V Community + Action

29 Activist DDoS, Community, and the Personal

Molly Sauter

Crowd-based actions, such as blockades and public marches, are not based on the discreet identities of individual participants to be successful. Distributed denial of service (DDoS) actions, a coordinated action wherein many individual computers target a central server, flooding it with requests until it is unable to properly function, rely on a similar dynamic to achieve their activist ends. The visual spectacle of the mass (or, in the case of DDoS, the imagined mass behind the signal flood) is more valuable than the individual as a self-contained entity in the greater campaign. Organizers rely on the visual image of streets crowded with marchers to convey the commitment of their supporters, or directly reference huge numbers of potential and actual activists in how they refer to their movements and actions, through evocative titles such as the Million Mom March. Tocqueville called this coming together of individuals the moment when "they are no longer isolated men but a power seen from afar …" (Tocqueville 2002). As a communicative act, it is the coming together as a community of action that is of importance. For each individual within that community, however, there is still a granularity of identity to be contended with, including the questions of anonymity, performed identity, responsibility, and technological elitism.

DDoS actions, which have been used as a form of digital activism since the mid-1990s, are hardly the only instance wherein the malleability and concealment of activist identities have become an issue. Recent attempts in the US, the UK, France, Germany, Spain, Switzerland, Denmark, and Austria (some successful, some not) to implement anti-mask legislation demonstrate both the popularization of identity concealment within certain activist communities as well as the state's deep distrust of the tactic. Canada's Bill C-309 is the most recent example of this type of restrictive legislation, which carries a potential penalty of 10 years in prison for wearing a mask during a riot or unlawful assembly. The assumed ease with which online activists can conceal their identities often attracts criticism. Leaders of the tech industry are often the source of these critiques, as when Randi Zuckerberg, then Director of Market Development at Facebook, stated that "Anonymity on the Internet has to go away," arguing that anonymity leads to bad behavior and abusive speech (CBS News 2011). Google CEO Eric

Schmidt has made similar statements in the past. Anonymous political speech is seen as not carrying the same weight as named political speech because it is widely perceived as less risky or allowing the speaker to avoid accountability. The opposition of tech executives to anonymous speech on, ostensibly, grounds of moral and political responsibility is striking due to their control of the very structures and platforms of expression that many rely on for political organizing. Moreover, this critique, though popular, often runs counter to the historical deployment of identity within activist actions, including DDoS actions.

Critiques of anonymous activism also reveal a tension at the base of the Western conception of political responsibility. Though anonymity can be granted to mainstream political activities, such as the use of the anonymous ballot, those political minorities whose democratic participation has been hamstrung by a failure of the public discourse to seriously consider a specific set of issues, or by outright disenfranchisement, are denied the protection of anonymous participation. Instead they are forced into legally and sometimes physically precarious situations as a type of public "authenticity" gauntlet, as the public abusively test the depth of their commitment to their claims. Similarly, there is little credence given to the idea that moral and political responsibility can attach to protest when performed under identities that are not state sanctioned. This combination leaves the Western state in ~~the~~ ~~sole~~ position to determine the validity of its critics, not based on the content of their criticism but on the performance of their critical identity. What's more, the simultaneous refusal to accept the validity of anonymous protest coupled with punitive overreaching on the part of the judicial system in response to innovative forms of disruptive civil disobedience has a distinctly chilling effect on the ability of many individuals to participate in the public political discourse. Rather, it encourages the expression of dissent only by those individuals willing to risk everything for the sake of a political point, or in Hannah Arendt's words, it fosters "single-minded fanaticism … mak[ing] impossible a rational discussion of the issues at stake" (Arendt 1972).

In short, the emphasis on identity-tied "responsibility," as determined and retributed by the state, which has an interest in discouraging novel forms of dissent, actively suppresses opportunities for wide political participation, discourse, and enfranchisement, rather than encouraging them. Civil disobedience, rather than being welcomed as an alternative mode of political participation, is pushed to the fringes of public political life where its practice becomes more extreme and fanatical, and easier for the political mainstream to dismiss.

This chapter is an attempt to bring to the fore the tensions of identity, responsibility, performance, and exclusion that sit at the core of the political use of DDoS actions. These tensions exist within the use of the tactic itself and in the tactic's interplay with the political processes of a discursive democracy in general.

A Technical Note on the DDoS and Its Role in Digital Protest

A denial of service action is a purposeful attempt to render a targeted computer server inaccessible to those looking to communicate with it for legitimate purposes. The action can originate from a single source, as with an exploit-based action, or it can be the result of a coordinated act coming from multiple sources. In the later case, ~~this~~ is known as a *distributed* denial of service action. Unlike other tactics of digital disruption like website defacement or data exfiltration, complicated tools or sophisticated skills are not necessary to wage a DDoS action. A group of people simultaneously refreshing the same webpage over and over could be considered a manual DDoS action, if their intention is to bring the webpage down for political reasons. However, modern Web infrastructure makes it extremely unlikely that such a "manual" DDoS would be effective against a major corporate or government website. More often, small programs called tools are used to dramatically multiply the number of requests that can be sent from a given machine in a short period of time. These tools can also include graphical user interfaces (GUIs), messaging functionalities, or even information about the activist action itself. Botnets, or networks of computers being controlled by a central command-and-control machine, have also been employed in activist DDoS actions. These machines may have been volunteered for duty by their owners, or, more problematically, may have been illicitly infected with a virus that allows them to be remotely controlled by someone other than their owners.

In its modern implementation, activist DDoS actions can serve as an easily accessible first step into engagement with disruptive online activism. DDoS actions have been used as a tactic of activism essentially since the arrival of the public network, with public-facing DDoS actions starting at least as far back as 1995 with the Italian Strano Netstrike action (Sauter 2014). DDoS tools like FloodNet and Low Orbit Ion Cannon (LOIC), developed by the Electronic Disturbance Theater and Anonymous-affiliated coders in the late 1990s and mid 2000s respectively, have accessible, point-and-click interfaces that allow participants with relatively low levels of technological sophistication to take part in activist DDoS actions. Both these tools have been open sourced, giving other activists and organizations the chance to build on the technology, adapting them for different activist populations. As the user population shifts, so too can the technological affordances of these open tools, enabling them to be used in the service of a variety of activist ends. Activist DDoS actions can be deployed as tactics of direct action, such as the 1999 *electrohippies* action targeting the email servers of the WTO Ministerial Conference in Seattle, or as tactics of media manipulation, such as the actions of the Electronic Disturbance Theater or Anonymous, or as tools of popular education, biographical impact, and recruitment.

DDoS and Impure Dissent

DDoS actions and the theatrics that surround them, particularly those indulged in by groups like the infamous hacker/trickster collective Anonymous (Coleman 2012), can and have often been dismissed as apolitical or antipolitical. The disruptive, trollish nature of the actions, and their seeming incapability, at the most fundamental, functional level, to contribute meaningfully to the public democratic discourse, makes the dissent practiced though DDoS actions easy to dismiss. In this way, activist DDoS actions can fall under the umbrella of what Tommie Shelby calls "impure dissent" (Shelby 2015). Impure dissent is that which does not take the form of traditional, morally exemplary civil disobedience or other anticipated forms of protest. Shelby's main subject of analysis is hip hop, but his analysis leaves room for confrontational, disruptive forms of street activism as well. To Shelby, impure dissent contains a mash-up of legitimate, meaningful political content, and other speech and conduct elements that dramatically break from the norms of typical political speech. It is these other elements that have the potential to undermine or counteract the political content of impure dissent. Shelby notes that these nonpolitical elements can include profanity, epithets, negative stereotypes, or violent or pornographic images (Shelby 2015).

By both design and practice, activist DDoS actions directly confront the privatized, communicative nature of the modern online space. Jodi Dean's theory of communicative capitalism gives us a framework that allows us to work through the specific impact of DDoS actions as a collective action. Dean's theory reveals as irrelevant the constant flow of additive communication that dominates the online environment. While the Web 2.0 community framework gives many people the chance to "participate," that participation is ultimately recursive and irrelevant to the structures of power which dominate the current landscape. While individuals may satisfy their "participation" itch with a constant flow of likes, retweets, comments, and shares, and may even build personally meaningful relationships and communities in the process, these actions and relationships are ultimately politically impotent (Dean 2009). While it is the nature of the online space to facilitate the additive flow of information, it is the nature of the DDoS action to disrupt that flow and to draw explicit attention to that disruption. DDoS actions can be seen as destructive, antisocial, and informatically deviant enough to completely undermine the intended political message of the action. The continued existence and practice of DDoS actions can be interpreted as dangerously undermining the stability of the online space to such an extent that any use is seen as deeply irresponsible at best, and acutely criminal and threatening at worst. This view can be seen reflected in news coverage of activist DDoS actions, particularly of early groups like the Electronic Disturbance Theater (EDT), who were active in the late 1990s and early 2000s. Press coverage of their pro-Zapatista actions would often associate the group with criminals or terrorists, often not acknowledging their explicit activist claims (Sauter 2014).

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

The interruptive nature of DDoS actions means that the role they can serve within a discursive democratic sphere is limited. Those who use the tactic are functionally incapable *in that moment* from participating in the democratic process as a discussant. It is here that DDoS actions are often criticized as a "heckler's veto" or an attempt to merely shout down the opposition without making any productive contribution to the public discourse (Ruffin 2000). But a disruptive political act of civil disobedience serves to alert the wider public that the normal channels of participation have failed for a certain population. The lack of signal that is the external manifestation of an activist DDoS action should be interpreted as making space for unheard dissent. That making-of-space, the creation of an awkward silence in the constant whirl of communicative capitalism, is not a breakdown of "authentic deliberation" but a chance to "reinstate a deliberative environment" which has suffered a participatory breakdown (Smith 2013).

A primary motivation for early practitioners of activist DDoS actions like the EDT and *the electrohippies*, a British group active in the early 2000s, was to establish the Internet as a viable space for civil disobedience and dissent. *the electrohippies* stated in one of their initial papers defending the use of DDoS actions:

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

However, despite their aspirations, the commercialization and privatization of the Internet continued. As of 2013, the online space is, as it stands, thoroughly privatized. Public spaces, as they are understood to exist in the physical world under the guise of parks, sidewalks, and roadways, do not exist online. As such, the expectations of speech rights online follow, not the norms of public spaces, but the norms of private property. In the United States, "public forum doctrine" governs both the law and the social norms here.

Of the three, sometimes four, broad categories identified by the U.S. Supreme Court, the most permissive in terms of speech restrictions is the "traditional public forum": streets, parks, sidewalks, town commons, and other areas traditionally recognized as being held in common for the public good. The most restrictive is private property, in so much as the owners of private property are relatively free in the restrictions they can place on the speech of others when it takes place on their property (McPhail et al. 1998).

The Internet is not a "traditional public forum." Online outlets for speech, such as blogging platforms, social networks, forums, or other wellsprings of user-generated content are privately owned. US-based ISPs could be subject to liability if they do not properly police their users' content. The Internet has developed into a zone of modern life lacking some crucial First Amendment protections. While the freedom of the press is relatively well protected in the online space, the rights of assembly and speech of the average individual remains unprotected. Given the Internet's current role as a basic outlet of personal expression, association, and communication, this is deeply troubling. While protests taking place in the various public fora in the physical world have a foundation of history and legal doctrine to support their legitimacy as valid and protected political speech, actions that take place in the online sphere can only ever infringe on privately held property. The architecture of the network does not, as of yet, support spaces held in common.

As a privately held public sphere, disruptive acts of civil disobedience online will always be in conflict with dearly held doctrines of private property. This conflict has a physical-world parallel. The initial Occupy Wall Street camp was established at Zucotti Park, a "privately held public space" that is ostensibly available for public use but still subject to the potential restrictions of private property. The free speech obligations/protections provided by such spaces are legally murky. Without substantial legal precedent supporting the rights of activists to stage potentially disruptive political actions, the use of DDoS as a tactic in and of itself has the potential to render the activist action impure by coming into conflict with private property rights, without the established cultural and legal protections that have developed around physical-world civil disobedience. This is disastrous for the development of civil disobedience online. By being continually compared with activism in a sphere with substantially different norms of property and speech (i.e., the physical world), civil disobedience online consistently

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

Early groups explicitly revealed and advertised the identity of the organizers of DDoS actions. This followed the position of the EDT and *the electrohippies* that DDoS actions were a direct adaptation of sit-ins and other street-based tactics, which incorporate a give-and-take with the state and law enforcement into their operational logic. However, this view of identification, responsibility, and state participation hasn't held in more recent DDoS actions. In particular, Anonymous, which maintains anonymity as an aspect of their culture, refuses to buy the claim that the state is engaging with digital activism in good faith. Moreover, Anonymous for the most part refuses to acknowledge that national governments, particularly that of the United States, have any legitimate role in governing the Internet at all.

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

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

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

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

These groups did not require participants to publicly identify themselves to the same degree as organizers; *the electrohippies* recommended the use of anonymous,

throw-away email addresses for their WTO email bombing campaign. However, the groups did acknowledge the likelihood and potential consequences of being identified as participants in these actions, as stated on the EDT's website, still using street activism as the dominant frame of reference:

> WARNING: This is a Protest, it is not a game, it may have personal consequences as in any off-line political manifestation on the street:
>
> Based on critiques from the Heart Hackers and other individuals about FloodNet:
>
> 1. Your IP address will be harvested by the government during any FloodNet action. When you click and enter FloodNet your name and political position will be made known to the authorities.
>
> (Similar to having your picture taking during a protest action on the street.)
>
> 2. Possible damage to your machine may occur because of your participation in the FloodNet action.
>
> (Just as in a street action—the police may come and hurt you.)
>
> 3. FloodNet clogs bandwidth and may make it difficult for many individuals using small pipelines around the world to get information. FloodNet may not impact the targeted website specifically as much as it disrupts traffic going to the targeted website, i.e., problems for Internet routes to the site.
>
> (This also happens when people take to the streets. Individuals may find themselves unable to get to work or buy a newspaper because of the action. FloodNet actions are short term and only disturb bandwidth during the time of the manifestation. The Electronic Disturbance Theater feels that even if FloodNet only functions as a symbolic action, that is enough to make the collective presence of activists felt beyond the electronic networks.)
>
> We hope that when you join our Virtual Sit-in's in support of global communities of resistance, you will take the above information to heart. (Karasic and Stalbaum 1998)

The EDT and *the electrohippies* reliance on physical-world structures of accountability indicate a belief that the assumptions of physical-world activism would hold true for activism in the online space as well, particularly assumptions around interactions with the state and its agents. The EDT's warning acknowledges the expected role law enforcement typically plays in street activism. In this conception, the state serves as a theatrical antagonist and legitimator of dissent by virtue of ~~their~~ reaction: as stated by Jerry Rubin in 1969, "The cops are a necessary part of any demonstration theater. When you are planning a demonstration, always include a role for the cops. Cops legitimize demonstrations" (Rubin 1969). Similarly, in his original conception of civil disobedience, when Thoreau says, "Under a government which imprisons any unjustly, the true place for a just man is also a prison" (Thoreau 1849), he values the spectacle of the state imprisoning a just man for its value as an illustration of the injustice of the state, to which others may react. William Smith calls this a "moral dialogue with authorities" in which the protestors, law enforcement, and general citizenry are all participants (Smith 2013). Insomuch as activists can provoke a punitive reaction from the state, they can

in turn also trigger a public dialogue as to the appropriateness of that response (Smith 2013).

Symbolic activism of the type practiced by the EDT and other co-temporaneous groups requires an interaction with the state to be effective. Though the reaction of the state to novel forms of dissent is not entirely predictable, it's clear from their writings that the EDT expected the state's response to fit broadly within the mold of its typical responses to street activism. They expected to be treated as activists. Like street activists, the EDT's actions were occasionally met with a militarized response: one of the EDT's FloodNet-powered actions prompted an aggressive "counter-hack" from the Pentagon, an action that was criticized as being an unreasonable cyber-attack against US-based civilians (Meikle 2002). This notwithstanding, the EDT maintained through its literature and practice an assumption that their actions would be treated as political in nature. By refusing to conceal their own legal identities, and by not providing their participants with the technical knowledge and means to evade identification, the EDT maintained a space for the state to participate as a useful actor in the processes they were trying to impact.

Contrary to this, Anonymous holds anonymity to be a core aspect of its culture. Anonymity is the default assumption, both in interpersonal interactions and particularly when engaging in public-facing actions. Individuals who out themselves are derisively referred to as "name-fags" and can sometimes receive a quite aggressive reaction (Coleman 2012). David Auerbach lays the credit for this cultural development at the feet of the technological systems upon which the Anonymous culture was built: fast-moving message boards that maintained no archive and were ephemeral and unsigned by nature (Auerbach 2012). While this explains where the value originated, it does not explain why it has penetrated so deeply into the culture's activist activities, nor why it has persisted at the levels of both technological systems and cultural practice.

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

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. (Barlow 1996)

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

In addition to simply denying the legitimacy of the state in governing dissent online, anonymity as an online activist practice contains within it a belief that the state and corporate actors targeted by the activists will not respond in good faith (Shelby 2015). Earlier groups drew on the history and scripts of street activism to anticipate interactions with states and law enforcement. Anonymous, operating some 10 years later, draws on a much different history of state antagonism toward hackers, DRM battles, and post-9/11 War on Terror surveillance and policing of dissent. Given the tradition in the United States of frankly ridiculous, overreaching Computer Fraud and Abuse Act-enabled computer crime prosecutions, this assumption of bad faith is not unreasonable. This is similar to the rationale behind the use of masks by Black Bloc actors during street actions. Thompson quotes Black Bloc activists citing "protect[ing] ourselves from illegal police surveillance" and "provid[ing] cover for activists engaged in illegal actions during the demo" (Thompson 2010) as reasons for the use of masks during street protests. The logic is clear: if your aim is to commit a political act not recognized as a privileged political act by the state, then taking actions to prevent yourself, as a political actor, from being assigned the role of criminal actor by the state is reasonable.

Anonymity as an outward-facing cultural practice strengthens the "relational equality" between the individual participant and the greater cultural movement (Thompson 2010). Anonymous relies on the perception of an inexhaustible mass for much of its rhetorical bite. The identical-ness of its masked, technologically anonymized participants fosters a sense of omnipresence, the type of "improperly named" mob noted by Deseriis (Deseriis 2013). Outward-facing anonymity prevents outside actors, like the media, from focusing on and privileging charismatic actors. Anonymous values the optics of the mass, the "hive," while simultaneously continuing to value internally individuality and individual initiative (Coleman 2012).

That said, though anonymity is the goal during these actions, it is not always achieved. The most popular versions of the LOIC DDoS tool used by Anonymous during its 2010 Operation Payback made no effort to cover their users' digital tracks. More sophisticated

DDoS tools will "spoof" IP addresses, generating a fake IP address to assign to the packets the program sends out, or take other steps to prevent the target of an action from tracing the packets back home. However, all packets sent with LOIC are tagged with the IP address of the sender. ISPs maintain records of the IP addresses of computers on their network and can match those IP records to the real names and addresses of their subscribers. Law enforcement can and often does subpoena those records when pursuing computer crime prosecutions. It was possible for an individual using LOIC, without taking additional security measures, to be identified on the basis of information contained in the packets he or she sent. The EDT's FloodNet tool and the adapted version used by *the electrohippies* also did not utilize any measures to mask the identities of participants. However, this should be seen as an extension of those groups' integration of physical-world/legal identity into their actions. Given Anonymous's history of anonymous action and the emphasis placed on anonymity within Anonymous culture, that LOIC does not conceal users' identities is more likely to be a mistake or hallmark of an inexperienced developer rather than an intentional decision.

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

Q: Will I get caught/arrested for using it?

A: *Chances are next to zero*. Just blame [sic] you have a virus, or simply deny any knowledge of it. (Operation Payback Setup Guide 2010) (emphasis added)

The media also picked up this line, and repeated it extensively, as in this article by Joel Johnson 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*. 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*. 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. (Johnson 2010; emphasis added)

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

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

An insistence that legal identity be tied to dissenting speech or disruptive activism benefits a state with an interest in tracking and suppressing those activities. The U.S. Supreme Court has noted the value of anonymous political speech, going so far as to recognize a right to anonymous pamphleteering, in the tradition of the anonymous and pseudonymous writings of Thomas Paine and the founding fathers (McIntyre v. Ohio Elections Comm'n, 1995). Just as an interruptive DDoS can open an opportunity for dissenting speech, the ability to engage in anonymous activism can create for individuals the opportunity to dissent. A chance to protest that is tracked and monitored is, for most of the public, no chance at all. It restricts the opportunities for dissent and disruption to the few who can bear the state-determined cost. As Tressie McMillan Cottom notes, "The penalty for raising hell is not the same for everyone" (Cottom 2014). An insistence on exposing oneself to legal threat as a cost to dissenting speech prices most people out of the discursive democracy market, regardless of their views. A democratic society that recognizes the right of citizens to political participation, and recognizes the value of civil disobedience as a reasonable and necessary manifestation of that right, must in turn recognize that anonymous civil disobedience and dissent is vital to the expression of those rights. Otherwise, we are using the excuse of "responsibility" to deny individuals their right to full political participation.

Accessibility in Technologically Defined Tactical Spaces

DDoS actions were taken up by digitally enabled activists as a more accessible, less geographically bounded tactic for activist expression than physical-world actions. While the CAE saw the move to the online space as tracking the movements of structures of

power to their new abode (Critical Art Ensemble 1996), later groups saw it as a way to lower the barriers to entry. As mass DDoS actions have continued to develop tactically over the years, different groups have continued to adapt it so that it is easier for individuals to participate. This adaptation occurs both on the level of tool design and information distribution, but also at a community level. During Operation Payback, for example, LOIC tutorials began popping up on YouTube and other locations around the Web. Though it would be impossible to get an exact figure, a YouTube search conducted in April 2013 for "LOIC tutorial" yields thousands of results. One video, "How to Use LOIC (Low Orbit Ion Cannon)," uploaded in mid-November 2010, had been viewed over 80,000 times by December 12, 2010, and had been viewed over 250,000 times by April 2013.

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

In some ways, the earlier webpage-based tools like the EDT's FloodNet may have been more diversely accessible than tools like LOIC or its successors. The early actions were also scheduled to last for only short amounts of time, at most an hour or two, to accommodate the restrictions and expense of participating in an action over a dial-up connection. The "occupation"-style DDoS actions organized by Anonymous, conversely, have run for days through broadband, cable, DSL, or fiber connections. So though advances in connectivity and computing power have made it possible for actions to last longer (and potentially have a greater impact on their target), taking advantage of those advancements can severely limit the potential participant pool.

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

the activist population, accessibility and cultural issues often create severe barriers to that goal.

DDoS Actions and the Law: A Conclusion

Activist DDoS actions are one of the few tactics of disruptive digital activism that rely on the bringing together of a coherent community of individuals in order to function. Due to their technological simplicity and the diffusion of easily adaptable tools, activist DDoS actions have become accessible, public-facing disruptive tactics capable of bringing together groups of novice activists, and introducing them to the methods and working theories of digital disruption as a valid form of political activism.

However, there are many aspects of disruptive digital activism in general, and activist DDoS actions in particular, which make it difficult for the broader political community to swallow. The anonymous or semi-anonymous nature of most activist DDoS actions are often seen as detracting from any serious political point such actions wish to convey. But anonymity itself plays a layered role within activist DDoS action, a role that has shifted over time and among the different groups that have made use of the tactic. These groups have often deployed anonymity tactically, revealing or withholding their identities to support differing philosophies of identity, accountability, and the role of the state in protest and the online space in general.

Similarly, the antics of groups like Anonymous, while often useful for internal culture-construction and group cohesion, can render attempts at public political dissent "impure," as described by the theories of Tommie Shelby. Ironically, the antisocial, trickster-like hacker persona that Anonymous intentionally casts in public has made them a much more attractive figure for media attention than earlier groups who also used the tactic of activist DDoS but whose public activist personas were more sedate, more fitting with the traditional view of a political actor. So Anonymous's public role play has had the contradictory effects of making them appealing targets of news media while at the same time delegitimizing them as valid political actors in the eyes of most of the public.

Finally, though activist DDoS actions have in many ways opened a door for genuinely accessible crowd-based activism in the online space, that accessibility is still shrouded in privilege. DDoS tools like LOIC must often be downloaded and run from a personal computer or phone, unlike earlier webpage-based tools like FloodNet. Whereas in the past actions were scheduled many days in advance and ran for a few hours at most, the actions coordinated by Anonymous occur on the fly and can run for many hours or even days. This requires that participants have access to an always-on Internet connection, a consistent power supply, and the financial means to support both. While Anonymous may have expanded the potential pool of participants through its media

savvy and LOIC's volunteer botnet capabilities, they are still drawing from the same technologically literate, web savvy, comparatively wealthy, and well-educated population. As a technologically based form of activism, DDoS remains inaccessible to huge swathes of the global population, and the issues that trigger its use are often those of specific interest to that privileged group.

It is useful in this context to consider whether disruptive digital activist tactics like DDoS can use the online space to transcend state lines, becoming truly transnational forms of activism. Certainly, early activist DDoS actions like the Strano Netstrike actions against French government websites or the EDT's pro-Zapatista actions or even *the electrohippies'* WTO actions carried activists' actions across borders. Groups operating under the Anonymous brand have staged actions with globally distributed participants, though some of Anonymous's subgroups have claimed distinct national identities, focusing primarily on issues and topics within those countries, like Anonymous Brazil's focus on the 2014 World Cup.

Despite the transnational sympathies of digital activists, however, activists are still subject to the laws of the jurisdiction in which they reside, or on occasion where the target is headquartered. These laws can vary widely between jurisdictions, with those in the US being particularly harsh. In 2013 the PayPal 14, a group of Anonymous-affiliated activists who had participated in Anonymous's 2010 Operation Payback DDoS action again PayPal, faced charges in the US which could have resulted in 15 years in prison and up to $500,000 in fines and restitution payments each. Ultimately the group received a plea deal that involved only a fraction of those threatened penalties, but the chilling effect is clear. While activist DDoS actions are inherently community- and group-based actions, state powers, particularly in the US, have a demonstrated interest in discouraging the evolution of this type of activism. So while DDoS actions themselves by their nature may encourage the construction and maintenance of transnational communities of digital activists, these communities are re-divided by both the divergent local and national interests of the participants as well as the legal regimes they may have to contend with if they are apprehended.

In the US, prosecutors are enabled to threaten defendants with massive, disproportionate penalties in order to encourage them to take a plea deal or to turn state's evidence. Because the US legal system relies on precedent, or previous legal decisions, to progress, the emphasis on plea bargaining actively prevents precedent from being established. Every activist DDoS case which is pled out by defendants who have been reasonably intimidated by the threat of unreasonably harsh penalties is a missed opportunity to set the legal precedent that activist DDoS actions are a rational, legitimate form of civil disobedience, and should be accorded the same level of political, social, and legal respect as a sit-in or an occupation in the physical world.

Author's Note

A version of this chapter was previously published in *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience*, published by Bloomsbury Academic in October 2014.

References

Arendt, Hannah. 1972. *Crises of the Republic*. San Diego: Harcourt Brace.

Auerbach, David. 2012. "Anonymity as Culture: Treatise," Triple Canopy 15. http://canopycanopycanopy.com/15/anonymity_as_culture__treatise.

Barlow, John Perry. 1996 "A Declaration of Independence for Cyberspace." https://projects.eff.org/~barlow/Declaration-Final.html.

CBS News. 2011. "Facebook: 'Anonymity on the Internet Has to Go Away.'" *CBS News*, August 2. Accessed April 3, 2015. http://www.cbsnews.com/news/facebook-anonymity-on-the-internet-has-to-go-away/.

Coleman, Gabriella. 2012. "Our Weirdness Is Free." *Triple Canopy*. Accessed February 25, 2014. http://www.canopycanopycanopy.com/contents/our_weirdness_is_free.

Cottom, Tressie McMillan. 2014. "Academic Cowards and Why I Don't Write Anonymously." http://tressiemc.com/2014/01/21/academic-cowards-and-why-i-dont-write-anonymously.

Critical Art Ensemble. 1996. *Electronic Civil Disobedience and Other Unpopular Ideas*. Brooklyn, NY: Autonomedia.

Dean, Jodi. 2009 "Technology: The Promises of Communicative Capitalism. In *Democracy and Other Neoliberal Fantasies: Communicative Capitalism and Leftist Politics*, 26–27. Durham, NC: Duke University Press.

Deseriis, Marco. 2013. "Is Anonymous a New Form of Luddism? A Comparative Analysis of Industrial Machine Breaking, Computer Hacking, and Related Rhetorical Struggles." *Radical History Review* 117: 35.

DJNZ/electrohippies. 2000. "Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act?" Electrohippies Occasional Paper, February. Last accessed February 25, 2014. www.fraw.org.uk/projects/electrohippies/archive/op-01/html.

Johnson, Joel. 2010. "What Is LOIC?" *Gizmodo.com*, December 8. Last accessed February 25, 2014. http://gizmodo.com/5709630/what-is-loic.

Karasic, Carmin, and Brett Stalbaum. 1998. "FloodNet Warning." Thing.net, September. Last accessed February 25, 2014. Archived at http://www.thing.net/~rdom/zapsTactical/warning.htm.

McIntyre v. Ohio Elections Comm'n (93–986), 514 U.S. 334 (1995).

McPhail, Clark, David Schweingruber, and John Mccarthy. 1998. "Policing Protest in the United States: 1960–1995." In *Policing Protest*, ed. Donatella Della Porta and Herbert Reiter. Minneapolis, MN: University of Minnesota Press.

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

"Operation Payback Setup Guide." December 2010. Accessed February 27, 2014. http://pastehtml.com/view/1c8i33u.html.

Perry, John B. 1996. "A Declaration of Independence for Cyberspace." February 8. Accessed February 25, 2014. https://projects.eff.org/~barlow/Declaration-Final.html.

Poulsen, Kevin. 2011. "In Anonymous Raids, Feds Work from List of Top 1,000 Protesters," *Wired*, June. Last accessed February 25, 2014. http://www.wired.com/threatlevel/2011/07/op_payback/.

Ruffin, Oxblood. 2000. "hacktivismo." *Cult of the Dead Cow Blog*. http://w3.cultdeadcow.com/cms/2000/07/hacktivismo.html.

Rubin, Jerry. 1969. "Yippie Manifesto." In *Free Pamphlet Series #1*. Vineyard Haven, MA: Evergreen Review, Inc.

Sauter, Molly. 2014. *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.

Shelby, Tommie. 2015. "Impure Dissent: Hip Hop and the Political Ethics of Marginalized Black Urban Youth." In *From Voice to Influence: Understanding Citizenship in a Digital Age*, ed. Danielle Allen and Jennifer Light. Chicago: University of Chicago Press.

Smith, William. 2013. *Civil Disobedience and Deliberative Democracy*. London: Routledge.

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

Thoreau, Henry David. 1849. *Civil Disobedience*.

de Tocqueville, Alexis. 2002. *Democracy in America*. Trans. H. C. Mansfield and D. Winthrop. Chicago: University of Chicago Press.

Zetter, Kim. 2011. "Feds Arrest 14 'Anonymous' Suspects over PayPal Attack, Raid Dozens More." *Wired*, June. Last accessed February 25, 2014. http://www.wired.com/threatlevel/2011/07/paypal-hack-arrests/.