Journal of Information, Communication and Ethics in Society

Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire?

David Douglas, José Jair Santanna, Ricardo de Oliveira Schmidt, Lisandro Zambenedetti Granville, Aiko Pras,

Article information:

To cite this document:
David Douglas, José Jair Santanna, Ricardo de Oliveira Schmidt, Lisandro Zambenedetti Granville, Aiko Pras, (2017) "Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire?", Journal of Information, Communication and Ethics in Society, Vol. 15 Issue: 01,pp. 90-104, doi: 10.1108/JICES-09-2016-0033
Permanent link to this document:
http://dx.doi.org/10.1108/JICES-09-2016-0033

Downloaded on: 11 April 2017, At: 04:01 (PT)

References: this document contains references to 27 other documents.

To copy this document: permissions@emeraldinsight.com

The fulltext of this document has been downloaded 51 times since 2017*

Received 5 September 2016
Revised 7 November 2016
Accepted 7 November 2016

Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire?

David Douglas
Universiteit Twente, Philosophy, Enschede, The Netherlands

José Jair Santanna and Ricardo de Oliveira Schmidt
Department of Electrical Engineering, Mathematics and Computer Science (EWI), Universiteit Twente, Enschede, The Netherlands

Lisandro Zambenedetti Granville
Institute of Informatics, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil, and

Aiko Pras
Department of Electrical Engineering, Mathematics and Computer Science (EWI), Universiteit Twente, Enschede, The Netherlands

Abstract

Purpose – This paper aims to examine whether there are morally defensible reasons for using or operating websites (called 'booters') that offer distributed denial-of-service (DDoS) attacks on a specified target to users for a price. Booters have been linked to some of the most powerful DDoS attacks in recent years.

Design/methodology/approach – The authors identify the various parties associated with booter websites and the means through which booters operate. Then, the authors present and evaluate the two arguments that they claim may be used to justify operating and using booters: that they are a useful tool for testing the ability of networks and servers to handle heavy traffic, and that they may be used to perform DDoS attacks as a form of civil disobedience on the internet.

Findings – The authors argue that the characteristics of existing booters disqualify them from being morally justified as network stress testing tools or as a means of performing civil disobedience. The use of botnets that include systems without the permission of their owners undermines the legitimacy of both justifications. While a booter that does not use any third-party systems without permission might in principle be justified under certain conditions, the authors argue that it is unlikely that any existing booters meet these requirements.

Practical/implications – Law enforcement agencies may use the arguments presented here to justify shutting down the operation of booters, and so reduce the number of DDoS attacks on the internet.

Originality/value – The value of this work is in critically examining the potential justifications for using and operating booter websites and in further exploring the ethical aspects of using DDoS attacks as a form of civil disobedience.

Keywords Internet, IT ethics, Civil disobedience, DDoS attacks, Hacktivism

Paper type Research paper

Journal of Information, Communication and Ethics in Society
Vol. 15 No. 1, 2017
pp. 90-104
© Emerald Publishing Limited
1477-996X
DOI 10.1108/JICES-09-2016-0033

1. Introduction

During the 2014 Christmas holidays, Microsoft and Sony both suffered massive distributed denial-of-service (DDoS) attacks on their games console internet services (Xbox Live and

PSN, respectively) that made them unavailable. It soon emerged that the motivation behind these attacks was not extortion or political protest, but advertising. The attackers, calling themselves "Lizard Squad", announced via Twitter on December 30, 2014 that their Web service "Lizard Stresser", which allowed customers to perform DDoS attacks on a target of their choice for a price, was now open for business (Turton, 2015). This incident is just the highest-profile example of the emergence of *booters*: internet services offering customers the ability to launch DDoS attacks on a target of their choice. They are also referred to as "DDoS-for-hire", "DDoS-as-a-Service" or "network stressers". The global network content delivery provider Akamai (2016) reports that:

> [. . .] most of the mega-attacks [higher than one hundred billion bits per second, which is enough to take the majority of systems on the Internet offline] seemed to use tools common to booters/ stressers.

DDoS attacks are not a new phenomenon and are illegal in most jurisdictions. Despite this, booter operators claim that their services have legitimate uses, such as testing a system or network's ability to handle heavy network traffic, and sometimes refer to their services as "network stressers" to emphasise this purpose (Krebs, 2013b). Plausible justifications have also been presented for regarding some DDoS attacks as examples of public protest or civil disobedience on the internet (Morozov, 2010; Sauter, 2014). This paper will not address the question of the overall legitimacy or otherwise of DDoS attacks as a form of protest. Such arguments can be found elsewhere (Calabrese, 2004; Klang, 2004; Sauter, 2014). Instead, we will focus specifically on how the particular characteristics of booters affect these justifications. We claim that booters differ from previous methods of launching DDoS attacks due to two new characteristics: the ease with which any individual can now launch a powerful DDoS attack and the involvement of a third party, the booter operator, who provides the infrastructure necessary to perform a DDoS attack as a "for-hire" service available to anyone. In this paper, we will argue that these differences undermine what we consider to be the most plausible argument in favour of performing DDoS attacks: that they are a legitimate form of civil disobedience.

In this paper, we argue against the use of booters as a means of "network stressing", and claim that only in a limited set of circumstances is there a plausible moral justification for operating or using booters. We begin by describing what booters are, including the infrastructure they use, the components that perform the attack itself and the various agents connected with operating them. We then turn to the question of whether any DDoS attack can be morally justified, and if so, whether the characteristics of booters affect such a justification. First, we consider the use of booters as "network stressers" by examining the roles played by the various agents associated with booters and discuss whether any of them can offer a reasonable moral justification for their actions. After that, we present an argument that while some DDoS attacks may be classified as acts of civil disobedience, it should be considered whether the particular characteristics of booters undermine the legitimacy of this justification.

2. Distributed denial-of-service attacks and booters

Denial-of-Service (DoS) attacks attempt to make a target system unavailable to its users. This might be due to an overwhelming number of access requests (an overload attack), exploiting system flaws that cause it to crash or otherwise become unresponsive or by causing physical damage to the system (destructive attacks) (Garfinkel *et al.*, 2003, pp. 767-768). Our focus is on network DoS attacks that attempt to make a networked computer inaccessible to its users.

As an extension of DoS, DDoS attacks use large numbers of coordinated attackers to make their target inaccessible to its users. The software performing the attack may be explicitly launched and controlled by the owners of the systems running them or are running secretly on systems without the owner's knowledge. This is often the result of a system's security being compromised by malware or by a third party exploiting security flaws to allow unauthorised software to run on it. What distinguishes booters from other methods of performing DDoS attacks is the ecosystem that makes such attacks available as a service for clients. The booter ecosystem is composed of the six elements depicted in Figure 1.

The *client* (1) is someone paying for an attack on a *target system* (6). The booter website (2) is a public frontend containing information about the services offered by the booter and their prices and an interface for launching attacks once they have been paid for. The client creates an account via the website to allow the operator to record the target for an attack and whether the client has paid for it. *DDoS protection companies* (DPCs) (3) are often found in this ecosystem protecting booter websites themselves against DDoS attacks. The *payment system* (PS) (4) collects clients' payments and transfers them to the booter operator. Once the client's payment is confirmed, the booter backend *infrastructure* (5) performs the DDoS attack ordered by the client.

The backend infrastructure of booters may contain up to three groups of machines, which we will call groups A, B and C. Group A machines are necessary to perform an attack, while those in groups B and C are optional. Each group may consist of dozens, hundreds or thousands of machines. When an attack is launched, the first machines contacted by a booter website belong to group A. This group is the most important to the booter infrastructure, as they orchestrate attacks by either performing them themselves (i.e. direct attacks) or by contacting the second group of machines (e.g. by acting as the "command and control" network of a botnet or web shell loader)[1]. If the second group of machines, group B, is contacted, the attack is *indirect* as the booter operator is using others' computers to perform the DDoS attack. Group B is composed of systems that send network traffic to target systems (i.e. perform attacks themselves) or contact a third level (group C) of machines. Group C machines run ordinary internet services (e.g. DNS and NTP servers)[2] that are misused to "reflect" and amplify attacks. The "reflection" occurs because these ordinary services do not validate the source of requests. By pretending to be the target system, attackers make services such as these send traffic to the target instead of the attacker. Amplification is another characteristic of group C machines, which attackers exploit because the size of responses is bigger than the requests for the majority of the online servers on the internet. This characteristic makes the reflected indirect attacks stronger in volume of traffic than a simple indirect attack.

Booters may offer several types of DDoS attacks, and the backend infrastructure may vary according the type of attack used. For example, a booter offering reflection and

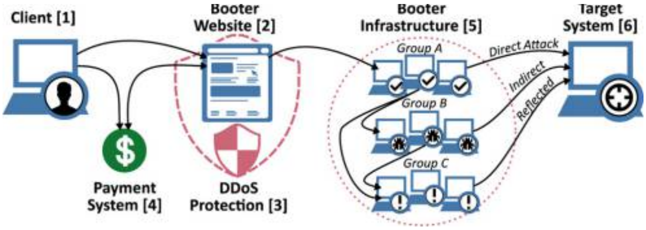

Figure 1.
Elements of the booter ecosystem

amplification DDoS attacks to its clients has a backend infrastructure that comprises machines belonging to groups A and C. In these attacks, group A machines send spoofed messages and group C machines reflect and amplify attacks on the target.

The source code of several booters has leaked onto the internet via websites such as *pastebin.com*. Anyone who downloads such code can begin operating their own booter once she fulfills three requirements:

- registering a domain name that points to a frontend created from the source code;
- reviewing the backend infrastructure used in the source code to ensure that it operates as planned; and
- creating a connection with a payment system.

Note, however, that if someone simply uses the source code it to create her own booter, it still contains the same vulnerabilities that once allowed someone to compromise, hack and release online the original booter's source code unless the new operator removes these vulnerabilities. Security specialists have used this fact to mitigate the impact of booters, as many of them appear to share the same source code, meaning that if (at least) one is compromised, others using the same source code are vulnerable to the same vulnerability and can be taken over themselves (Krebs, 2013a).

3. Justifications for using booters

Booters have targeted the internet sites of schools, personal websites, game servers and government websites. Ironically, booter operators themselves are frequently targets for other booter users (Santanna *et al.*, 2015, p. 249). The variety of targets suggest a range of motives for using booters, but most appear to be some form of self-interest or malice against the target.

While booter clients do not ordinarily declare their motives, it is possible to draw reasonable conclusions from the targets they attack. This task is helped considerably by the leak of several client databases from booter operators, which list the targets and frequency of attacks paid for by clients. For example, Karami and McCoy (2013, p. 4) conclude in their analysis of the leaked TwBooter client database that the most popular targets were game servers and forums. Such uses of booters deliberately interfere with how others communicate and interact for personal gain. Malicious self-interest in limiting others' ability to communicate and play is the apparent motive in these cases.

Despite this, there are two possibilities for using booters that do not fall into the category of malicious self-interest. The first is that booters offer a way of testing how well a service handles heavy network traffic. This is the use-case promoted by calling booters "network stressers". In this case, the DDoS attack is targeted at the user's own server or to a server that the user has permission to test. The other potential justification for using a booter is based on the argument that DDoS attacks are defensible acts of civil disobedience. It is possible that the TwBooter attacks on government websites that Karami and McCoy (2013, p. 4) describe (two sites belonging the Indian government and the website of the Los Angeles Police Department) are political protests. Courts have already recognised some DDoS attacks as forms of activism. For example, the Higher Regional Court of Frankfurt in Germany recognised Andreas-Thomas Vogel's DDoS attack on the Lufthansa website as a method of influencing public opinion (Sauter, 2014, pp. 53-54)[3]. Before considering this possibility, we will examine the justification for booters as a tool for network stress testing.

3.1 Justifying booters as network stress testing tools

Portraying booters as a means of testing a system's ability to handle heavy network traffic depicts them as a neutral service that can be used for both moral and immoral purposes. A network stress test performed on one's own systems could be defended as a self-regarded action, following John Stuart Mill's arguments for the liberty of the individual over actions that concern only herself and the maxim *volenti non fit injuria*: no-one is unfairly harmed by an action to which she has consented (Brink, 2014). These justifications that the network stress test does not harm others or that anyone else's systems that are used in the attack have given consent for them to be used in this way. We will return to the question of moral legitimacy later. The separate question of whether operating a booter is legally legitimate is more straightforward: DDoS attacks are illegal in most jurisdictions, so their intended and advertised purpose is illegal (Kostadinov, 2013; Sauter, 2014, pp. 12-15).

What if the booter operator is in a jurisdiction where DDoS attacks are legal? For the sake of the argument let us suppose that:

- there are legal uses for a booter; and
- that it is possible to distinguish between legal and illegal uses before the attack occurs (i.e. when the client requests and attempts to pay for an attack).

Under these assumptions, the operator is justified in allowing attacks that meet these two criteria and the operator confirms that the client is requesting a legal use. This is the ideal "network stresser" case many booter operators advertise to legitimise their services[4].

Despite the claims of booter operators, the ideal "network stresser" case does not justify operating or using their services. There are alternative methods of testing the resilience of servers and networks that do not require sending overwhelming amount of network traffic across public networks generated by booters and DDoS attacks. For instance, the network gateway connecting a server or local network to the internet itself could generate the traffic needed to simulate a DDoS attack. While this is of course a simulation of a DDoS attack, it does not involve the abuse and exploitation of the internet services, devices and traffic of others (through reflection and amplification attacks) that actual DDoS attacks involve.

For the sake of the argument, let us assume that a "network stresser" is necessary for testing the resilience of a server or network and that there is no alternative means of performing this test. If Assumptions 1 and 2 hold in this case, it would be acceptable to operate a booter. What about cases where both 1 and 2 hold, but the operator does not confirm that the request is legal? The operator might reply that it is not her responsibility to confirm an attack's legality, and that this responsibility falls to the client. The booter (and by extension, the operator) is portrayed here as being morally neutral. However, this neutrality is compromised by the second assumption that legal and illegal uses of the booter can be distinguished before it performs a DDoS attack. Given that the only morally permissible use of a booter is as a network stress test under a specific set of conditions, the booter's frontend could be designed so that it will only accept attack requests if those specific conditions are met. For instance, after receiving a request for a DDoS attack, the operator could contact the target and confirm that the request is legitimate and that the target has actually agreed to it. If the request is confirmed, then the operator could proceed with the attack and seek payment from the client. Otherwise, the operator would reject the request.

The legal illegitimacy of booters creates difficulties for the other agents that are associated with booters. In addition to the clients wishing to launch DDoS attacks and the operator maintaining the frontend and backend systems necessary to attract clients and perform attacks, there is the payment system that transfers money between the clients and the operator and the DPC protecting the booter from similar attacks. The payment system and the DPC offer support services necessary for the booter to function, either directly or indirectly. The payment system is necessary for the booter to operate as a paid-for service, so the transfer of money between the clients and the operator directly supports the booter's operation. The DPC's service only indirectly supports the booter's operation, as it is not a necessity for a booter to operate: while it might be a practical necessity, given the frequency of booters themselves being DDoS targets, the concept of a booter as a "DDoS-for-hire" service does not in theory entail using a DPC.

Both the payment system and the DPC can claim that they are neutral between the uses of their services. Both have a stronger case for such neutrality than the booter operator, as both services have many clear legitimate uses. Both the payment system and the DPC should only be involved if the two assumptions mentioned earlier hold; otherwise, any use of a booter is illegal. This suggests that both the payment system and the DPC have a prima facie duty to end their relationship with a booter once they are aware of the illegality of its business. Payment system operators and DPCs usually have acceptable use policies that prevent their services from being used for illegal purposes[5]. These policies give a straightforward means for such services to sever their relationship with a booter operator[6]. A booter might continue to operate without the support of a payment system or a DPC, but it would be a less effective tool for allowing *anyone* to perform DDoS attacks.

Before moving on, we will briefly mention a potential conflict of interest that DPC operators might have in this context. DDoS protection is only necessary if DDoS attacks occur. DDoS attacks will be easier to perform if booters are active and available and demand for DDoS protection will increase accordingly. The increasing use of DPC requires more powerful booters to effectively perform DDoS attacks. Given that booters are often targets of DDoS attacks themselves, if DPC services did not protect booters, there would potentially be fewer sources of DDoS attacks[7]. While it is not a symbiotic relationship, as the need for DPC services would remain even if booters disappeared, there is a potential incentive for a particularly wily booter operator to operate a DPC as well and vice versa[8].

3.2 Justifying booter attacks as civil disobedience

We have now established that operating booters does not have any legal legitimacy, given that performing DDoS attacks is illegal. But what can be said about any potential moral legitimacy such attacks may have? As mentioned earlier, DDoS attacks have been recognised as a form of civil disobedience. Before discussing whether booters may be used for this purpose, we need to explore the concept of civil disobedience itself.

3.2.1 Identifying civil disobedience. Civil disobedience is a contested concept, so relying to any single definition to determine whether an act is legitimate civil disobedience is problematic. However, it is possible to identify general features that acts of dissent should have if they are to be regarded as civil disobedience. Brownlee (2007, pp. 180-181) notes two reasons for resorting to illegal protest as an effective means of conveying moral or political dissent: it encourages media coverage of the issue that may otherwise not occur, and it allows protesters to demonstrate the strength of their convictions by showing the public their willingness to face the legal consequences for their actions. These features may be called the *conscientiousness* (in the sense of seriousness and sincerity of belief) and *communicative* features necessary for an illegal act to be a form of civil disobedience (Brownlee, 2004, p. 344). The conscientiousness of civil disobedience is the seriousness and sincerity of belief in the cause motivating the protest. The desire to act, break the law and to face the consequences of doing so, serve as evidence of the dissident's beliefs about the injustice she is protesting. Illegal acts lacking this serious consideration and sincere motivation are likely to be dismissed as criminal behaviour without any political objective.

Civil disobedience is not alone in exhibiting conscientiousness. Participants in radical protest who are indifferent to damaging property and using force against persons, and who frequently attempt to avoid legal accountability for their actions, may also share this sincerity and seriousness of belief. (Radical protest without such conscientiousness is merely violent crime.) The communicative feature of illegal protest is what distinguishes civil disobedience from radical protest. Communication is necessary to provoke the political or social response necessary to end the injustice that motivates the protest. Without effectively communicating the motivation to an audience able to bring down change, civil disobedience cannot serve its intended purpose[9]. How this communication distinguishes civil disobedience from radical protest is that civil disobedience suggests that change is still possible within the existing social and political structure. It recognises that the existing political and legal system is capable of bringing about the desired response, even if it requires changes to these systems themselves. Radical protest suggests that the cause motivating the protest is impossible to achieve within the current social and political structure and seeks to replace or undermine them through coercion. It rejects the possibility that the desired response is possible through the existing political and legal systems, even if they are reformed through the existing means of making such changes. The communicative aspect of the protest is why non-violence is frequently (but not always) given as a requirement for legitimate civil disobedience, as violence and coercion may compromise the communicative features of the protest. Acts of violence may discredit the cause motivating them by making the public reject the views of those who commit them. Civil disobedience aims to provoke debate and engage both the public and the government in considering and hopefully accepting the protesters' view, while radical protest seeks to end debate and compel others to accept the protesters' view.

Finally, a useful distinction may be drawn between *direct* and *indirect* acts of civil disobedience. Direct acts of civil disobedience violates the law or policy that is the motive for dissent, while indirect acts do not themselves violate the laws or policies that they are protesting against (Rawls, 1971, pp. 364-365). Obstructing the entrances of public buildings as a protest against a state's military activities overseas is indirect civil disobedience, while obstructing the entrances to a forest to protest the logging of that forest is direct civil disobedience.

3.2.2 Using booters to perform acts of civil disobedience. Based on the account presented above, a DDoS attack may be classified an act of civil obedience if is an illegal action that has the features of conscientious motivation and the aim of communicating dissent to the public. Unless it is protesting the illegality of DDoS attacks themselves, these actions will be indirect forms of civil disobedience (Sauter, 2014, p. 34)[10].

We can also distinguish between protest and network integrity perspectives on DDoS attacks as civil disobedience. The protest prospective sees DDoS as a legitimate form of *hacktivism*: political and social activism that operates primarily via the internet. Such "mass action" hacktivism regards itself as comparable to a physical sit-in protest (Jordan, 2015, p. 185). The protesters "create a space" for their message to be heard by interrupting or interfering with Internet traffic. Sauter (2014) presents an in-depth defense of this view. In contrast, the network integrity perspective sees DDoS attacks as damaging to both the network and to freedom of expression[11]. Rather than creating a space for protesters to convey their message, the interruption caused by a DDoS attack silences the victim. Ruffin (2000) expresses this view.

The network integrity view rejects almost any usage of booters. The only possible usage for such services is as a voluntary self-directed network stress test. As mentioned earlier, current booter services fail this justification. Most booters use indirect methods to perform

DDoS attacks, either through compromised systems (group B machines) or by abusing publicly accessible services (group C machines). The compromised systems operate without the knowledge or consent of their operators. It is possible for a booter to perform direct attacks if the participating systems either belong to the booter operator or the system owners choose to contribute to the attack. However, the difficulty of identifying the backend controlling the attacks (and thus identifying who is controlling the attack) makes it difficult to distinguish potentially "legitimate" direct attacks from "illegitimate" indirect ones. Using direct attacks instead of indirect ones would also be worth advertising to potential clients wishing to avoid legal concerns about using compromised computers in performing network stress tests of their own systems. The fact that booter operators do not advertise this is revealing in itself.

Let us return to the protest perspective of DDoS attacks. As the protest perspective accepts the use of DDoS attacks as legitimate acts of civil disobedience, we need to examine whether using a booter to perform the attack compromises the conscientiousness and communication features that would otherwise make it an act of civil disobedience.

Sauter (2014, pp. 14-15, p. 49) qualifies her justification of DDoS attacks as "electronic civil disobedience" by emphasising the symbolic value of launching such attacks rather than the actual disruption they cause. She refers to the Starbucks website as an example, explaining that this site serves more as a poster representing the company rather than the means through which it conducts its business of selling coffee (Sauter, 2014, p. 14). Many government websites may also be thought of as being similar to this. The primarily symbolic nature of such attacks highlights their communicative nature. It appears straightforward to attribute this characteristic to booter-launched DDoS attacks as well.

Despite this, a civil disobedience justification for using booters faces the problem that DDoS attacks performed through a booter are mass actions controlled by one person rather mass actions performed by distinct individuals motivated by a common goal. Booter DDoS attacks lack the "democratic accountability" of DDoS attacks performed by a mass of individuals working together. In defending their DDoS attacks against the internet sites of the World Trade Organization (WTO) in November and December 1999, *the electrohippies collective* stated that:

> [o]ur method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure (DJNZ and The Action Tool Development Group of the Electrohippies Collective, 2000).

Relying on the number of individual participants for the effectiveness of a DDoS attack means that it can only succeed if large numbers of people (and thus, a large number of direct attackers) voluntarily participate. This democratic accountability becomes part of the communicative feature of the attack: it demonstrates that a large number of people were motivated to contribute to the protest.

Whether civil disobedience requires a group to perform it or whether it can describe the actions of an individual is controversial. Arendt (1972, pp. 67-68) argues that civil disobedience must be the work of a group that is a minority within society. This perspective would reduce the justification for using a booter, as it allows a single individual to perform a DDoS attack: it could still be a protest, but it would not be civil disobedience as such. On the other hand, the term *civil disobedience* itself comes from Henry David Thoreau's justification of his individual protest against the US government's actions in Mexico by refusing to pay his taxes[12]. For the sake of the argument, we will leave open the possibility that an individual may perform an act of civil disobedience.

Group civil disobedience increases the public spectacle and enhances the communicative aspect of the dissent. Of course, this only holds if the group members are acting on their own belief in the cause and are sincere in their motivation. A lone protester hiring a large number of actors to participate in a sit-in may succeed in creating a spectacle that nevertheless does not indicate that she is the only one there motivated to act upon her cause. This significantly weakens the sincerity of the act: the actors inflating the size of the protest are being paid to do so, regardless of how sincere the protester herself might be in promoting her cause. With this in mind, it should be clear how using a booter compromises the conscientiousness aspect of performing a DDoS attack as a form of civil disobedience. The additional participants in a DDoS attack that a booter provides are not motivated by a sincere conviction in the cause but by the instructions of the booter operator, who is being paid by the client to perform the attack. Booter DDoS attacks do not exhibit the necessary sincerity and seriousness required for illegal acts to be considered acts of civil disobedience.

Booters also obscure the attribution of the protest act, which affects the communicative aspect of using DDoS attacks as a form of protest. The client is paying the booter operator to perform the protest, and this transaction obscures the communication of the motivation for performing a civil obedience. Consider the DDoS attacks performed by the group Anonymous that began in 2010 under the name “Operation Avenge Assange”. These attacks were directed at organisations and groups that disrupted the operation of the WikiLeaks website (Sauter, 2014, pp. 67-69; Coleman, 2014, pp. 128-136)[13]. The Anonymous DDoS attacks, despite the relative anonymity of the participants, are attributable to the group Anonymous itself. The group publicised and claimed responsibility for the actions, and presented its justifications for doing so[14]. Those who chose to download Anonymous’ DDoS tool [the so-called “Low Orbit Ion Cannon” (LOIC)] and participated in the protest were performing direct attacks, even if the software itself was remotely controlled. *The electrohippies* went further, publicly explaining their actions and posting links to arguments for and against the WTO on its website so that potential participants could make an informed decision about joining the DDoS attack (DJNZ and The Action Tool Development Group of the Electrohippies Collective, 2000). To ensure that the action effectively communicates the motivation that makes the act civil disobedience rather than vandalism or other criminal activity, the booter client or operator would have to claim responsibility for the DDoS attack and explain their reasons for doing so. *The electrohippies* and Anonymous publicly justified their actions by appealing to political principles: anti-globalisation and freedom of expression and association, respectively. Their actions were intended to influence political policy by publicly expressing dissent with political actions. Lizard Squad, however, presented their DDoS attacks as an advertisement for their LizardStresser booter. Their motivation is self-interest, and there was no desire to influence political policy or social institutions to correct injustice.

In response to these arguments for DDoS attacks as civil disobedience, it may be said that the relatively low threshold for participating in the Anonymous DDoS attacks reduces its legitimacy as an expression of popular dissent. The argument portrays contributing to these attacks as little more than “slacktivism”, irrelevant and ineffective displays of political opinion on the internet that express support without making a meaningful contribution or risking themselves in working towards achieving the political goal (Morozov, 2010, pp. 189-191). This objection appeals to the conscientiousness feature of civil disobedience: someone who has carefully considered the costs of being caught performing illegal activity and still does so based on political or moral conviction displays the seriousness of their motivation (Brownlee, 2004, pp. 341-342). If legal consequences are unlikely and the effort required to participate is minimal, a protester may be less serious in her commitment to the belief motivating the protest.

This objection can be challenged by arguing that it appeals to a conception of civil disobedience that is too beholden to historical cases (Sauter, 2014, pp. 26-27). Participating in a DDoS attack may have legal consequences, as the later arrest of some of those involved in the Anonymous DDoS protests demonstrates (Coleman, 2014, pp. 135-136)[15]. However, even if we accept the charge of slacktivism it still grants the Anonymous protests a degree of legitimacy that booter attacks do not share because the consent of the computer users involved. The difference between a user knowingly participating in a DDoS attack and a user's system participating in a DDoS attack without her knowledge and consent is enough to undermine the legitimacy of a booter-controlled indirect DDoS attack as an act of civil disobedience.

Returning to the distinction between direct and indirect DDoS attacks will further clarify this point. The most basic direct DDoS attack is a large number of people connecting to one website and continually trying to reload it. Websites that are unprepared for a link from a highly visible and active internet community often suffer this unintended side effect of such exposure. All the participants in such attacks, intentional or otherwise, are direct attackers as they control the computers attempting to connect to the target. A single user or group (whom we will call the "DDoS attacker") can control a direct attack if they have been voluntarily granted access to other computers, such as by others voluntarily installing software that gives the DDoS attacker such access to their computer and are aware of the purpose that it will be used for. This is what those who downloaded and installed the LOIC software to contribute to the Anonymous protests did: they volunteered computer time and capability to the purpose of the protest. In this sense, they are little different from people who donate money or resources to activist groups to support their cause. Participating in an active DDoS attack therefore is more than mere "slacktivism", unless the term should also cover those who make donations to activist groups without otherwise participating in their activities.

Indirect attacks are a different matter. Here, the software giving the DDoS attacker access to a computer has been installed without the user's knowledge or agreement, and she is unaware that her computer is contributing to the attack. The DDoS attacker has appropriated the user's computer time and capability without her permission. A user volunteering her computer for use by a DDoS attacker can withdraw her system by refusing to participate or by removing the software if she disagrees with the purposes of the attack. Unwitting participants in indirect attacks have no such option unless they discover the software running on their computers themselves and remove it (and even then, they are unlikely to know for what purpose their computer has been used for). Using indirect attacks also fails the claim of democratic accountability, as those whose systems are used are unaware of their participation and their contributions to the DDoS attacks cannot be interpreted as protests on their behalf.

Sauter (2014, p. 132) rejects using indirect attacks in DDoS protests for similar reasons: "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". Sauter (2014, p. 132) also rightly argues that using indirect attacks damages the legitimacy of voluntary contributors to DDoS attacks by making it easier to disregard the protest as merely a criminal act rather than a political one. It obscures the communicative features of the protest by violating the rights of the users of compromised computers to control the usage of their own computers, exposing unwitting participants to legal risks (and raising fears that one may have unwittingly contributed to the protest) and by calling in question the voluntariness of the contributions to the protest.

There is a final possible argument in defense of using a booter for civil disobedience. Direct DDoS attacks performed manually by activists working in concert are increasingly unlikely to disrupt well-resourced websites (Sauter, 2014, p. 130). It can be said that using a booter is necessary to achieve the scale of DDoS attacks necessary for the action to be noticeable, especially given the inequality of resources that governments or multinational corporations have compared to activists. A group of activists might use a booter (or several booters) to perform a DDoS attack that would be more effective against a well-resourced target than if they relied solely on direct DoS attacks from their own computers, like *the electrohippies* protest against the WTO. This partially addresses the objection of democratic accountability, as it is the action of multiple individuals rather than just one. It is still weaker in its communicative aspect than a direct DDoS attack, however. The effect of the protest is multiplied by using a booter, and so does not convey the same breadth of concern and sincerity among the public that a direct DDoS attack of the same scale that requires a significantly greater number of participants would do.

Using a booter to ensure the effectiveness of their attack as a protest is also compromised by the fact that the booter operator is being paid for her role in performing the attack, which weakens the claim that those involved all share a sincere political motivation. Such an action might be more effective, but it would only be legitimate if the booters all used direct attacks (so that no computers are used without permission) and both the clients and booter operators publicly announced the motivation and claim responsibility for the action. The operators' public announcement of attribution and support is necessary to show that they are acting from mixed motives: both the political motive in support of the client's actions and the business motive of charging for a service. If the booter operator allowed the protester(s) performed DDoS attacks on a specified target for free, it would prevent the operator's profit motive from diluting the communicative aspects of the DDoS attack. The operator would effectively be acting as a fellow protester, or at least as a supporter by donating resources to her cause.

It also helps to clarify that the protesters are not trying to hide the fact that the effect of their protest is greater than it would have been if they had only used individual direct attacks. The requirement of sincere political motivation is further strengthened if the booter operators donate the use of their service to the clients, making them contributors and supporters of the protest. In effect, donating their infrastructure for the protesters' use makes the booter operators protesters as well. This case offers the possibility for booters to be legitimately used for civil disobedience, provided that it uses only direct attacks that use computers and systems that the booter operator has legitimate control over. Otherwise, the objections to using indirect attacks in DDoS protests and the difficulties they raise for the communicative and conscientiousness features of civil disobedience still hold.

However, the need to use booters to ensure the necessary scale to effectively disrupt a well-resourced target is itself questionable. The attack's effectiveness is secondary to the attack's visibility, including both the publicity surrounding it and that someone (or some group) was motivated to perform it. As civil disobedience intends to draw attention to injustice, publicising the act and explaining the motivation behind it is vital. Without raising public awareness of the injustice motivating the act, acts of civil disobedience cannot prompt the social or political change they aim to achieve. In terms of DDoS attacks as civil disobedience, the success of the attack itself is often secondary to the publicity generated for the motivation behind it (Sauter, 2014, pp. 59-75). Performing a massive DDoS attack, such as that possible by using several booters to attack a target simultaneously, might be counter-productive as the publicity gained by the impact of the attack (including the use of others' computers without permission, if indirect attacks are involved) might overwhelm the publicity for the motivation behind it.

A parallel can be drawn here with violent protest (radical or otherwise). When violence (planned or otherwise) occurs during a protest, public reporting of the protest often portrays the violence as undermining the legitimacy of the protesters' motivation. As Sauter (2014, p. 64) rightly notes, any public protest faces the challenge of drawing public and media attention to the motivation for the protest, rather than the protest itself. A DDoS attack that makes a major internet service unavailable must be careful in announcing and promoting its motivation to ensure that it is not overshadowed by reports and interest in the disruption it causes. While the democratic accountability of direct DDoS attacks launched by enough motivated individuals to impact a major internet service may mitigate this (as the large number of people motivated to join the attack is itself noteworthy, and the motive for doing so is likely to be publicised by the individuals themselves), an attack of similar size that relies on booters lacks the noteworthiness of a large number of people attacking in concert for a political or social goal.

4. Conclusion

Booters are a serious threat to any system connected to the internet. We describe, however, one argument in which booters could be legally and morally justifiable: *when a booter is an ideal "network stresser"*. In this case, attacks are used against a target that has given permission for a DDoS attack to be performed against it, and the booter *only* performs direct DDoS attacks (in contrast to indirect attacks exploiting third-party internet services or using compromised systems). Nonetheless, based on observations of current known booters and their attacks, we conclude that this case is unlikely to happen.

In terms of a moral justification for using a booter, there is little to say in defense of using booters out of self-interest. A DDoS attack, by definition, attempts to disrupt the target's ability to communicate with others. It deliberately prevents the target from interacting with others via the internet without the legitimate authority to do so. Civil disobedience offers a possible justification, provided that the DDoS attack demonstrates the seriousness and sincerity of the protester's motivation and attempts to communicate the political or social change that motivates her. However, it is important that the systems used in a booter attack that is intended as civil disobedience must be direct attackers. Using indirect attacks, either by abusing publicly accessible servers or by gaining control of compromised systems, dilutes the communicative aspect of the attack. Then there are problems of conscientiousness in motivation and attribution, as the clients are paying the booter operator to perform the attack on their behalf. Using a booter to perform civil disobedience is morally justifiable only if the booter performs direct attacks and the clients and operators publicly announce the attack and their motivations for doing so.

Notes

1. A botnet is a set of machines either infected with malware or otherwise compromised by an attacker that allows them to be controlled via a third party that sends them tasks to be performed. A Web shell is a program running on a server that allows a remote user to execute code on it.
2. DNS (Domain Name Service) servers convert internet URLs (such as www.wikipedia.org) into network addresses (such as 192.168.0.1). NTP (Network Time Protocol) servers report the time on request.
3. Sauter (2014, p. 7) uses the term "DDoS action" rather than "DDoS attack" because of the violence implied by the term "attack". While we acknowledge the significance of the point Sauter makes with this change in terminology, we continue to use the term "DDoS attack" to remain consistent with the networking and security literature.

4. The fact that booter frontends also often offer services as such Skype resolvers that identify the IP address associated with a Skype username which would allow a DDoS attack on that user (Krebs, 2013b) suggests that such claims of legitimacy are disingenuous. Such a service would be unnecessary for an operator stress testing her own network, as she would already know this information.
5. For example, the conditions of use for the PayPal PS state that "may not use the PayPal service for activities that [. . .] violate any law, statute, ordinance or regulation; [. . .] facilitate or instruct others to engage in illegal activity". See "PayPal Acceptable Use Policy", available at: www.paypal.com/ua/webapps/mpp/ua/acceptableuse-full (accessed 12 July 2016).
6. However, it may be impossible for a Booter to be disconnected from these services. For instance, using a crypto-currency such as Bitcoin as a payment system would make it impossible to prevent a booter operator from using it.
7. This assumption can be questioned if another operator can control the indirect components of the booter. The infrastructure for performing DDoS attacks would remain: all that would be removed is one source for controlling it. To make this a stronger claim, the infrastructure itself would have to be removed. This complication does not affect the argument, as removing one controller still removes at least one source of launching DDoS attacks.
8. Krebs (2015b) describes an alleged occurrence instance of this.
9. Milligan (2013, pp. 16-21) is sceptical of the significance of communication in civil disobedience and instead emphasises civility as an identifying feature of such acts. However, communication seems important *strategically* for dissenters, as popular support and public sympathy are important at least instrumentally for the dissenters' wishes to be implemented.
10. This should not be confused with the difference between *direct* DDoS attacks and *indirect* DDoS attacks.
11. Jordan (2015, pp. 185-186) calls this perspective "digitally correct hacktivism".
12. As Brownlee (2016) notes, "[I]t is interesting that the action of the man who coined the term 'civil disobedience' is regarded by many as lying at the periphery of what counts as civil disobedience".
13. It is worth noting that some of Anonymous' targets were payment systems, like those necessary for Booters to operate, that withdrew their support or refused to do business with WikiLeaks (Coleman, 2014, pp. 118-119).
14. As mentioned in the introduction, the group behind the Lizard Stresser booter did just that, although the motivation they announced for their attacks was to advertise their own Booter service (Krebs, 2014).
15. It may be argued that at least some of the participants in these protests were ill informed about the legal risks they were taking in contributing to a DDoS attack (Coleman, 2014, pp. 133-134). However, this and other examples of arrests for DDoS attacks show that at least some level of serious consideration is necessary before choosing to participate in this form of protest.

References

Arendt, H. (1972), *Crises of the Republic: Lying in Politics, Civil Disobedience on Violence, Thoughts on Politics, and Revolution*, Houghton Mifflin Harcourt, New York, NY.

Akamai (2016), "Akamai's state of the internet: security", Vol. 3 No. 1, pp. 8-12, available at: www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf (accessed 4 September 2016).

Brink, D. (2014), "Mill's moral and political philosophy", in Zalta, E.N. (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2014 Edition), available at: http://plato.stanford.edu/archives/fall2014/entries/mill-moral-political/ (accessed 4 September 2016).

Brownlee, K. (2004), "Features of a paradigm case of civil disobedience", *Res Publica*, Vol. 10 No. 4, pp. 337-351.

Brownlee, K. (2007), "The communicative aspects of civil disobedience and lawful punishment", *Criminal Law and Philosophy*, Vol. 1 No. 2, pp. 179-192.

Brownlee, K. (2016), "Civil disobedience", in Zalta, E.N. (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2016 Edition), available at: http://plato.stanford.edu/archives/spr2016/entries/civil-disobedience/ (accessed 4 September 2016).

Calabrese, A. (2004), "Virtual nonviolence? Civil disobedience and political violence in the information age", *Info*, Vol. 6 No. 5, pp. 326-338.

Coleman, G. (2014), *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, London and New York.

DJNZ, and Action Tool Development Group of the Electrohippies Collective (2000), "Electrohippies occasional paper no. 1: client-side distributed denial-of-service: valid campaign tactic or terrorist act?", available at: www.iwar.org.uk/hackers/resources/electrohippies-collective/op1.pdf (accessed 4 September 2016).

Garfinkel, S.L., Spafford, E.H. and Schwartz, A. (2003), *Practical UNIX and Internet Security*, 3rd ed, O'Reilly, Sebastopol, CA.

Jordan, T. (2015), *Information Politics: Liberation and Exploitation in the Digital Society*, Pluto Press, London.

Karami, M. and McCoy, D. (2013), "Understanding the emerging threat of DDoS-as-a-service", *6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, Washington, DC.

Klang, M. (2004), "Civil disobedience online", *Journal of Information, Communication and Ethics in Society*, Vol. 2 No. 2, pp. 75-83.

Kostadinov, D. (2013), "Legality of DDoS: criminal deed vs. act of civil disobedience", *InfoSec Institute*, available at: http://resources.infosecinstitute.com/legality-ddos-criminal-deed-vs-act-civil-disobedience/ (accessed 4 September 2016).

Krebs, B. (2013a), "The obscurest epoch is today", *Krebs on Security*, available at: http://krebsonsecurity.com/2013/03/the-obscurest-epoch-is-today/ (accessed 4 September 2016).

Krebs, B. (2013b), "DDoS services advertise openly, take paypal", *Krebs on Security*, available at: http://krebsonsecurity.com/2013/05/ddos-services-advertise-openly-take-paypal/ (accessed 4 September 2016).

Krebs, B. (2014), "Lizard kids: a long trail of fail", *Krebs on Security*, available at: http://krebsonsecurity.com/2014/12/lizard-kids-a-long-trail-of-fail/ (available 4 September 2016).

Krebs, B. (2015b), "Spreading the disease and selling the cure", *Krebs on Security*, available at: http://krebsonsecurity.com/2015/01/spreading-the-disease-and-selling-the-cure/ (accessed 4 September 2016).

Milligan, T. (2013), *Civil Disobedience: Protest, Justification, and the Law*, Bloomsbury, New York & London.

Morozov, E. (2010), "In defense of DDoS", *Slate*, available at: www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html (accessed 18 October 2016).

Rawls, J. (1971), *A Theory of Justice*, 1st ed., Harvard University Press, Cambridge, MA.

Ruffin, O. (2000), "Hacktivismo", *Cult of the Dead Cow*, available at: http://w3.cultdeadcow.com/cms/2000/07/hacktivismo.html (accessed 4 September 2016).

Santanna, J.J., Durban, R., Sperotto, A. and Pras, A. (2015), "Inside booters: an analysis on operational databases", 14th IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE, pp. 432-440.

Sauter, M. (2014), *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*, Bloomsbury, New York & London.

Turton, W. (2015), "Lizard squad's Xbox live, PSN attacks were a 'marketing scheme' for new DDoS service", *The Daily Dot*, available at: www.dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/ (accessed 4 September 2016).

Further reading

Krebs, B. (2015a), "Lizard stresser runs on hacked home routers", *Krebs on Security*, available at: http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/ (accessed 4 September 2016).

Morozov, E. (2011), *The Net Delusion: How Not to Liberate the World*, Penguin Books, London.

Corresponding author

David Douglas can be contacted at: d.m.douglas@utwente.nl