American Behavioral Scientist
http://abs.sagepub.com/

"LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks

Molly Sauter

American Behavioral Scientist published online 15 March 2013
DOI: 10.1177/0002764213479370

The online version of this article can be found at:
http://abs.sagepub.com/content/early/2013/03/15/0002764213479370

Published by:
SAGE
http://www.sagepublications.com

Additional services and information for *American Behavioral Scientist* can be found at:

Email Alerts: http://abs.sagepub.com/cgi/alerts

Subscriptions: http://abs.sagepub.com/subscriptions

Reprints: http://www.sagepub.com/journalsReprints.nav

Permissions: http://www.sagepub.com/journalsPermissions.nav

>> OnlineFirst Version of Record - Mar 15, 2013

What is This?

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

American Behavioral Scientist
XX(X) 1–25
© 2013 SAGE Publications
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/0002764213479370
abs.sagepub.com
SAGE

"LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks

Molly Sauter[1]

Abstract

This article explores the role of tool design and media coverage in the relative success of Operation Payback and earlier activist distributed denial-of-service (DDOS) actions. Through a close reading of changes in the tool's interface and functionality across several iterations, the article considers the evolution of the Low Orbit Ion Cannon (LOIC) DDOS tool, from one that appealed to a small, inwardly focused community to one that engaged with a larger population. The article further considers Anonymous's contribution to the reframing of DDOS actions from a tool of direct action to a tool of media manipulation and identity construction as well as the news media's role in encouraging individuals to participate in the Operation Payback actions.

Keywords

social movements, Internet, hackers, Anonymous, hacktivism

On November 28, 2010, WikiLeaks and its five partner news organizations began releasing documents from a leaked cache of 251,287 unclassified, classified, and secret U.S. diplomatic cables, copied from the closed Department of Defense network SIPRnet (Borger & Leigh, 2010). In the following days, various organizations and corporations took concrete steps to distance themselves from WikiLeaks: Amazon WebServices refused to continue to provide hosting to WikiLeaks and removed its

[1]Massachusetts Institute of Technology, Cambridge, MA, USA

Corresponding Author:
Molly Sauter, 121 North Sugan Road, New Hope, PA, 18938.
Email: molly.sauter@gmail.com

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

content from its servers on December 1 (Pelofsky, 2010); on December 2, EveryDNS declared that it could no longer provide Domain Name System (DNS) services to the site, as it was suffering massive distributed denial-of-service DDOS attacks from anti-WikiLeaks parties, and dropped the website from its entries (Pelofsky, 2010).[1] Financial services companies, such as PayPal, PostFinance, MasterCard, Visa, and Bank of America, stopped processing online payments to WikiLeaks, effectively halting the flow of monetary donations to the organization (Hope, 2010).

The travails of WikiLeaks attracted the attention of a loose group of Internet denizens known as Anonymous. Anonymous, a highly fluid collective of Internet users that had its origins in the unmoderated online image board 4chan, had a history of supporting causes of free speech and Internet freedom (Coleman, 2011a). It had been engaged in a retaliatory DDOS campaign known as Operation Payback targeting the Motion Picture Association of America (MPAA) and other pro-copyright, anti-piracy groups since September 2010 (Anderson, 2010). The collective's members, known as Anons, were happy to extend Operation Payback's range of targets to include the forces arrayed against WikiLeaks and its public face, Julian Assange, as well. On December 6, they launched their first DDOS attack against the website of the Swiss banking service PostFinance. During the course of the next 4 days, Anonymous would launch DDOS attacks against the websites of the Swedish Prosecution Authority, EveryDNS, senator Joseph Lieberman, MasterCard, two Swedish politicians, Visa, PayPal, Amazon.com, and others, forcing many of the sites to experience at least some amount of downtime (Correll, 2010).

The actions taken by Anonymous should be understood not as unique events but as an evolution in digital activist tactics, particularly in the realms of media manipulation, recruitment, and participant impact. In this article, I argue that Anonymous, in Operation Payback, has expanded on the DDOS tactics used by earlier groups in the 1990s. Whereas earlier actions by groups such as the Electronic Disturbance Theater (EDT) typically consisted of an activist core organizing a relatively small population of other media activists, artists, and special interest groups, Anonymous pushed a horizontal structure that opened the tools and mechanisms of protest organizing and action to the population of the Internet at large. In looking at how the design of DDOS tools can affect the participant population and the levels of diversity within that population, I consider how the design and development cycle of these tools reflect changes in protest strategy and in the activist space at the time they were created. These factors, particularly, a close analysis of the lexical tropes and memes present in the tool interface, can help to locate the tool both in time and in context with its developer and intended user population. Through a close reading of changes in the tool's interface and functionality across several iterations, the article considers the evolution of the Low Orbit Ion Cannon (LOIC) DDOS tool, from one that appealed to a small, inwardly focused community to one that engaged with a larger population. Furthermore, I argue that it is these changes in tool design, along with specific aspects of the news media coverage, that strongly contributed to the large numbers of participants active in Operation Payback. I also argue that Anonymous's use of DDOS as an activist tactic further pushed the reframing of DDOS actions initiated by the EDT from a tool of

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

direct action to a tool of media manipulation and identity construction—from an *action*-oriented tactic to an *attention*-oriented tactic.

In the following section, I provide a brief technical note, explaining how DDOS attacks are waged and defended against and some general factors to consider in their analysis. Next, I place Anonymous in context in the overall history of "hacktivism" as a social movement strategy. After that, I place Operation Payback in the history of Anonymous as a community. Next, I examine the EDT's DDOS tool, Floodnet, and two versions of the Anonymous DDOS tool, LOIC. Then, I examine the role of the media in publicizing and popularizing the Anonymous DDOS attacks. Finally, I offer my conclusions.

DDOS Attacks: A Technical Note

At its most basic level, a denial-of-service attack seeks to render a server unusable to anyone looking to communicate with it for legitimate purposes. When this attack comes from one source, it is called a denial-of-service, or DOS, attack. When it comes from multiple sources, it is called a *distributed* denial-of-service, or DDOS, attack. Complex or sophisticated tools are not necessary to launch a DDOS attack. A group of people reloading the same website again and again at the same time could constitute a manual DDOS attack 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 attacking machines. A ping is a request for availability, one computer asking another, "Are you there?" However, when employed as part of a DDOS attack, 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 attack: "downtime" on the targeted server.

A DDOS attack 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 attack. Other, far less labor-intensive ways of waging such an attack 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 attacks carried out with botnets comprising compromised machines, voluntary botnets, and individuals operating

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

autonomous machines. Although the use of nonvolunteer botnets has a significant effect on the perceived ethical and political validity of an activist DDOS action, a detailed dissection of those implications is beyond the scope of this article.

To defend against a DDOS attack 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 an attacker to spoof an endless series of IP addresses, turning simple blocking into an endless game of Whac-A-Mole. If the attack is distributed across a sufficiently large number of machines, the number of attack packets sent by each machine need not be particularly large, making it difficult to tell legitimate traffic from illegitimate. One could acquire the servers, processing power, and memory necessary to absorb the additional traffic until the attack abates. This avenue is generally available only to large corporations able to absorb its high costs. As a result, smaller sites can sometimes be driven offline completely by a DDOS attack of relatively short duration (Zuckerman et al., 2010).

DDOS attacks are considered illegal in most jurisdictions. In the United States of America, DDOS attacks are prosecuted under Title 18, Section 1030 (a)(5) of the U.S. Code.[2] The crime described by the statute is the "intentional . . . damage" of "protected computers," broadly defined as computers used, in whole or in part, by financial institutions or the U.S. government. However, there was much confusion about the legal status of DDOS attacks in 2010 during Operation Payback on the part of organizers, participants, and the news media.

There are many confluences of computational circumstances that appear identical in form to a DOS or DDOS attack but that are not DDOS attacks. For example, a website operator may use an automated "stress-testing" tool to generate an exceptional amount of traffic pointed at a particular server to see how the machine reacts, essentially launching a DOS attack 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.[3] 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 Computer Fraud and Abuse Act (1984) be "intentional" and that there be the burden to prove that intentionality, as with the establishment of mens rea in cases of criminal culpability, important ones.

Similarly, identical actions that intend to knock a site offline could be undertaken for significantly different motivations. A DDOS attack 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 Internet service provider (ISP) to host the content. Online publications and small ISPs are particularly vulnerable to this type of attack. An example of this occurred in 1997, when a large, popularly supported DDOS campaign was launched against the ISP Institute for Global Communications (IGC) 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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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.

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 attack, 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 that 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. I will be exploring the repercussions of this legal classification later in this article.

The technological simplicity behind a DDOS attack 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 attack also lends itself conceptually to metaphors and comparisons to physical-world activism. Activists have often called DDOS attacks "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. Rather than grasping at metaphors, it is better to understand the activist case of DDOS in its own context. 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.

The Position and Criticism of DDOS in Digital Activism

The Anonymous actions were only the most recent episodes in a history of activists who use DDOS attacks as a protest tactic. Their actions served as step in the tactic's development, particularly in the areas of media manipulation and community building through tool construction and sharing, but their innovations were incremental,

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

building on the established actions of others. In particular, the Anonymous innovations serve as a bridge between two previous conceptions of online activism: those ideas held by net-native hacktivist organizations that privileged skill and the freedom of information versus mass participation and those espoused by activist organizations that saw the Internet as a tool for information dissemination and borderless recruitment and action. To grasp the shape and relevance of these innovations, one must first have an understanding of the history of DDOS use as a tactic and of the broader trend of using the Internet and digital tools in activism overall.

Political action online did not begin with the DDOS. It is important to distinguish between hacktivist groups, such as Cult of the Dead Cow and Hacktivismo, 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, 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 online. Oxblood Ruffin, a prominent member of the Cult of the Dead Cow, wrote in response to an activist DDOS action in 1999, "No rationale, even in the service of the highest ideals, makes [DDOS attacks] 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, as quoted in Koerner, 2000). 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).

As activists who were experienced in traditional forms of civil disobedience in the physical world began to move their actions into the digital realm, they attempted to bring those practices with them. Seeing a parallel, some early practitioners of digital activism adapted the established concept of the sit-in and dubbed their DDOS actions "digital" or "virtual sit-ins" (Rolfe, 2005). In this, they separated themselves from other protest actions that used DDOS as a tool of direct action, such as the IGC/*Euskal Herria Journal* action mentioned earlier or the etoy "toywar," which took place in 1999 (Fahimian, 2004).[4] To groups such as the EDT and the *electrohippies*, the purpose of a DDOS was to draw popular attention to an issue and to generate public debate but also to directly engage with the target in a form of direct action. The DDOS was viewed as an auxiliary political act, a way to "leave one's computer protesting at home and then hit the streets to do the same" (Dominguez, 2009, p. 1810). 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 EDT was particularly conscious of media attention paid to its actions, taking care to distribute press releases to major media outlets and to announce all actions publically beforehand (Dominguez, 2009).

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

However, its bids to attract participants were hampered through its use of limited platforms, such as specialized mailing lists and message boards, for recruitment and the professionalized, occasionally alienating language used throughout its recruitment and press materials and in the FloodNet tool itself. These factors will be examined more closely later in this article.

Compare this to the "media strategy" of other hacktivist groups. 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 firewalls 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).

So the EDT and groups like it, with their ethic of mass participation and public discussion, represent a view of the Internet's place in political protest that is at odds with that of hacktivists. But their goals are not mutually exclusive. Anonymous's media-heavy strategy, including the use of videos and graphical manifestos and announcements released online, aligns it with groups such as the EDT, and its digital-native culture and net-freedom ideology places it on the same ground as hacktivist groups such as the Cult of the Dead Cow.

When attempting to place activist DDOS actions, such as the EDT and Anonymous actions, in what has been termed "the repertoire of electronic contention," I am here following Sasha Costanza-Chock's (2003) characterization of DDOS attacks as "disruptive tactics." However, in this characterization, it is interesting to note that the EDT developed its DDOS campaigns specifically to mimic more conventional street mobilizations. It is the dubious legal status of DDOS and the character of its participants, not any inherent qualities of the tactic, that necessarily render it any more "disruptive" than a march down Main Street. Anons in particular have continually played with societal stereotypes of the hacker and other shadowy online threats to foster a sense of danger around their actions and tactics (Phillips, in press).

The History of DDOS in Anonymous

The precise nature of Anonymous is a difficult thing to pin down. Anonymous has been described as "a group, in the sense that a flock of birds is a group. How do you know they're a group? Because they're traveling in the same direction" (Landers,

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

2008). Others have described Anonymous as a "culture" (Norton, 2011a). Individuals associated with Anonymous have consistently and repeatedly denied that the group has any formal leadership or membership structure (Norton, 2011a). Anons have communicated with each other using a variety of means during the group's history, from message and image boards to throwaway websites and Internet relay chat (IRC) channels to a diverse handful of social media outlets (Norton, 2011a). For most of Anonymous's existence, speaking to outsiders about the group has been strongly discouraged (Tsotsis, 2009). Because of all this, any attempt to chronicle the history of Anonymous will be incomplete and messy. However, the group's evolution from an inward-facing group concerned with its own amusement at the expense of outsiders to an open culture adept at manipulating media attention and attractive to the uninitiated is clear. This shift from insularity to visibility is key context to understanding the evolution of Anonymous use of DDOS.

Prior to the WikiLeaks-related actions of 2010, Anonymous attracted sporadic media attention for the various "raids" it conducted across the Internet. Sometimes these raids were DDOS attacks; 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 in these raids was the aesthetic of "doing it for the lulz," an 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 attacks 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. 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-speech absolutism, moderate levels of anarchy (Coleman, 2011a), and a strongly held belief in the ethical treatment of cats ("Dusty the Cat," 2011).

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 a retaliatory DDOS campaign targeting the MPAA, the Recording Industry

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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).[5] Anonymous viewed the DDOS attacks 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.[6] The Anonymous-led DDOS attacks against the RIAA, MPAA, and Aiplex continued for more than a month. All three targets reported downtime (Anderson, 2010).

The attacks on the Pirate Bay and the websites of the MPAA and the RIAA had strikingly different motivations and actual effects. The 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 attacks 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 attacks on the MPAA and the RIAA was to disrupt their operations and cause the organizations to spend money and resources fending off the attacks (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 is examined below), 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 attacks 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. During the course of 4 days, Anonymous 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, forcing many of the sites to experience at least some amount of downtime (Correll, 2010). These attacks were powered by volunteers using the LOIC DDOS tool and were augmented by nonvolunteer botnets (Coleman, 2012; Olson, 2012).

DDOS Tools: FloodNet and LOIC

Much of the functionality present in LOIC, the DDOS tool used by Anonymous during Operation Chanology and Operation Payback, was present in earlier DDOS tools, such as FloodNet, a tool developed by the EDT in the late 1990s. In this section, I will be tracing the development of the FloodNet and 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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

the LOIC tool, one developed contemporaneously with Operation Chanology and a later version used during Operation Payback.

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.[7] 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 dynamic was replicatedthe core functionality with th during the Operation Payback action as well.

The EDT held several 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 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. 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, 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.

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

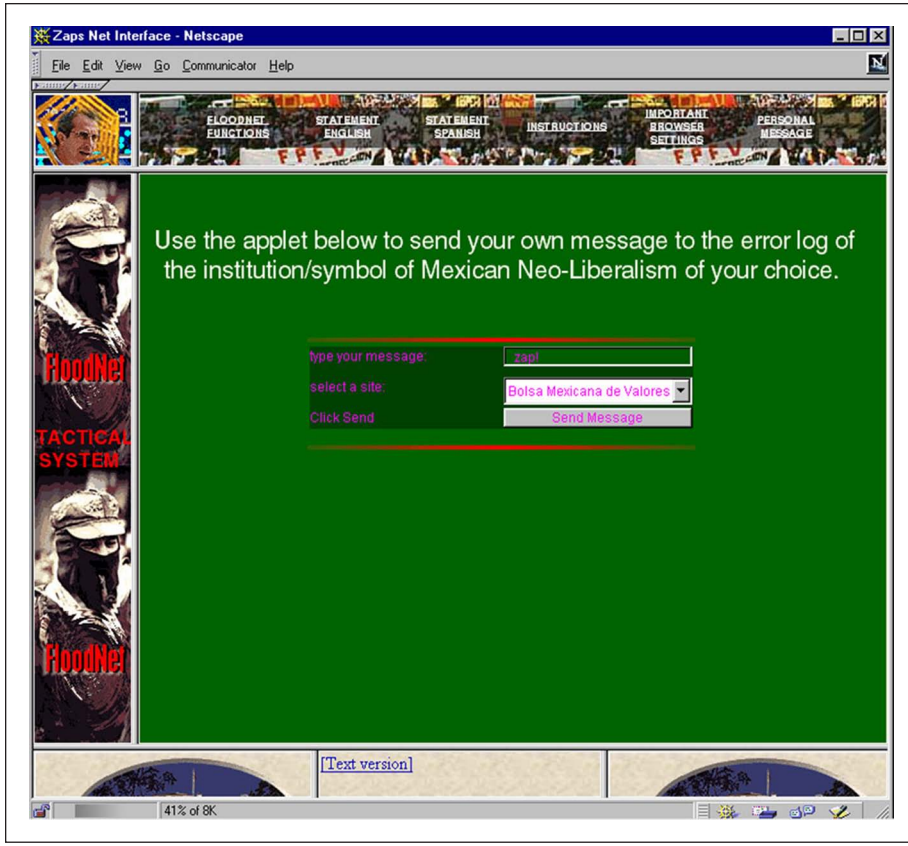

Figure 1. FloodNet screenshot.

The program Anonymous used during its DDOS attack, LOIC, is similar to FloodNet but differs in significant ways. Bu 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.[8] 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 an open-source developer known as praetox (Norton, 2011b) as a server stress-testing 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. For

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

the purposes of this article, I am going to group those projects that are based on praetox's original code and that retain the LOIC name and the core functionality under the name LOIC, although I will be examining some of the forks individually, as they reflect the previously examined shifts in the Anonymous 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.

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 participated in the development of LOIC, making it possible for them 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 mid-2009 (abatishchev, n.d.; see Figure 2). This version of LOIC was downloaded 105,411 times in December of 2010, up from 39,515 times in at the beginning of Operation Payback in September (abatishchev, n.d.). To compare, in August of 2010, this version of LOIC was downloaded 4,701 times (abatishchev, n.d.). Together, the September (when Operation Payback initially began) and December (when the Avenge Assange portion of Operation Payback took place) 2010 downloads make up nearly a quarter of the 468,163 downloads abatishchev's version of LOIC racked up from June of 2009 to October of 20011 (abatishchev, n.d.). 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. 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 (NewEraCracker, n.d.; see Figure 3). From its creation in September 2010 to December 2011, NewEraCracker's version of the tool was downloaded 80,660 times (unfortunately, GitHub does not offer finer-grained statistics than that, at least not publicly) (NewEraCracker, n.d.).

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

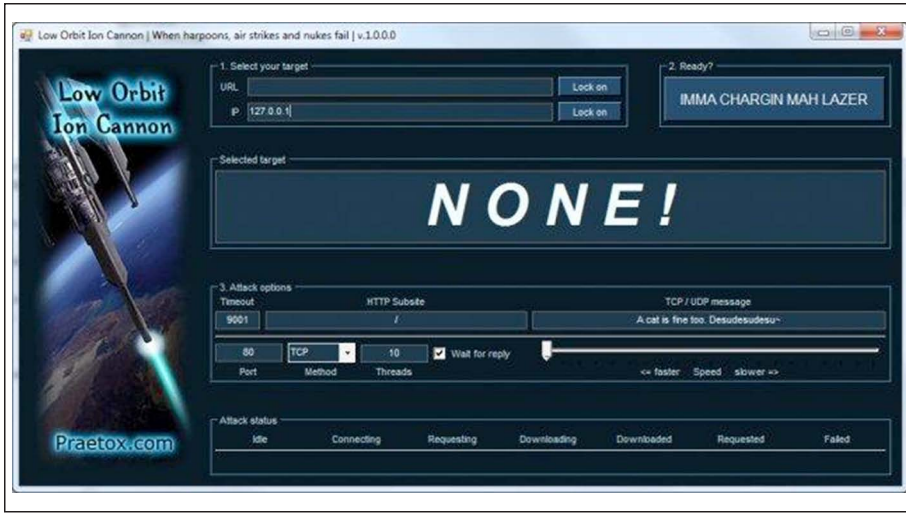

Figure 2. A screenshot of abatishchev's version of LOIC.

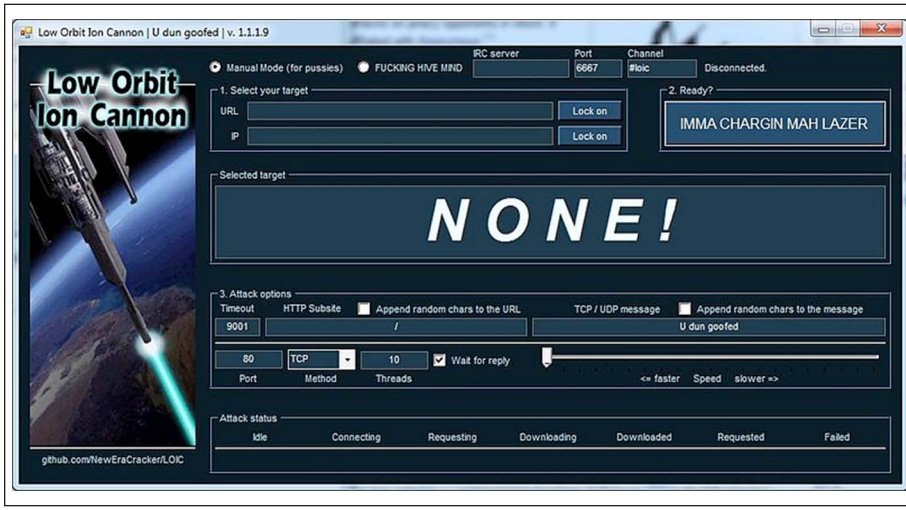

Figure 3. A screenshot of NewEraCracker's version of LOIC.

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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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.[9] These differences can be used to position the different versions of the tool in 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, 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). 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. 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 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.

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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

the original viral video from which the meme sprang, "U dun goofed" is followed shortly by the line "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 waging DDOS attacks, 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. This added functionality also represents a important advancement from FloodNet, which, like abatishchev's LOIC, operated in only one mode, similar to what I have previously identified as "manual." 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 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 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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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.

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 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 by a factor of 1,000 during the action. 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. 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. Even those whose favored mode of participation is turning on Hive Mind and walking away are just as important to the success of the action as those who man their terminals for the duration. 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. It allowed those who had considered themselves to be an audience in the world of politics and industry to become actors, strengthened by the invisible yet palpable presence of thousands of their new comrades-in-arms.

Sources from within Anonymous have claimed that a large percentage of the participants in the Avenge Assange stage of Operation Payback were new participants, people who had not previously been associated with Anonymous or frequented 4chan (Coleman, 2012; Norton, 2011b; Olson, 2012). The profusion of LOIC tutorials in such widely trammeled Internet locales as YouTube seems to support that claim. One such video, titled "How to Use LOIC (Low Orbit Ion Cannon)" has been viewed more than 118,000 times (GameProsProductions, 2010). Certainly, the size of the Operation Payback DDOS attacks during that week in December implies that the number of participants had risen sharply compared to previous DDOS actions. But large numbers of Internet civilians did not simply wake up one day and decide to join up with the one Internet subculture blessed with the worst reputation in town. Rather, I argue that this explosion of individuals willing to associate themselves with Anonymous was, in large part, attributable to the extensive and relatively uncritical media coverage given to the December stage of Operation Payback.

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 attack 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.

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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.

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. Virtually none 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.)

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.

In this article in particular, Johnson mistakenly states that a server targeted by a DDOS attack 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 attacks 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 federal computer crimes statute I referenced at the beginning of this article (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 attacks on December 9th and 10th, 2010 (Poulsen, 2011), something sites such as Gizmodo had previously claimed was impossible.

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

DDOS as a Media Manipulation Tactic

The EDT primarily spread word of its actions via activism, performance art, and issue-centered e-mail lists and message boards (Dominguez, 2009). As a result, their participants were, more often than not, well versed in the practices and risks of on-the-streets activism. Although they may have had an incomplete understanding of the online space they were moving to, it is safe to assume that they had an understanding of the legal risks often associated with acts of civil disobedience. As the EDT was primarily engaged in drawing an explicit linkage between traditional forms of civil disobedience and digital actions, such as DDOS attacks, they were also aware of the illegal nature of the acts they were undertaking and the risks they were exposed to.

The EDT did not pursue participants beyond its core demographic of activists, artists, and issue specialists. Although this meant that its contemporaneous influence was restricted mostly to other net activists, it also meant that its core knowledge base of activist practices and protocols remained relatively undiluted. It was able to carry with it an understanding of the real-world implications of its protest actions even as the locus of those actions moved online.

This was not the case with Anonymous. The culture and population of Anonymous underwent a major shift, beginning with Operation Chanology (Coleman, 2011a). Activism-minded individuals came onto the scene with little to no real awareness of the traditional tactics and motivations of Anonymous, and Anons themselves typically lacked any real activism experience. Their tactics were often innovative and interesting, but they lacked a core awareness of the basic risks of activism. Given time to evolve, Anonymous may have acquired a knowledge base of activist practices organically by attracting individuals with that particular profile. However, the storm of media attention in December 2010 sped up the cycle of change, essentially forcing Anonymous into the risky world of high-profile civil disobedience, perhaps before its members were ready. Anonymous's sudden high profile also raised the stakes for those forces arrayed against it, namely, law enforcement and the targeted corporations, making it more likely that those participating in Anonymous DDOS actions would be pursued by law enforcement.

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 on the ground. There was genuine fear that any organization or individual could be Anonymous's next target, and very few people were willing to hang a target on their back by being publicly critical of them, particularly, journalists and news organizations that did not fully understand the technological weapons being so freely deployed. In many cases, this led to news organizations' embedding Anonymous videos and call-to-action posters directly in news stories, as happened in *The Washington Post* (Bell, 2010) and the social media news site Mashable (Erlich, 2010). The public at large harbors fundamental misunderstandings and assumptions about hacker and Internet culture. Hackers are very often depicted as dangerous, immature, and powerful, capable of ruining an average person's life with a few keystrokes. Coverage of Anonymous

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

reflected those preconceptions, which further romanticized the group. Furthermore, very few journalists possess the deep specialized knowledge of networking technology or computer law to make judgments about the functionality and safety of a tool such as LOIC, and so most often, they simply repeated what Anons had written about the tool, as occurred in the Gizmodo piece quoted earlier. Unfortunately, those Anons also lacked the knowledge and experience to evaluate the tool appropriately.[10]

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.[11] 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? Eventually, Anonymous set up a press channel on one of its IRC servers, where members of the press could chat with Anons, but many members of the press were simply not aware of it or lacked the technological skills to access the channel on their own. The combination of the demands of the 24-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.

The practices of Internet-based news coverage are not settled yet. They are being developed on a daily basis as more news coverage moves to the online medium. Many journalists have adopted practices of deep-linking to primary sources in their news coverage: If your sources are available online, say as a PDF of a scientific report or a video of a press conference, why not link to it? In this case, however, deep-linking within coverage of Anonymous often meant linking to pages where one could download LOIC, join an IRC channel, or find information on scheduled raids, as happened with *Time* magazine (Aamoth, 2010) and the popular blog BoingBoing (Frauenfelder, 2010). The practice provided a sheen of endorsement to the linked materials, for why would a news organization or blog make it so easy to access these materials if it did not believe them worthy of the resultant attention and influence? In the past, news organizations have taken explicitly approving stances toward DDOS actions, as happened in the IGC *Euskal Herria Journal* case cited earlier in this article: Initially, *El Pais* and other Spanish newspapers supported the DDOS attacks against IGC, publishing target e-mail addresses and other information before ultimately withdrawing their support for the action (Gor, 1997). None of what the media outlets cited above published went so far as *El Pais*'s overt endorsement in 1997. However, it is apparent that direct linking is a powerful and not yet fully understood tool of news coverage that affects public actions in ways that must be taken into consideration. Although disputes about the press coverage of protest actions and civil unrest are common, in this case, I want to highlight the impact of both the practice of direct linking to activist tools and materials and the erroneous coverage that made the DDOS actions seem less legally risky than they in fact were.

That direct linking is a type of statement in and of itself is something already tacitly understood in the online community. After all, it is not an unheard-of practice for blogs to write about a website or video that they find offensive or exploitative but to refuse

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

to link to it, thus forcing the reader to take the positive step of Googling for the offending content. It is not that the content would be difficult to find without the link but that that particular blog or news organization refuses to appear to be the endorsing conduit through which that content is received. This practice is supported at the code level with a bit of code called the "no-follow" tag. This tag, when embedded within an HTML link, allows one website to link to another website without affecting that site's Google ranking, as links and especially clicked links will improve that site's ranking in Google's search results. The no-follow tag allows a blog, for instance, to link to a site while at the same time declaring (to Google) that it does not want its actions or the actions of its readers to have any impact on that site's rank (Google Support, n.d.). If the deep-linking that occurred in the majority of Anonymous coverage contained some type of human-readable no-follow tag, perhaps it would have been more difficult to read into such links a tacit endorsement, or at least a conspicuous lack of condemnation, of the materials so linked.

Conclusions

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. In the movement from the EDT to Anonymous, I have shown how the realm of activism has 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 this article, I have considered how the design and development of the tools used in those actions reflect changes in technology and strategy and how they reflect the activist space as it existed at the time they were created. I have argued that the success of Operation Payback in particular was attributable in part to a confluence of technological, community, and news media–related factors. I have considered the arguments for and against the use of DDOS as an activist tactic and the roles played by the media and law enforcement in the development of the political use of DDOS. Finally, I have concluded that a major advancement made by Anonymous in the use of DDOS as an activist tactic lies in the continued reframing of DDOS actions from a tool of direct action to a tool of media manipulation and identity construction.

I would like to return briefly to the hacktivists mentioned earlier in this article. As noted then, many hackers hold low opinions of those groups that use DDOS attacks as an activist tactic. Those same hackers generally hold an even lower opinion of Anonymous. The epithet most commonly used to describe Anonymous is "script kiddies" (Coleman, 2011b). If a hacker is someone who writes code for reasons of intellectual curiosity, a script kiddie is the leech of his or her labor. A script kiddie is one who, for lack of skill and motivation, does not write his or her own code but instead uses only prewritten code, or scripts, to achieve his or her ends. Anonymous use of LOIC during Operation Payback is often cited as proof of script kiddieness and proof of generally how unworthy script kiddies are of using digital tools to make political points (Goldstein, 2010). I would like to emphasize again that Anonymous is not the

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

beginning of the political awakening of the Internet but rather a continuation of it. The skill-heavy, closed, mastery-focused world of the hacktivist need not be read as in conflict with the horizontal, open, attention-oriented world of the EDT and Anonymous. Anonymous did not create DDOS as an activist tactic but rather innovated on the history of experience, skills, and code of activists and hackers who came before. What is being dismissed as script kiddieness should rather be recognized as resourcefulness. To bake an apple pie from scratch, it is really necessary only to invent the universe once (Sagan, 1980)[12]—preferably early on. And it may be better if someone else does it first.

Author's Note

Because of the legal circumstances surrounding distributed denial-of-service attacks, I declined to interview any Anons who may have participated in these actions for this article.

Acknowledgment

I would like to acknowledge the excellent guidance and support I received while working on this article from faculty and colleagues at MIT and elsewhere and from within the activist-hacker community. I would particularly like to acknowledge Ethan Zuckerman, James Paradis, David Thorburn, William Urrichio, Sasha Costanza-Chock, Gabriella Coleman, Jonathan Zittrain, Zeynep Tufekci, J. Nathan Matias, Quinn Norton, Brian Martin, Space Rogue, and the attendees at HOPE Number Nine for their incisive questions.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

Notes

1. The DNS, or the Domain Name System, is the system by which alphanumeric URLs are converted to numerical IP addresses.
2. This section, known as the Computer Fraud and Abuse Act (1984), forbids

   (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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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.

3. 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 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.)
4. However, to complicate the issue, the Electronic Disturbance Theater also participated in the "Twelve Days of Christmas" DDOS campaign associated with the etoy toywar action, which was specifically intended to disrupt the business model of the toy company eToys during the course of a dispute over the URL, etoy.com (Wark, 2006, p. 50).
5. 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.
6. 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.
7. 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.
8. 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.
9. 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 memes serve as markers of community involvement, shibboleths to differentiate those who are part of the community from those who are not.
10. Parmy Olson (2012) tells in chapter 8 of her book *We Are Anonymous* of conflicts that arose within Anonymous Internet relay chat channels about the safety of LOIC during Operation Payback. She states that those individuals who tried to warn others about the dangers inherent in the tool's design were ignored, accused of trying to sabotage the operation, or kicked off the channel.
11. Pastebin.com and similar sites, such as pastie.org, are designed to share plain-text content. Users cut and paste chunks of text onto the site, which assigns their "paste" a unique URL. Originally, these types of sites were created to allow programmers to share code snippets with each other, but their simple, anonymous, and free nature has made them popular among Anons and other hacktivists for posting press releases, manifestos, documents drops, and info dumps.

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

12. Carl Sagan's (1980) original quote is found on page 218 of his book *Cosmos*: "If you wish to make an apple pie from scratch, you must first invent the universe."

References

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/

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

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

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

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

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

Critical Art Ensemble. (1996). *Electronic civil disobedience and other unpopular ideas*. 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://canopycanopycanopy.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.

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), 1806-1812.

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

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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

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

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

Google Support. (n.d.). "rel='nofollow'. Retrieved from https://support.google.com/webmasters/bin/answer.py?hl=en&answer=96569

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

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

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

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.

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

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-idUSTRE6B05EK20101202

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013

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/

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

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

Sagan, C. (1980). *Cosmos*. New York, NY: Random House.

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

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-troublemakers

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/

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/

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 Research.

Author Biography

Molly Sauter is a graduate student in comparative media studies at MIT, a research assistant at the Center for Civic Media at the MIT Media Lab, and a fellow at the Berkman Center for Internet and Society at Harvard. Her research is centered on the cultural and sociopolitical analysis of technology, hacktivism, Internet culture, and technology in the media.

Downloaded from abs.sagepub.com at MASSACHUSETTS INST OF TECH on March 17, 2013