FOREWORD BY ETHAN ZUCKERMAN

A university is a fine place to pick a fight.

Don't be fooled by the quiet of stately buildings, the whispering trees. Beneath the buzz of classrooms, the rustle of pages, the hum of the hallways, listen and you'll hear the underlying music of the university: the sound of argument. If the goal of academic life is knowledge, argument is the best documented path to that goal.

(And if the goal is something other than knowledge—perhaps status, security, or employment in perpetuity—these are fine topics for sparking arguments as well.)

A week into her career at MIT—3 months into mine—Molly Sauter came into my office and picked a fight. Specifically, she picked a fight with me on an issue I thought I knew inside and out: the ethical standing of a form of online protest, the denial of service attack.

I had recently finished an extended report on distributed denial of service attacks (DDoS), where multiple computers flood an internet server with traffic in order to silence it, and I felt pretty confident about my position that DDoS was A Bad Thing. My research demonstrated that these attacks, once mounted by online extortionists as a form of digital protection racket, were increasingly being mounted by governments as a way of silencing critics. They were an especially insidious form of government censorship, particularly offensive in that they were difficult to attribute to any agency and easy to deny, allowing governments to silence speech while avoiding accusations of censorship.

DDoS attacks also violate one of the best-known maxims of freedom of speech. As Justice Louis Brandeis wrote in his concurrence on Whitney v California (1927):

> To courageous, self-reliant men, with confidence in the power of free and fearless reasoning applied through the processes of popular government, no danger flowing from speech can be deemed clear and present unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion. If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.

Or, as it's more pithily remembered, "The remedy for bad speech is more speech." The enforced silence of the DDoS attack doesn't permit us to uncover falsehoods and fallacies, which should make us suspicious that these are techniques favored by those afraid of defending their ideas in an open argument.

Over the 2 years Molly and I have worked together, she has persuaded me to consider online protest, and denial of service in particular, in a different light. While Molly acknowledges the many ways in which denial of service attacks are "impure dissent," less ethically neat in practice than they are often presented in analogies, they are, according to her, a response to a key shortcoming of the contemporary internet, the absence of public space.

Yochai Benkler and others hope that the internet will emerge as a digital public sphere, inviting arguments that are more diverse, multifaceted, and participatory than the two-sided, partisan conversations so common in the broadcast age. But the danger of the digital public sphere is not exclusion but invisibility. As Herbert Simon observed, a surplus of information leads to a surfeit of attention; in a digital public sphere, anyone can speak, but not everyone can be heard.

The most pressing threat to online speech may be the one Jerome Barron warned of in 1967. Without a right to be

heard—which Barron characterizes, consistent with the media of the time, as a right of access to the press—First Amendment protections of the right to free speech may be ineffective. Protecting a right to protest where protesters are guaranteed not to be heard (now common in the Orwellian "free speech zones" erected at American political conventions) does little to enable the public political debate necessary for an open society.

In physical space, activists demand an audience by occupying public, or quasi-public space. The Civil Rights Movement boycotted buses and occupied lunch counters to demand equality of access to these places. One of Molly's key contributions in this book is the exploration of the idea that there is no public space on our contemporary internet, only complex, nested chains of private spaces. We might protest corporate malfeasance in the physical world by demonstrating on the public sidewalk outside the respective corporation's headquarters. But there are no sidewalks in online spaces, and the online alternative of creating a protest website that no one will see is an insufficient remedy. Problematic as it is, occupying a corporation's website is a way to ensure that dissent finds a relevant audience.

Ultimately, Molly's argument isn't about the technicalities of online protest technologies, though this book is an excellent introduction to that complex and fascinating space. The reason her book is critical reading even for those whose main focus is not the internet is that the questions she tackles are core to understanding the future of argument and debate. While the dangers of polarization to political discourse in America are starting to become apparent, the deeper worry is that we are moving toward a surfeit of spaces where people can express their opinions and the near absence of spaces where we are forced to encounter voices we do not choose to hear. Molly's book is less a defense of those who silence online speech than it is a plea to consider the consequences of engineering a space where protest is near invisible and impactful dissent near impossible.

We value civic arguments, whether they unfold in the halls of government, a protest encampment, or the comments thread of an internet post, because we believe in the power of deliberation. We elect representatives rather than vote directly on legislation because we hope, perhaps in vain, that the debates our legislators engage in will help us craft solutions more nuanced and balanced than they might propose in isolation. And if these arguments don't lead to finding common ground with our rivals, at least they can sharpen our positions, revealing what's weak about our own stances and positions.

The best arguments aren't the ones that lead to a compromise or resolution. They are the ones that transform those involved. I am a better scholar and a better person after 2 years of sparring intellectually with Molly, less certain that my positions are the right ones, but more sure of which priorities and beliefs are core. Molly Sauter wants to pick a fight with you, and you should be grateful for the opportunity.

Introduction: Searching for the digital street

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.[1] The US government was furious. In the days that followed, different organizations and corporations began distancing themselves from Wikileaks. Amazon WebServices declined to continue hosting Wikileaks' website, and on December 1, removed its content from its servers.[2] The next day, the public could no longer reach the Wikileaks website at wikileaks.org; Wikileaks' Domain Name System (DNS) provider,[i] EveryDNS, had dropped the site from its entries on December 2, 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.[3]

AQ: Please note the edit made to "Wikileaks's" as per house style, here and in other instances.

[i]DNS 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 (such as www.wikileaks.org) into numerical IP addresses (such as 108.162.233.13). Without a DNS provider, such translations would not occur, and a website would only be accessible via the numerical IP address.

Wikileaks' troubles attracted the attention of Anonymous, a loose group of internet denizens, and in particular, a small subgroup known as AnonOps, who had been engaged in a retaliatory distributed denial of service (DDoS) campaign called Operation Payback, targeting the Motion Picture Association of America and other pro-copyright, antipiracy groups since September 2010.[4] 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 4 days, Anonymous and AnonOps would launch DDoS actions 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.[5]

For many in the media and public at large, Anonymous' 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. As will be discussed in Chapter 3, this coverage was inconsistent in its characterization but was open to the idea that these actions could be legitimately political in nature. 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

AQ: Please note the edit made to "Anonymous's" as per house style, here and in other instances.

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 political 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, freedom of expression, and civil disobedience. Early practitioners of DDoS 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 cities today, such as Zucotti Park, the home of the original Occupy Wall Street encampment.[6] In this frame of privatization, disruptive activism is forced 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 all-encompassing 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 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 accidents of evolution and 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 activist actions such as DDoS actions are condemned for being an unreasonable violation of others' rights, they are also derided as being too easy. This "slacktivist" critique posits that most tools of digital activism, from disruptive tactics such as DDoS actions to changing your Facebook profile picture to proclaim your support of a cause, are lazy, simplistic modes of engagement that 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][7]

Oxblood Ruffin, one of the founding members of the influential hacktivist organization Cult of the Dead Cow, made a similar critique of Anonymous' 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.[8]

Evegeny Morozov has similarly called internet-based activism "the ideal type of activism for a lazy generation," explicitly contrasting these actions to sit-ins and other iconic protest actions in past that involved "the risk of arrest, police brutality, or torture."[9]

These critiques make 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.[ii] 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 "slacktivist" 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 (i.e., online activism) that has not been around long enough to either adapt the existing body of 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 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 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

[ii]This mode of critique will be addressed more specifically in Chapter 1.

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 multipurpose 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, and 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 toward an interpretation of violence and harm, I do not use the term "DDoS attacks" throughout this book, but rather refer to all uses of DDoS as "DDoS actions."

Today's DDoS actions are part of a history of denial of service (DoS) actions. Actions such as strikes, work slowdowns, blockades, occupations, and sit-ins all serve as ideological and theoretical antecedents to the digitally based DDoS action. Activist DDoS actions have undergone basic shifts in practice, purpose, and philosophy over the last two decades. Beginning as an exercise by experienced activists looking to stake out the internet as a new zone of action, 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 book will situate DDoS actions within the spheres of both online and off-line activism, addressing its development over the last two decades, and the particular aspects and challenges that separate it from similar types of disruptive activism in the physical world. Through this analysis, I address the broader issue of civil disobedience and the practice of disruptive activism in the online space. The internet is a vibrant 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 aid in the practice of civil disobedience on the internet, its perception as a valid form of contemporary political activism, and of the online space as an appropriate zone for disruptive political speech and action.

I begin with two brief notes, which will explain some of the technical and legal aspects of DDoS actions.

Chapter 1 positions DDoS actions within the theory and history of civil disobedience particularly as it is practiced in Western democracies. Here I argue that DDoS actions fits within the legal and theoretical framework that supports the "moral rights" understanding of modern civil disobedience and disruptive activism, and that critiques of disruptive activist practice, which base themselves in historical comparisons to the Civil Rights Movement and other iconic moments in activist history, are inappropriate and ultimately discourage innovation in political activism.

Chapter 2 examines several activist DDoS actions that fit into the category of *direct action*. These are those actions that seek to disrupt a specific process or event first and secondarily to trigger a cascade of responses on technological, political, media, and social levels. Direct action DDoSes give us an opportunity to examine issues of place in digital activism, and to address criticisms that compare DDoS actions to censorship.

Chapter 3 looks at how activist DDoS actions are covered by the media and how some groups have used these actions to explicitly funnel media attention to a particular cause. The chapter discusses different strategies groups have used to deal with the media and how successful these have been. This chapter also addresses some criticisms specifically directed at media-oriented DDoS actions, including the Critical Art Ensemble's (CAE) principal critique that such acts of "symbolic protest" were, in the online space, fundamentally ineffectual.

Chapter 4 looks closely at how activist DDoS actions contribute to the identity construction of individual activists within the collective action and the surrounding culture. Here I use Doug McAdam's concept of *biographical impact* to analyze how participating in an internet-based collective action like a DDoS could foster the development of a political activist identity.

Chapter 5 follows the previous chapter to discuss issues of identity, anonymity, and responsibility within a DDoS action. This is an attempt to bring to the fore the tensions of identity, responsibility, performance, and exclusion that sit at the core of the political use of DDoS actions. The anonymity that can be part of a DDoS action has become a particularly contentious issue among critics of DDoS actions. 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. These tensions exist within the use of the tactic itself and in the tactic's interplay with the political processes of a discursive democracy in general.

Chapter 6 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 these tools 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 political "seriousness" of the action. This chapter looks at the design and development of the Electronic Disturbance Theater's (EDT) FloodNet tool, and two versions of Anonymous' Low Orbit Ion Cannon (LOIC) tool, paying particular attention to the changing functionality and interfaces of the tools.

Chapter 7 is an attempt to place the responses of corporate and state entities to activist DDoS actions in context within several trends in the regulation and governance of the online space. Here I examine how states and corporations, which are usually the targets of these activist actions, respond to DDoS actions, and the implications those responses have for free speech and emergent cyberwar policy. The result is a legal, cultural, and technical environment that chills the development of innovative technological outlets for political action and speech.

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 DoS, action. When it comes from multiple sources, it is called a 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.[10] An e-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.[11]

As mentioned earlier, 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.[12] Sometimes these are voluntary botnets, where users have volunteered their computing power by downloading and running a program. It is important to distinguish between actions carried out with botnets comprised of compromised machines, voluntary botnets, and individuals operating autonomous machines. The use of nonvolunteer botnets has a significant effect 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 IP addresses, turning simple blocking into an endless game of Whac-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, such as internet service providers (ISPs).

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 US Code.[iii] The crime described by the statute is the "intentional . . . damage" of "protected computers," which are broadly defined as

---

[iii]This section, known colloquially as the CFAA (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 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."

computers used, in whole or in part, by financial institutions or the US 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 test 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.[iv]

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 effect is the same. This makes the stipulations that crimes under the CFAA be "intentional" an important one.

Similarly, identical actions that intend to knock a site off- line 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

---

[iv] As noted by havonsmacker (2010) at the "loiq" DDoS tool download page:

> LOIQ stands for LOIC 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 analogy in the sale of glass pipes in head shops "for use with tobacco only." This is seldom their ultimate use case. (Thanks to Ethan Zuckerman for pointing out this parallel.)

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)[13] in an effort to force it to stop hosting a Basque web publication, *Euskal Herria Journal*.[14] IGC's servers were knocked off-line, rendering inaccessible the websites and e-mail of more than 13,000 subscribers. Although 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.[15] 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 off-line 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[16] 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" (ECD) or

valid online protest.[17] The US 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.[18] 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.

Notes

1 Julian Borger, and David Leigh, "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*, November 28, 2010. Last accessed March 3, 2014, http://www.guardian.co.uk/world/2010/nov/28/siprnet-america-stores-secret-cables.

2 Jeremy Pelofsky, "Amazon stops hosting WikiLeaks website," *Reuters*, December 2, 2010. Last accessed March 3, 2014, http://www.reuters.com/article/2010/12/02/us-wikileaks-amazon-idUS-TRE6B05EK20101202.

3 Christopher Hope, "WikiLeaks' money woes brings end to leak of secrets," *Daily Telegraph*, October 24, 2011. Last accessed March 3, 2014, http://www.telegraph.co.uk/news/worldnews/

wikileaks/8845294/WikiLeaks-money-woes-brings-end-to-leak-of-secrets.html.

4 Nate Anderson, "Operation Payback attacks to go on until we 'stop being angry,'" *Ars Technica*, September 30, 2010. Last accessed February 27, 2014, http://arstechnica.com/tech-policy/news/2010/09/operation-payback-attacks-continue-until-we-stop-being-angry.ars.

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

6 Lisa Foderaro, "Privately Owned Park, Open to the Public, May Make Its Own Rules," *New York Times*, October 13, 2011.

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

8 Oxblood Ruffin, "Old School Hacker Oxblood Ruffin Discusses Anonymous and the Future of Hacktavism," *Radio Free Europe/Radio Liberty*, April 26, 2013. Last accessed March 3, 2014, http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html.

9 Evgeny Morozov, "Foreign Policy: Brave New World of Slacktivism," *NPR*, May 19, 2009. Last accessed March 3, 2014, http://www.npr.org/templates/story/story.php?storyId104302141.

10 W. Eddy, "RFC 4987: TCP SYN flooding attacks and common mitigations," August 2007. Last accessed March 3, 2014, https://tools.ietf.org/html/rfc4987.

11 Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey, *2010 Report on Distributed Denial of Service (DDoS) Attacks* (Berkman Center for Internet and Society Research Publication No. 2010–16) (Cambridge, MA: Berkman Center for Internet and Society, 2010).

12 Zuckerman, et al., *2010 Report on DDoS Attacks*.

13 Institute for Global Communications, "Statement on the suspension of the Euskal Herria Journal website." July 18, 1997. Last accessed February 25, 2014. Originally published at http://www.igc.org/ehj/. Retrieved from http://www.elmundo.es/navegante/97/julio/18/igc-ehj-en.html.

14 Chris Nicol, "Internet censorship case study: *Euskal Herria Journal*," Melville, South Africa: Association for Progressive Communications. Last accessed February 25, 2014. Retrieved from http://europe.rights.apc.org/cases/ehj.html.

15 Institute for Global Communications, "Statement on the suspension of the Euskal Herria Journal website." July 18, 1997. Last accessed February 25, 2014. Originally published at http://www.igc.org/ehj/. Retrieved from http://www.elmundo.es/navegante/97/julio/18/igc-ehj-en.html.

16 Randall Munroe, "CIA," *XKCD*, August 1, 2011. Last accessed February 25, 2014. Retrieved from http://xkcd.com/932/.

17 Caroline Auty, "Political hacktivism: Tool of the underdog or scourge of cyberspace?" *ASLIB Proceedings: New Information Perspectives*, 56 (2004): 212–21; Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Brooklyn, NY: Autonomedia, 1996), 10–11.

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