Sauter, Molly. "Against the man: State and corporate responses to DDoS actions." *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic, 2014. 137–157. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781628926705.0013>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 10:25 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 SEVEN

Against the man: State and corporate responses to DDoS actions

Confrontational activism, like activist DDoS, is a conversation with power, often state or corporate power. Activists make a statement or take a stand, and the response of the state or corporate target often has a strong impact on the perceived success or even legitimacy of the activist action. Responses to activist DDoS actions by states and corporations have varied widely over the years the tactic has been in use. In at least one case, the case of Andreas Vogel, a court of law has declared DDoS actions to be valid forms of activism and condoned their use as a tool of collective action. In others, as we shall see, the judicial response has not been nearly so sympathetic, resulting in high fines, significant jail time, and other costs for participants.

This chapter is an attempt to place the responses of corporate and state entities to activist DDoS actions in context within several trends in the regulation and governance of the online space. The attempts to turn the internet into a business-friendly marketplace noted by the EDT and *the electrohippies* have not abated. In recent years and months, these regulatory efforts in support of the business community (both in the United States and abroad) have been augmented by attempts to make the internet

“surveillance-friendly” on a technological level, turning the online space into a zone open to monitoring by state organizations looking to root out terrorism, as well as those with an interest in turning the online space into a legitimate field of warfare. These interests have melded with those of the pro-business sector, and the result has been a collision of corporate and state efforts to lockdown nontraditional uses of technology and to heavily discourage vocal and visible displays of disruption and dissent. This, combined with the issues of politically legitimating media coverage covered earlier, result in a legal, cultural, and technical environment that chills the development of innovative technological outlets for political action and speech.

Terrorism accusations and the CFAA

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

As a result of the WTO action *the electrohippies collective* were labeled as terrorists. . . . The problem with the knee

ⁱMost of the organizers and activists in *the electrohippies* were British and operated from the United Kingdom.

jerk response of politicians and e-commerce gurus is that we run the risk of losing legitimate electronic action as governments use the excuse of “hackers” to criminalize certain activities. We must make sure that both the positive and negative aspects of internet activism are clearly debated, and that cyberspace is not excised from the everyday realm of constitutional rights and freedoms.¹

This classification mostly took place in the media. Other analysts, such as Dorothy Denning, paid greater attention to groups’ self-characterization:

While the above incidents were motivated by political and social reasons, whether they were sufficiently harmful or frightening to be classified as cyberterrorism is a judgment call. To the best of my knowledge, no attack so far has led to violence or injury to persons, although some may have intimidated their victims. Both the EDT and *the electrohippies* view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction. Most activists, whether participating in the Million Mom March or a Web sit-in, are not terrorists. My personal view is that the threat of cyberterrorism has been mainly theoretical, but it is something to watch and take reasonable precautions against.²

Denning’s testimony before the House Armed Services Committee, combined with *the electrohippies*’ statement, highlights a number of issues pertinent to the influence and roles of states in digital protests. While Denning acknowledges the role of self-identification in judging the activist value of an action, *the electrohippies* point out that if the online space as a zone is judged to be unavailable for activist action, then the self-identification matters little. As the internet developed from a pseudopublic academic intra-net into a vital part of everyday life for many people, it was inevitable that those who opposed the privatization of a perceived commons

would be systematically marginalized by both the corporate and state interests that stood to benefit financially and politically from stabilization of the network. So, although Denning hangs her definition of terrorism on the hook of personal harm and violence, she also acknowledges that a “judgment call” is required when classifying new disruptive behaviors.³ When the relevant “judge” is also the target of the disruptive protest, it is in their interests to reclassify legitimate protest as ideological violence.

There have been several cases of activist DDoS actions that have gone to trial or been pleaded out, in the United States and internationally. A significant case is that of Andreas-Thomas Vogel, a German national who ran the libertad.de website during the 2001 Deportation Class action against Lufthansa Airlines. Vogel had posted a call to action on libertad.de and was arrested on charges on coercion. Initially in 2005, a lower court in Frankfurt found Vogel guilty of using force against Lufthansa, based predominantly on the economic losses the airline had suffered during the campaign, both in terms of lost sales and the costs of acquiring additional bandwidth to soak the protesters’ traffic. Vogel was sentenced to either pay a fine or serve 90 days in jail. However, the next year, a higher court overturned the verdict, finding, “. . . the online demonstration did not constitute a show of force but was intended to influence public opinion.”⁴ Libertad responded to the ruling with a statement that echoed those we have seen from *the electrohippies* and the EDT: “Although it is virtual in nature, the Internet is still a real public space. Wherever dirty deals go down, protests also have to be possible.”⁵

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

action from Lufthansa; the action's intention was to impact public opinion first.

There has been no such precedent-setting case thus far in the US courts. This is in part due to the limited number of arrests resulting from DDoS actions until recently, and such cases very rarely make it to trial. Two individuals were arrested in connection with Anonymous' Operation Chanology DDoS actions against the Church of Scientology in 2007 and 2008. Both cases resulted in guilty pleas.⁶ One, Dmitri Guzner, was sentenced to serve 366 days in federal prison and pay \$37,500 in restitution to the Church of Scientology.⁷ The second, Brian Thomas Mettenbrink, also served a year in prison and was ordered to pay \$20,000 in restitution to the church. Eric J. Rosol, a Wisconsin truck driver, participated in a DDoS action against the Koch Industries website in 2011, running LOIC for approximately 60 seconds.ⁱⁱ He pleaded guilty in December 2013 to one misdemeanor count of accessing a protected computer, and was sentenced two years' probation and ordered to pay \$183,000 in restitution to Koch Industries, a multinational conglomerate which reported revenues of over \$115 billion in 2013.⁸ The Operation Payback DDoS actions resulted in 14 individuals (including one minor) being charged under the CFAA with participating in the DDoS action against PayPal. Each defendant was charged with two felony counts, which could have resulted in up to 15 years in prison and fines of up to \$500,000.⁹ In early December 2013, the PayPal14 struck a deal. Of the 14 individuals charged, 11 pleaded guilty to one felony count of conspiracy and one misdemeanor count of damaging a protected computer, and agreed to pay \$5,600 in restitution to PayPal. Two others from the group pleaded guilty to the misdemeanor only, and were sentenced to 90 days in prison as well as the \$5,600 restitution payment. The final

ⁱⁱAs a result of the collective action Rosol participated in, which was part of a larger protest against the governor of Wisconsin's move to strip public employees of their collective bargaining rights, the Koch Industries website was inaccessible for approximately 15 minutes.

defendant faced a concurrent indictment for charges stemming from another Anonymous action, and was ineligible for the plea deal. Others have been convicted in connection with the action internationally.¹⁰

Potential sentences for DDoS actions in the United States are high compared to other crimes and especially compared to other types of traditionally recognized activist activities. For example, in the United States a sit-in would typically result in charges of trespass, if anything. In the state of Massachusetts, the punishment for criminal trespass is “a fine of not more than one hundred dollars or imprisonment for not more than thirty days or both such fine and imprisonment,”¹¹ substantially lower than the terms agreed to by the PayPal14 deal. Resisting arrest, another typical charge, results in a term of imprisonment of up to “two and one-half years or a fine of not more than five hundred dollars, or both.”¹² DDoS actions are prosecuted under Title 18, Section 1030 (a)(5) of the US Code, otherwise known as the CFAA. DDoS actions, along with other computer crimes, and are classified as fraud. US sentencing guidelines, laid out yearly in the United States Sentencing Commission Guidelines Manual, which are used as recommendations regarding federal cases within the US legal system, contain a series of adjustments that can be applied to a “base offense level” according to a number of factors. The resultant “offense level” is then used to determine the recommended sentence. Particularly relevant to the case of DDoS actions are those adjustments that involve the amount of financial losses suffered¹³ and the number of victims.¹⁴ PayPal claimed in a British court that the Operation Payback action cost them £3.5 million in losses, or roughly \$5.5 million.¹⁵ That loss figure would add 18 levels to the base offense level for fraud of 7. PayPal did not disclose in court the number of victims it believes was impacted by Operation Payback, but we can assume it was probably higher than 250, which is the maximum listed in the US Sentencing Guidelines, for an additional 6 offense levels, giving us a total offense level of 31. For an individual with no previous criminal record,

the recommended sentence for an offense level of 31 is 135 months, or more than 11 years. This is without the “special skills” or “sophisticated means” adjustments, both of which would add several more offense levels.

A “special skill” is defined by the US Sentencing Guidelines as “a skill not possessed by members of the general public.”¹⁶ “Sophisticated means” is defined as “complex” or “intricate offense conduct pertaining to the execution or concealment of an offense.”¹⁷ Whether or not these enhancements are applied depends heavily on the discretion, and the technical sophistication, of the judge handing down the sentence. To someone with little experience with computers or the internet, directing your web traffic through a proxy may count as “sophisticated means” of concealment, and running an IRC channel or even just running LOIC may constitute a “special skill.” This means that, for now, individuals arrested for crimes involving computers are at particular risk for being sentenced based not on what they actually did, but based on how little the arbiters of justice know. In instances where those individuals know and understand little about the technical specifics of the actions before them, they are more likely to fall back on cultural stereotypes and media depictions to make their judgment. Though internally Anonymous may delight in the bad-boy-hacker and Internet Hate Machine images the media uses to describe them, in a court of law the hacker-as-folk-devil figure makes it more likely that activists, mischief-makers, and even researchers will be treated as dangerous members of a criminal elite.

There are no established requirements for determining the figures for losses or number of victims in these cases. PayPal and the prosecution stated during the UK trial of Christopher Weatherhead that they included the “considerable damage to its reputation and loss of trade” that resulted from the actions in their calculations.ⁱⁱⁱ In Rosol’s case, the \$183,000 figure came

ⁱⁱⁱWeatherhead was sentenced to 18 months’ jail time for his role in Operation Payback, which did not include participating in the actual DDoS actions.

not from the actual financial losses the company reported to the court, which amounted to less than \$5,000. Rather, Koch Industries claimed the DDoS action resulted directly in their hiring a consulting firm to improve their web infrastructure, at a cost of \$183,000.

Because the CFAA is fraud statute, charges filed give plaintiffs the ability to extract restitution from defendants as part of the resulting criminal judgment. This is in addition to the criminal fines described in the sentencing guidelines. In 46 out of the 50 US states, defendants may also be subject to joint and several liability, which means that in the event a plaintiff is found to have been injured by more than one person, the plaintiff can recover all of their damages from one defendant, regardless of that defendant's individual liability. Joint and several liability enables plaintiffs to shift the burden of liability distribution and collection to the defendants, while the plaintiff quickly recovers damages from a single party. Joint and several liability is how Eric Rosol found himself liable for Koch Industries's \$183,000 consulting bill. It is also the reasoning behind Dmitri Guzner's \$37,500 restitution payment to the Church of Scientology, and Brian Thomas Mettenbrink's \$20,000 payment. In these cases, the use of joint and several liability is imposing a devastating and chilling cost on individuals for their participation in a collective action. The line of causality is clear: participate in an act of collective civil disobedience online, and run the risk of being held liable for hundreds of thousands of dollars in damages. Trespass, resisting arrest, or disorderly conduct, charges that most commonly result from on-the-street collective action, are not legally formulated in the United States to result in victims who have the ability to extract damages from a defendant. When used to prosecute activist DDoS actions, the CFAA directly gives the targets of protest the ability to extort payments from activists for their dissent and disruption. When coupled with the innovative reality of online activism, the CFAA literally renders the internet a space where you can

be charged hundreds of thousands of dollars for participating in a collective protest.

The CFAA is a bad law for many reasons, but there are specific aspects to it that make it particularly ill-suited to handle collective online political actions. The lack of oversight in the calculation of damages and the low maximum number of victims mean that the judicial system is predisposed to come down hard on the participants and organizers of these actions. Threats of long prison terms and extreme fines lead to most individuals pleading out before trial, which could delay a precedent-setting court decision such as the Vogel decision in Germany, which could legitimate disruptive civil disobedience online in the United States. “Special skills” and “sophisticated means” sentencing enhancements exacerbate the lack of technical knowledge among members of the judiciary and can easily result in substantially more severe sentences for defendants. Finally, the liability structure created by the CFAA, coupled with joint and several liability, creates a system by which the targets of protest and dissent can impose direct costs for that dissent on activists, creating a massive chilling effect on digital activism as a whole.

GCHQ’s rolling thunder and the (re)militarization of the internet

That DDoS actions are widely considered illegal has not stopped states from using the tactic as a tool of harassment, censorship, or cyberwarfare. In breathtaking displays of hypocrisy, states have been known to target DDoS actions against those groups that have faced prosecution for running their own activist DDoS actions.

In February 2014, journalist Glenn Greenwald and others at NBC released a story based on some of the files released by NSA leaker, Edward Snowden.¹⁸ The story revealed that the

Government Communications Headquarters (GCHQ), the British signals intelligence and information assurance agency, had launched a series of exploit-based DoS actions^{iv} against Anonymous IRC servers and engaged in other attacks against the online resources of hacktivist groups. The operation, known as Rolling Thunder, targeted the IRC channels used by Anonymous with the intention of disrupting communication and potentially scaring away participants. By some estimates, the server disruption lasted for over 30 hours.¹⁹

This is not the first time state forces have explicitly launched “hack back” attacks against digital activists. In September of 1998, the Pentagon responded to an EDT FloodNet action by unleashing a piece of countermeasure code called “Hostile Applet,” which causes any browser running the FloodNet program to crash.²⁰ A *Wired* article quoted a Defense Department spokesperson as saying, “Our support personnel were aware of this planned electronic civil disobedience attack and were able to take appropriate countermeasures. . . . Measures were taken to send the countless demands [from the attacker’s servers] into the great beyond.”²¹ The appropriateness of the Pentagon’s response was questioned at the time. There were questions as to whether the US military should be deploying “cyber-attacks” within the United States even as a “defensive measure,” or against civilians.²² The “hostile applet” was arguably the first use of military-grade “cyberweapons” against civilians, but it comes in a long line of military technology being deployed to control protest and dissent in the US. This history includes the use of barbed wire for human containment in the 1800s, tear gas for crowd control in the 1920s, rubber bullets and beanbag projectiles in the 1970s, and military-grade pepper spray being adopted for regular police use in the 1990s.^v More recently,

^{iv}From the information available at the time of writing, it appears that this was not technically a *distributed* denial of service action, but rather an exploit-based action using a technique called an SYN flood.

^vI am indebted to Professor Anna Feigenbaum of Bournemouth University for explaining this history to me.

the Long Range Acoustic Device (LRAD) sonic weapon was deployed at the 2009 G20 meeting in Pittsburgh, Pennsylvania to control and suppress street demonstrations. The LRAD creates a focused beam of sound that can reach up to 150 decibels, and can cause instant, incapacitating headaches and permanent hearing loss at a range of 100 meters.²³ While the use of military technology like the “hostile applet” to stifle a political protest was hardly new, it signaled an intention on the part of the US Department of Defense to extend the military-style policing of dissent from the streets to the internet.

The revelations about GCHQ’s Rolling Thunder operation have met with strong criticism as well. As Gabriella Coleman wrote in *Wired*, one doesn’t have to agree with the political goals or tactics of Anonymous to conclude that it is a deeply hypocritical abuse of power for states to attempt to disrupt the activities of activists using tactics that the state itself has declare illegal and worthy of prosecution. Coleman writes, “When Anonymous engages in lawbreaking, they are always taking a huge risk in doing so. But with unlimited resources and no oversight, organizations such as the GCHQ (and theoretically the NSA) can do as they please. And it’s this *power differential that makes all the difference*.”²⁴ Coleman points out that the Rolling Thunder denial of service actions disrupted the activities of thousands of Anonymous participants, many of whom were not even involved in the Operation Payback DDoS actions. The GCHQ specifically and intentionally disrupted the rights to speech and assembly of thousands of individuals.

When used by political activists, disruptive tactics like DDoS actions can act as power levelers: they enable activists to funnel media and public attention to unnoticed causes and events, and as direct action tactics DDoS actions allow activists to translate their political speech into an action which demands a response. Disruptive tactics are valuable to those underfunded or unpopular causes that sit outside the mainstream of attention and support. The power to disrupt is vital to the potential of these causes and their supporters

to be influential in the world. GCHQ and the Pentagon don't need the power to disrupt the organizing activities of activists with impunity in order to be influential in the world. By using these tactics, organs of state power such as the GCHQ colonize them, making them less appealing, less useful, and less effective for dissident groups. They alter how the use of those tactics will be received by the media, the public, and the political community.

The use of these tactics, declared illegal for use by any other type of actor, is deliberate. I argue that the use of these tactics in the name of law enforcement and national security is a deliberate move to extend the Hobbesian state monopoly on force to include code that states see as "offensive" or "weaponized." This could include DDoS tools, DoS exploits such as the SYN flood used by the GCHQ, scripts to scrape large amounts of data from a website or server, or any other chunk of code that could be used for a disruptive, destructive, or perhaps simply nontraditional purpose. As more bits of code and uses of technology can be removed from the public domain and monopolized by the state as part of its war-fighting domain stable, online actions that were previously innocuous, irritating or even criminal can be reclassified as the tools and tactics of war. The internet can be progressively classified as a valid war-making space, or even as an active battlefield. Where *the electrohippies*, in their worst case scenario, saw a creeping marketplace mind-frame ready to transform the internet into a capitalistic wonderland, the use of SYN flood DoS actions by the GCHQ, and the Pentagon's "Hostile Applet" before that, could portend the establishment of a semipermanent state of cyberwar, with any potentially disruptive code held by states as monopolized "cyberweapons." A state of active cyberwarfare existing anywhere on the network could substantially increase levels of surveillance, while expansive definitions of what counts as "weaponized code" or "cyberweapons" could result in the widespread classification of civilians as "cyberterrorists" or enemy combatants.

The internet as melded commercial/military space

The dual forces of commercialization and the defense interests of states have combined to foster an online environment that is increasingly hostile to innovative or disruptive modes of political engagement and dissent. State security and commerce have become blended concerns, each supporting the other both in furtherance of their goals and in the construction of their mutual enemies. Anna Feigenbaum has traced what she calls an “elision . . . in which social welfare and the protection of commerce become joint enterprises—solvable only through integrated alliances between government and business.”²⁵ This elision of goals also combines means and targets: “. . . the conflation of cybercriminals and cyberterrorists works to legitimate forms of surveillance, policing and prosecution that infringe individuals’ civil liberties and apply terrorism legislation against a wide range of the population, particularly political protesters.”²⁶ Feigenbaum goes on to note examples of corporate executives, such as Sony’s Kaz Hirai, offering a view of the world which conflates crimes against individuals and actions which rock the infrastructural stability that online commerce relies on. “Under this logic,” Feigenbaum concludes, “the anti-capitalist protester can be easily understood as a criminal, and at times, a ‘domestic extremist’ or ‘domestic terrorist’ . . .”²⁷

Beyond the ways in which corporate and state security interests have been conflated lies the very real manner in which corporations and other commercial entities have taken a strong, some might say primary role, in governing the online space, both through influence over traditional, state level regulatory agencies and multinational organizations and agreements, but also through direct, “ground level” tools such as terms of service user agreements and more subtle choices at the levels of code and interface design. Because of this, many corporations, most

of which provide services that are “invisible” to the user, such as content delivery networks, operate as de facto governance entities in the online space. But these are not governance entities for which the public’s rights of participation, protest, or dissent are fully legally or even culturally established. Rather, it would appear that the online space is being or has already been abdicated to a capitalist-commercial governance structure, which happily merges the interests of corporate capitalism with those of the post-9/11 security state while eliding democratic values of political participation and protest, all in the name of “stability.” The manner in which the public may engage discursively, productively, and politically with entities that disclaim status as governmental entities yet whose actions and policies clearly have distinct governmental impact in the online space has not yet been settled. We are left with a collection of corporately structured governmental entities that cannot be meaningfully talked to, using the language of a discursive democracy.

Some can hardly be talked to at all. As an example, in the summer of 2011 Google rolled out a “real name policy” on Google+, a social network deeply embedded in the constellation of Google products, and in July 2011 began suspending accounts that did not use (or did not appear to use) legal names. This caused widespread criticism over Google’s seemingly arbitrary decisions as to what constituted a “real” name, and their apparent refusal to consider the reasons why people may not want to use their legal names on public social networking services, including reasons of privacy and personal safety.²⁸ However, Google didn’t (and still doesn’t) have an “ombudsman” or “community manager”-type individual to whom users could reach out with their concerns or negative experiences. Google waited till October 2011 to announce that it would begin supporting pseudonyms.²⁹ However, at this time, the Google+ “Create Your Google+ Profile Name” page, as of February 2014, still states, **“First and last name required:** You need to provide both your first and last name for your Google+ profile so it’ll help you find people and enable people to find

you. Using only one name is not permitted,” and requires users who use mononyms to go through a lengthy appeals process.³⁰ Despite crows of victory³¹ from groups like the EFF at Google’s October 2011 announcement, it is far from clear that Google has reconsidered their stance on real names or seriously considered the concerns of those who objected to the policy. By not meaningfully adjusting their policy in the face of reasonable and well-founded criticism, or even fully following through on a pledge that they would, Google demonstrates the unaccountable nature of the influence they wield in the online space and over the actions and abilities of those individuals who spend time there.

This has left us with a catch-22. There are no meaningfully accessible democratic channels through which to communicate dissent or protest to these entities, as they have functionally used the structures of corporate capitalism to opt out of the processes of discursive democracy. But attempts to express dissent and protest through disruptive activism or other innovative digitally based tactics are attacked as not belonging to the stable of popularly acceptable protest tactics, or condemned as criminal or terroristic departures from democracy. The functional advantage of a DDoS in this de-democratized context lies in how it serves a translation function, turning the democratic language of a collective action into the loss/gain, signal/silence, on/off language of these techno-capitalist governance entities.

The avatar nature of online brand presence

DDoS actions expand potential modes of interaction between individuals or groups of individuals, and techno-capitalist corporations. Corporate websites allow for a symbolic and actual centralizing of the normally distributed brand reality of a corporate entity. Just as a corporate headquarters acts as the physical-world manifestation of a corporation’s brand

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

As holistic representations of corporate entities, websites are high value brand manifestations. As such, interference or disruption of predictable continuity can provoke a response that other activist tactics are unlikely to elicit. By imbuing corporate websites and digital, branded storefronts with the symbolic selfhood of avatars, corporations have effectively reduced their public resilience to be equal only to the resilience of that website. Downtime, instability, or even poor design can lead to a poor public opinion of the company itself. The symbolic investment of corporate selfhood in these online presences should not be interpreted as either reducing the ability of the corporation to exploit other lines of public communication (through spokespeople, press conferences, etc.) or as permission to reduce the actual and legal vulnerability of such corporate avatars to disruption and disparagement, either through DDoS actions, parody, satire, or appropriation. Mickey Mouse may be precious to Disney, but (for now, at

least) he can still be used as a tool of derision against his parent company. Any crack in that digital facade requires immediate attention, as it has the potential to reflect on the entire corporation, not just one part. In its pre-internet, distributed incarnation, any number of slights, insults, or disruptions could have gone unremarked upon. But as a website now can be the manifestation of an entire corporate entity or brand, continuity disruptions cannot be disregarded. Again, this necessity-of-response empowers activists by acting as a forcing function with regard to the responses of corporations. Rather than having to wait and hope that corporations will respond to an activist action, with the very likely result that the action will simply be ignored, offenses to the sanctity of the digital brand representation come too close to disrupting the image of corporate continuity and stability to be ignored. By virtue of the symbolic value they have invested in the digital brand representation, corporate entities have obligated themselves to engage with the public disruption, thus providing activists with a trigger point, provoking a public response.

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

In the face of this, the question arises: why go for the symbolic disruption of a corporate homepage when core systems, such as PayPal's payment processing systems might have been disrupted instead? This response echoes the critiques of the CAE, namely that attention-oriented activism, or activism which aims to influence media and public opinion first, is not as effective as direct action models. This criticism, however, does not consider that there may be multiple, equally viable goals to an activist DDoS campaign, and that not all goals

are equally served by simple, covert disruption. If the goal is to publicize, say, PayPal's participation in Wikileaks Banking Blockade, disrupting their payment processing system does little to further that goal. This goal is markedly different than attempting to disrupt the internal operations of an already high-profile event like the WTO. Within an analysis of a disruptive action, the nuances of what is disrupted and how are relevant. In some cases, it is more useful to disrupt an image, while in others it is more useful to disrupt a process.

Notes

- 1 DJNZ/electrohippies, "Client-side Distributed Denial-of-Service."
- 2 Dorothy Denning, "Prepared Statement of Dorothy E. Denning Georgetown University Before the House Armed Services Committee Oversight Panel on Terrorism," *Federal News Service*, May 23, 2000. LexisNexis.
- 3 Denning, "Prepared Statement."
- 4 "Higher Regional Court says online demonstration is not force," Heise Online, June 2, 2006. Originally published at <http://www.heise.de/english/newsticker/news/73827>, currently Archived at <http://post.thing.net/node/1370>. Last accessed February 27, 2014.
- 5 Hans-Peter Kartenberg, quoted in *Heise Online*, "Higher Regional Court."
- 6 Dan Goodin, "US teen admits to 'Anonymous' DDoS attack on Scientology," *The Register*, October 17, 2008. Last accessed February 27, 2014, http://www.theregister.co.uk/2008/10/17/scientology_DDoS_guilty_plea/; John Leyden, "Second man jailed over Scientology DDoS attacks," *The Register*, May 25, 2010. Last accessed February 27, 2014, http://www.theregister.co.uk/2010/05/25/second_scientology_DDoSer_jailed/.
- 7 Associated Press, "Dmitriy Guzner: Teen Sentenced in Scientology Cyber Attack," *Huffington Post*, November

- 18, 2009. Last accessed February 27, 2014, http://www.huffingtonpost.com/2009/11/18/dmitriy-guzner-teen-sente_n_362713.html.
- 8 Ryan J. Reilly, "Loading Koch Industries Website Too Many Times In 1 Minute Just Cost This Truck Driver \$183,000," *Huffington Post*, December 2, 2013. Last accessed February 2014, http://www.huffingtonpost.com/2013/12/02/anonymous-koch-attack_n_4374365.html.
- 9 Curt Hopkins, "Anonymous to show up in person for 'PayPal 14' trial," *The Daily Dot*, February 28, 2013. Last accessed February 27, 2014, <http://www.dailydot.com/news/anonymous-rally-paypal-14-court-trial/>.
- 10 Chloe Albanesius, "Anonymous Hacker Gets 14 Months for PayPal, MasterCard Attacks," *PC Magazine*, January 24, 2013. Last accessed February 27, 2014, <http://www.pcmag.com/article2/0,2817,2414674,00.asp>.
- 11 Massachusetts General Laws, Part IV, Title 1, Chapter 266, Section 120: "Entry upon private property after being forbidden as trespass; prima facie evidence; penalties; arrests; tenants or occupants excepted. Retrieved from <http://www.malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter266/Section120>.
- 12 Massachusetts General Laws, Part IV, Title 1, Chapter 268, Section 32B: "Resisting arrest." Retrieved from <http://www.malegislature.gov/Laws/GeneralLaws/PartIV/TitleI/Chapter268/Section32b>.
- 13 United States Sentencing Commission Guidelines Manual, 2B1.1.b.1, (2012).
- 14 United States Sentencing Commission Guidelines Manual, 2B1.1.b.2 A-C, (2012).
- 15 Sandra Laville, "Anonymous cyber-attack cost PayPal £3.5m, court told," *The Guardian*, November 22, 2012. Last accessed February 27, 2014, <http://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court>.
- 16 US Sentences Commission Guidelines, 354.
- 17 *Ibid.*, 94.
- 18 Mark Schone, Richard Esposito, Matthew Cole, and Glenn Greenwald. "War on Anonymous: British Spies Attacked

- Hackers, Snowden Docs Show,” *NBC News*, February 4, 2014. Last accessed February 27, 2014, <http://www.nbcnews.com/news/investigations/war-anonymous-british-spies-attacked-hackers-snowden-docs-show-n21361>.
- 19 Schone et al., “War on Anonymous.”
- 20 Meikle, *FutureActive*, 153.
- 21 Niall McKay, “Pentagon Deflects Web Assault,” *WIRED*, September 10, 1998. Last accessed February 27, 2014, <http://www.wired.com/politics/law/news/1998/09/14931>.
- 22 Meikle, *FutureActive*, 154.
- 23 “The future of crowd control,” *The Economist*, December 2, 2004. Last accessed February 27, 2014, <http://www.economist.com/node/3423036>.
- 24 Gabriella Coleman, “The New Snowden Revelation Is Dangerous for Anonymous—And For All of US,” *WIRED*, February 4, 2014. Last accessed February 27, 2014, <http://www.wired.com/opinion/2014/02/comes-around-goes-around-latest-snowden-revelation-isnt-just-dangerous-anonymous-us/>.
- 25 Anna Feigenbaum, “Security for Sale! The visual rhetoric of marketing counter-terrorism technologies,” *The Poster 2* (2011): 85.
- 26 Feigenbaum, “Security for Sale!” 85.
- 27 *Ibid.*, 86.
- 28 For an overview of the Nymwars, Eva Galperin’s article, “2011 in Review: Nymwars,” provides an excellent, well-linked starting place, available at <https://www.eff.org/deeplinks/2011/12/2011-review-nymwars>.
- 29 Greg Finn, “Google+ To Allow Pseudonyms & Will Support Google Apps Accounts,” *Search Engine Land*, October 20, 2011. Last accessed February 27, 2014, <http://searchengineland.com/google-to-allow-pseudonyms-will-support-google-apps-accounts-97825>.
- 30 “Create your Google+ profile name,” 2014. Last accessed February 27, 2014, <https://support.google.com/plus/answer/1228271?hl=en>.

- 31 Eva Galperin, and Jillian, C. York, "Victory! Google Surrenders in the Nymwars," *Electronic Frontier Foundation Deep Links Blog*, October 19, 2011. Last accessed February 27, 2014, <https://www.eff.org/deeplinks/2011/10/victory-google-surrenders-nymwars>.