Chapter 11
Virtual Sit-Ins, Civil Disobedience and Cyberterrorism

Mathias Klang

> Those who profess to favor freedom, yet deprecate agitation, are men who want crops without plowing up the ground … This struggle may be a moral one; or it may be a physical one; or it may be both moral and physical; but it must be a struggle. Power concedes nothing without a demand. It never did and it never will.[1]

Introduction

The purpose of this chapter is to investigate the foundations justifying denial of service (DoS) attacks. The main thrust of this examination is whether or not such attacks may be seen as an acceptable form of civil disobedience.

In order to accomplish this, the concept of civil disobedience must be explored further, with a focus on its role in contemporary political activism. The term itself carries many ideas and concepts and is by no means straightforward. Within online civil disobedience the metaphor of the sit-in has been used by those who carry out attacks, and therefore this chapter will explore the mechanics of DoS attacks and compare them to the basics of the sit-in as a valid tactic of disobedience.

In the attempt to search for truth, legal academics and philosophers are both prone to the same mistake: attempting to ascertain the true meaning of a word in order to find out what the concept really means. Popper called this exercise nominalism[2] and, while this is an interesting and, at times, individually educational exercise, it may sometimes seem to be rather futile. The temptation is to follow the advice of Humpty Dumpty, who claimed: 'When I use a word it means just what I choose it to mean – neither more nor less.'[3] However, it is important to observe that in the discourse on online activism today one of the terms being used with alarming regularity is cyberterrorism.

When invoking the spectre of terrorism it is important to remember that today the relevance of the correct label in this case is far from academic. If the action of DoS is seen to be disobedience the courts may show tolerance; if it is seen to be criminal the courts will punish it; but if it is seen as terrorism then society will neither tolerate the actions nor forgive the proponents.

Terrorism and cyberterrorism

In his thesis on political terrorism, Bauhn notes that defining terrorism often hinges on the innocence of the victim. While he disagrees that the act should be defined by

---

1 Douglass, F, 'The significance of emancipation in the West Indies' [1857] in Blassingame, J (ed), *The Frederick Douglass Papers, Series One: Speeches, Debates and Interviews*, Volume 3: 1855–63, 1985, New Haven, CT: Yale UP, p 204.

2 Popper, K, *The Open Society and its Enemies*, 1966, London: Routledge and Kegan Paul.

3 Carroll, L, *Through the Looking Glass*, 1999 [1872], Mineola, NY: Dover.

the victim's innocence, he sympathises with previous authors' attempts to define the actions of the politically motivated terrorist. His own definition is founded upon an understanding of the difficulties of definition. He defines the terrorist as the perpetrator of terror, and states that 'political terroristic acts are violent, intimidatory and … have political purpose'.[4]

While in the main the negative connotation remains, the general concept of terrorism has been under development, particularly so since 2001. The political discourse on terrorism has shifted the focus from the methodology of violent action to the descriptive term for those who would oppose the established order. The main change is that whilst in the past a violent political group was not necessarily terrorist, today a terrorist group does not necessarily have to have committed an act of violence.

The liberation of the terms terrorist and terrorism from the actual act of terror has allowed for a more flexible use of the label. Those who fight against terrorism are justified since terrorism is something reprehensible. This legitimacy is important since the violence perpetrated by the counter-terrorist can at times be greater than the violence carried out by the terrorist.[5]

While the removal or reduction of the need for violent activity[6] from the definition of terrorist has made it easier for the counter-terrorist to legitimise violence in the name of combating terrorism, it has also allowed for the creation of a more confusing concept of cyberterrorism, which is defined by Denning as the convergence of terrorism and cyberspace. Since the attacks are online, Denning's terrorist has to be redefined as one who attacks or threatens to attack information; she also adds the requirement that the attack should 'result in violence against persons or property, or at least cause enough harm to generate fear'.[7] This final part is worrying, since the attack need not cause devastation for the label of cyberterrorism to apply; it is enough if the attack generates fear. The qualification of fear has not been a necessity when defining or discussing offline terrorism. Whether the government or populus is afraid has little bearing upon the justification in applying the term terrorism to a political action. This addition of fear may be due to the fact that there have been few cyberterrorism attacks of any dignity, if indeed there have been any at all.[8] Despite the publicity and discussions of the vulnerability of the information society, the cyberterrorist remains a ghost in the machine rather than a serious threat.

---

4 Bauhn, P, 'Ethical aspects of political terrorism' (1989) 1 *Studies in Philosophy*, Lund: Lund UP.

5 Gearty, C, 'Terrorism and morality' (2003) *EHRLR* 377.

6 Gearty talks of 'the deliberate or reckless killing of civilians, or the doing of extensive damage to their property, with the intention of thereby communicating a political message of some sort to a third party, usually but not necessarily a government'. *Ibid*.

7 Denning, D, 'Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives', May 2000, at www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

8 Vegh, S, 'Hacktivists or cyberterrorists? The changing media discourse on hacking' 7(10) *First Monday*, at http://firstmonday.org/issues/issue7_10/vegh/index.html.

Civil disobedience and the sit-in

There is a *prima facie* moral duty of the individual to follow the law. To some, this obligation to obey the law is absolute. Socrates, for example, believed in following the rules of society. So firm was his belief that even when Crito suggested that an escape could be arranged he refused, took his penalty and drank the fatal poison. Socrates expanded his position by explaining that he was obligated to the state and had accepted its rules, and it would be wrong to disobey those rules; therefore there could never be justification for doing wrong.[9] For most, this duty to obey the law is based upon the belief that without this obedience either the state would be unable to function or without total obedience some would gain unfair advantages.[10]

Whilst the rigour of Socrates' position may well be admired, it is seldom emulated. The discussion of whether there is a duty to obey the law is rarely taken to this extreme. However, the question of whether there is a duty of obedience towards the law and the state is an active one, since the question of when disobedience is valid remains. Practitioners of civil disobedience tend to justify their actions by pointing to the fact that they are fighting a larger injustice and in this role they have the right, some would even claim the duty, to break the law. Therefore, the disobedients are doing what they believe to be morally right despite the fact that their actions unfortunately come into conflict with the enforced rules. The term civil disobedience itself contains two important parts: civil action and disobedience. Dr King needed four criteria for his action to be legitimate: documented injustice, negotiation, self-purification, and direct (non-violent) action.[11]

Opposing the state on a large scale tends to border upon rebellion or revolution. Opposing parts of the state – or more correctly opposing certain of the state's commands – has become known as civil disobedience. It is important to bear in mind that there is a fine line between rebellion and civil disobedience. In what is probably the most famous protest against the social effects of technology, the Luddites, protesting against the mechanisation of the textile industry, destroyed factory machinery. The Luddites were defeated by armed soldiers, and the leaders were either executed or deported in 1813. On a smaller scale, but with an enduring legacy, Henry David Thoreau felt that his country was acting immorally and reached the conclusion that once a government no longer behaved morally, its citizens no longer had an obligation to support it. He recommended that citizens withdraw from their obligations towards the state. In England, Emmeline Pankhurst and her daughters formed the Women's Social and Political Union, whose purpose was to speed up the enfranchisement of women. Its members, commonly known as suffragettes, believed that their cause needed publicity and to further this goal they committed illegal acts (eg, chaining themselves to railings and setting letterboxes alight) to shine the light of publicity on their cause. Such violence and destruction of property is not accepted by all activists.

---

9 Plato, *Five Dialogues*, Grube, GMA (trans), 2002, Indianapolis: Hackett.

10 These positions have been challenged by legal academics: see, eg, Raz, J, 'Obligation to obey: revision and tradition', in Edmundson, W (ed), *The Duty to Obey the Law*, 1999, Boulder, CO: Rowman & Littlefield; Smith, M, 'Is there a *prima facie* obligation to obey the law?' (1973) 82 *Yale LJ* 950; Wolff, R, *In Defence of Anarchism*, 1970, Berkeley, CA: University of California Press.

11 King, M, 'Letter from Birmingham City Jail', in Bedau, H (ed), *Civil Disobedience in Focus*, 1991, New York: Routledge.

Mohandas Gandhi was a great believer in non-violent protest. His ideas were formulated at the onset of the South African campaign for Indian rights and can be best seen in the Indian struggle for independence from the British Empire. One of the most impressive non-violent campaigns was the Salt campaign, in which 100,000 Indians were jailed for deliberately violating the Salt Laws. Since the creation of the doctrine of non-violent resistance formulated by Mohandas Gandhi, the term 'civil disobedience' regularly includes non-violence as an additional qualification. Spurred on by the success of non-violent resistance, the methodology was adopted by Martin Luther King in his successful campaign to bring an end to racial segregation laws. While the origins of the sit-in are difficult to locate, a popular point of origin stems from 1960 when four African American college students in Greensboro, North Carolina protested against the whites-only lunch counter by sitting there every day. After the publication of an article in the *New York Times* they were joined by more students and their actions inspired similar protests elsewhere.

The concept of disobedience as conceived by Gandhi and developed by Dr King was to draw attention to the injustice and in this manner to commence a political discussion that would lead to the creation of more just society, which is the purpose of civil disobedience.[12] For many, the implementation of information and communications technology (ICT) for the same end was inevitable. The earliest formal connections seem to be made as early as 1996, when the Critical Art Ensemble published a book containing a chapter on the topic of Electronic Civil Disobedience.[13]

Distributed denial of service

The DoS attack is usually described as an incident which prevents a legitimate user or organisation from accessing a systems resource or the delaying of systems operations and functions. The incidents or attacks can be related to a specific network service such as email, or to the domain name of the target. Attacking the domain name has the added advantage for the attacker of tending to diminish all the victim's online functions since the domain name cannot be resolved. This means legitimate users attempting to access a web-based service are unable to connect to the server, since they are unable to acquire the necessary IP address to do so. This is due to the fact that the server under attack is busy responding to its attackers' requests and is unable to reply to legitimate users' requests. The legitimate user, unaware of the ongoing attack, will only receive an error message from her browser that the server is unavailable.

Traditionally, the distributed DoS attack entailed the co-ordination of traffic to a designated website; this first required the marshalling of many protesters to be prepared at their computers to send information at a given time to a specific target. These attacks were complex affairs, and required a great deal of social cohesion and organisation amongst the protesters, who sat alone in front of their computers with only the virtual presence of others. To overcome some of these organisational

12 Rawls, J, *A Theory of Justice*, 1999, Oxford: OUP.

13 Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas*, 1996, New York: Autonomedia.

problems, co-ordinating software may be used by protestors. Such attacks are known as co-ordinated point-to-point DoS attacks. In these kinds of attacks the attackers may use software with the same effects as that used in the point-to-point DoS attacks. Naturally, the more users and the more sophisticated the software, the more efficient the attack. The important issue with this type of attack is that it still requires a user to be involved in the attack, and to be efficient it requires the gathering of a large group of people who have the time, technology and will to carry out the attack.

While there are different forms of DoS attack, such as TCP SYN flooding, ICMP flooding, UDP flooding and ping of death, the most common is TCP SYN flooding, which will be explained briefly here.

When attempting to view a web page, the browser attempts to establish a contact with the server upon which the information is stored. The initial contact is made up of the client and server exchanging a set sequence of messages known as the three way handshake:

1 The browser (client) begins by sending a SYN message to the server.
2 This is acknowledged by the server by sending a SYN-ACK message to the client.
3 The final message is an ACK message sent by the client.

After the handshake, the connection between the client and server is established. The required data can thereafter be exchanged between the client and the server, whether it is email, a web page or any other TCP-based service.

This system is at its most vulnerable when the SYN-ACK message has been sent by the server since, at this stage, the server is awaiting the final ACK message. At this point the connection is half open. Since the memory of the server is finite and the system requires the server to save to memory any half-open communications awaiting the final ACK message, the system can be caused to overflow if too many unfinished connections are made. In order to intentionally create the half-open connection, a technique known as IP spoofing is used. This technique entails the sending of SYN messages to the server with non-responsive client systems, ie systems which are unable to respond to any SYN-ACK messages received. The effect of too many half-open connections is that the server's memory will be filled and the system will be unable to accept any new SYN messages until the list of awaiting half-open connections have been completed or timed out. Existing or outgoing connections will in most cases not be affected. When the attackers stop sending spoofed IP messages the server will time out those messages awaiting response and recover; however, for this to occur the attacker must stop sending the messages.

These types of attack that still involve the physical intervention of the user have sometimes been called client-side DoS, to differentiate them from server-side DoS. While the client-side DoS requires the active participation of many like-minded individuals, the server-side DoS has no such requirement. To be effective the server-side DoS attack requires only one individual and the creation of an army of zombies. In this context, a zombie is a computer containing a hidden software program that enables the machine to be controlled remotely. For the purpose of the DoS this remote control of other people's computers is done with the intent of attacking a specific victim server.

The most efficient method of introducing software into other people's computers with the capability of taking control of them at a specified date is either by hacking into the computer and installing the software directly, spreading the program in the form of a virus, or including the code within a piece of desirable software that the user will download and install himself.

Two well publicised examples of server-side DoS attacks are the Mafiaboy attack, where a 15 year old known only as Mafiaboy successfully attacked websites operated by Yahoo!, eBay and Amazon.com,[14] and the 13 year old who used a DoS attack to take down a California-based computer security site.[15]

The advantage of using zombies to carry out the attack on a server is that the attacker does not need to disadvantage himself by persuading and co-ordinating other users in participating in the attack. There is an added advantage of increased anonymity, since the attacker's machine is not directly involved in the DoS attack but acts only via its unwitting intermediaries – the zombies. With adequate time and effort in preparation, the number of zombies created can be sufficient to create havoc with even the most sophisticated of servers. Naturally, the more time spent in preparation, the more likely it is that the plans will be uncovered prior to the attack and defences will be created that will limit the effects of the attack.

Online activists: the electrohippies

There has been insufficient research into hacker culture and psychology to create a nuanced picture of what motivates people to carry out DoS attacks. This has left the field open for simplification, generalisation and the creation of the image of the hacker as a technically sophisticated but naïve young man who is driven by ignorance, a desire for destruction or purely criminal impulses. This image is the one most often used in media and has been mirrored in films from *WarGames* (1983) to *Swordfish* (2001).

However, when attempting to comprehend the driving forces behind the hacker, it is important to look beyond our own media imposed images. In his research into hacker culture, Taylor[16] identifies six main driving forces that motivate hackers (addiction, curiosity, boredom, power, peer recognition and opposition); within the section on peer recognition, Taylor includes politically motivated actions. The book is an excellent starting point for those wishing to understand the hacker; however, it is important to recognise that it is based upon research carried out prior to the growth of online activism. Today, a book on hackers must recognise the effects of a larger group of politically motivated online activists.

14 Jaffe, J, 'Attacks fell an online community', 27 January 2003, at www.wired.com/news/infostructure/0,1377,57392,00.html.

15 Gibson, S, 'The strange tale of the denial of service attacks against grc.com', Gibson Research Corporation, at http://iso.grc.com/dos/grcdos.htm.

16 Taylor, P, *Hackers*, 1999, London: Routledge.

The actions of DoS attackers are, or are rapidly becoming, illegal. The question which therefore needs to be addressed is what it is that drives these people to carry out such actions. If they are merely criminals, then we need hardly proceed any further. The question is whether there can be any legitimacy in their actions. In order to explore this further, we must take a closer look at the motives underpinning online activists. However, this is not as simple as it may sound, since the current legal environment does not promote the development of an open dialogue between attacker and society.

A group of activists dedicated against the trend of clandestine action is the *electrohippies collective*. This group uses client-side DoS as a protest method and it does so in an open manner. They write: '… we do not try to bury our identities from law enforcement authorities; any authority could, if it chose to, track us down in a few hours. However, because some of us work in the IT industry, we do not make our general membership known because this would endanger our livelihoods.'[17] Furthermore, the group has taken pains to publish its views in a series of publications available online.

In an attempt to create a dialogue on the subject of the use of DoS as a political activism tool, the electrohippies have employed the sit-in as a metaphor and they term their attacks virtual sit-ins. Since they use the client-side method they do not employ zombie machines, and without zombies their actions must be supported by those willing to carry them out. One of their claims of legitimacy is that they have the popular support of the protesters: 'Our 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.'[18]

Since they are dependent upon popular support, in order to have any effect their actions must be deemed worthy of support by the protesting individuals. To obtain this support, the collective established four principles, which govern any action they undertake. The principles are proportionality, speech deficits, openness and accountability. Proportionality refers to the insight that it is not acceptable to disrupt communications without justification; the attack itself must not be the focus. The tactic is a means and not an end: it brings publicity to an event which *is* the focus of the action.[19] The action can only be legitimate if a speech deficit exists, ie a lack of equality between the actors within the public discourse. The attack must therefore be used to draw attention to this inequality and is not in itself the intended goal. The principles of openness and accountability refer to the legitimacy of the attack, since without these it would be difficult to argue that the ultimate goal is an open discourse.

The electrohippies' views are not unopposed; another group of activists argue that since DoS attacks are a violation of people's freedom of expression and

17 DJNZ and the Action Tool Development Group, 'Client-side distributed denial-of-service: valid campaign tactic or terrorist act?' (2000) *The Electrohippies Collective Occasional Paper No 1*, February 2000, at www.fraw.org.uk/ehippies/papers/op1.html.

18 *Ibid*.

19 As an example, they cite their actions against the WTO, which coincided with the offline protests in Seattle. *Ibid*.

assembly, 'No rationale, even in the service of the highest ideals, makes them anything other than what they are – illegal, unethical, and uncivil'.[20] The electrohippies are aware of the paradox of using DoS attacks for the purpose of promoting open and free speech since they are curtailing the speech of others, but they maintain that their actions are justified if their principles are adhered to.[21]

In March 2003, virtual sit-ins organised by the electrohippies against the war in Iraq managed to disrupt the Prime Minister's website (www.number-10.gov.uk), causing it to be unavailable on several occasions. In response to criticism, they argued that their actions did not prevent any communications between the allies but were intended to show the use of official websites as a part of the propaganda directed at 'seeking to sanitise their violation of International human rights law. Action by the Collective is therefore valid in order to highlight their violation of fundamental rights by a method that seeks to restrict their misuse of the right to freedom of expression under the UN Universal Declaration'.[22]

Denial of service and law

The Computer Misuse Act (CMA) 1990 provides no remedy against DoS attacks. It creates three offences: unauthorised access to computer material, unauthorised modification of such material, and unauthorised access with intent to commit or facilitate commission of further offences. This means that the CMA can only be applied in server-side DoS attacks since these attacks require the use of zombies.

The UK realised that legislation in this area needed to take technological developments into account, and in May 2002 an amendment to the CMA was introduced to the House of Lords, which *inter alia* dealt with DoS attacks. It defined what DoS is, and the terms under which a DoS action is a criminal offence. The amendment also included changes to ensure that a person could be prosecuted for a DoS attack where proof of the action was available within the jurisdiction of the United Kingdom. However, the Bill was never passed. Legislation which can be used against DoS attacks includes the Terrorism Act 2000, which defines terrorism in this context as the use or threat of action that is designed to seriously interfere with or seriously disrupt an electronic system for the purpose of advancing a political, religious or ideological cause.

Internet-based crime led to calls for harmonisation of the substantive and procedural security laws of EU Member States, and for the UK to ratify the European Cybercrime Convention and the European Commission's proposal for a Council Framework Decision on attacks against information systems.[23] Article 4 of this Decision deals directly with the criminalisation of DoS attacks.

---

20 Oxblood Ruffin, Cult of the Dead Cow (17 July 2000) Response to Electrohippies, at www.cultdeadcow.com/archives/000865.php3.

21 *Op cit* fn 17.

22 Electrohippies Collective's online protest against the Iraq War, 2003, at www.internetrights.org.uk/casestudies.shtml.

23 COM(2002) 173 final. Adopted in April 2002, it provides a general framework to approximate and increase judicial and police co-operation in relation to attacks against information systems. Member States had until 31 December 2003 to implement the proposed framework.

These developments have had the effect of criminalising DoS attacks. Additionally, the Convention on Cybercrime reinforces the legal position that these acts are criminal offences or should be criminalised, leaving little room for interpretation of DoS as a tool of protest. In the case of DoS attacks, actions which hinder the functioning of a computer system by suppressing computer data are criminalised by Article 5 of the Convention.[24] However, despite the increase in legislation in this area, several issues of legal interpretation remain unresolved[25] and this creates an unsatisfactory position vis à vis the predictability of the law.

Toleration of disobedience

In the press conference presenting the Commission's proposal for a Framework Decision on attacks against information systems, the Commissioners created clear links between DoS and terrorism.[26] Since September 2001, as we have seen, discourse on the response to terrorism has become increasingly harsh. This has led to greater calls for the criminalisation of DoS attacks with little attention being paid to their role as a method of peaceful democratic protest.

It is often pointed out that freedom of expression is the foundation upon which any democracy stands, since without the ability to freely spread and collect ideas there cannot be a functioning democracy. Naturally, even this right must be balanced so as not to seriously hamper the rights of others. In the physical world, we tolerate (to a varying degree) our lives being occasionally disrupted. Animal rights protesters may hamper our ability to enter fast food restaurants; anti-war demonstrators may hinder our ability to travel through city centres as we normally do. Our daily lives are also hampered by jubilant rugby supporters cheering the homecoming team, crowds viewing royal pageants, or roadblocks and diversions set up to protect visiting politicians. Around the world on New Year's Eve there is mass disobedience in the streets as the New Year is ushered in. These events are tolerated by society since they are deemed important to society.

Most protesters believe in the importance of their actions. To the rest of society, these actions are annoyances. Despite this, such annoyances are important since they are the voice of dissent, and it is only through the growth of dissent into mainstream thought that social development can take place. Despite the fact that we today feel that the causes people such as Dr King and Gandhi fought for were just and their methodology is seen as being worthy of our admiration, this does not mean that civil disobedience is commonplace and acceptable in society. The goals and methods of civil disobedients in the past are always easier to accept than the goals of those protesting against the status quo today.

---

24 *Ibid*.

25 Kerr, O, 'Cybercrime's scope: interpreting "access" and "authorization" in computer misuse statutes' (2003) *NYU L Rev* 1596.

26 Commissioner Vitorino (Speech/02/174) and Commissioner Liikanen (Speech/02/175), 23 April 2002.

On the surface it would seem that society cannot create a right of civil disobedience since there can be no permission to disobey. Those who fear civil disobedience see a state of anarchy where individuals disobey rules on a whim. Fear of this anarchy maintains the status quo: a belief in the ideals of civil disobedience, a respect in the past practitioners, but no desire to create a toleration of disobedience.

A common position adopted by those who oppose disobedience is that civil disobedience has no place in a democratic society. This argument is based upon the belief that democracy is the ultimate form of self-rule, which allows the greatest amount of input from the individual on the rule of law.[27] Therefore, disobedience against the system is not the answer since the system itself is meant to be self-correcting and inequalities can be changed from within.

It is important to make the distinction that while the state may be democratic, it does not necessarily follow that all practices therein are just. To be able to redress an injustice within this system, those who are affected by it must appeal for change. This appeal is the process of bringing the injustice under the gaze of those who have the ability to create change. Singer has defined the process of disobedience as one method for a minority to appeal to the majority to reconsider an injustice.[28] The need for disobedience in such an appeal is necessary when the democratic process itself prolongs the injustice. Disobedience is therefore not intolerance towards the system but the view that allowing the democratic process to run its course perpetuates the injustice. Dr King goes further and states that there is an obligation to disobey in the situation where the law is unjust:

> For years now I have heard the word 'Wait!' It rings in the ear of every Negro with piercing familiarity … We must come to see, with one of our distinguished jurists, that 'justice too long delayed is justice denied'. … You express a great deal of anxiety over our willingness to break laws. This is certainly a legitimate concern. Since we so diligently urge people to obey the Supreme Court's decision of 1954 outlawing segregation in the public schools, at first glance it may seem rather paradoxical for us consciously to break laws. One may ask: 'How can you advocate breaking some laws and obeying others?' The answer lies in the fact that there are two types of laws: just and unjust ... One has not only a legal but a moral responsibility to obey just laws. Conversely, one has a moral responsibility to disobey unjust laws.

This still does not resolve the concern about what would happen if everyone disobeyed. Thoreau and Gandhi argue that disobedience is not a bad thing; they base this conclusion on their conception of anarchy as an equitable form of government. However, this argument does not put most of us at ease. The fear is that the legitimate actions of people like Dr King will be copied by the less scrupulous. While Dr King ensured the justification of his actions by using four stages[29] and also insisting upon non-violence from his supporters, it is often

27 Harrison, R, *Democracy*, 1995, London: Routledge.

28 Singer, P, *Practical Ethics*, 2nd edn, 1993, Cambridge: CUP.

29 Determining whether injustices exist; negotiation; self-purification; and direct action. *Op cit* fn 11.

assumed that copycats will be less thorough. This increase in lawlessness due to the acceptance of disobedience has, however, been disputed.[30]

There is another problem: if we are to objectively accept that disobedience is justified for a certain group, then how may disobedience be limited for others? This type of argument is often referred to as the slippery slope, the idea being that we cannot allow any disobedience since the moment we accept any form of disobedience we will rapidly slide to the bottom of the slope and be required to accept all disobedience.

Those who argue that the slippery slope will lead us to anarchy would prefer that no disobedience be allowed. This is a simple and elegant solution which provides us with an easily remembered rule. However, the problem of disobedience is already complex, and attempting to simplify it with absolute rules is not an equitable solution. Using the slippery slope to create a feeling of insecurity is not an acceptable solution. Such arguments have been used and abused over a long period of time;[31] their complexity may create a desire to simplify. Let us not deny justice for the sake of simple arguments.

If the protest, even the DoS, is an appeal from a minority group to the majority to reconsider and to pay attention to what is occurring within a certain situation, then it fulfils a worthwhile purpose. If the effects of DoS attacks are ephemeral, the purpose also justifies the cost. Therefore, the creation of legislation with the intent of criminalising protest under the guise of terrorism is to minimise the openness we presently enjoy in society.

Conclusion

The politically motivated online disobedient is actively partaking in a political discourse, the goal of which is to create a more equitable society. The disobedient is exercising fundamental rights of expression (and virtual assembly). Traditionally such rights are not limited without serious cause. The present legislative trends which criminalises DoS attacks in the name of terrorism are much too far reaching and seriously hamper the enjoyment of individuals' civil rights.

The blanket limitation of civil rights within a society should only be tolerated if the limitation also has the effect of removing a serious threat to the society which faces those limitations. The threat of cyberterrorism has been greatly overstated and is founded upon a lack of understanding of the technology, or even technophobia. If the threat comes not from terrorists but rather from criminal use of the DoS technique, then the legislation goes too far in its attempts to create order.

30 Dworkin, R, 'Civil disobedience', in *Taking Rights Seriously*, 1978, Cambridge, MA: Harvard UP.

31 Volokh, E, 'The mechanisms of the slippery slope' (2003) 116 *Harv L Rev* 1026.