International Review of Law, Computers & Technology, 2014
http://dx.doi.org/10.1080/13600869.2014.870638

Routledge
Taylor & Francis Group

CURRENT DEVELOPMENT

The changing face of protests in the digital age: on occupying cyberspace and Distributed-Denial-of-Services (DDoS) attacks

Argyro P. Karanasiou*

Lecturer in Law, Centre for Intellectual Property, Policy and Management (CIPPM), Business School, Bournemouth University, Bournemouth, UK

(*Received 15 September 2013; accepted 16 October 2013*)

On 7th January 2013 the Anonymous hacking collective launched a White House petition asking the Obama administration to recognize DDoS[1] attacks as a valid form of protest, similar to the Occupy protests. The 'Occupy' movement against financial inequality has become an international protest phenomenon stirring up the debate on the legal responses to acts of civil disobedience. At the same time, online attacks in the form of DDoS are considered by many as the digital counterparts of protesting. While the law generally acknowledges a certain level of protection for protesting as a manifestation of the rights to free speech and free assembly, it is still unclear whether DDoS attacks could qualify as free speech. This paper examines the analogies between offline protests and DDoS attacks, discusses legal responses in both cases and seeks to explore the scope for free speech protection.

Keywords: DDoS; free speech; digital sit-in; anonymous; first amendment

1. Drawing analogies: the metaphor of 'occupying cyberspace' and DDoS attacks

The 2011 massive protests in Europe, the US, Canada and Australia presented us with an unprecedented phenomenon of global protesting activity against financial inequality and wealth disparity. In spite of their different foci, these protests have generally followed a similar pattern of 'sit-in demonstrations': encampments occupying squares and public places gave people the necessary space for deliberation, transfer of knowledge and exchange of ideas. This atmosphere is vividly depicted in the resolutions issued by the delegates of the Occupy Wall Street movement in Zuccotti Park (Shepard 2012):

> By claiming public space for a public purpose, OWS (Occupy Wall Street) has increased the freedom for all of us to take political action. Remaining confrontational but non-violent, OWS has exposed the criminalization of peaceful protest in this city and created a space for all of us to exercise our right to speak up and act up.[2]

Such protests have now been joined by an emergent form of contemporary protesting: online protests. The Internet has been instrumental in the success and outreach of the Occupy protests: online social networking platforms have facilitated discussion and brought together many of the movement's supporters. At the same time, the internet has

*Email: akaranasiou@bournemouth.ac.uk

also provided a new playing field hosting a number of alleged 'digital sit-ins'. Distributed-Denial-of-Service attacks, widely known as DDoS, are believed by many to be one such case of online civil-disobedience (Morozov 2011). A criminal assault in most jurisdictions, DDoS attacks artificially create heavy traffic flow to a website rendering its services temporarily inaccessible. That being said, both DDoS and the 'Occupy' protests operate in a similar manner: occupation is used as a means of getting a message across. In January 2013 the Anonymous hacking collective highlighted this point in their petition to the White House to recognize DDoS as a valid form of protesting. Putting aside their anarchic ideologies, the Anonymous members asked the Government to accept DDoS attacks as acts of protesting and to afford them full protection under the First Amendment:

> With the advance in internet technology, comes new grounds for protesting. Distributed denial-of-service (DDoS), is not any form of hacking in any way. It is the equivalent of repeatedly hitting the refresh button on a webpage. It is, in that way, no different than any 'occupy' protest. Instead of a group of people standing outside a building to occupy the area, they are having their computer occupy a website to slow (or deny) service of that particular website for a short time.[3]

To what extent are DDoS attacks occupying cyberspace, the same way protestors occupy public spaces and squares to promote their causes? This paper will examine whether DDoS are indeed the digital counterpart to sit-ins. It seeks to explore on what grounds – if any – DDoS could qualify as free speech meriting constitutional protection. The repertoire (Tilly 1984) of collective actions gaining new dimensions online is a topic often explored in the field of social sciences[4], yet is somewhat under-discussed with respect to its legal status. With regard to DDoS, law scholars have addressed relevant questions of cybercrime legislation (Edwards 2006; Fafinski 2008), philosophical dimensions (Klang 2004a, 2004b), liability (Kreimer 2001) and democratic engagement (McLaurin 2011); however its constitutional protection as free speech is an area hardly explored in the literature. This paper offers a snapshot of DDoS as 'digital sit-ins': their understanding as a form of online civil disobedience combined further with the viability of a free speech defence will hopefully inform the literature as to this new form of collective action.

In doing so, this paper approaches the issue from three different vantage points: a technical, a philosophical and a legal inquiry seek to explore the nature of DDoS attacks. First the technical aspects of DDoS are briefly examined. Identifying DDoS' main features and functions will contribute towards addressing further the analogy between DDoS attacks and physical protests. While they seem to share similar patterns and features, this by itself would not be enough to justify the legality of DDoS as protected acts of protest. For this purpose, the paper first explores the link between DDoS and civil disobedience. Regarded in isolation, this may be of little significance to a legal evaluation of DDoS; civil disobedience itself embracing the idea of transgressing the law. Next, the paper goes on to evaluate DDoS as acts meriting free speech protection. Ultimately, the paper strives to further provide criteria for the legal definition and understanding of DDoS and to inform the relevant literature.

Relevant case law and legislation is reviewed for this purpose, while a technical overview of DDoS is deemed essential to give a much needed background to the paper. Although a detailed analysis would fall outside the scope of this paper, understanding how DDoS generally occur will help in reviewing whether such attacks can be regarded as the digital equivalent of sit-ins. Next follows a brief account of the main methods employed to orchestrate DDoS attacks as well as their key features.

2. Technical aspects and main features of DDoS attacks

DDoS,[5] short for Distributed-Denial-of-Services attacks, is a proscribed act in most jurisdictions: in the UK it is an offence, under sections 3[6] and 3A[7] of the Computer Misuse Act 1990, while in the US, DDoS are considered a felony under the Computer Fraud and Abuse Act at 18 USC. § 1030. The pervasive manner, in which these attacks operate, explains why DDoS are treated as punishable criminal acts. DDoS operate on the orchestrated actions of users en masse. Distribution is the main feature of this kind of web attacks: An overload of requests for information is sent simultaneously to the web-server under attack from various distributed non-users. To complicate things further, these requests can also be generated automatically by a remotely controlled botnet, namely a coordinated network of software programmes that perform an automated process. In doing so these attacks seek to create false traffic, saturate the network's available resources and to ultimately disrupt its normal function by making it unavailable for its actual users.

There are many techniques to overload a system's server, all of which seem to exploit the net infrastructure and the way in which communication between computers is set out. That being said a detailed account of all possible cases of DDoS would be more suitable for a paper focusing on the taxonomy of DDoS attacks; as such, it would not add to this paper's purpose, which is the legal evaluation of DDoS as forms of protest. One point is worth noting here: regardless of the specific technique used to launch a series of DDoS attacks, their function is based, in the majority of cases, on exploiting the basic elements of the net infrastructure. This observation helps us to identify the main features of the DDoS attacks, which can be summarised in the following three key points.

(1) *Massive participation*
Generating multiple requests to overwhelm the targeted website is a task that normally presupposes massive participation of users synchronising their requests.[8]
(2) *Disruption of communication as a means of getting a message across*
Users participating in DDoS attacks anticipate temporary failure of the targeted website while at the same time also accept the possibility of personal damage.
(3) *Exploitation of the security holes of the server and the net infrastructure Online communication*
relies heavily on mutual trust between peers: interdependent security is a conceptual element of the net architecture, which unfortunately also makes it very vulnerable to hacking.

Since the early documented cases of DDoS attacks, the methods, motives and ideologies supporting them have undergone some major changes: from purely politically driven acts, DDoS are now launched for various reasons, including vigilantism, blackmailing and revenge. Note, for example, the 2013 DNS attack on Spamhaus, described as one of the biggest cyber-attacks in history, affecting millions of users. The escalating attacks against Spamhaus have been attributed to Cyberbunker, a web hosting provider, as retaliation for the latter's inclusion in Spamhaus spammer blacklists. Yet, in spite of a broader course of action and motives, DDoS are still largely characterized by massive participation, disruption of communications and reliance on the net's structural vulnerabilities. Most importantly, these features can be further discussed in the context of civil disobedience: discussing what constitutes an act of civil disobedience and comparing such cases to DDoS could provide useful guidance as to whether they would merit free speech protection.

3. DDoS as an act of civil disobedience? A philosophical inquiry

In one of the first documented cases of DDoS, the Electronic Disturbance Theatre (EDT) attacks against the websites of the White House and the Mexican president Zedillo (Dominguez 2009; Lane 2003) in 1998, a series of automatically generated bad requests were used to block access as a means of protest for paramilitary practices against indigenous people in Chiapas. EDT's co-founder, Ricardo Dominguez, has described these attacks as acts of civil disobedience, equivalent to a digital sit-in. In this respect, he appears to be echoing Rawls' definition of a civil disobedience act being a 'public, non-violent and conscientious act contrary to law ... with the intent to bring about a change in the policies or law of the government' (Rawls 1996). The remainder of this paper critically examines whether this proposition holds any truth.

There has been much debate as to whether DDoS are to be perceived as acts of online civil disobedience or should be approached with scepticism as to their impact and methods. Denning (2001) introduces three main categories of online social movements: activism, 'hacktivism' and 'cyberterrorism'. Whereas online activism is largely a non-violent computer mediated means of protest,[9] 'hacktivism' and 'cyber-terrorism' suggest disruptive and thus illegal uses of computers. Samuel (2004) posits that 'hacktivism' in particular relies on:

> the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development.

As such, 'hacktivism' is found to be consistent with the philosophy of civil disobedience (Manion and Goodrum 2000; Wray 1998), whose acts are illegal by definition and employ non-violent methods to restore the injustices encountered in law.[10] Yochai Benkler has recently described the 'Anonymous' online network group, known for its wide use of DDoS attacks, as

> [A]n idea, a zeitgeist, coupled with a set of social and technical practises. Diffuse and leaderless, its driving force is 'lulz' – irreverence, playfulness, and spectacle. It is also a protest movement, inspiring action both on and off the internet that seeks to contest the abuse of power by governments and corporations and promote transparency in politics and business.

Benkler then goes on to identify four techniques used by the 'Anonymous' hacking collective to launch their attacks -one of which is DDoS- and highlights their non-violent nature. DDoS, he argues:

> causes disruption, not destruction, and the main technique that Anonymous has used requires participants to join self-consciously and publicly, leaving the internet addresses traceable. By design these are sit-ins: Participants illegally occupy the space of their target.[11]

Benkler's view has been met with scepticism. It has been argued[12] that DDoS do not qualify as a form of acceptable civil disobedience for two reasons: the low personal cost assumed by the participants and their operating routine, which is predominantly an attack against data-flow. The relatively easy participation in DDoS attacks, which does not incur any significant personal cost for the participants, takes away the element of a public act, normally met in acts of civil disobedience. In other words, cyber-attacks lack the public quality of normal acts of civil disobedience, since the latter are meant to make a statement through the risk incurred for their participants. This type of online activism by simply contributing

with a few clicks from the safety of one's home fits better the description of 'slacktivism':[13] 'feel good online activism that has zero political or social impact' (Morozov 2010).

3.1. *Low participatory threshold*

The distinction drawn between internet-supported and internet-based action in the Van Laer and Van Aelst's (2010) typology of the 'new digitalized action repertoire' clarifies this point further. The additional criteria of low or high participatory thresholds in these two sets of actions present us with four sets of online collective actions: internet-supported action with low and with high participatory thresholds, and internet-based action with low and with high participatory thresholds.[14] According to the same typology, DDoS are furnishing us with an example of an internet-based action with a low participatory threshold: the often low personal costs entailed, the weak ties noticed between the participants and the adversarial nature of such acts instigated by the 'hacktivism ethics' seem to be key in most DDoS attacks.

DDoS seem to be quite similar yet somehow different from cases of civil disobedience; the latter is, by definition, illegal as it involves overcoming the general duty to obey the law due to its conflict with the Rawlsian 'more stringent obligations' (Rawls 1971). However, the fact that participation in DDoS is facilitated by simply downloading a certain piece of software, without assuming any additional risks or putting in extra efforts to join these attacks, suggests that DDoS are of somewhat inferior rigour to acts of civil disobedience. Even if we accept that the openness and accountability of DDoS attacks[15] suggest that some personal costs might be entailed through participation in such attacks, this would still not be high a sufficiently high threshold to fully equate DDoS with offline cases of civil disobedience.

That being said, participation in DDoS attacks does not presuppose a high level of expertise in hacking techniques (Yar 2006). Take, for example, the Low Orbit Ion Cannon (LOIC) used in the 'Anonymous' DDoS attacks. LOIC is an application developed by hackers that, when activated, renders control of the computer to a central Anonymous Administrator to reload a targeted website, generate a great number of requests and to ultimately overwhelm the website causing it to crash. In a way, this could be described as willingly rendering authorization to a hacker to take control of a computer's network connection. The low risk a LOIC user run is combined with the ease of participating by simply downloading this application. As such, participation in the Anonymous DDoS attacks suggests a lower threshold compared with offline acts of civil disobedience.

3.2. *Disruption of communication*

Another argument put forth to justify free speech protection for DDoS as acts of civil disobedience is that hacking collectives launch these attacks to allegedly 'promote free speech'. Anonymous have often referred to freedom of speech by linking this right to their online activity: while launching a DDoS attack on Warner Bros and IFPI in 2010 after a court decision against Pirate Bay, the group linked their actions to free speech through the following words of warning: 'We will continue to attack websites of those who are a danger to freedom on the internet. We will continue to attack those who embrace censorship'.[16] According to another Anonymous statement, the 'intentions are to change the current way the governments of the world and the people view true Freedom of Speech and The Internet.'[17]

On the other hand many of their launched DDoS attacks target websites that are considered to be promoting internet censorship: in 2009, Anonymous took down the Australian

Prime Minister's site following governmental plans for ISP-level blocking. One year later, Anonymous launched DDoS attacks on Sony for taking legal action against two coders whose tools allowed for Linux to run on the PS3. In 2011, several DDoS attacks were launched on 91 websites of the Malaysian Government as a response to ISP-level denial of access to the WikiLeaks website. The list of documented DDoS attacks for promoting the rights of free speech and access to information online is long.

As Coleman observes (2011), hackers seem to embrace liberal values such as free speech, however their politics are somewhat different from traditional liberalism as they 'are fundamentally grounded in acting through building'. However, whether this link with free speech is sufficient for DDoS to be considered as a digital sit-in akin to the civil rights movement remains to be seen.

4. DDoS as an act of protest meriting free speech protection?

In 1960, four black students entered a Woolworth's department store in Greensboro in North Carolina, USA, and took seats in a whites-only area. The arrest of those participating sparked a series of similar sit-ins. In the end, it was the black community's boycott against Greensboro's department stores and the revenue losses caused by the sit-ins that led to the shop owners changing their segregation policies. Could DDoS be described as acts of civil disobedience along the lines of Greensboro sit-ins?

In the previous section, it was shown that DDoS attacks seem to share some common traits with acts of civil disobedience; however, their technical aspects and participatory standards would not allow for a direct analogy to sit-ins. The remainder of the paper will consider the general argument that such an analogy suggests: DDoS as a protesting act meriting free speech protection. This argument has been used time and again for the legal defence used in cases of arrested hackers involved in DDoS attacks. In September 2011, Jay Leiderman, the defence lawyer of a hacker accused of attacking the computer servers of Santa Cruz County in California, described DDoS as a protest, being 'no different than physically occupying a space'. Suggesting with his defence that DDoS attacks are protected under the First Amendment, Leiderman added that DDoS 'is no different from occupying the Woolworth's lunch counter in the civil rights era'.[18] In a similar vein, following the arrest of the student Mercedes Haefer on July 2011 for being a member of the 'Anonymous group' involved in DDoS attacks, her lawyer regarded this prosecution as political, offering the following analogy: 'When Obama orders supporters to inundate the switchboards of Congress, that's good politics, when a bunch of kids decide to send a political message with roots going back to the civil rights movement and the revolution, it's something else'.[19]

It is of course no coincidence that such an argument has been put forward in the US, where First Amendment protection is frequently sought to avoid the distressing application of the law in such cases as those under review here. The First Amendment doctrine embodies principles that forbid the abridgement not only of speech but also of conduct (Nimmer 1973). In the words of Justice Brennan, conduct may be 'sufficiently imbued with elements of communication to fall within the scope of the First and Fourteenth Amendments'.[20] If the conduct under review is found to convey a political message, it falls within the remit of political speech, and as such it is granted First Amendment protection. This explains the added emphasis in this paper on the legal status of DDoS under the First Amendment and less on its free speech protection in other jurisdictions.

In reviewing DDoS as free speech, the remainder of the paper explores whether the arguments supporting the view that DDoS are akin to sit-ins are strong enough to grant them free speech protection. Next, there follows a discussion of DDoS on the justificatory

basis of expressive conduct, public forum and proportionality. The initial observations in the first part of this paper describing DDoS will now be further utilized to provide for answers.

4.1. *The expressive boycott argument*

The treatment of DDoS as expressive boycotts could provide an argument for granting such acts free speech protection. At first glance, it seems that the main features of DDoS attacks assimilate those of expressive boycott, namely protesting acts of an obstructive nature. Fenwick (1999) suggests that protesting acts can be grouped into the following categories: 'peaceful persuasion, offensive or insulting persuasion, intimidation, symbolic or persuasive physical obstruction or interference, actual physical obstruction or interference, forceful physical obstruction and violence'. DDoS seem to fall under the remit of the fourth category, i.e. the acts could be described as persuasive interference as they seem to be combining both interference, as well as the intention to convey a message through the act. DDoS involve direct action in order to draw public attention to a cause and appear to be both obstructive and persuasive in the sense that they seek to gain publicity and convey a message to the public by overloading a targeted website.

When reviewing acts of persuasive interference, judges are willing to accept any illegalities and to grant free speech protection provided that the act of protest has resorted to obstruction as a means of gaining publicity and getting a message across, which would otherwise have been impossible. The reason for protecting such obstructive acts, as Fenwick explains, is equality. Minorities and marginalised groups, whose causes are often poorly represented in the media, should be granted a certain level of free speech protection even at the expense of the rights of others. Fenwick (2002) reminds us of a few obstructive protesting cases concerning environmental issues, UK in the late 1980s, such as hunting or fishing saboteurs, motorway bypass protesters and those protesting against the supply and sale of veal.

The similarity such acts bear with DDoS is uncanny; in this respect there might be room for manoeuvre in asking for free speech protection on the grounds of equality. However, it would be objectionable to suggest that the hacking groups behind DDoS attacks are marginalized minorities. Anonymous have linked their name with many DDoS attacks: Operation Payback in 2010 and Operation Darknet in 2011 are a few notable examples of their highly diverse online actions. However, they could hardly be described as a marginalized group with no other outlet to communicate their messages: the fact that they feature in the *Time's* list of the 100 most influential people in the world and in the well-attended 'Million Mask March' demonstrations organized on 5 November 2013 in 400 cities in support of Anonymous are strong evidence of a highly popular group.

That being said, the argument of expressive boycott would be particularly attractive in the US, as the relevant case-law there seems to favour free speech protection to allow the disadvantaged minorities in order that their voices be heard. Justice Black has described such a constitutional protection as 'essential to the poorly financed causes of little people'[21] in accepting the right to distribute leaflets door-to-door. In a similar vein, Justice Brennan quoting Justice Black in his dissent in FTC v. Superior Court Trial Lawyers Association, stating that:

> expressive boycotts are irreplaceable as a means of communication because they are essential to the 'poorly financed causes of the little people'. It is no accident that boycotts were used by the American colonists to throw off the British yoke and by the oppressed to assert their civil rights.[22]

The concern for promoting the right to free speech on equal grounds for all, even those with unpopular views, has always been at the heart of the First Amendment. However, limitations are still in place, especially when the level of violence in the protesting acts is disproportionate to the means used. As noted in NAACP v. Clairborne Hardware Co (458 U.S. 916–917):

> The First Amendment does not protect violence . . . . No federal rule of law restricts a State from imposing tort liability for business losses that are caused by violence and by threats of violence. When such conduct occurs in the context of constitutionally protected activity, however, 'precision of regulation' is demanded . . . . Specifically, the presence of activity protected by the First Amendment imposes restraints on the grounds that may give rise to damages liability and on the persons who may be held accountable for those damages.

In the first part of this paper, it has been explained that DDoS incur significant economic losses for the targeted websites and are generally regarded as a highly dangerous threat of cyber security. It can therefore be concluded that the free speech protection on expressive boycotts would not stand much chance under judicial review. On the other hand, the claim that the state has a positive duty in promoting free expression and assembly online on the grounds of preserving an open public forum could be a more convincing proposition. Next, follows a legal evaluation of the public forum argument and the ways this could apply in DDoS.

4.2. *The public forum argument*

4.2.1. *Websites as forums*

The public forum doctrine evoked in a series of convictions of protesters in the civil rights movement of the late 1950s, and the Anti-war movement of the 1970s seems to be a strong argument for considering DDoS as protected speech. Under this doctrine, space is acknowledged as a substantive element of the right to free speech; to exercise this right a forum is required. Mitchell (2003) posits that this may also apply to electronically mediated speech. Hence, in not allowing someone to address an audience effectively in a public forum, the state might be infringing his right to free speech. Of course, this is not to imply that the state carries the absolute obligation to refrain from any regulation of speech and assembly. The levels of scrutiny to which free speech regulations are subject vary depending on the type of forum: traditional public forums, such as parks and streets, entail more restrictions on the way speech and assembly are to be regulated, whereas non-public designated forums and privately-owned property allow for a higher level of speech restriction (Post 1987).

With regard to DDoS, it still remains unclear whether the doctrine of public forum would be deemed sufficient to justify such attacks in spite of the tresspassory nature. Although there has been much debate in the literature as to online spatiality and property (Burk 2000; Epstein 2003; Grimmelmann 2010; Karanasiou 2012), it is generally accepted that a website can be a privately-owned space. This seems to be implied also by Section 3 of the UK Computer Misuse Act 1990,[23] which criminalized all acts of interfering with a computer knowingly without authorization.

Whenever UK jurisprudence is faced with the question of balancing between the rights to assembly and private property, it has always sought an answer to the law of trespass (Clayton 2000). Section 14 of the Public Order Act 1986 is clear on this matter, as it regards as tresspassory assemblies held in privately/semi-privately owned places with restricted or no access for the public. Although the doctrine of public forum is generally recognised in the relevant UK case-law, s.16 of the Public Order Act 1986 defines public

forum in terms of expressed or implied permission for public access. In this respect, one might initially be under the impression that DDoS are actually not unauthorized acts, as the main purpose of a website lies in the very fact of accepting online visitors.

This point has actually been argued by the defendant in DPP v Lennon,[24] the first reported DDoS conviction in the UK concerning a case of mass emails. In this case, the court initially ruled that DDoS were not covered by the Computer Misuse Act, as they were not authorised acts. This was, however, overturned on appeal and resulted in the addition of Sections 33–36 of the Police and Justice Act 2006 to broaden the scope of the Computer Misuse Act so as to include DDoS as well.[25] No implied consent can de deduced 'from the fact that the server has an open as opposed to a restricted configuration'.[26] It is therefore clear that DDoS as a criminally proscribed act suggests trespass and as such it does not qualify for free speech protection in the UK. On a further note, it is likely that DDoS would also not fall within the protective scope of art 10 ECHR. The ECtHR has in certain cases[27] accepted that restrictions of peaceful yet obstructive protests can be disproportionate, yet it is doubtful whether DDoS could be seen as a type of peaceful protest.

On the other side of the Atlantic, open access in the US has been regarded as a main feature of public forums, even when they are privately owned (Kreimer 2001). Take, for example, the cases of protesting in shopping malls, regarded as expressive conduct in quasi-private places. In Robins v Prune Yard Shopping Centre,[28] the California Supreme Court held that shopping malls constituted an invaluable forum for exercising free speech, as they were freely accessible by the public (Epstein 1997). Could DDoS be justified along these lines on the understanding that targeted websites are openly accessible online? The fact that there are cases[29] where the system itself allows for easy access seems to suggest that trespass cannot be easily argued. As shown earlier, the net infrastructure is actually aiding the success of DDoS (Mirkovic and Reiher 2004): the core net principles of trust between peers, distributed control and interdependent security make the internet exploitable to DDoS. However, on its own, the ability to use the system so as to launch such attacks does not suffice justifying DDoS as authorized acts. DDoS are most likely to be reviewed as protests on private forums and, as such, any possible free speech defences are to be sought in this respect.

4.2.2. *Symbolic forums and the rule of law*

Taking a closer look at case law addressing protests on private forums, it appears that First Amendment protection may still be applicable for symbolic reasons. Namely, in cases where public protests occur on certain private properties, which are symbolic and essential for drawing attention to and conveying a message, the First Amendment protects these acts unless there are ample alternatives for gaining wide attention.[30] In this vein, it has been ruled that boycotting,[31] picketing near schools[32] or outside abortion clinics[33] are cases falling within the protective scope of the First Amendment. However, if we are to consider DDoS as an act of civil disobedience, similar to civil rights movements and sit-ins, it should be noted that 'violent conduct is beyond the pale of constitutional protection'.[34] Namely, in cases of civil rights movements, although it is generally recognised that sit-ins are a powerful method of communication and protest[35] – which should not be restricted simply because they occur on private property – such acts do not enjoy absolute free speech protection at the expense of private property.

The sit-in case of Bell v. Maryland offers an interesting analogy to DDoS in this respect. In the times of the racist practices of segregation in places of public accommodation in the American South of the 1960s, 12 students were arrested and charged with criminal trespass

for entering and occupying a 'whites only' eating area at a restaurant in Baltimore. The appellants' position that 'the right of free speech is not circumscribed by the mere fact that it occurs on private property'[36] was not able to convince the Court of Appeals that public protest could not trump the personal autonomy of the proprietor to conduct business by exercising discriminatory practices on this property. As the Court of Appeals noted further, the right 'to speak freely and to make public protest does not impart a right to invade or remain upon the property of private citizens, so long as private citizens retain the right to choose their guests or customers'.[37] The Supreme Court however had a different view, which could perhaps be of use in building a free speech defence for DDoS. In their concurrences, Justices Douglas and Goldberg argued for a right to access public accommodations along the lines of the Fourteenth Amendment guarantees of equal protection. Granting the protestors a right to access, Justice Goldberg further noted that 'the broad acceptance of the public in this and in other restaurants clearly demonstrates that the proprietor's interest in private or unrestricted association is slight.'[38] Could this also be argued in the case of DDoS attacks?

In the previous section it has been shown that DDoS attacks could be considered acts of civil disobedience, whose expressive component is a non-verbal type of symbolic speech. That being said, it has also been contended that the state's duty to secure public order justifies certain restrictions to avoid the breach of peace. Namely, it is generally understood that under no jurisdictions are public protests immune to total restriction, especially when there is danger that a breach of peace will occur. The need for the state to secure public order outweighs the significance of speech on such occasions, even when speech takes place in a public forum. This perception of public order as a value of utmost importance is mostly evident in the UK public protest cases,[39] yet can also be found in US case law[40] in general. Given their disruptive nature and the fact that they target communications per se, it seems unlikely that DDoS are assimilating the Greensboro sit-ins. In Bell, the Supreme Court has been able to reach this decision based on the fact that the protestors peacefully took seats in the restaurant and read their school books when the staff denied services. As there was no danger that a breach of peace might occur, their constitutional right to free speech and assembly still applied and granted them the right to access a place of public accommodation.[41] However, regarding DDoS, it seems that regarding them as a peaceful sit-in would not be an attractive argument due to their pervasive nature.

The Anonymous describe DDoS as a way of overwhelming a server with UDP traffic, which 'does no permanent damage and doesn't involve breaking into services or stealing data'.[42] However, DDoS are indeed a punishable action in most jurisdictions, which can cause serious damage to the targeted website in terms of economic loss: losses in revenue, market capitalisation and consumer confidence are added to the extra cost incurred for developing a robust protective infrastructure to protect the website from future DDoS; a 2012 Neustar report estimated that they cost online retailers an average of $100,000 per hour.[43] Such findings highlight the pervasive and harmful nature of DDoS and thus leave in place ample authority for the proposition that the claim for the right to free speech of those launching DDoS attacks would have a low chance of success in judicial review.

Returning to Bell, Justice Black based his opinion on performing a balancing act between free speech and rule of law, instead of private property. While admitting that petitioners had a constitutional right to express their views, he remarked that this would not yield them a right to 'force other people to supply a platform or a pulpit' (344, 345). He further added that 'whatever power it may allow the States or grant to the Congress to regulate the use of private property, the Constitution does not confer upon any group the right to substitute rule by force for rule of law' (346). In this respect, it would be unlikely that DDoS could be considered as a sit-in protected by the First Amendment.

4.3. *DDoS and the slippery slope of free speech restriction*

The previous sections examined the arguments of expressive boycott and public forum and found that the scope of their application in cases of DDoS attacks is narrow. In addition, free speech protection for DDoS would also be problematic in terms of proportionality. For if we were to declare that DDoS merits constitutional protection as free speech, at the same time we would meet with the most emphatic contradiction: as DDoS is nothing but a tool destined to cause disruption, it has also been frequently associated with attacks on human rights and media sites, resulting in online censorship of their content.

A series of cases reported in recent years of DDoS used as cyber censorship tools show this. In March 2012, the news site Uznews.net in Uzbekistan was reported to be offline due to severe DDoS attacks. A similar case was also reported in 2010 when six human rights organisations suffered DDoS attacks after the airing of controversial video footage exposing human rights abuses. Moreover, the purposes of launching DDoS attacks against a website are not always related to noble causes. In some reported cases DDoS are used as means of pursuing illegal activities, most specifically online extortion: in 2011 a Düsseldorf court convicted a man of hiring the services of a Russian botnet, who blackmailed German bookmaking websites under the threat of DDoS attacks during the World Cup in South Africa.

The reports published by the Berkman Centre for Internet 2010 football and Society at the University of Harvard (Roberts et al. 2011; Zuckerman et al 2010) demonstrate some alarming findings regarding the threatening effects that DDoS might have for online freedom of speech. The study surveyed 317 independent media organisations in nine countries and discovered media reports of 140 DDoS attacks against more than 280 different human rights sites. To sustain such attacks, the targeted sites would have to partly sacrifice their independence and seek protection from giant companies such as Google and Facebook, which are substantial hosting providers who could defend the attacked websites. In the reports, DDoS are described as an increasing 'technique for silencing human rights and independent media sites', posing major internet security challenges.

In this vein, it is further noted that DDoS are not just harmful for the personal autonomy and entrepreneurial activity of the proprietor of the targeted website but they also infringe on his or her right to free speech and on the users' right to online access. As such, not only would DDoS not qualify as free speech but their legal treatment could further involve a positive obligation of the state to guarantee the right to free speech for everyone. This is made explicit by Frank La Rue, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> Given that access to basic commodities such as electricity remains difficult in many developing States, the Special Rapporteur is acutely aware that universal access to the Internet for all individuals worldwide cannot be achieved instantly. However, the Special Rapporteur reminds all States of their **positive obligation** [emphasis added] to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, **including the Internet** [emphasis added].[44]

5. Concluding remarks

The argument that DDoS are the digital equivalent of sit-ins is an attractive one. The fact that such acts largely rely on massive participation (at least in principle) and employ obstructive means to get their message across highlights a similarity with acts of civil disobedience. Carl Kaplan offers a fairly accurate description of DDoS in this respect, placing

this activity 'somewhere between a digital sit-in and "cybotage"', the act of sabotaging computers in a rather aggressive manner. Of course, the similarity to civil disobedience should not be overlooked. In the words of Critical Art Ensemble, a group of hacktivists:

> as in civil disobedience, primary tactics in electronic civil disobedience are trespass and blockage. Exits, entrances, conduits, and other key spaces must be occupied by the contestational [sic] force in order to bring pressure on legitimized institutions engaged in alleged unethical or criminal actions.[45]

However, this cannot further suggest that DDoS merit the free speech protection granted to the civil rights movement protests decades ago. This paper has explored all grounds on which free speech protection for DDoS could be argued. First, their free speech protection as expressive conduct is explored. At first glance, this seems a convincing proposition: in spite of their obstructive nature, such acts may be granted free speech protection to ensure equality of expressive outlets. However, it can hardly be argued that the Anonymous are a marginalized group. Even so, most DDoS attacks result in significant economic losses for the targeted websites, and they seem to be the most destructive of all available means of getting a message across online; the potential of free speech protection on grounds of equality would thus lack proportionality. Their destructive nature has also been key in rejecting any free speech protection on the grounds of securing a public forum. Although it is agreed that the internet is an open communicatory platform, accessible to all to voice their opinion, this does not offer absolute immunity to otherwise proscribed acts. Moreover, the mere fact that DDoS obstruct online communications is enough to preclude free speech protection; on the contrary, positive state action under the First Amendment might be sought against them. It may sometimes be the case that DDoS target websites in order to stifle free speech by blocking access.

That said, the possibility of free speech protection for DDoS cannot be completely ruled out. This paper has considered all possible defences and has theoretically examined their validity. However, there is no such thing as one size fits all. Bearing in mind the variety of methods employed and the main features of DDoS attacks, ambiguity and complexity have hitherto been unavoidable. The arguments provided here should be contextualized and further discussed on an ad hoc basis. At the moment there is a lack of documented cases of judicial review of DDoS on the grounds of free speech protection. However, the increase in volume, duration and frequency of such attacks suggests that it is only a matter of time before such claims are lodged. The paper has kept a clear focus on the US free speech jurisprudence: in the wake of President Obama's 'Improving Critical Infrastructure Cyber-security' executive order, issued in February 2012, combating DDoS is now vital on the grounds of national security. Whether DDoS still fall within the protective scope of the First Amendment remains to be seen, and should be an interesting development.

On balance, the overall picture seems to be that DDoS cannot be considered as the digital parallel to the occurrence of sit-ins in offline reality: the fact that DDoS are proscribed acts of a particularly aggressive nature combined with the threats incurred for free speech online would undercut the feasibility of granting them free speech protection. As a final remark, it should be noted that instead of resorting to misleading metaphors, it is essential to articulate a robust conceptual framework regarding DDoS and other acts of 'hacktivism', which deserves more attention than this paper has been able to give it. To do otherwise would risk criminalising the tools and net architectural principles exploited to facilitate DDoS attacks.

Acknowledgements

I wish to thank Ken Brown (Bournemouth University) and the anonymous reviewers for their valuable comments on previous versions of this paper. Any errors or omissions remain my sole responsibility.

Notes

1. Distributed Denial of Service attacks, thereafter referred to as DDoS
2. Shepard (2012, 125–126).
3. https://petitions.whitehouse.gov/petition/make-distributed-denial-service-ddos-legal-form-protesting/X3drjwZY.
4. For more see Ayres (2003, 132–143); Clark and Themudo (2003, 109–126); Costanza-Schock (2003, 173–191); Diani (2000, 386–401); Garrett (2006, 202–224); Rheingold (1993); Van Laer and Aelst (2010, 1–26); van de Donk et al. (2004).
5. Although this paper examines the case of DDoS, it tends to use DDoS and DoS interchangeably for reasons of simplicity and coherence. It should however be noted that there are certain differences between the two.
6. Added by section 36 of the Police and Justice Act 2006.
7. Which came into force on 1 October 2008.
8. However, it should also be noted that there are other ways to automatically generate multiple requests with the use of botnets controlled by one single person launching the attacks.
9. See also McCaughey and Ayers (2003).
10. For an interesting comparison between the philosophies underpinning civil disobedience and online civil disobedience acts, mostly undertaken by the online collective of electro hippies see Klang (2004a).
11. Y Benkler 'Hacks of Valor: Why Anonymous is Not a Threat to National Security', Foreign Affairs, available online at http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor., accessed 3 May 2013. For a similar view see also Klang (2004b).
12. Tom Watson 'Denial of Service, Denial of Speech', available online at http://tomwatson.typepad.com/tom watson/2010/12/denial-of-service-denial-of-speech.htm, accessed 3 May 2013.
13. See Gladwell and Shirky (2011) arguing that social movements in general are not made possible just by utilising online media. On the other side of this debate, there are also theorists who believe in the great power social media in general have to mobilize the masses and to bring about social change (Castells 2012). For a good account on the relevant debate see Fuchs (2012).
14. An internet-supported action with low participatory threshold is, for example, an online donation, whereas an example of the same action with a high participatory threshold is the organisation of transnational social movements such as the World Social Forum.
15. Note, for example, the electrohippies collective stating that their identities are easily traceable online as they do not use encrypted methods of communication (http://www.iwar.org.uk/hackers/resources/electrohippies-collective/op1.pdf, accessed 3 May 2013).
16. http://anti-ddos.blogspot.co.uk/2010/12/incesed-by-court-decision-to-jail.html, accessed 3 May 2013.
17. http://www.abc.net.au/technology/articles/2010/12/09/3089466.htm, accessed 3 May 2013.
18. R Reilly, ''Homeless Hacker' lawyer: DDOS isn't an attack, it's a digital sit-in', available online at http://web.archive.org/web/20130120090931 at http://idealab.talkingpointsmemo.com/2011/09/homeless-hacker-lawyer-ddos-isnt-an-attack-its-a-digital-sit-in.php, accessed 3 May 2013.
19. M. Masnick, 'Lawyer for accused: DDoS is a legal form of protest', available online at http://www.techdirt.com/articles/20110930/02323316145/lawyer-accused-ddos-is-legal-form-protest.shtml, accessed 3 May 2013.
20. Texas v. Johnson, 491 U.S. (1989).
21. Martin v. City of Struthers, 319 U.S. 141, 146 (1943).
22. FTC v. Superior Court Trial Lawyers Association, 493 U.S. 411, 451 (1990).
23. Added by section 36 of the Police and Justice Act 2006.
24. DPP v Lennon [2005] EWCA Crim 2150.
25. See also Fafinski (2008) 53.

26. DPP v Lennon [2006] EWHC 1201 (Admin), [2006] All ER (D) 147 at [14].
27. Steel and Others v United Kingdom (1998) 28 EHRR 603.
28. 592 P. 2d 341 (Cal. 1979).
29. It has been argued that pure DDoS attacks caused by sending non-malformed standard data packets are not an illegal access to a website but an action allowed by the system itself (http://forum.theregister.co.uk/forum/1/2012/02/08/DDoS_attack_trends, accessed 3 May 2013).
30. Hill v. Colorado, 530 U.S. 703 (2000).
31. NAACP v. Claiborne Hardware Co., 458 U.S. 886 (1982).
32. Police Department v. Mosely, 408 U.S. 92 (1972).
33. Madsen v. Women's Health Center, 512 U.S. 753 (1994).
34. NAACP v. Claiborne Hardware Co., 458 U.S. 886, 933–34 (1982).
35. 'Concerted action is a powerful weapon. History teaches that special dangers are associated with conspiratorial activity. And yet one of the foundations of our society is the right of individuals to combine with other persons in pursuit of a common goal by lawful means.' NAACP v. Claiborne Hardware Co., 458 US 886, 933–34 (1982).
36. Brief for Appellants at 15, Bell v. State, 27 Md. 302, 176 A.2d 771 (1962) (No.91).
37. Bell, 227 Md. At 305, 176 A.2d at 772.
38. Bell, 378 US at 314 (Goldberg J, concurring). See also cf. J Black dissenting: 'And none of our prior cases has held that a person's right to freedom of expression carries with it a right to force a private property owner to furnish his property as a platform to criticize the property owner's use of that property', Bell v. Maryland 378 US 226 (1964) at 325.
39. Feldman (1993, 785).
40. 'A law which primarily regulates conduct but which might also indirectly affect speech can be upheld if the effect on speech is minor in relation to the need for control of the conduct', Justice Black dissenting in Barenblatt v United States 360 US 109, 134 (1959) at 141). See also Brown Shoe Co., Inc. v. United States 383 US 154 (1962).
41. Note, however, Justice Black's warning of the danger of 'government paralysis' carried by the invasion of public buildings for various purposes outside their designated use. Brown v. Louisiana 383 U.S. 131 (1966) at 165.
42. Digital Sit-ins: DDoS is legitimate civil disobedience – Anonymous: We Are Legion, available online at http://anonyops.org/post/16585162289/digital-sit-ins-ddos-is-legitimate-civil-disobedience, accessed 3 May 2013.
43. DDoS Survey: Q1 2012 - When Businesses Go Dark, available online at http://hello.neustar.biz/rs/neustarinc/images/neustar-insights-ddos-attack-survey-q1-2012.pdf, accessed 3 May 2013.
44. Report of the special Rapporteur on the Promotion and protection of the Right to Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/17/27 (2011) at 66.
45. Ensemble (1996, 18).

References

Ayres, J. 2003. "From Streets to the Internet: The Cyber Diffusion of Contention." *The Annals of the American Academy of Political and Social Science* 566 (1): 132–143.

Burk, D. 2000. "The Trouble with Tresspass." *J Small & Emerging Bus. L.* 4: 27.

Castells, M. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge: Polity Press.

Clark, J., and N. Themudo. 2003. "The Age of Protest: Internet-based 'Dot Causes' and the 'Anti-globalization' Movement." In *Globalizing Civic Engagement, Civil Society and Transnational Action*, edited by J. Clark, 109–126. London: Earthscan Pub Ltd.

Clayton, G. 2000. "Reclaiming Public Ground: The Right to Peaceful Assembly." *The Modern Law Rev* 23 (2): 252.

Coleman, G. 2011. "Hacker Politics and Publics." *Public Culture* 23 (3): 514.

Costanza-Schock, S. 2003. "Mapping the Repertoire of Electronic Contention." In *Representing Resistance: Media, Civil Disobedience and the Global Justice Movement*, edited by D. Pompper, and A. Opel, 173–191. London: Praeger.

Denning, D. 2001. "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime and Militancy*, edited by D. Rohnfeld and J. Aquila. Santa Monica: RAND Corporation.

Diani, M. 2000. "Social Movement Networks: Virtual and Real." *Information, Communication and Society* 3 (3): 386–401.
Dominguez, R. 2009. "Electronic Civil Disobedience: Inventing the Future of Online Agitprop Theater." *PMLA Publications of the Modern Language Association of America* 124 (5): 1806–1812.
Edwards, L. 2006. "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies." *Cardozo Arts & Ent L J* 24 (1): 23–62.
Ensemble, Critical Art. 1996. *Electronic Civil Disobedience and Other Unpopular Ideas*. Brooklyn: NY.
Epstein, RA. 1997. "Takings, Exclusivity and Speech: The Legacy of PruneYard v. Robins." *The University of Chicago Law Rev* 64 (1): 21–56.
Epstein, A. 2003. "Cybertrespass." *University of Chicago Law Rev* 70: 73–88.
Fafinski, S. 2008. "Computer Misuse: The Implications of the Police and Justice Act 2006." *Journal of Criminal Law* 72 (1): 53–66.
Feldman, D. 1993. *Civil Liberties and Human Rights in England and Wales*. Oxford: Clarendon. 785.
Fenwick, H. 1999. "The Right to Protest, The Human Rights Act and the Margin of Appreciation." *The Modern Law Rev* 62: 494.
Fenwick, H. 2002. *Civil Liberties and Human Rights*. 3rd ed. London: Cavendish Pub. 427–430.
Fuchs, Christian. 2012. "Some Reflections on Manuel Castell's Book Networks of Outrage and Hope." *tripleC* 10 (2).
Garrett, R. 2006. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication and Society* 9 (2): 202–224.
Gladwell, M., and Clay Shirky. 2011. "From Innovation to Revolution: Do Social Media Make Protests Possible?" *Social Affairs* 90 (2): 153–154.
Grimmelmann, J. 2010. "The Internet is a Semi-Commons." *Fordham L. Rev* 78: 2799–2842.
Karanasiou, A. 2012. "Respecting Context: A New Deal for Free Speech in the Digital Era." *European Journal of Law and Technology* 3 (3).
Klang, M. 2004a. "Civil Disobedience Online." *Journal of Information, Communication & Ethics in Society* 2 (2): 75–83.
Klang, M. 2004b. "Virtual Sit-ins, Civil Disobedience and Cyberterrorism." In *Human Rights in the Digital Age*, edited by M. Klang, and A. Murray. London: Cavendish Publishing.
Kreimer, S. 2001. "Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet." *U. Pa. L. Rev* 150: 119–171.
Lane, J. 2003. "The Digital Zapatistas." *The Drama Review* 47 (2): 129–144.
Manion, M., and A. Goodrum. 2000. "Terrorism of Civil Disobedience: Toward a Hacktivist Ethic." *Computers and Society* 30 (2): 14–19.
McCaughey, M. and M. Ayers. 2003. *Cyberactivism: Online Activism in Theory and Practice*. New York: Routledge.
McLaurin, J. 2011. "Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks." *Yale Law & Policy Rev* 30: 239–246.
Mirkovic, J., and P. Reiher. 2004. "A Taxonomy of DDoS Attack and DDoS Defence Mechanisms." *ACM SIGCOM Computer Communications Review* 34 (2): 40.
Mitchell, D. 2003. "The Liberalization of Free Speech: Or How Protest in Public Space is Silenced." *Stanford Agora: An Online Journal of Legal Perspectives (4)* 1: 1, 2 n 52.
Morozov, E. 2010. *The Net Delusion: How Not to Liberate the World*. London: Allen Lane.
Morozov, E. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs 227–229.
Nimmer, M. 1973. "The Meaning of Symbolic Speech Under the First Amendment." *UCLA L Rev* 21: 29.
Post, R. 1987. "Between Governance Management: The History and Theory of the Public Forum." *UCLA L Rev* 34: 1713.
Rawls, J. 1971. *Theory of Justice*. Massachusetts: Harvard University Press.
Rawls, J. 1996. "Civil Disobedience and the Social Contract." In *Morality and Moral Controversies*, ed. J. Arthur. New Jersey: Prentice Hall College Div 356.
Rheingold, H. 1993. *The Virtual Community: Homesteading on the Electronic Frontier*. Reading MA: Addison-Wesley.

Roberts, H., E. Zuckerman, E. Faris, J. York, and J. Palfrey. 2011. "The Evolving Landscape of Internet Control: A Summary of Our Recent Research and Recommendations." *The Berkman Center for Internet and Society at Harvard University*, August 2011.

Samuel, A. 2004. *Hacktivism and the Future of Political Participation*. Cambridge MA: Harvard University Press.

Shepard, H. 2012. "Labor and Occupy Wall Street: Common Causes and Uneasy Alliances." *The Journal of Labor and Society* 15: 125–126.

Tilly, Ch. 1984. "Social Movements and National Politics." In *Statemaking and Social Movements: Essays in History and Theory*, edited by C. Bright, and S. Harding, 297–317. Ann Arbor, MI: University of Michigan Press.

Van Laer, J., and P. Van Aelst. 2010. "Internet and Social Movement Action Repertoires." *Information, Communication and Society* 1–26: 230–254.

Wray, S. 1998. "On Electronic Civil Disobedience." *Peace Review* 11 (1): 107–111.

Yar, M. 2006. *Cybercrime and Society.* London: Thousand Oaks: Sage Publications Ltd.

Zuckerman, E., H. Roberts, R. McGrady, J. York, and J. Palfrey. 2010. "2010 Report on Distributed Denial of Service (DDoS) Attacks." *The Berkman Center for internet and Society at the Harvard University*, December 2010.