, homogenized news media still dominates much of the agenda setting, resorting to extreme tactics in the hopes of heard is often a better option for the dissenter than simply waiting to be heard by grace and chance. In this way, disruption of some kind is a necessary part of the modern repertoire of contention. Online, that disruption may take the form of a DDOS action, while in the physical world it may look like a sit-in or occupation. What is critical is that the status quo, the normal flow of information must be disrupted is dissenting voices are to be both voiced and heard.

Disruption is not the most appropriate tactic in all activist cases. It is important to consider in a given action whether disruption moves a dialogue forward by challenging architectures, structures, and entities previously imagined to be solid and unalterable, or if it is an attempt to silence un-replaceable speech. Similarly, it is useful to consider that not all disrupted speech is silenced, as corporations and states often have a number of outlets for speech, especially through intermediaries like the news media. However, disruptive actions that are not accompanied by effective public messaging run the risk of being misinterpreted by targets, the media, and the public, or not being noticed at all.

Intended effects and actual effects

As mentioned above, DDOS actions have historically been characterized as being little more than crowdsourced censorship, a sort of digitized heckler's veto. This characterization, certainly appropriate in some cases, such as those instances of state-initiated DDOS actions against independent media sites analyzed by Ethan Zuckerman and others (2010), is easily and inappropriately generalized to the use of the tactic as a whole. This often occurs because identical technological ends states (such as a site being slowed or going down entirely) can be arrived at by different actors with dramatically different motivations, which are not necessarily immediately evident. This motivation myopia is exacerbated by the absence in US law of any useful analysis of motive in the determination of the criminality of a DDOS action. A DDOS action launched to extort money from a site operator is considered legally equivalent to an activist action against a large corporate site for the purpose of drawing attention to an issue. However, when attempting an ethical classification of these acts, it is vital to take into account both the *intended effects* of an action, and the *actual effects* of the action. To illustrate this point, I will examine three different actions that particularly highlight this analytical factor: the 1997 IGC/*Euskal Herria* action, the 2001 Deportation Class action against Lufthansa Airlines, and the eToys/etoy 1999 toywar campaign.

IGC/Euskal Herria Journal action

Oxblood Ruffin's accusation that DDOS actions are nothing more than "illegal, unethical, and uncivil" (Ruffin, 2000) 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* (Nicol, n.d.). This was a populist minded action; at one point, the major Spanish newspaper *El Pais* threw its support behind the mailbombing campaign and published target email addressed for the IGC, though it later retracted its support and removed the emails from its website (Gor, 1997). The campaign included network level actions and an email campaign, eventually rendering inaccessible the websites and email of IGC's over 13,000 subscribers. 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 providing hosting to *Euskal Herria Journal*, though it did so under protest (IGC, 1997).

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 on IGC strikes a violent blow to the core of the organization directly. Furthermore, 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 email-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.

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. So, in *actual effect*, the action caused the *intended effect*. 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, multi-national corporation. 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, multi-pronged protest against the German government's use of the airlines' flights to deport immigrants. Using an adaptation of the Electronic Disturbance Theater'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 (Dominguez, 2009). 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 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," (Munroe, 2011) with the implication that the action is technologically simplistic and has little practical impact on the organization targeted. It is a symbolic action rather than a direct action, performed for the benefit of those participating and those watching.

The stated goal of the Lufthansa action was to 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 gross fiat.

The etoy toywar

In December of 1999, the EDT, the Swiss art group etoy, and RTmark 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 (Wark, 2003). 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" campaign was intended, according to Ricardo Dominguez, to "...represent the present of a global group of people gathered to bear witness to a wrong" (Dominguez quoted in Wark, 2003).

While the action may have been intended to symbolically represent the displeasure at the bullying tactics of a large e-commerce corporation, it also had a significant impact on eToys Inc business. Though the e-retailer's site never crashed, it was significantly slowed during the course of the action, rendering it unusable through most of the peak holiday shopping season. Over the course of the campaign, the share price of eToys Inc dropped from $67 to $15, for a net loss of $4.5 billion, which etoy reported as the "most expensive performance in art history" with evident glee (Grether, 2000). It is also worth noting that this was a battle between two innovative, internet-centered organizations. etoy, the art group, existed primarily through their electronic projects, experiments, and performances, while eToys Inc was a successful e-commerce retailer, its operational business consisting of little more than an online storefront (etoys.com) and a massive warehouse. As both executed denial-of-service-actions against each other (eToys Inc via a judicial injunction forcing Network Solutions to remove the etoy.com URL from the internet and etoy via its FloodNet powered DDOS campaign), both aimed their actions at their opponents' core. The toywar campaign, however, enjoyed the support of some 1,700 participants, whose participatory weight added credence to its ethical claims (McKenzie, 2001). This judgment is bolstered by the fact that in January of 2000 eToys Inc dropped its lawsuit and paid the court costs of etoy.

Technology utilized

As mentioned previously, it is becoming increasingly difficult for a purely volunteer, manual style DDOS action (which require a body in a chair for the duration of the action and can claim the strongest line of symmetry to physical world sit-ins) to have a noticeable effect on a large, robust corporate website. This is due to advances in technology as well as the vending of DDOS defense services to at-risk companies by companies like Akamai and Arbor Networks. This had led to the use of botnets, traffic multipliers, automated tools, and other exploits to bring the power of such actions in line with the defenses employed by targets. While the use of such technological tools doesn't automatically negatively affect the validity of an activist DDOS action, the use of non-volunteer botnets is a particularly worrying turn. Volunteer botnets present their own ethical concerns, but are less immediately objectionable.

Another aspect to consider is how advances in infrastructure and connectivity have changed the nature of DDOS actions over time. Groups like Strano, the EDT, and others active in the 1990s and early 2000s structured their actions to be of basically short duration. The Strano Netstrike action, taking place on December 21, 1995, lasted for an hour (Thomas, 2001). The EDT's "Tactical Theater Schedule," a list of the FloodNet actions taking place in 1998, notes that actions run from "10:00 a.m. to 12:00 p.m. and 4:00 to 6:00 p.m...Mexico City Time" for each of the thirteen dates listed.[51] The technical and financial realities of dial-up internet prevented, for the most part, more ambitious actions of longer duration. *the electrohippies* 1999 WTO action was unique in

[51] This schedule is currently archived at http://www.thing.net/~rdom/ecd/ecd98.html and was last accessed April 23, 2013.

that it was designed to take place continually over a number of days.[52] The transition from telephone-based internet connections to cable and fiber connections has altered the duration calculus for DDOS actions. With the high speed, always on internet connections available to many participants, DDOS actions have the potential to go on for days, or weeks, or indefinitely. While organizers were once constrained simply by technical capacity, other concerns, including ethics, must now come into play when determining the duration of DDOS actions.

Volunteer and non-volunteer botnets

In the winter of 2010, the controversial online group Anonymous launched Operation Payback, targeting various organizations that had arrayed themselves in opposition to Wikileaks in the wake of the latter's release of a large cache of diplomatic cables exfiltrated from the US State Department. The DDOS action was predominantly powered by the Low Orbit Ion Cannon DDOS tool, which contained functionalities for both "Manual" mode, which required the user to target and fire the tool independently, and "Hive Mind" mode, which allowed the user to join a volunteer botnet, controlled via a central IRC channel. In her 2012 book, Parmy Olson stated that in addition to Low Orbit Ion Cannon, non- volunteer (i.e. criminal) botnets were employed in the Operation

[52] The November 29, 1999 call-to-action email states, "The sit-in will begin 08.00 USA & Canada (Pacific time) 30th November...and will finish four days later." The email notes that those with dial up connections may not be able to stay online for the whole planned four days, and so advises, "If you cannot afford to spend much time online then concentrate on November 30th (or Dec. 1rst for those in the East. But we would like people to aim to go online for 12.00 Pacific time on December 3rd (add 4 hours to the above timetable for your local time) until the end of December 4th."

Payback DDOS raids that resulted in the most downtime per target. Non-volunteer botnets are created by infecting computers with a program which allows them to be controlled by a remote server without the owners' knowledge. The use of someone's technological resources without their consent in a political action, particularly one that carries high legal risk, is a grossly unethical action. Moreover it cheapens the participation of the activists who are consensually participating, and makes it easier for critics to dismiss DDOS actions as criminality cloaked as free speech.

Prior to Anonymous's Hive Mind powered volunteer botnets, the tactic had been used by pro-Israeli activists in 1999. A group of Israeli students calling themselves Help Israel Win released a tool that allowed people to participate in DDOS actions, ostensibly targeting anti-Israel websites. Like LOIC's Hive Mind mode, individuals who downloaded the Patriot DDOS software package from help-israel-win.tk could link their computers to an IRC server and participate in DDOS actions. Unlike LOIC, Patriot runs solely in the background and does not allow for user input of any kind (Carr, 2011). The original website is no longer online or archived, however Jeffrey Carr quotes the group's self-characterization as "a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering." Their goal of "unit[ing] the computer capabilities of many people around the world...in order to disrupt our enemies efforts to destroy the state of Israel" (as quoted in Carr, 2011) echoes similar articulations by *the electrohippies* around their WTO action.

The release of the tool itself garnered a moderate amount of media attention, attracting coverage in *Wired* [53] and blogs.[54] *The Wired* article notes that at one point there were roughly 1,000 computers hooked into the botnet, and Help Israel Win claimed credit for bringing down sarayaalquds.org and qudsvoice.net.

Volunteer botnets also raise issues of consent, ones that are incumbent on the organizers to address. Volunteer botnets make it easy for different people to participate in DDOS actions without encountering the hardships that sitting in front of a computer and searching for targeting and scheduling information might present to working individuals, students, or people in different time zones than the primary organizers. Rather, they can pledge their support and resources to a given cause and trust the organizers to utilize those resources wisely. This then places a responsibility on the organizers to maintain strong, open communications channels with those participants and not make significant changes to the operation of the DDOS campaign without their consent. It is also necessary that organizers publicize information on how one might withdraw from a voluntary botnet if individuals should wish to do so.

Context within a greater campaign

The EDT and other groups have repeatedly termed activist DDOS actions "digital" or "virtual sit-ins" (Auty, 2004). This nomenclature is highly evocative, and

[53] Shachtman, Noah (2009, January 8) Wage Cyberwar Against Hamas, Surrender Your PC. *Wired*. Retrieved from http://www.wired.com/dangerroom/2009/01/israel-dns-hack/

[54] Zuckerman, Ethan. (2009, January 18) Install a trojan for Israel? Uh, no thanks. *My Heart's in Accra*. Retrieved from http://www.ethanzuckerman.com/blog/2009/01/08/install-a-trojan-for-israel-uh-no-thanks/

allows activists to build off the pedagogical and cultural capital of historical physical world sit-ins (Rolfe, 2005). However, the metaphor is imperfect, and 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 US with the establishment of "protest zones" near locations deemed to be sensitive, the physical closeness of protest actions to direct or symbolic targets is a valuable part of activist messaging, as was discussed in Chapter One.

This type of proximal messaging is not natural in the online space. DDOS actions in particular may by invisible to the public. Rather, 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. For this reason, it is incumbent on the organizers of such actions to maintain a high profile messaging campaign in addition to any activist DDOS actions that are taking place, as well as exploring other avenues of digital message distribution that may be spontaneously discovered by the public, such as Google-bombing, typo-squatting, or defacements.

Power relations between organizers, participants, and targets

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 occurs at scales of distance previously unheard of, as well as fostering interactions between individuals and entities which may have been previously impossible, such as allowing individuals to enter into direct confrontation with the 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 policies of the French government. Similarly, the EDT's Zapatista actions were organized in the US, but targeted the websites of the Mexican president Ernesto Zedillo, as well as the Frankfurt Stock Exchange, among others, in order to protest the Mexican governments treatment of the Zapatistas. Additionally, participants may be drawn from a grab-bag of countries and jurisdictions. This practice of "transnational activism" (Tarrow 2005) 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 interstate 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 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.

Conclusions

If activist DDOS actions are to continue to be a tool in the repertoire of digital activism, there needs to be a structured method for determining the ethical validity of those actions. This is necessary both for the benefit of organizers considering the use of the tactic, as well as for the legal and political arguments that arise as activists push for the tactic's widespread acceptance and legitimacy. Here I have tried to lay out that framework, using examples from the history of activist DDOS actions as illustrations. That said, this is still a reflective framework, and works best as an analytical tool to be deployed in the aftermath of an action, though prescriptive lessons could certainly be drawn from it.

CONCLUSION

The Future of DDOS

Over the course of this work, I've attempted to arrive at a thorough description of the history and current practice of activist distributed denial of service actions, as well as presenting the framework for a reflective ethical analysis of actions. The question now is, will the practice of activist DDOS actions continue, or are practical, theoretical, and ethical challenges faced too great to allow for the tactic to be effective?

As I described earlier, downtime is notoriously hard to achieve for an all-volunteer activist DDOS action, especially against a large corporate target. An "arms race" dynamic has ensued, which encourages the use of non-volunteer botnets and exploits to augment volunteer efforts and which also diminishes the ethical validity of activist DDOS actions. The defensive capabilities of for-hire firms like Prolexic and Arbor Networks, responding mainly to the advancements in criminal DDOS actions, continue to outstrip the capabilities of nearly all activist campaigns.

As downtime continues to become more and more difficult to ethically achieve, media exhaustion also becomes a concern. As of 2013, criminal DDOS actions received more coverage than activist DDOS actions, and coverage often does not make clear the distinctions between the two types of actions. Could activist DDOS actions simply become invisible in the sea of criminal actions? Or could the media landscape go the other way, with DDOS actions of all stripes becoming so commonplace that they warrant no coverage at all? Either outcome would be devastating for the publicity and messaging goals of activist DDOS actions.

The use of DDOS as a tactic of extortion, criminality, and nation-state-initiated censorship is damaging to its perceived legitimacy as an activist tactic. This association hampers the perception of activist DDOS actions as legitimate and worthwhile acts of political activism, and also prevents the further diffusion of the tactic. The flamboyant, anti-social pantomime performed by Anonymous and other similar groups further restricts *open* use of the tactic to an online fringe.

Because of its enduring associations with criminality and extreme online subcultures, in addition to its current legal status and particular technical challenges, I think it is unlikely at this time that DDOS actions will ever become a part of the popularly accepted activist repertoire of contention in the near future, unlike similar physical world tactics like sit-ins or occupations. However, I predict that DDOS actions will remain popular among internet-based fringe groups and subcultures, particularly those which adhere to a Barlowian view of the independent, self-contained nature of the Internet. As high-profile hacker and computer crime cases come to trial, particularly the upcoming trials of the Paypal 14, these will serve as radicalizing events, "group grievances," for the transgressive, technologically-mediated subcultures which are currently serving as cultural laboratories for disruptive online activism.

This radicalization, which occurs most strongly in the aftermath of convictions (such as those of Andrew Aurenheimer, also known as weev; or Jeremy Hammond) or tragedies (such as the suicide of Aaron Swartz), further underlines the perceived disjuncture between behavioral norms in these subcultures (or, in some cases, in more mainstream, technologically sophisticated populations) and the legal response delivered by the state. The popular association of activist DDOS actions with criminality is often not of interest to these radicalized groups, and may even be a point of attraction. The disapproval of the state can serve to underscore its cluelessness with regard to the internet and technologically-mediated transgressive subcultures, a cluelessness which these subcultures in turn often see as something to mock and exaggerate.

Is the use of DDOS by these groups abridging their ability to develop other innovating forms of online activism? The answer to this is an unequivocal no. Though not examined in this work, the resurgence of tactics like doxing, "human flesh search," information exfiltration, leaking, defacement, software development, the remote organization of backup internet connectivity in the event of nation-level shutdowns, and large scale data analysis, either automated or human-distributed, are all indicators of innovative developments in tactical and strategic activism. However, many of these are advanced activities, requiring significant skill, organization, support, and planning to pull off. They are not entry-level activities. As such, the pool of potential participants is much smaller, and would not necessarily benefit from a massive influx of inexperienced but nonetheless eager participants. Moreover, many of the tactics listed above and others are not attention-oriented in the same way that many activist DDOS actions are: massive amounts of media attention are not their goal, and may be detrimental. The attention-oriented nature of activist DDOS actions lends itself to encouraging media coverage at a level that other tactics might not.

As a "street-less" space, that the internet runs counter to many assumed practices of speech and public politics appears to belie Nathan Jurgenson's "digital dualism" fallacy (Jurgenson, 2011). The "speechy" nature of the online space had led to this seeming contradiction, wherein existing speech online is so highly valued that we drastically de-value other types of disruptive, activist speech which are tolerated, even specifically valued, in the offline world. If we acknowledge that civil disobedience and disruptive activism are valuable tools of activist speech and political discourse in the physical world, than it must also be acknowledged that they should be equally valuable and desirable in the online space. In the online space, dissenting speech should have a platform and a voice, ones that we are occasionally obligated to encounter, just as we encounter them in the physical world. As an avenue for speech, the internet should also be open to dissenting, potentially disruptive speech. Without forced encounters with dissent, our society will stagnant.

Activist DDOS actions started as an exploration into the activist potential of the internet by activists experienced in "on the streets" activism. In its modern incarnation, activist DDOS is practiced mainly by fringe actors, who consider the online space a primary zone of interaction, socialization, and political action. Though in many ways an extremely accessible stepping stone to more involved methods of online activism, DDOS actions remain privileged in many ways, including their basic technological nature, the specific populations involved, and the specific legal and cultural challenges inherent in modern non-mainstream computer use. Though DDOS itself may become increasingly marginalized as an activist practice, high profile campaigns like Operation Payback and its ensuing legal battle have opened the debate on the validity, desirability and potential of disruptive activism and civil disobedience in the online space. This work is presented as a step towards the robust analysis of these repertoires of contention in the online space that has become such an integral part of our modern culture.

ACKNOWLEDGEMENTS

Ethan Zuckerman and James Paradis provided consistently amazing support through not only the writing of this thesis, but also throughout my time at Comparative Media Studies and the Center for Civic Media. My experience would have been markedly different without them, and I am grateful for their guidance, wisdom, and occasional (much appreciated) pep talks.

J. Nathan Matias and Charlie De Tar at the Center for Civic Media were excellent brain storming partners and late-night co-workers, who have consistently over the past two years humbled me with their knowledge and intellectual generosity.

Kate Crawford of MSR, Jonathan Zittrain of Harvard Law School, Sasha Costanza-Chock of MIT, Gabriella Coleman of McGill, Willow Brugh, and Jonathon Penney of the Berkman Center all generously gave their time to comment on this work in various drafts, and their insights were invaluable.

Some sections of this work were previously published in the *American Behavioral Scientist*, in a special issue edited by Zeynep Tufekci and Deen Freelon. I'd like to thank Zeynep in particular for her editorial guidance throughout the peer-review publication process. Her insights ultimately helped shape the final form of this larger work.

Some sections of this work were previously published on *HiLoBrow*, and I'd like to thank Joshua Glenn for helping me to articulate my thoughts on the role of the Guy Fawkes mask in Anonymous culture.

I'd like to thank Hanni Fakhoury and everyone else at the Electronic Frontier Foundation, who gave me the opportunity to research sentencing practices related to CFAA violations, work which made its way into this project.

I'd like to thank the Berkman Center for Internet and Society at Harvard University, which in addition to giving me the opportunity to enjoy the amazing community of Berkman Fellows this year, also gave me the chance to present a section of this work at a lunch talk in January, 2013. The questions, comments, and insights of the attendees and Fellows were incredibly helpful and very much appreciated.

Sections of this work were previously presented at PCA/ACA in Boston, HOPE Number Nine in New York, and 29c3 in Hamburg, Germany. I'd like to thank the attendees of these conferences for their sharp and observant questions and comments.

The Hacker Culture Reading Group at the Berkman Center gave me a chance to inflict my background reading on my friends, and so I'd like to thank Kendra Albert, Ryan Budish, Jonathon Penney (again), Andy Sellars, Diana Kimball, and Kit Walsh for joining me in talking through so many of the issues that became central to this thesis without them even knowing.

Deb Chachra, Andrew Sempere, Todd Harper, Nancy Baym, and many others provided excellent practical advice in 140-character chunks over the course of this project. I'd also like to thank Twitter for providing the platform.

Jess Tatlock and Shannon Larkin made sure that none of the grad students in Comparative Media Studies starved or missed important deadlines, for which we are eternally grateful.

My parents, Beth Olanoff and Eric Sauter, and my brother, Aaron Sauter, have been incredibly supportive throughout my academic career, through many ups and downs. I'm thankful they think studying the internet is a real thing, and so far haven't made me get a real job.

Ed Platt has provided many cups of tea, dinners, and late night trips to Tosci's. They were all very much appreciated. :)

My colleagues in Comparative Media Studies and the Center for Civic Media were the best people to make this giant slog with, and I'm grateful to have had their company and mutual support throughout this long long process. We did it! Thumbs up for rock and roll!

Finally I'd like to thank the activists, hackers, and researchers who took the time to talk with me, correct my misperceptions and mistakes, point me towards materials and archives, as well as doing the activism and making the history that I've been studying for the past year and half. Thank you for your generosity, and for sharing your experiences and insights with me.

References

2012 United States Sentencing Commission Guidelines Manual (effective 2012, November 1) Retrieved from http://www.ussc.gov/Guidelines/2012_Guidelines/index.cfm

A cat is fine, too. (2009). *Know Your Meme.* Retrieved from http://knowyourmeme.com/ memes/a-cat-is-fine-too

Aamoth, D. (2010, December 9). Operation Payback: Who are the WikiLeaks "hacktivists"? *Time.com*. Retrieved from http://techland.time.com/2010/12/09/operation-payback-who- are-the-wikileaks-hactivists/

abatishchev. (n.d.). *LOIC.* Retrieved from http://sourceforge.net/projects/loic/

Aho, J. A. (1994) *This Thing of Darkness: A Sociology of the Enemy*. Seattle, WA: University of Washington Press

Albanesius, C. (2013, January 24) Anonymous Hacker Gets 14 Months for PayPal, MasterCard Attacks. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,2817,2414674,00.asp

Anderson, N. (2010, September 30) Operation Payback attacks to go on until we "stop being angry." *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/news/2010/09/operation-payback-attacks-continue-until-we-stop-being-angry.ars

Auerbach, D. (2012) Anonymity as Culture: Treatise. *Triple Canopy*. 15. Retrieved from http://canopycanopycanopy.com/15/anonymity_as_culture__treatise

Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *ASLIB*
Proceedings: New Information Perspectives, *56*(4), 212-221.

Barlow, J. P. (1996, February 8) A Declaration of Independence for Cyberspace. Retrieved from https://projects.eff.org/~barlow/Declaration-Final.html

Barron, J. (1967) Access to the Press—A New First Amendment Right. *Harvard Law Review*. 80(1641), pp. 1641-1678

Bell, M. (2010, December 8). Anonymous attacks Visa.com, Mastercard.com in support of WikiLeaks. *The Washington Post.* Retrieved from http://voices.washingtonpost.com/blog-post/2010/12/mastercardcom_hacked_by_wikile.html

Boczkowski, P. & De Santos, M. (2007) When More Media Equals Less News: Patterns of Content Homogenization in Argentina's Leading Print and Online Newspapers. *Political Communication.* 24(2), pp. 167-180

Borger, J., & Leigh, D. (2010, November 28). Siprnet: Where America stores its secret cables. Defence department's hidden Internet is meant to be secure, but millions of officials and soldiers have access. *Guardian.* Retrieved from http://www.guardian.co.uk/world/2010/ nov/28/siprnet-america-stores-secret-cables

Carr, J. (2011). *Inside Cyber Warfare.* Sebastropol, CA: O'Reilly Media.

Critical Art Ensemble. (1996). *Electronic civil disobedience and other unpopular ideas.* Brooklyn, NY: Autonomedia.

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

Coleman, G. (2011a). Anonymous: From lulz to collective action. *Media Commons.* Retrieved from http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective- action

Coleman, G. (2011b). *Geek politics and Anonymous.* Retrieved from http://re-publica.de/11/ blog/panel/geek-politics-and-anonymous/

Coleman, G. (2012). Our weirdness is free. *Triple Canopy*, 15. Retrieved from http://canopycanopy.com/15/our_weirdness_is_free

Computer Fraud and Abuse Act, 18 U.S.C., §1030 (1984).

Correll, S. (2010, December 15). Tis the season of DDOS: WikiLeaks edition [Web log post]. *PandaLabs Blog.* Retrieved from http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/

Costanza-Chock, S. (2003). Mapping the repertoire of electronic contention. In A. Opel & D. Pompper (Eds.), *Representing resistance: Media, civil disobedience and the global justice movement* (pp. 173-191). Greenwood, NJ: Praeger.

Denning, D. (2000, May 23) Prepared Statement of Dorothy E. Denning Georgetown University Before the House Armed Services Committee Oversight Panel on Terrorism. *Federal News Service*. Retrieved from LexisNexis.

Denning, D. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Networks and Netwars : The Future of Terror, Crime, and Militancy*, J. Arquilla and D. F. Ronfeldt (Eds.). pp. 239-288

Desu. (2009). *Know Your Meme*. Retrieved from http://knowyourmeme.com/memes/desu

Dominguez, R. (2009). Electronic civil disobedience: Inventing the future of online agitprop theater. *Proceedings of the Modern Language Association of America: Theories and Methodologies*, *124*(5), pp. 1806-1812.

DJNZ/electrohippies, (2000, February) Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act? *Electrohippies Occasional Paper*. Retrieved from www.fraw.org.uk/projects/electrohippies/archive/op-01/html

Douglas, W. (1951) *Dennis v. United States*. 341 US. 494,584.

Dusty the cat. (2011). *Know Your Meme*. Retrieved from http://knowyourmeme.com/memes/events/kenny-glenn-case-dusty-the-cat

Eddy, W. (2007). *RFC 4987: TCP SYN flooding attacks and common mitigations*. Retrieved from https://tools.ietf.org/html/rfc4987

Electrohippies collective (2000, December). Cyberlaw UK: Civil rights and protest on the Internet. Retrieved from http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf

Erlich, B. (2010, December 9). Operation Payback targets Amazon.com. *Mashable.com*. Retrieved from http://mashable.com/2010/12/09/operation-payback-amazo/

Fahimian, G. (2004). How the IP guerrillas won. *Stanford Technology Law Review*. Retrieved from http://www.rtmark.com/more/articles/howtheguerrillaswon.doc

Fiss, O. (1996) *The Irony of Free Speech*. Cambridge, MA: Harvard University Press

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

Frauenfelder, M. (2010, December 8). The push-button tool being used to shutdown Visa, MasterCard, and other sites. *BoingBoing.com.* Retrieved from http://boingboing. net/2010/12/08/the-push-button-tool.html

GameProsProductions. (2010). *How to use LOIC (Low Orbit Ion Cannon).* Retrieved from https://www.youtube.com/watch?v=sQRu-J3f_Kw

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

Gladwell, Malcolm (2010, October 4) Small Change: Why the Revolution Will Not Be Tweeted. *The New Yorker.*

Goodin, D. (2008, October 17) US teen admits to 'Anonymous' DDOS attack on Scientology. *The Register.* Retrieved from http://www.theregister.co.uk/2008/10/17/scientology_ddos_guilty_plea/

Goldstein, E. (2010, December 10). Press release: 2600 Magazine condemns denial of service attacks [Press release]. Retrieved from http://www.2600.com/news/view/article/12037

Gor, F. (1997, September 14). Internet y ETA. *El Pais.* Retrieved from http://elpais.com/diario/1997/09/14/opinion/874188011_850215.html

Graeber, David. (2007) On the Phenomenology of Giant Puppets: broken windows, imaginary jars of urine, and the cosmological role of the police in American culture. Retrieved from http://www.libcom.org/files/puppets.pdf

Grether, R. (2000) How the eToy campaign was won. *Leonardo.* 33(4) pp. 321-324

Harmon, A. (1999, October 31) Hacktivists of All Persuasions Take Their Struggle to the Web. *New York Times.*

Havonsmacker. (2010). *loiq.* Retrieved from http://sourceforge.net/projects/loiq/

Higher Regional Court Says Online Demonstration is Not Force (2006, June 2) Retrieved from http://post.thing.net/node/1370

Hope, C. (2011, October 24). WikiLeaks' money woes brings end to leak of secrets. *Daily Telegraph.* Retrieved from http://www.telegraph.co.uk/news/worldnews/wikileaks/8845294/WikiLeaks-money-woes-brings-end-to-leak-of-secrets.html

Hopkins, C. (2013, February 28) Anonymous to show up in person for 'PayPal 14' trial. *The Daily Dot.* Retrieved from http://www.dailydot.com/news/anonymous-rally-paypal-14-court-trial/

Institute for Global Communications. (1997). *Statement on the suspension of the Euskal Herria Journal website*. Retrieved from http://www.elmundo.es/navegante/97/julio/18/igc-ehj-en.html (Originally published at http://www.igc.org/ehj/)

Jessi Slaughter. (2010). *Know Your Meme*. Retrieved from http://knowyourmeme.com/memes/jessi-slaughter

Johnson, J. (2010, December 8). What is LOIC? *Gizmodo.com*. Retrieved from http://gizmodo.com/5709630/what-is-loic

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwar: Rebels with a cause*. New York, NY: Routledge.

Jurgenson, N. (2011, February 24). Digital Dualism versus Augmented Reality. *Cyborology*. Retrieved from http://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/

Kettmann, S. (1999, December 17) 'Be Grateful for Etoy.' *WIRED*

Koerner, B. (2000, July 20). To heck with hacktivism. *Salon.com*. Retrieved from http://www.salon.com/2000/07/20/hacktivism

Landers, C. (2008, April 2). Serious business: Anonymous takes on Scientology (and doesn't afraid of anything). *Baltimore City Paper*. Retrieved from http://www2.citypaper.com/arts/story.asp?id=15543

Lasker, J. (2002, May 14) Hackers Use Computer Skills to Promote Politically Motivated Mischief, Mayhem. *Buffalo News*

Leiby, R. (1999, December 10) Etoys vs Etoy: A Clash of Commerce and Art. *Washington Post*

Leyden, J. (2010, May 25) Second man jailed over Scientology DDOS attacks. *The Register*. Retrieved from http://www.theregister.co.uk/2010/05/25/second_scientology_ddoser_jailed/

Ludovico, A. (n.d.) "Error loading..." Ten years ago, the first netstrikes took place. Retrieved from http://www.springerin.at/dyn/heft_text.php?textid=1590&lang=en%5D

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

McAdam, D. (1989) The Biographical Consequences of Activism. *American Sociological Review*. 54(5) pp. 744-760

McKenzi, J. (2001) Towards a Sociopoetics of Interface Design. *Strategies*. 14(1)

McPhail, C., Schweingruber, D., McCarthy, J. (1998) Policing Protest in the United States: 1960-1995. In D. della Porta & H. Reiter (Eds.) *Policing Protest* (pp 49-69) Minneapolis, MN: University of Minnesota Press

Munroe, R. (2011, August 1). CIA. *XKCD*. Retrieved from http://xkcd.com/932/ NewEraCracker. (n.d.). *LOIC*. Retrieved from https://github.com/NewEraCracker/LOIC

Nicol, C. (n.d.). Internet censorship case study: *Euskal Herria Journal*. Melville, South Africa: Association for Progressive Communications. Retrieved from http://europe.rights.apc.org/ cases/ehj.html

Norton, Q. (2011a). Anonymous 101: An introduction to the lulz. *Wired*. Retrieved from http://www.wired.com/threatlevel/2011/11/anonymous-101

Norton, Q. (2011b). Anonymous 101 part deux: Morals triumph over lulz. *Wired*. Retrieved from http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux/all/1

Olson, P. (2012). *We are Anonymous*. New York, NY: Little, Brown.

Operation Payback setup guide. (n.d.). Retrieved from http://pastehtml.com/view/1c8i33u.html

Pelofsky, J. (2010, December 2). Amazon stops hosting WikiLeaks website. *Reuters*. Retrieved from http://www.reuters.com/article/2010/12/02/us-wikileaks-amazon-idUS-TRE6B05EK20101202

Pfaffenberger, B. (1992) Technological Dramas. *Science, Technology, & Human Values*, 17(3), 282-312.

Phillips, W. (in press). The house that fox built: Anonymous, spectacle and cycles of amplification. *Television and New Media*.

Poulsen, K. (2011). In Anonymous raids, feds work from list of top 1,000 protesters. *Wired*. Retrieved from http://www.wired.com/threatlevel/2011/07/op_payback/

Raley, R. (2009) *Tactical Media*. Minneapolis, MN: University of Minnesota Press

Regan, T. (1999, July 1) When terrorists turn to the Internet. *Christian Science Monitor*

Rolfe, B. (2005). Building an electronic repertoire of contention. *Social Movement Studies*, 4(1), 65-74.

Rubin, J. (1969) Yippie Manifesto. *Free Pamphlet Series #1*. Vineyard Haven, MA: Evergreen Review, Inc.

Ruffin, O. (2000, July 17) Hactivismo. *Cult of the Dead Cow Blog*. Retrieved from http://w3.cultdeadcow.com/cms/2000/07/hacktivismo.html

Ruffin, O. (2004, March). *cDc, show and prove*. Paper presented at the Yale Law School Cybercrime and Digital Law Enforcement Conference, New Haven, CT. Retrieved from http://www.cultdeadcow.com/cDc_files/cDc-0384.html

Ruffin, O. (2013, April 26) Old School Hacker Oxblood Ruffin Discusses Anonymous and the Future of Hacktavism. *Radio Free Europe/Radio Liberty*. Retrieved from http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html

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

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

Shelby, T. (2012) Impure Dissent: Hip Hop and the Political Ethics of Marginalized Black Urban Youth. Unpublished manuscript, Harvard University, Cambridge, MA

Shoop da whoop. (2009). *Know Your Meme*. Retrieved from http://knowyourmeme.com/memes/shoop-da-whoop-i%E2%80%99m-a%E2%80%99-firin%E2%80%99-mah-lazer

Tarrow, S. (2005) *The New Transnational Activism*. Cambridge, UK: Cambridge University Press.

Thoreau, H. D. (1849) Resistance to Civil Government (Civil Disobedience). *The Thoreau Reader.* Retrieved from http://thoreau.eserver.org/civil.html

Thomas, J. L. C. (2001, January 12) Ethics of Hacktivism. SANS Institute. Retrieved from http://www.aribo.eu/wp-content/uploads/2010/12/Thomas_2001-copy.pdf

Thompson, A. K. (2010) *Black Bloc, White Riot: Antiglobalization and the Genealogy of Dissent.* Oakland, CA: AK Press

Tsotsis, A. (2009, February 4). My date with Anonymous: A rare interview with the elusive Internet troublemakers. *LA Weekly*. Retrieved from http://www.laweekly.com/2009-02- 05/columns/my-date-with-anonymous-a-rare-interview-with-the-illusive-internet-trouble-makers

Van Slambrouck, P. (1999, June 18) Newest tool for social protest: the Internet. *Christian Science Monitor*

Vichot, R. (2009). *"Doing it for the lulz?": Online communities of practice and offline tactical media* (Master's thesis). Georgia Institute of Technology, Atlanta. Retrieved from http://hdl.handle.net/1853/28098

Wark, M. (2006). Toywars: Conceptual art meets conceptual business. *M/C:A Journal of Media and Culture*, *6*(3). Retrieved from http://journal.media-culture.org.au/0306/02-toywars.php

Warren, C. (2010, December 9). How Operation Payback executes its attacks. *Mashable. com*. Retrieved from http://mashable.com/2010/12/09/how-operation-payback-executes-its-attacks/

Williams, C. (2013, January 24) Anonymous hacker 'Nerdo' jailed for 18 months over attacks in support of Wikileaks. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/internet-security/9825089/Anonymous-hacker-Nerdo-jailed-for-18-months-over-attacks-in-support-of-Wikileaks.html

Wray, S. (1998). Electronic civil disobedience and the World Wide Web of hacktivism: A mapping of extraparliamentarian direct action net politics. *Switch*, *4*(2). Retrieved from http://switch.sjsu.edu/web/v4n2/stefan/

Zetter, K. (2011). Feds arrest 14 "Anonymous" suspects over PayPal attack, raid dozens more. *Wired*. Retrieved from http://www.wired.com/threatlevel/2011/07/paypal-hack-arrests/

Zick, T. (2009) *Speech Out of Doors: Preserving First Amendment Liberties in Public Places.* Cambridge, UK: Cambridge University Press

Zuckerman, E., Roberts, H., McGrady, R., York, J., & Palfrey, J. G., Jr. (2010). *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.