Sauter, Molly. "LOIC will tear us apart: DDoS tool development and design." *The Coming Swarm: DDoS Actions, Hactivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic, 2014. 109–135. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781628926705.0012>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 09:25 UTC.

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

CHAPTER SIX

LOIC will tear us apart: DDoS tool development and design

In activist DDoS actions, the tool used sets the first level of community, literally serving as the collective launch point for the action. Participants will often all use one tool or one of a family of tools recommended by the organizers. Though there have been several different tools used during these actions, some ad hoc, some more polished, the two most notable tools for activist DDoS actions have been the EDT's FloodNet tool, and Anonymous' LOIC. Because both these tools were released open source, other groups in the case of FloodNet and participants within the Anonymous collective in the case of LOIC were able to progressively adapt these tools for the needs of any given action. This adaptability extended the life and influence of these tools past the initial actions they were developed for. Through being adopted and adapted by other groups, individuals, and actions, the successive versions of these tools act as a connective string of influence, as the technological affordances, design assumptions, specific functionalities, and interface choices impact each new action that uses them.

In this chapter, I trace the development of the EDT's FloodNet and the Anonymous' family of LOIC DDoS tools.

I'm particularly interested in complex of language, memes, and references used in the interface design of these tools and their paratextual materials, such as tutorial videos and how-tos, as well as scheduling and recruitment documentation. The specific language and references used can show not only the targeted user group for the tool (and thus the intended participants for the action), but can also give clues as to the lineage of the tool and the specific development of the groups using it.

The previous chapter was an attempt to address DDoS actions at the level of social movement theory. This chapter takes the technological tools used during these actions as a base for the analysis of these actions. Rather than looking at them on a purely technological level, this chapter examines these tools in the context of activist actions and communities, at how their existence impacts campaigns. The design and affordances of the tool used can define a variety of aspects of the actions, including the level of engagement expected from participants, as well as indicating, after the fact, the types of individuals who were recruited and active, and the amount of political "seriousness" indicated by the action.

The Electronic Disturbance Theater and FloodNet

FloodNet was developed in 1998 by EDT members Carmin Karasic and Brett Stalbaum, with Stalbaum as the primary developer and Karasic handling the interface design and testing. Written in Java, the tool exploited something called the "applet reload function," with the tool requesting a reload of webpages or sections of webpages from the targeted server several times a minute. In the earliest version of the tool, these reload requests were triggered every 7 seconds. Later versions were able to increase the request load to once every 3 seconds.

FloodNet was a browser-based tool. Participants navigated to a specific webpage that hosted the tool, selected certain parameters, often from a drop-down menu, and allowed the tool to run in the background. “Messages” of a kind could also be sent to the targeted server. FloodNet could send requests for specific files to the targeted server. A request for “human rights” would generate a “404_file not found” message in the server’s logs: “human_rights not found on this server.”¹ Such a message could be found by a systems administrator later. This performative “messaging” functionality would appear in Anonymous’ LOIC tool. This type of messaging is not particularly useful as a mode of communication. It’s very unlikely that anyone other than a systems administrator will ever see these logged messages. So these messages and the messaging functionality of the FloodNet tool itself is best viewed as an outlet for the activists themselves. A small point of individually determined personal expression in a tool that otherwise provided few opportunities to stray from the choreography of the action.

The EDT held 13 pro-Zapatista actions in 1998 using FloodNet, targeting websites ranging from those of the Clinton White House and the Pentagon to those of Mexican president Ernesto Zedillo and the Frankfurt Stock Exchange, with mixed success. These actions attracted up to 18,000 participants but did not generate much focused media attention.² On January 1, 1999, the source code for the FloodNet tool was released, allowing other groups to use the tool in their own actions. It was this version that was adapted by *the electrobippies* for their 1999 WTO action, and by the “Deportation Class Action” activists in 2001. Its design was simple and for the most part undifferentiated version to version. Participants either selected a target from a preselected list of targets, or the tool could be set up such that target selection was automatic. Participants were not asked to manually input targeting information. The only free user-input aspect of the tool, as mentioned above, was the text field where one could type their message to the server.

FIGURE 1 A screen shot of the web-based version of the EDT's FloodNet DDoS tool.

Figure 1 is the version of FloodNet used by the EDT during their pro-Zapatista actions in 1998. These actions were strictly scheduled, running for only 1 or 2 hours on a given day. The language used in the interface clearly marks 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. The tool invites 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 Zapatista struggle, and other related topics. 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.³ 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. It also added another point of contention and confusion between these internet-enabled activists, and hacktivists, who saw FloodNet as technologically inefficient and poorly designed from a network standpoint.⁴ However, for the EDT, the technological inefficiency of FloodNet was a feature, not a bug, as it allowed the “voice” of each participant to be meaningfully present in a collective action, without running the risk of being drowned out by automated machine noise. FloodNet hamstrung the efficiency of the machine in order to place a higher value on the input of the human participants. As we will see next, not all those who followed the EDT’s path cared to follow this logic.

Anonymous, Operation Payback and LOIC

Operation Payback began in September of 2010 as what Anonymous claimed was a retaliatory DDoS campaign targeting the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and other targets after those organizations had (according to Anonymous) hired an Indian firm, Aiplex to DDoS the Pirate Bay, a file-sharing website.⁵ The MPAA and the RIAA are the major lobbying groups for the content industry in

the United States 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. Individuals within Anonymous argued the DDoS actions by the RIAA and the MPAA as a threat to file sharing and torrenting and as a further example of the abuses perpetrated by the corporate content and IP industries.¹ Specifically, the use of DDoS tactics by the RIAA in an attempt to completely disable the Pirate Bay, which only existed in its online state, while Anons had been imprisoned for launching DDoS actions against the websites of the Church of Scientology, which existed primarily in the physical world as a complex organization, was presented as breathtakingly hypocritical. A group of Anons called AnonOps led the DDoS actions against the RIAA, MPAA, and Aiplex, which continued for more than a month. All three targets reported downtime.⁶

While it's clear that Aiplex had engaged in the past in for-hired DDoS actions against torrent sites including the Pirate Bay, it is far from clear that the MPAA and the RIAA ever specifically hired Aiplex to target the Pirate Bay. This first phase of Operation Payback, properly called Operation Payback is a Bitch, which had initially been conceived as an anti-ACTA protest, switched to targeting Aiplex after the publication and global spread of an article from an Indian newspaper wherein the managing director admitted that the firm was often hired by the film industry to stop the pirating of material through various means. After a first strike against Aiplex, considered by Gabriella Coleman to be a botnet powered wildcat action directed by just one person, Anonymous launched a series of collective actions against Aiplex, the MPAA, and RIAA, the International Federation of the Phonographic Industry, and a British IP law firm. These actions relied on the narrative that these lobbying

¹Torrenting 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.

organizations had hired Aiplex to conduct extralegal DDoS attacks against the Pirate Bay. This narrative was widely accepted by both Anons and the press, which repeated the story extensively.⁷

The ease with which this narrative was accepted tells us something about how these initial stages of Operation Payback were viewed. Under this lens, 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.⁸ The MPAA and others are cast, not as wanting to call attention to the issue of online file sharing but, rather, as wanting to obliterate the informatic entity known as the Pirate Bay. This would not be an entirely unrealistic course of action for them to take. A 2007 article in *Wired* reported that in 2005, the MPAA hired a hacker to exfiltrate confidential information from the servers of TorrentSpy, a popular torrent tracker.⁹ That the MPAA would fight dirty to combat online movie piracy is far from unlikely.

The Pirate Bay and the MPAA are different types of organizational entities. The Pirate Bay functions like a directory, a compendium of paths to data. It has no public presence beyond its internet presence and serves no function beyond making certain files available to users. Alternatively, the RIAA and the MPAA do not exist primarily online. Their websites are little more than informational homepages. No business is conducted there, and the hearts of the organizations do not reside online. The stated motivation for the Anonymous actions on the MPAA and the RIAA was to disrupt their operations and cause the organizations to spend money and resources fending off the DDoS actions,¹⁰ but the primary benefit of the actions lay in the media attention and new participants it attracted, who sympathized with Anonymous' views and could participate in future actions. It functioned, in part because of media coverage, as a recruitment drive.

December 6, 2010, marked the beginning second stage of Operation Payback, sometimes known as Operation Avenue Assange. This second wave of DDoS actions targeted

organizations and individuals Anonymous believed were acting against the interests of WikiLeaks, either by cutting off its channels of financial support, by refusing to provide hosting to the website and its domain name, or by speaking out against the organization publicly. Over the course of 4 days, Anonymous launched DDoS actions against over a dozen sites, causing downtime and service outages at several.¹¹ These actions were powered by volunteers using the LOIC DDoS tool and were augmented by nonvolunteer botnets.¹²

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

LOIC was originally developed and distributed by a developer using the handle praetox¹³ as a server “stress-testing” tool. It’s likely that this tool was never strictly intended to be used as a legitimate stress-testing tool, and the classification is instead a useful cover for the tool’s actual purpose: to disrupt the websites of others. 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.

ⁱⁱTo “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.

I 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. I will be examining some of the forks individually, as they reflect the previously discussed shifts in the Anonymous population, strategy, and political goals. The evolution of this particular tool further serves as a case study in the attempt to mainstream DDoS as a tool of political protest.

A forked comparison: abatishchev and NewEraCracker

When the first version of LOIC was made available on the internet is difficult to determine, but it was in use in 2008, during Operation Chanology.¹⁴ 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 concurrently participated in the development of LOIC, making it possible for the tools to more accurately reflect the needs, whims, and tastes of the target audience. By December of 2010, versions of LOIC could be run on Windows, Mac, and Linux PCs as well as Android phones and jailbroken 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.¹⁵

The most widely downloaded versions of LOIC in December of 2010 were posted to SourceForge and GitHub by abatishchev (Figure 4) and NewEraCracker (Figure 5), respectively. These two

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

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

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

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

versions will be examined because they represented a particular line of evolution for the tool, were very often linked in media coverage and LOIC tutorials, and were extremely popular, counting by the download numbers. Both hewed closely to praetox's original code while updating the graphical user interface (GUI) and adding features. The version from abatishchev is the older of the two, initially uploaded to SourceForge in June of 2009.¹⁶ This version of LOIC was downloaded 116,988 times in December 2010, up from 61,936 times in at the beginning of Operation Payback in September (see Figures 2 and 3). To compare, in August 2010, before the launch of the first wave of Operation Payback, this version of LOIC was downloaded 5,318 times.¹⁷ Together, the September 2010 (when Operation Payback initially began) through December 2010 (when the Avenge Assange portion of Operation Payback took place) downloads make up nearly a third of the 567,476 downloads abatishchev's version of LOIC racked up from June of 2009 to October of 2011 (see Figure 2). Just under a third of those downloads occurred during the week of Operation Payback's Avenge Assange campaign. It is impossible to tell from SourceForge records how many of those downloading the tool actually used it during the course of Operation Payback, but it is an impressive and telling spike.

NewEraCracker uploaded his version of LOIC to GitHub in late September 2010, stating clearly that his work was based on abatishchev's version of the original praetox tool, as was written in the project's README file¹⁸: "LOIC—An open source network stress tool, written in C#. Based on Praetox's loic project at <https://sourceforge.net/projects/loic/>." Note that NewEraCracker credits Praetox but links to abatishchev's SourceForge project. From its creation in September 2010–December 2011, NewEraCracker's version of the tool was downloaded 80,660 times (unfortunately, GitHub does not currently offer finer-grain analytics on projects).¹⁹

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 LOIC moniker. Both GUIs are peppered with references to memes and video games that would be instantly recognizable to individuals associated with Anonymous or familiar with internet meme culture, although the references differ between the two versions in ways that make the tools temporally and politically distinct. 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. 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 (see Figure 6), began appearing on 4chan and /b/ in 2006.²⁰ “Desudesudesu,” also included in the TCP/UDP message field, references a separate meme, also popular on 4chan in 2006.²¹ NewEraCracker replaces that message with “U dun goofed,” a reference to the Jessi Slaughter meme, which became widespread during the summer of 2010²² (see Figure 7). The abatishchev version also includes the subtitle “When harpoons, air strikes and nukes fail,” a reference to the video game series *Command and Conquer*, from which the name “Low Orbit Ion Cannon” is taken.

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 2006.²³ Whereas “IMMA CHARGIN MAH LAZER” and “U dun goofed” enjoyed widespread popularity beyond 4chan, “A cat is fine, too”

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

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

references an obscure bestiality meme derived from Japanese manga. It did not achieve recognition or popularity beyond 4chan and similar image boards, such as SomethingAwful and YTMND. Given the proliferation of 2006 internet memes in the older versions of LOIC, and given that 2006 predates any significant media coverage of Anonymous or 4chan, it is reasonable to assume that the original developer of LOIC was most likely active on /b/ and with Anonymous, saw the target audience as members of the same community, and developed the tool sometime during 2006.

These two versions of LOIC are semiotically tagged with memes popular within different populations at the time of development. The abatishchev and, theoretically, original praetox versions reflect memes that occurred predominantly within the community of /b/ and 4chan and did not leak out into the wider internet culture. The NewEraCracker version replaced those more obscure references, either because the developer did not recognize them or because he wanted to explicitly realign the cultural references of the tool with memes that had attracted the attention of the more mainstream internet culture. At the time, the Jessi Slaughter “U dun goofed” meme had attracted the attention of popular internet culture blogs, such as Gawker, and the mainstream news media.²⁴ 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. This shift in rhetorical tone can also be interpreted as a reflection of Anonymous’ overall move away from its 4chan roots, toward a new activist identity.

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

viral video from which the meme sprang, “U dun goofed” is followed shortly by the line “The consequences will never be the same.”²⁵ So whereas the praetox and abatishchev LOIC can be seen as calling out to a specific, rather limited group of like-minded individuals, the NewEraCracker LOIC throws its net much more broadly and advertises its vengeful motives much more overtly. This messaging functionality is identical to the one found in the original FloodNet tool. The message many never be seen by the target and, as such, serves more as a rhetorical flourish for the benefit of the sender, adding a weight that might not be carried by the hurling of bits alone, and augments the sense of communal participation.

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

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

This added functionality also represents an important advancement from FloodNet, which, like abatishchev’s LOIC,

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

operated in only one “manual” mode. Although the tool automated the process of sending packets, a user still had to target and engage the tool manually. Hive Mind mode allowed the tool be controlled remotely, through the IRCⁱⁱⁱ protocol. During Hive Mind mode, the user was essentially volunteering his or her machine to be part of a botnet, wherein many different machines were controlled by one. 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’ 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. 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,”²⁶ it was Anonymous that actually took advantage of the protocol’s physics-defying potential. Hive Mind mode enabled Anonymous to engage with participants who did not, for whatever reason, follow the targeting and scheduling information that Anonymous was constantly releasing and updating. A lower level of commitment was required. Although Anons may not have “hit the streets” as EDT envisioned, Hive Mind mode did enable them to go to school, work, sleep, or anywhere while still participating in DDoS actions as they arose. Hive Mind mode was not the

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

first time an activist DDoS campaign used volunteer botnets. An earlier instance, the Help Israel Win campaign in 2008, is examined in the next section.

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 quotes one Anon as saying that the number of participants on the Operation Payback IRC servers rose from an average of 70 participants to over 7,000. The ease with which one could participate in the Operation Payback actions was rivaled only by the ease with which one could take on the identity of an Anon. As noted previously, the Anonymous identity meme is based on the strengthening of a central core via the participation of many individuals who move in and out of different active or passive states. This subsumption of personal agency has the potential for a strong biographical impact on the participants, particularly, those who had not previously considered themselves political actors, by merging their agency with other active participants. This merging allows for the temporary sharing of an activist identity, which subsequently becomes more easily adopted by those participants who opt to remain involved.

Changes in the technology

It is becoming increasingly difficult for a purely volunteer, manual style DDoS action (which require a body in a chair for the duration of the action and can claim the strongest line of symmetry to physical-world sit-ins) to have a noticeable effect on a large, robust corporate website. Advances in technology as well as the vending of DDoS defense services to at-risk sites by companies like Akamai and Arbor Networks mean that even automated, strictly volunteer-supported DDoS actions are unlikely to cause downtime. This had led

to the use of botnets, traffic multipliers, automated tools, and other exploits to bring the power of such actions in line with the defenses employed by targets. While the use of such technological tools doesn't automatically negatively affect the validity of an activist DDoS action, the use of nonvolunteer botnets is a particularly worrying turn. Volunteer botnets present their own ethical concerns, but are less immediately objectionable.

Another aspect to consider is how advances in infrastructure and connectivity have changed the nature of DDoS actions over time. Groups like Strano, the EDT, and others active in the 1990s and early 2000s structured their actions to be of short duration, 2 or 3 hours at most. The Strano Netstrike action, which took place on December 21, 1995, lasted for only an hour.²⁷ The EDT's "Tactical Theater Schedule," a list of the FloodNet actions taking place in 1998, notes that actions run from "10:00 a.m. to 12:00 p.m. and 4:00 to 6:00 p.m. . . . Mexico City Time" for each of the thirteen dates listed.²⁸ The technical and financial realities of dial-up internet prevented, for the most part, more ambitious actions of longer duration. *The electrohippies'* 1999 WTO action was unique in that it was designed to take place continually over a number of days. The November 29, 1999 call-to-action e-mail states, "The sit-in will begin 08.00 USA & Canada (Pacific time) 30th November . . . and will finish four days later."²⁹ The e-mail notes that those with dial up connections may not be able to stay online for the whole planned 4 days, and so advises:

If you cannot afford to spend much time online then concentrate on November 30th (or Dec. 1st for those in the East). But we would like people to aim to go online for 12.00 Pacific time on December 3rd (add 4 hours to the above timetable for your local time) until the end of December 4th.³⁰

The transition from telephone-based internet connections to broadband, DSL, cable, and fiber connections has altered

the duration calculus for DDoS actions. With the high speed, always-on internet connections available to many participants, DDoS actions have the potential to go on for days, or weeks, or indefinitely. While organizers were once constrained simply by technical capacity, other concerns, including ethics, must now come into play when determining the duration of DDoS actions.

In addition to the Hive Mind supported volunteer botnet, there were several large nonvolunteer botnets involved in Anonymous' Operation Payback.³¹ Nonvolunteer botnets are created by infecting computers with a program that allows them to be controlled by a remote server without the owners' knowledge. The use of someone's technological resources without their consent in a political action, particularly one that carries high legal risk, is a grossly unethical action. Moreover it cheapens the participation of the activists who are consensually participating, and makes it easier for critics to dismiss DDoS actions as criminality masquerading as free speech.

Prior to Anonymous' Hive Mind powered volunteer botnets, the tactic had been used by pro-Israeli activists in 1999. A group of Israeli students calling themselves Help Israel Win released a tool that allowed people to participate in DDoS actions, ostensibly targeting anti-Israel websites. Like LOIC's Hive Mind mode, individuals who downloaded the Patriot DDoS software package from help-israel-win.tk could link their computers to an IRC server and participate in DDoS actions. Unlike LOIC, Patriot runs solely in the background and does not allow for user input of any kind.³² The original website is no longer online or archived, however Jeffrey Carr quotes the group's self-characterization as "a group of students who are tired of sitting around doing nothing while the citizens of Sderot and the cities around the Gaza Strip are suffering."³³ Their goal of "unit[ing] the computer capabilities of many people around the world . . . in order to disrupt our enemies efforts to destroy the state of Israel"³⁴ echoes similar sentiments articulated by *the electrohippies* around their WTO action.

The release of the tool itself garnered a moderate amount of media attention, attracting coverage in *Wired*³⁵ and blogs.³⁶ The *Wired* article notes that at one point there were roughly 1,000 computers hooked into the botnet, and Help Israel Win claimed credit for bringing down sarayaalquds.org and qudsvoice.net.

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

Notes

- 1 Jordan and Taylor, *Hacktivism and Cyberwar*, 87.
- 2 Dominguez, "Electronic civil disobedience," 1807.
- 3 Jordan and Taylor, *Hacktivism and Cyberwar*, 81.
- 4 Ibid.
- 5 Nate Anderson (2010), "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>.
- 6 Anderson, "Operation Payback attacks."

- 7 Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Story of Anonymous* (Brooklyn, NY: Verso Forthcoming).
- 8 Anderson, "Operation Payback attacks."
- 9 David Kravets, "Exclusive: I Was a Hacker for the MPAA," *Wired*, October 22, 2007. Last accessed February 27, 2014, http://www.wired.com/politics/onlinerights/news/2007/10/p2p_hacker?currentPage=all.
- 10 Anderson, "Operation Payback attacks."
- 11 Correll, "Tis the season of DDoS."
- 12 Coleman, "Our weirdness is free."; Parmy Olson, *We Are Anonymous* (New York, NY: Little Brown, 2013).
- 13 Quinn Norton, "Anonymous 101 part deux: Morals triumph over lulz," *Wired*, December 2011. Last accessed February 27, 2014, <http://www.wired.com/threatlevel/2011/12/anonymous-101-part-deux/all/1>.
- 14 Coleman, "Geek Politics and Anonymous."
- 15 Christina Warren, "How Operation Payback executes its attacks," *Mashable.com*, December 9, 2010. Last accessed February 27, 2014, <http://mashable.com/2010/12/09/how-operation-payback-executes-its-attacks/>.
- 16 Relevant development dates and other statistical information on the abatishchev version of LOIC are available from the LOIC project page on SourceForge, <http://sourceforge.net/projects/loic/>.
- 17 abatishchev LOIC SourceForge project page.
- 18 The README file for NewEraCracker's version of LOIC is available at <https://github.com/NewEraCracker/LOIC#readme>.
- 19 These statistics are available on the NewEraCracker GitHub project page, <https://github.com/NewEraCracker/LOIC>.
- 20 Know Your Meme, "A cat is fine, too," *Know Your Meme*, 2009. Last accessed February 27, 2014, <http://knowyourmeme.com/memes/a-cat-is-fine-too>.
- 21 Know Your Meme, "Desu," *Know Your Meme*, 2009. Last accessed February 27, 2014, <http://knowyourmeme.com/memes/desu>.
- 22 Know Your Meme, "Jessi Slaughter," *Know Your Meme*, 2010. Last accessed February 27, 2014, <http://knowyourmeme.com/memes/jessi-slaughter>.

- 23 Know Your Meme, "Shoop da whoop," *Know Your Meme*, 2009. Last accessed February 27, 2014, <http://knowyourmeme.com/memes/shoop-da-whoop-i%E2%80%99m-a%E2%80%99-firin%E2%80%99-mah-lazer>.
- 24 Know Your Meme, "Jessi Slaughter."
- 25 Ibid.
- 26 Dominguez, "Electronic civil disobedience," 1810.
- 27 Julie Thomas, "Ethics of Hacktivism," SANS Institute, January 12, 2001. Last accessed February 27, 2014, <http://www.giac.org/paper/gsec/530/ethics-hacktivism/101266>.
- 28 This schedule is currently archived at <http://www.thing.net/~rdm/ecd/ecd98.html> and was last accessed April 23, 2013.
- 29 chippies@tesco.net, "WTO Sit-in open!"
- 30 Ibid.
- 31 Olson, *We Are Anonymous*; Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Story of Anonymous* (Brooklyn, NY: Verso, forthcoming).
- 32 Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2011), 28.
- 33 Carr, *Inside Cyber Warfare*, 28.
- 34 Ibid.
- 35 Noah Shachtman, "Wage Cyberwar Against Hamas, Surrender Your PC," *Wired*, January 8, 2009. Last accessed February 27, 2014, <http://www.wired.com/dangerroom/2009/01/israel-dns-hack/>.
- 36 Ethan Zuckerman, "Install a trojan for Israel? Uh, no thanks," *My Heart's in Accra*, January 18, 2009. Last accessed February 27, 2014, <http://www.ethanzuckerman.com/blog/2009/01/08/install-a-trojan-for-israel-uh-no-thanks/>.