Towards a New Framework for the Ethical Analysis of Activist DDOS Actions

Molly Sauter
Comparative Media Studies/MIT

Introduction to Civic Media/Costanza-Chock
December 12, 2012
Final Paper

INTRODUCTION

Though distributed denial of service attacks have been used as a tool of digital activism for the past two decades, the past few years has seen an explosion in the popularization of the tactic and a sharp increase in the attention its use attracts from the media and state actors. All this attention has brought with it loud criticism from various stakeholders in the digital space, including other digital activists. However, both the tactic's critics and defenders seek to declare the tactic as a whole good or bad, without a nuanced understanding of the variety of circumstances and contexts that can render the tactic's use ethical or unethical. In this paper, I aim to lay down the preliminaries for a framework by which to perform an ethical analysis of activist DDOS actions in individual use contexts.

I begin by providing some brief technical background on how a DDOS action is carried out, as well as how it is viewed legally by different state actors. Then I address the three dominant lines of criticism that are often trained against activist DDOS actions: that they are the equivalent of censorship, that as symbolic activism they are not as effective as direct action, and that they have unfocused success conditions. In the next section I lay out three aspects of the proposed ethical framework, providing historical examples to clarify the use of the tactic and its analysis within the framework. I end by proposing other factors that could be incorporated into the analytical framework and how the framework might be adapted from a reflective model to a prescriptive model for use by organizers in the development of future actions.

BRIEF TECHNICAL NOTE

A denial of service attack seeks to render a server unavailable to legitimate use or users. This can be achieved by one individual via an exploit or other attack, or by many people attacking the target server at once. This is then termed a distributed denial of service (DDOS) attack. In a DDOS attack, the methodology may be as simple as many people refreshing a targeted website repeatedly, or the power of the participants may be augmented with traffic multipliers, botnets, exploit scripts, or other tools. A technologically augmented DDOS typically exploits the concept of "inefficient computing," tying up the servers resources with process-intensive requests until traffic is slowed or the server crashes altogether. Different types of "services" can be "denied," as well. A mail-bomb attack focuses on email servers, causing legitimate emails to bounce. An attack can monopolized the lines connecting a target to the rest of the internet, or focus on processes within the server, like search functions" to crash the site. (Zuckerman et al. 2010) The use of these tools and tactics, particularly the use of volunteer and non-volunteer botnets, and their implications for the ethics of activist DDOS actions, will be addressed later in this paper.

A DDOS attack is a difficult thing to defend against, and can present a drain on a target's financial, as well as their computational, resources. Blocking traffic at the IP level is an option, but practices such as IP spoofing can render this defense ineffectual. Moreover, if the number of participants is high enough, it may be difficult to discern legitimate traffic from illegitimate traffic. Often the easiest available defense is to simply acquire extra servers to soak the additional traffic, but this route is often expensive and available only to large corporations who can afford it. Smaller sites can be driven offline, not by DDOS attacks themselves, but by the sudden high bandwidth costs or ISPs unwilling to stomach the continued risk of DDOS attacks (Zuckerman, et al. 2010).

DDOS attacks are illegal in most, but not all, jurisdictions. Such actions are prosecuted, in the US, under Title 10, Section 1030 of the US Code. Technically considered a type of computer fraud, the crime is described as the "intentional…damage" of "protected computers," which the statute broadly defines as computers used, in whole or in part, by financial institutions or the US government[1]. In a case resulting from an activist DDOS action against Lufthansa

[1] This section, known as the Computer Fraud and Abuse Act, forbids

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

A "protected computer" is defined in Title 18, Section 1030 (e)(2) as

> a computer— (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication, including a computer located

Airlines that will be examined in greater detail later in this paper, a German court found that DDOS actions were a valid form of political protest, finding "…the online demonstration did not constitute a show of force but was intended to influence public opinion" (Dominguez 2009). The discrepancies in the responses of states and corporations internationally mean that organizers bear an ethical responsibility to their participants to provide correct and timely information on the legal risks participation in DDOS actions would incur, something that unfortunately does not always occur.

CRITICISM OF DDOS ACTIONS WITHIN DIGITAL ACTIVISM

The use of DDOS as an activist tactic has come under intense criticism from several sides. Hacktivist groups, such as the Cult of the Dead Cow and Hacktivismo, have denounced DDOS actions as censorship. Jordan and Taylor (2004) have classified this as the "digitally correct" view, wherein the integrity of the network and the right of individuals to an unfettered flow of information take precedence over the political ideals of activism and civil disobedience present in activist DDOS actions. Ruffin and other hacktivists like him considered the primary goal of hacktivsm to be defeating censorship and the disruption of communications online via the creation and distribution of tools to evade censorious regimes (Jordan and Taylor 2004, Raley 2009). Writing in response to

> outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

the electrohippies DDOS actions against the World Trade Organization in 1999, Oxblood Ruffin, a prominent member of the Cult of the Dead Cow, wrote, "No rationale, even in the service of the highest ideals, makes [DDOS attacks] anything other than what they are—illegal, unethical, and uncivil. One does not make a better point in an public forum by shouting down one's opponent" (Ruffin quoted in Koerner, 2000).

In the essay, "Electronic Civil Disobedience" (Critical Art Ensemble 1996), the Critical Art Ensemble, a performance art and activist group active in the United States and Europe, posited an evolution on the traditional, physical world model of civil disobedience. As systems of power migrated from the brick and mortar infrastructure of physical buildings to reside primarily as data constructs on the internet, the CAE argued, so too must systems of resistance and protest. Electronic civil disobedience as conceived of by the CAE sought to translate the philosophies of disruptive protest from the physical world to the networked world via a system of small, semi autonomous cells of specialized practitioners, each performing a specific action or role within a larger organization, while simultaneously maintaining individual identities within the larger group (Critical Art Ensemble, 1996). Central to the CAE's vision was the clandestine and essentially closed nature of the actions, an aspect the CAE terms an "inversion" of traditional civil disobedience (CAE 2001). This sprang from a belief that electronic civil disobedience "is an underground activity that should be kept out of the public/popular sphere (as in the hacker tradition) and the eye of the media…"

because "…there is no corporate of government agency that is not fully prepared to do battle in the media" (CAE 2001). The CAE criticized the actions of groups like the Electronic Disturbance Theater (a spin-off from the CAE) and others for engaging in public, spectacle-oriented "simulated" actions over "clandestine policy subversion" and direct action.

Oxblood Ruffin and the CAE crystallize two major lines of criticism levied against the use of DDOS as an activist tactic: that its use is little more than censorship, and that its use as a tool of media manipulation is ineffective and counterproductive when compared with direct action and similar action-oriented tactics. Though both these criticisms are often made of the tactic in general, they often do not apply to the ways in which the tactic is used in practice. Drawing an equivalency between the actions of private, non-state actors and censorship, traditionally conceived of as a state-mediated action, opens up questions about what entities are capable of performing censorship, particularly in the online space. While DDOS is undoubtedly a "disruptive" tactic (Costanza-Chock, 2001), does disruption always equal a denial of someone's speech rights? Later we will examine examples of DDOS actions where I argue that though certain aspects of an organization's data presence were disrupted, their ability to engage in public speech was not disrupted, causing the censorship conception to fall flat. However, in some instances the criticism is appropriate, most often when the tactic is targeted against organizations that operate primarily online, such as stand-alone blogs, file-sharing sites, or ISPs.

The CAE's criticism of DDOS as a tactic of spectacle in opposition to a tactic of direct action turns out to be simplistic and a-historical. *the electrohippies'* 1999 WTO action directly engages with the practices of direct action, as did the etoy toywar action. Where the use of DDOS as a tactic of direct action becomes problematic is when the change sought is the removal of information from the network. Examples of this type of action will be examined later in this paper. The CAE's conception of DDOS also lifts the tactic out of the context of larger actions or campaigns it might be associated with. As I argue later in this paper, it is important to consider the tactic in context. The validity of the tactic is equally dependent on the activist structure that surrounds it as any qualities inherent in itself. Moreover, DDOS actions were not primarily conceived of as stand-alone actions. EDT member Stephen Wray notes "we are likely to see a proliferation of hybridized actions that involve a multiplicity of tactics, combining actions on the street and actions in cyberspace" (Wray quoted in Raley, 2009). To divest DDOS of its "component" nature (Raley 2009) is to place on its shoulders a weight of ontological justification that no tactic alone could bear.

A third common criticism of DDOS activist actions is the question of measures of success. While I separate internally-generated measures of success from external judgments of ethical validity, it is an issue worth briefly addressing here. At a technological level, it is becoming more and more difficult for volunteer-based DDOS action to cause any downtime on major corporate sites. It would be virtually impossible for such an action to crash a site without technological augmentation. Even in the early 2000s, the FloodNet powered DDOS actions run by the EDT rarely resulted in downtime (Wray 1998). So if denial-of-service caused by server downtime is an unlikely result of an activist DDOS action, what then is an appropriate measure of the success of any given action? In this, the CAE's criticism of DDOS actions as symbolic and simulated reverses to become its virtue. Worth considering are the value of tactics used within a broader action to focus attention and impart biographical impact by expanding opportunities for engagement and participation, what Foucalt termed the "plurality of resistances," each a provocation with not-necessarily-certain desired result (Foucault quoted in Raley 2009). Ricardo Dominguez termed this phenomenon "permanent cultural resistance; there is no endgame" (Dominguez quoted in Raley 2009). The value of this symbolic resistance is not necessarily in its overt effect on the system it ostensibly targets, but rather in its effects on its participants and on the reflective fields that surround it as it occurs, including media and culture. Particularly in its value as tool of biographical impact, DDOS acts tool for the revelation of "hidden transcripts" of resistance (Scott 1990). This is particularly apparent in the case of the Anonymous Operation Payback, wherein the vast majority of the actions and organization took place online among individuals who had not met in the physical world. As a tactic whose strength is in the digitized power of a crowd, the DDOS serves as an open action wherein individual participants "recognize the full extent to which their claims, their dreams, their anger is shared by other subordinates with whom they have not been in direct touch" (Scott 1990). This is a quality which will become increasingly valuable as digital activism continues to be unbounded by state borders and moves towards a transnational operational norm.

OUTLINE OF ETHICAL FRAMEWORK

The purpose of this ethical framework is to provide a basis for the analysis of DDOS actions that have already occurred. The framework considers the use of the tactic within broader campaigns, taking into account activists' motivations for using the tactic, the intended and actual effects achieved, and the technological capacities used. Taken together, these factors create a holistic, qualitative system for evaluating the ethical validity of a given DDOS action, and can be used to create models to guide the use of the tactic, and similarly disruptive tools of digital activism in the future.

INTENDED EFFECTS AND ACTUAL EFFECTS

As mentioned above, DDOS actions have historically been characterized as being little more than crowdsourced censorship, a sort of digitized heckler's veto. This characterization, certainly appropriate in some cases, such as those instances of state-initiated DDOS attacks against independent media sites analyzed by Ethan Zuckerman and others (2010), is easily and inappropriately generalized to the use of the tactic as a whole. This often occurs because identical technological ends states (such as a site being slowed or going down entirely) can be arrived at by different actors with dramatically different motivations, which are not necessarily immediately evident. This motivation-myopia is exacerbated by the absence in US law of any useful analysis of motive in the determination of the criminality of a DDOS action. A DDOS attack launched to extort money from a site operator is considered legally equivalent to an activist action against a large corporate site for the purpose of drawing attention to an issue. However, when attempting an ethical classification of these acts, it is vital to take into account both the *intended effects* of an action, and the *actual effects* of the action. To illustrate this point, I will examine three different actions that particularly highlight this analytical factor: the 1997 IGC/*Euskal Herria* action, the etoy toywar action in 2000, and the 2001 EDT action against Lufthansa Airlines previously mentioned.

IGC/EUSKAL HERRIA ACTION

Ruffin's censorship accusation is correct when the goal of a DDOS action is to permanently render inaccessible speech on the internet that has no other outlet. One such example is the popular DDOS action launched in Spain against the internet service provider IGC in 1997. The stated goal of the action, initiated and led by persons at this point unknown to this author, was to force IGC to stop hosting the Basque publication *Euskal Herria Journal* (Nicol). This was a populist minded action; at one point, the major Spanish newspaper *El Pais* threw its support behind the mailbombing campaign and published target email addressed for the IGC, though it later retracted its support and removed the emails from its website (Gor 1997). The campaign included network level attacks and email-bombs, eventually rendering inaccessible the websites and email of IGC's over 13,000 subscribers. In the interest of continuing to provide service to its other subscribers, many of which were also minority political publications, IGC was forced to stop providing hosting to *Euskal Herria Journal*, though it did so under protest (IGC 1997).

As an ISP, IGC exists primarily, if not entirely, online. Removing IGC's ability to be present online removes its raison d'être and its ability to function as a corporation. A DDOS attack on IGC strikes a violent blow to the core of the organization directly. Furthermore, the stress placed on the IGC network crippled the entire IGC apparatus. System outages affected more than just the *Euskal Herria Journal*'s site, and the email-bombing campaign hampered the communications of all who used the IGC's mailservers. The levels of collateral damage at the level of basic communications were high.

The goal of the action against IGC was to force the removal of the *Euskal Herria Journal* website from its servers. This was an objection to content being available on the internet. For as long as it was successfully running, the DDOS action rendered that content unavailable. So, in *actual effect*, the action caused the *intended effect*. The goal of the DDOS action, and the surrounding campaign was the permanent imposition of its immediate effects.

EDT/LUFTHANSA ACTION

Not all disruptions of content are equivalent to the silencing of speech, however. This is particularly true when the intent of an action is to change something not wholly present on the internet, such as the behavior of a large, multi-national corporation. In 2001, the EDT launched the "Deportation class" action against Lufthansa Airlines, a coordinated, multi-pronged protest against the German government's use of the airlines' flights to deport immigrants. Using EDT's DDOS tool, FloodNet, some 13,000 people participated in a DDOS action against the airline's homepage, which did experience some downtime over the course of the action (Dominguez). Shortly after the action, which included press releases and physical world actions at stockholder meetings, Lufthansa stopped allowing the German government to use its flights to deport immigrants.

The EDT action targeted the website of a major airline. While the site itself was rendered briefly inaccessible, the actual corporation, its ability to fly planes, maintain normal operations, and communicate internally and with the media remained, for practical purposed, unaffected. Unlike the IGC action, which effective prevented the basic functions of business for the organization, this action neither sought nor achieved a fatal disruption in either the airline's normal operations or modes of communicating internally or externally. This type action, which only affects the homepage of an organization that does not primarily exist online, has been described as '[tearing down a poster hung up by the CIA," (Munroe 2011) with the dual implications that the action is technologically simplistic and that whether the site is functioning is often of little importance to the organization targeted. It is a symbolic action rather than a direct action, performed for the benefit of those participating and those watching.

The stated goal of the Lufthansa action was to draw public attention to a specific aspect of the airline's business model, and through the focused attention change the corporation's behavior. Though the DDOS action took place on the internet, the effect it sought was not limited, was not even present in the online space. In and of itself, this DDOS action could not have achieved what the EDT set out to accomplish. It took positive behavior on the part of Lufthansa for the "Deportation class" action to achieve its goals, as opposed to the IGC action, which was designed to accomplish its intended effect by gross fiat.

ETOY/TOYWAR

In December of 1999, the EDT, the Swiss art group etoy, and RTmark launched "The Twelve Days of Christmas" action using the EDT's FloodNet DDOS tool. Their target was the retail site eToys.com, which had filed a lawsuit against the etoy group over the ownership of the URL etoy.com (Wark 2003). As part of the greater toywar campaign, which involved physical world demonstrations, publicity and letter writing campaigns, and a multiplayer online game, the "12 Days of Christmas" campaign was intended, according to Ricardo

Dominguez, to "…represent the present of a global group of people gathered to bear witness to a wrong" (Dominguez quoted in Wark 2003).

While the action may have been intended to symbolically represent the displeasure at the bullying tactics of a large e-commerce corporation, it also had a significant impact on eToys Inc business. Though the e-retailer's site never crashed, it was significantly slowed during the course of the action, rendering it unusable through most of the peak holiday shopping season. Over the course of the campaign, the share price of eToys Inc dropped from $67 to $15, for a net loss of $4.5 billion, which etoy reported as the "most expensive performance in art history" with evident glee (Grether 2000). It is also worth noting that this was a battle between two innovative, internet-centered organizations. etoy, the art group, existed primarily through their electronic projects, experiments, and performances, while eToy Inc was a successful e-commerce retailer, its operational business consisting of little more than an online storefront (etoys.com) and a massive warehouse. As both executed denial-of-service-attacks against each other (eToy Inc via a judicial injunction forcing Network Solutions to remove the etoy.com URL from the internet and etoy via its FloodNet powered DDOS campaign), both aimed their actions at their opponents' core. The toywar campaign, however, enjoyed the support of some 1,700 participants, whose participatory weight added credence to its ethical claims (McKenzie 2001). This judgment is bolstered by the fact that in January of 2000 eToy Inc dropped its lawsuit and paid the court costs of etoy.

CONTEXT WITHIN A GREATER CAMPAIGN

The EDT and other groups have repeatedly termed activist DDOS actions "digital" or "virtual sit-ins" (Auty 2004). This nomenclature is highly evocative, and allows activists to build off the pedagogical and cultural capital of historical physical world sit-ins (Rolfe 2005). However, the metaphor is imperfect, and glosses over many challenges inherent to the digital form, particularly that of proximity to messaging. In a physical world sit-in, the communication of grievances and rational is part and parcel to the art of disruption. This is no air gap between the act of protest and the message of the protest. This is not true in the case of an activist DDOS action. Rather, a user attempting to access a targeted site may have no exposure to the protest's messaging at all and may not even register that an action is taking place. All that is apparent to them is that the site they are looking for is operating poorly or not at all. Though the toywar campaign enjoyed coverage in the mainstream press, including *Wired, The New York Times*, and the Associated Press wire service, coverage of the technological woes of the eToys Inc retail site did not always mention the campaign as a reason for the site's unreliability (McKenzie 2001). Not only does this represent a failed opportunity for the campaign, but it also shifts blame/credit to the target. For this reason, it is incumbent on the organizers of such actions to maintain a high profile messaging campaign in addition to any activist DDOS actions that are taking place, as well as exploring other avenues of digital message distribution that may be spontaneously discovered by the public, such as Google-bombing or typo-squatting.

TECHNOLOGY UTILIZED

As mentioned previously, it is becoming increasingly difficult for a purely volunteer, manual style DDOS action (which require a body in a chair for the duration of the attack and can claim the strongest line of symmetry to physical world sit-ins) to have a noticeable effect on a large, robust corporate website. This is due to advances in technology as well as the vending of DDOS defense services vended to at-risk companies by companies like Akamai and Arbor Networks. This had led to the use of botnets, traffic multipliers, automated attack tools, and other exploits to bring the power of such actions in line with the defenses employed by targets. While the use of such technological tools doesn't automatically negatively affect the validity of an activist DDOS action, the use of non-volunteer botnets is a particularly worrying turn. Volunteer botnets present their own ethical concerns, but are less immediately objectionable.

ANONYMOUS/OPERATION PAYBACK

In the winter of 2010, the controversial online group Anonymous launched Operation Payback, targeting various organizations that had arrayed themselves in opposition to Wikileaks in the wake of the latter's release of a large cache of diplomatic cables exfiltrated from the US State Department. The DDOS action was predominantly powered by the Low Orbit Ion Cannon DDOS tool, which contained functionalities for both "Manual" mode, which required the user to target and fire the tool independently, and "Hive Mind" mode, which allowed the user to join a volunteer botnet, controlled via a central IRC channel. In her 2012 book, Parmy Olson stated that in addition to Low Orbit Ion Cannon, non-volunteer (ie criminal) botnets were employed in the Operation Payback DDOS raids that resulted in the most downtime per target. The use of someone's technological resources without their consent in a political action, particularly one that carries high legal risk, is a grossly unethical action. Moreover it cheapens the participation of the activists who are consensually participating, and makes it easier for critics to dismiss DDOS actions as criminality cloaked as free speech.

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

CONCLUSION

If activist DDOS actions are to continue to be a tool in the repertoire of digital activism, there needs to be a structured method for determining the ethical validity of those actions. This is necessary both for the benefit of organizers considering the use of the tactic, as well as for the legal and political arguments that arise as activists push for the tactic's widespread acceptance and legitimacy.

As the framework continues to develop, additional factors to consider include the role of state and state related actors in this actions, both from the perspective of states as targets of such tactics, but also the roles of semi-state actors, such as patriotic hackers, who use tactics like DDOS in the name of or with the tacit support of states. How does an individual or organization's relationship with the rhetoric of state power affect their activism? Given the ability of online activism to attract a wide variety of participants with varying levels of experience with the risks and practices of political activism, the makeup of the participant and organizer pool must also be considered. Particularly relevant to this discussion are the levels of training, support, and contextual information provided by the organizers, especially in the areas of risk awareness and enabling the informed consent of all participants.

In its current form, this framework only operates as a reflective tool, appropriate for the analysis of actions after they have occurred. However, as more events are analyzed, predictive models can be abstracted which can then be used in the planning of future actions.

In this paper I have reviewed and addressed criticisms of activist DDOS actions that classified the tactics as either censorious or ineffectually symbolic. I have laid out a preliminary framework for the ethical analysis of such activist actions, further illustrated with historical examples of the use of the tactic in the wild. In conclusion, I have posited some additional factors that may be incorporated into the analytical framework, and ways in which the framework may be adapted from a reflective to a prescriptive model.

WORKS CITED

Auty, C. (2004) Political hactivism: tool of the underdog or scourge of cyberspace? *ASLIB Proceedings: New Information Perspectives.* Vol. 56 No. 4.

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

Critical Art Ensemble. (2001) *Digital Resistance: Explorations in Tactical Media*. Autonomedia. Brooklyn, NY.

Costanza-Chock, S. (2003) Mapping the Repertoire of Electronic Contention. *Representing Resistance: Media, Civil Disobedience and the Global Justice Movement*, eds Opel, A.; Pompper, D. Praeger. Greenwood, NJ.

Dominguez, R. (2009) Electronic Civil Disobedience: Inventing the Future of Online Agiprop Theater. *Proceedings of the Modern Language Association of America: Theories and Methodologies*. Vol. 124 No. 5. Pp 1806-1812

Grether, R. (2000) How the etoy Campaign Was Won. *Leonardo*. Vol. 33, No. 4. Pp 321-324

Gor, F. (14 September 1997) Internet y ETA. *El Pais*. http://www.elpais.com/articulo/opinion/ESPANA/PAIS_VASCO/ASOCIACION_DE_USUARIOS_DE_INTERNET_/AUI/EL_PAIS/ETA/HERRI_BATASUNA_/HB/EL_PAIS_/_DEFENSOR_DEL_LECTOR/EL_PAIS_/_EL_PAIS_DIGITAL/elpepiopi/19970914e lpepiopi_11/Tes

Institute for Global Communications. (18 July 1997) Statement on the suspension of the *Euskal Herria Journal* website. Originally published at http://www.igc.org/ehj/, currently mirrored at http://www.elmundo.es/navegante/97/julio/18/igc-ehj-en.html

Jordon T. and Taylor, P. (2004) *Hacktivism and Cyberwar: Rebels with a Cause*. Routledge. New York, NY.

McKenzi, J. (2001) Towards a Sociopoetics of Interface Design. *Strategies*. Vol. 14. No. 1.

Nicol, C. (ND) Internet Censorship Case Study: Euskal Herria Journal. *The APC European Internet Rights Project*. Accessed 1 November 2011. http://europe.rights.apc.org/cases/ehj.html

Olson, P. (2012) *We Are Anonymous*. Little, Brown and Company. New York

Raley, R. *Tactical Media*. (2009) University of Minnesota Press. Minneapolis, MN.

Rolfe, B. (May 2005) Building an Electronic Repertoire of Contention. *Social Movement Studies*. Vol. 4, No. 1, pp 65-74

Ruffin, O. (28 March 2004) cDc, Show and Prove. *Yale Law School Cybercrime and Digital Law Enforcement Conference*. http://www.cultdeadcow.com/cDc_files/cDc- 0384.html

Scott, J.C. (1990) *Domination and the Arts of Resistance*. Yale University Press. New Haven, CT.

Wark, M. (2003, June 19). Toywars. M/C: A Journal of Media and Culture. http://www.media-culture.org.au/0306/02-toywars.php

Wray, S. (1998) Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics. *Switch*. Vol. 4 No. 2

Zuckerman, E.; Roberts, H.; et al. (2010) 2010 Report of Distributed Denial of Service (DDOS) Attacks. *Berkamn Center for Internet and Society Research Publication*. No. 2010-16.