LAW – 7000X - DISSERTATION

LLM IN MEDIA LAW, POLICY AND PRACTICE

UNIVERSITY OF EAST ANGLIA

LAW SCHOOL

LLM. DISSERTATION

CAN HACKTIVISM EVER BE JUSTIFIED?

by

Saba Şahika Tahmaz Üzeltürk

August, 2019

Supervisor: Dr. Karen Mc Cullagh

Word length: 13180

© This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with the author and that no quotation from the thesis, nor any information derived therefrom, may be published without the author's prior written consent.

TABLE OF CONTENTS

ABBREVIATIONS

APIG	All Party Parliamentary Internet Group
CFAA	Computer Fraud and Abuse Act
CMA	Computer Misuse Act
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECD	Electronic Civil Disobedience
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDT	Electronic Disturbance Theatre
EU	European Union
HRA	Human Rights Act
ISP	Internet Service Providers
LOIC	Low Orbit Ion Cannon
NASA	National Aeronautics and Space Administration
UK	United Kingdom
US	United States (of America)

ABSTRACT

As Electronic Civil Disobedience is a form of protest, and freedom of expression, some forms of it should be justifiable in order to maintain democratic values. This study submits that hacktivist acts should be justified if the actions could be considered Electronic Civil Disobedience. According to the criteria which the author created inspired by various scholars, in order for hacktivism to be classified as electronic civil disobedience, the act must be a form of expression, be a conscientious act in terms of not resulting in any personal or financial gain, and should be violent only if it is proportionate and does not constitute any physical harm. When these criteria are applied to the typology created by the author, it is seen that some the types of hacktivism should be legally justified, such as voluntary DDoS attacks, DoS attacks, virtual sit-ins, mail bombing, and site parodies. Therefore, the study asserts that CMA and Convention of Cybercrime should have a defense for justified acts of hacktivism and be amended accordingly.

I. INTRODUCTION

With the Internet 2.0 era, people started to express themselves through the internet, which had resulted in the expansion of the definition of freedom of expression. Technology opened up possibilities for human rights, both positively and negatively: while some events promote human rights, some of them are shaped as suppression[1]. Lately, the ECtHR recognized the essentiality of the internet and stated that it is a vital platform to exercise freedom of expression[2]. Right to protest eventually was affected by this expansion due to its link with the freedom of expression.

The Internet is making public discourse more accessible as it is non-elite, where everyone could join. There are also no national borders on the internet, which offers more opportunity and promotes people to find ideas. It empowers people by creating new voices on the platform who have felt voiceless[3]. Although all the positive characteristics which the internet creates, hacktivism, which is a form of online protest, is still considered as a crime. This led the author to work on this topic and to suggest regulation which could be practical to decriminalize such acts. Since no other

[1] Mahmood Monshipouri, 'Human Rights in the Digital Age: Opportunities and Constraints' [2017] Public Integrity 123-135, 123.
[2] Siofra O'Leary, 'Balancing Rights in a Digital Age' [2018] 59 Irish Jurist 59-92, 69.
[3] Dan Gillmor, *We the Media Grassroots Journalism by the People, for the People* (1st Edition, O'Reilly Media 2004) xviii.

political or social activism throughout the time had achieved such effectiveness as much as virtual activism, the author sincerely believes that hacktivism was worth to create a study.

The question which will be answered is whether hacktivism could be legally justified? In order to answer this question, the study will, first of all, talk about basic concepts to understand this term. Hence, the study will talk about concepts of civil disobedience and electronic civil disobedience and analyze the differences. Moreover, it will set out the term hacktivism and how can it be differentiated from cyberterrorism and online activism. While analyzing hacktivism, the Zapatista case will be mentioned as an example. Later on, the research will present the relationship of hacktivism with freedom of expression and freedom of assembly and will talk about the regulation of the Computer Misuse Act. Moreover, the study will assert that CMA and Convention of Cybercrime should be amended in order to have a defense for justified forms of hacktivism.

Chapter 3 will be about setting criteria to have a justification for hacktivism. It sets out the ideas of scholars such as Rawls, Electrohippies, Klang, and O'Malley and will try to create a legal justification for hacktivism based on those ideas. It will lead to the assertion that electronic civil disobedience should be legally justified if it meets certain criteria, namely that is expressive, conscientious in the means of not exercising the protest to have financial or personal gain, and violence is only appropriate if it is a proportionate response that does cause physical harm.

Chapter 4 will discuss different forms of hacktivism, apply the criteria developed in Chapter 3 to each form in order to assess if those forms could legally be justified or not. To illustrate this assessment, I have developed a typology illustrated in a color-coded pyramid, which will show which forms of hacktivism should be legally protected and which should not. Therefore, the ones that are shown with the red color will symbolize the forms which could not be justified. While yellow ones will suggest that it is unlikely to be protected legally but could be justified depending on the facts of the case, green ones indicate the forms which could and should be justified according to our criteria.

In summary, the study will conclude that information theft should not be justified, website defacement and site redirects are unlikely to be justified, and denial of service attacks, mail bombing, virtual sit-ins, and site parodies should be protected as a legitimate form of protest.

II. BASIC CONCEPTS AND THE CURRENT SITUATION

A. Civil disobedience in the pre-internet era

Offline protests have occurred since the beginning of humanity, even if they were not named as "protest". The idea of dissenting goes all the way to the ancient Greek era[4]. The tragedy of "Antigone" by Sophocles, takes the matter of dissenting to human-made laws because of those which did not have a moral value[5].

Moreover, the concept still exists because it is in human nature to question and be critical. This means that forms of protests such as marches, sit-ins, and barricades were and are always going to be a part of our lives[6]. Since people who disobey the law have moral values which justifies their action, deep inside, they think they are pointing a greater injustice while committing an illegal action[7]. This is called civil disobedience. The purpose is to create a political discussion to bring justice to that very subject[8].

A philosophical approach on civil disobedience has been analyzing after the 19th century, with theorists such as Thoreau, Bedau, and Rawls[9]. This study, however, will only analyze criteria which Rawls placed to justify civil disobedience in Chapter 3.

B. Electronic Civil Disobedience as an over-arching concept

Electronic Civil Disobedience is, in simplest terms, a political action using technology[10]. It brings methods of civil disobedience to the virtual world and therefore is an over-arching concept which also includes hacktivism[11].

---

[4] Vasileios Karagiannopoulos, 'The Regulation of Hacktivism in Contemporary Society: Problems and Solutions' (PhD. Thesis, University of Strathclyde 2013) 53.
[5] Ibid.
[6] Xiang Li, 'Hacktivism and the First Amendment: Drawing the Line Between Cyber Protest and Crime' [2013] 27 Harvard Journal of Law & Technology 301-333, 306.
[7] Mathias Klang, 'Virtual Sit-Ins, Civil Disobedience and Cyberterrorism' in Mathias Klang and Andrew Murray, *Human Rights in the Digital Age* (Cavendish Publishing, 2004)135-147, 137.
[8] Ibid 138.
[9] Mathias Klang, 'Civil Disobedience Online' [2004] 2 Journal of Information, Communication and Ethics in Society 75-83, 78.
[10] Richie Bartels, 'The Virtual Sit-in' (Master Thesis, Leiden University 2015) 16.
[11] Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy' in John Arquilla and David Ronfeldt, *Networks and Netwars* (1st edition, RAND 2001) 239-289, 263; Graham Meikle, 'Electronic Civil Disobedience and Symbolic Power' in Athina Karatzogianni Cyber Conflict and Global Politics (1st Edition, Routledge 2008)

The term was first used by a group of theorists called "Critical Art Ensemble" in 1994[12]. Critical Art Ensemble defined electronic civil disobedience as "hacking that is done primarily as a form of political resistance" and "with less expressive and more disruptive tactics"[13].

Some groups prefer calling hacktivism electronic civil disobedience; however, the author agrees with scholars who assert that not every hacktivism is considered as electronic civil disobedience[14]. Therefore, ECD is more expanded as some forms of hacktivism is lacking political and social goal and public interest[15].

Electronic Civil Disobedience does not do violence or destructive acts; instead it exposes wrongdoings of public or private institutions, reveals the unethical implementation of laws, protests against them and raise awareness to subject matter of the protest[16]. A more detailed analysis will be provided while differing online and offline protests.

C. Virtual Protests

Hacktivism is the combination of terms "hack" and "activism"[17]. It links hacking talents and social consciousness of the political protestors, which leads to demonstrating against political and social matters by using computers[18]. Hacktivists are also called "wired activists," which means that they

<https://dspace.stir.ac.uk/bitstream/1893/6577/1/Electronic%20Civil%20Disobedience%20and%20Symbolic%20Power.pdf> accessed 21 June 2019 10.

[12] Stefan Wray, 'Electronic Civil Disobedience and the World Wide Web of Hacktivism' [1998] <https://www.arifyildirim.com/ilt510/stefan.wray.pdf> accessed 17 July 2019 15; Meikle 5.

[13] Karagiannopoulos 27; Meikle 5.

[14] Jeroen Van Laer and Peter Van Aelst, 'Internet and Social Movement Action Repertoires' [2010] 13 Information, Communication & Society 1146-1171, 1159; Kenneth Einar Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' in Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking and Society* (1st Edition, Jones and Bartlett Publishers, Inc 2007) 73-99, 87.

[15] John Rawls, *A Theory of Justice: Revised Edition* (Oxford University Press 1999) 321; Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 87.

[16] Mark Manion and Abby Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking and Society* (1st Edition, Jones and Bartlett Publishers, Inc 2007) 61-73, 62.

[17] Andrew T. Illig 'Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists' [2015] 119 Penn St. L. Rev 1033-1057, 1033; Luke Goode, 'Anonymous and the Political Ethos of Hacktivism' [2015] 13 Popular Communication 74-86, 75.

[18] Illig 1033; Manion and Goodrum, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' [2000] 30 Computers and Society 14-19, 14; Tim Jordan and Paul A. Taylor *Hacktivism and Cyberwards: Rebels with a Cause?* (1st Edition, Routledge 2004) 1,30.

are skilled enough to be productive to the subject of their protest by disrupting servers and websites[19].

The term "hacktivism" was firstly used in 1996[20]. However, the first documented cyber-attack was in 1989, when NASA and the US Department of Energy were compromised to demonstrate against nuclear power[21].

The confusion of understanding the differences between "hacking" and "hacktivism" gives us a reason to explain the difference between those two terms. Hacking is included in the hacktivism concept; once electronic civil disobedience is made with hacking; it is called hacktivism.

The author, for this part, would like to follow the typology of *Denning* on virtual protests, which are online activism, cyberterrorism, and hacktivism[22].

1. Differences between hacktivism and online activism

Online activism is protests which are considered legal compared to hacktivism. While online activism is considered as legal protests, hacktivist acts are usually illegal. *Manion and Goodrum* gives a clear example to set out the distinction: If a US citizen creates a website and speaks out against a country's government it will be considered as online activism; however, if that person runs a program such as FloodNet, it will be considered as hacktivism because that program's aim is to create a blockade[23]. Therefore, there should be an unauthorized digital intrusion in order for us to call the act hacktivism. Otherwise, it will be considered as online activism because by nature, hacktivism is supposed to be disruptive; though, online activism does not constitute disruption [24].

[19] Vegh 83; Callum Beamish 'Denial of Service Attacks: Ineffective U.K. Legislative Overkill, How the Americans Do It and the Recurring Issue of Regulation' [2012] 2 Southampton Student L. Rev. 1-24, 3; Jordana J. George and Dorothy E. Leidner, 'From Clicktivism to Hacktivism: Understanding Digital Activism' [2019] Information and Organization https://doi.org/10.1016/j.infoandorg.2019.04.001 accessed 21 June 2019 17.
[20] Illig 1035.
[21] Ibid 1035.
[22] Denning 241.
[23] Manion and Goodrum in *Internet Security: Hacking, Counterhacking and Society* 63.
[24] Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 87; Julie L. C. Thomas, 'Ethics of Hacktivism' [2001] <https://www.arifyildirim.com/ilt510/julie.thomas.pdf> accessed 17 July 2019.

2. Differences between hacktivism and cyberterrorism

Cyberterrorism means hacking with the intent of terrorism[25]. In order for us to call the act cyberterrorism, perpetrators should cause damages so immense, that they should induce fear into the society as offline terrorism would do[26].

Hacktivism nowadays is interpreted so widely, that it even is being mentioned as an equivalent of the term cyberterrorism[27]. Hacktivists are seen as cyberterrorists mostly because they usually target governments and corporations[28].

What is different between hacktivism and cyberterrorism is their focus and motivation. Cyberterrorists wish to cause physical damage and harm people; hacktivists achieve to make their voices heard and make a political point[29]. While hacktivism does not have a goal to cause serious damage, cyberterrorists intent is to cause fear, and attacks lead to serious harms: either physically or financially[30].

3. Hacktivism -Definition

Hacktivism is politically-motivated hacking[31]. Hackers have the intent to have personal gain while hacktivists have the intention to gain political aim to their protests[32]. Hacktivism is narrower compared to hacking, and the difference is that in hacktivism, the motivation is to oppose any unjust practice[33]. In summary, it is using unauthorized digital means to protest or adduce the political agenda[34].

---

[25] Thomas
[26] Karagiannopoulos 171.
[27] Ibid 26.
[28] Galina Mikhaylova 'The "Anonymous" Movement: Hacktivism as an Emerging Form of Political Participation' (Master of Arts Thesis, Texas State University 2014) 4; Sandor Vegh 'Classifying Forms of Online Activism: The case of Cyberprotests against the World Bank' in Martha McCaughey and Michael D. Ayers, *Cyberactivism: Online Activism in Theory and Practice (*1st edition, Routledge 2003) 71-97, 81.
[29] Andrew T. Illig. 'Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists' [2015] 119 Penn St. L. Rev 1033-1057, 1037.
[30] Tiffany Marie Knapp 'Hacktivism- Political Dissent in the Final Frontier' [2015] 49 New Eng. L. Rev. 259- 295, 264.
[31] Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 87; Ryan Seebruck, 'A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model' [2015] 14 Digital Investigation 36-45, 38.
[32] Knapp 263; Noah C. N. Hampson, 'Hacktivism: A New Breed of Protest in a Networked World' [2012] 35 B. C. Intl'l & Comp. L. Rev 511-542, 515.
[33] Kenneth Einar Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 87.
[34] Ibid.

Hacktivism shares some of the ideas of hackers such as anarchy and libertarianism[35]. However, malicious hackers hack a computer to steal private data or to cause harm, but hacktivists do similar activities to feature political or social causes. Hacktivism is a way of strategy to pursue civil disobedience[36].

Despite hacktivism's motivation, however, which is to bring attention to the public politically or socially, it is regulated as a crime[37]. The author believes that hacktivism is the first approach which society has faced as a virtual protest[38]. The world has to absorb the fact that hacktivists are there a should be acknowledged by the society which tries to adjust itself to the differences of the virtual era[39]. Therefore, the skepticism towards hacktivism will eventually be wiped away as it happened when we were introduced with social media and many online platforms[40].

4. Zapatista: A Case Study

In 1998, Electronic Disturbance Theatre (EDT) orchestrated a high-profile operation which would introduce us to the modern days of hacktivism[41]. Zapatista Movement was one of the most famous examples of hacktivism, happened in October 1998, when the website owned by Mexican President Zedillo was attacked by Electronic Disturbance Theatre[42]. Their motivation was to protest against serious human right breaches and reject the idea of utilizing capitalism and its globalization to commit the acts of genocide and ethnic cleansing[43].

Started as a local basis, the motivation behind this rebellion was to support the struggle of indigenous people of Chiapas[44]. The EDT focused on protesting against anti-Zapatista entities

[35] Mikhaylova 4.
[36] George O'Malley, 'Hacktivism: Cyber Activism or Cyber Crime' [2013] 16 Trinity C. L. Rev. 137-160, 140; Jerrod D. Simpson, 'Unauthorized Expression: Does "Hacktivism" Have a Viable First Amendment Defense?'[2014] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473245> accessed 15 June 2019 37.
[37] Mark G. Milone, 'Hactivism: Securing the National Infrastructure' [2002] 58 Bus. Law 383-413, 386.
[38] Jordan and Taylor 172.
[39] Ibid.
[40] Ibid.
[41] Alexandra Samuel, 'Digital Disobedience: Hacktivism in Political Context' ("The Internet as Agent of Change: Bridging Barriers to Cultural, Political and Activist Discourse" Panel, San Francisco, CA, September 2001) 7; Stefan Wray, 'On Electronic Civil Disobedience' [1999] 11 Peace Review 107-111, 109; Manion and Goodrum, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' 16.
[42] Manion and Goodrum, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' 16; Denning 264; Karagiannopoulos 29.
[43] Denning 264; Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' 14.
[44] Vegh 76; Van Laer and Van Aelst 1147.

such as Mexican and US governments[45]. This activist movement drew attention to the socioeconomic system of the region included discrimination, racism, and economic inequality[46]. EDT held 13 actions supporting Zapatista movement, which at the end was engaged with 18.000 participants[47].

In order to automate the attack, EDT created an application called "Floodnet"[48]. FloodNet is a Java applet which sends reload commands[49]. It simplifies and automates virtual sit-ins because it is not possible anymore to crash the website by reloading pages manually[50]. What the group did, later on, was to aim their participants into FloodNet sites which directs them to the software[51]. Therefore, the directed software would give access to the targeted website every few seconds[52]. It also would let people publish their personal message so the regular users would understand what the reason behind the error log is[53].

This movement is a typical example of electronic civil disobedience because instead of aiming to damage alleged violators, they try to draw attention to those violated rights by disrupting computers[54].

D. How do online and offline protests differ from each other?

Online and offline protests are similar in many ways. They are both politically and socially motivated; their goal is to get attention and publicity from the relevant audience such as members of the society or organizations[55].

The preliminary idea, the very reason for demonstrating with a purpose has not changed. It only evolved into a broader scope. The world needed refreshing tools in order to make a point, and the

[45] Vegh 76; Thomas.
[46] Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking and Society* 64.
[47] Molly Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* (1st Edition, Bloomsbury 2014) 111.
[48] Vegh 76; Sauter *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 61; Alexandra Whitney Samuel, 'Hacktivism and the Future of Political Participation' (PhD. Thesis, Harvard University 2004) 76.
[49] Wray, 'Electronic Civil Disobedience and the World Wide Web of Hacktivism' 19.
[50] Meikle 7.
[51] Denning 265; Karagiannopoulos 31.
[52] Denning 265; David S. Wall *Cybercrime* (3rd Edition, Polity Press 2011) 61.
[53] Denning 265; Wall 61
[54] Mark Manion and Abby Goodrum, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' 15.
[55] Li 309.

internet gave new tools to civil societies to support their claims[56]. The concept of protesting remained, while the tools to exercise this right have developed. Unfortunately, the situation which online protest is using different tools was not acknowledged by the majority of people. Instead, legislators made regulations and acts which would restrict most of the forms of virtual protest. In 2013, Anonymous filed an online petition called "We the People" stating to White House that DDoS attacks should be considered as a legitimate form of protest but was not acknowledged[57].

One of the reasons why the concept of hacktivism became popular would be because of the regulation of online protest is more laborious than offline protests. First of all, there are many types of hacktivism, and they do not all give the same amount of damage and effect[58]. Thus, it is impossible to regulate hacktivism which would include all forms; but under some circumstances, hacktivism too could be justified by leaving some of the forms aside. The difficulty to regulate hacktivism might be apparent, but it is not impossible.

Although technological development started years ago, the approach of the society towards online protests have not fully developed. Since societies are not all yet familiar with this idea, it would cause them to be more opponent and distant towards hacktivism[59]. The word "hacking" is included in this term also worsens their skepticism. People are afraid of the term hacktivism because they would consider the term as criminal, frightening behavior of one or group of people with computer knowledge[60]. *Klang* states that one of the reasons why electronic civil disobedience is seen as a "dangerous" tool is due to the "technophobia" of people[61]. The society thinks that the whole way of people expressing their thoughts is changing and becoming dangerous with the internet. Therefore, hacktivists are being mistreated due to the misconceived point of views towards

[56] Van Laer and Van Aelst 1147; David J. Gunkel, 'Editorial: Introduction to Hacking and Hacktivism' [2005] 7 New Media & Society 595-597, 595.
[57] Dara Kerr, 'Anonymous Petitions U.S. to see DDoS attacks as legal protest' Cnet (9 January 2013) <https://www.cnet.com/news/anonymous-petitions-u-s-to-see-dDoS-attacks-as-legal-protest/> accessed 4 January 2019; Joseph Cox, 'The History of DDoS Attacks as a Tool of Protest' Motherboard (1 October 2014) accessed 20 December 2018; Argyro P. Karanasiou, 'The Changing Face of Protests in the Digital Age: on Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks' [2014] 28 International Review of Law, Computers & Technology 98-113, 98.
[58] Illig 1043.
[59] Benjamin Monarch 'The Good Hacker: A Look at the Role of Hacktivism in Democracy' [2015] <http://dx.doi.org/10.2139/ssrn.2649136> accessed on 15 July 2019 3.
[60] Molly Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet' (Master Thesis, MIT 2013) 15; Tiffany Marie Knapp 'Hacktivism- Political Dissent in the Final Frontier' [2015] 49 New Eng. L. Rev. 259- 295, 262; Meikle 12.
[61] Klang 'Civil Disobedience Online' 82.

technology. This is what makes hacktivism turn into a chilling effect because hacktivists could refrain themselves from launching those actions due to prejudices, negativity, and excessive sanctions they are facing[62].

A promising occurrence regarding hacktivism happened in 2001, with the virtual sit-in organized against *Lufthansa*, an essential development for the legality of hacktivism occurred with the Frankfurt Appellant Court's decision[63]. A DDoS attack launched with the participation of 13.000 German activists which caused some downtime to the airline's homepage organized by "Kein Mensch ist illegal (No man is illegal)" and "Libertad!" [64]. The main reason for the protest was because *Lufthansa* was allowing the German government to use its flights to deport asylum seekers[65]. Those groups used an adapted version of Floodnet which was created by the EDT and eventually their website shutdown[66]. Therefore, the company stopped aiding the government for deportation, and the protest was quite successful[67].

Yet, it did not stop the judicial branch to file a suit against Andreas Thomas Vogel who was an activist and the man behind the "Libertad.de" site, and he was fined and given imprisonment of 90 days serving with either paying fines or imprisonment[68]. The lower Court of Frankfurt found Vogel guilty due to the economic losses which *Lufthansa* had experienced caused by the attacks[69].

However, the next year, the higher court overturned the verdict by asserting that his acts are recognized as contributions to public debate[70]. The court also stated the virtual sit-in did not cause any violence but was made to change the public opinion[71]. The court, thus, protected the free speech of the protestors[72]. As a result, since hacktivists attacked a major company, the disruption was not

[62] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 7.
[63] *Oberlandesgerichts Frankfurt am Main v Thomas Vogel* No.1 Ss 319/05.
[64] William E. Scheuerman, 'Digital Disobedience and the law' [2016] 38 New Political Science 299-314, 300; Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 53; Meikle 8; EDRI, 'Frankfurt Appellate Court Says Online Demonstration is not Coercion' (7 June 2006) https://edri.org/edrigramnumber4-11demonstration/ accessed 31 July 2019.
[65] Scheuerman 300; EDRI.
[66] Meikle 7; Bartels 27.
[67] Scheuerman 300.
[68] Bartels 30; *Oberlandesgerichts Frankfurt am Main v Thomas Vogel* No.1 Ss 319/05.
[69] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 140.
[70] Scheuerman 300; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (1st edition, Public Affairs 2011) 228.
[71] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 140.
[72] Karagiannopoulos 48.

amounted to that company to cease its services, which means that the company kept functioning[73]. *Lufthansa* was able to fly planes and maintain their communication internally; that is why the protest was considered proportionate[74]. These actions show us that even if hacktivist actions can be disruptive; this is not the primary goal[75]. The main goal is to act to get attention on the subject matter, which shows us the conscientiousness of hacktivism[76].

The counter effect of this case, however, is not very encouraging because the verdict was held before the criminalization of DDoS attacks by the treaties[77], which made it impossible for Germany to give a similar verdict[78]. This means that the court will be bound to apply international rules[79]. Still, this case shows us the acknowledgment of hacktivism as an expression even if it does not mean that we can exonerate protesters using this case anymore[80].

One other common character between online and offline protests is that they both occupy some space. While the offline protest occupies streets, online protests occupy virtual space.

As we all know, the internet is not tangible. Therefore, it is very argumentative to decide whether it is a public or private space[81]. What is known for sure is that currently there is no public space on the internet[82]. Even if there are platforms specifically created to express thoughts, they are owned by a private company, and the content is owned and surveilled by Internet Service Providers[83].

While civil disobedients of the non-virtual world have undisputable locations such as general public spheres to protest, this is not the case for hacktivists. It seems absurd not to cover the right to freedom of expression held in a public space for the virtual world which is one of the most influential and popular platforms where people prefer to exercise their right to freedom of

[73] Bartels; Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 53,54.
[74] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 53.
[75] Ibid.
[76] Ibid 54.
[77] Convention of Cybercrime 2001; EU Council Framework Decision 2005/222/JHA On Attacks Against Information Systems.
[78] Karagiannopoulos 50.
[79] Ibid.
[80] Ibid.
[81] Bartels 23.
[82] Bartels 24; Hampson 532; Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet'13.
[83] Bartels 24; Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet' 12.

expression[84]. The situation is, as *Sauter* states, "the critique goes 'Can't you come up with a way to protest that does not step on somebody else's toes?' But the internet, as it were, is all somebody else's toes" which is enough to explain the whole situation of the internet not having appointed public spheres[85].

Case law in Europe and the US gives more importance to private property rights when it is conflicting with freedom of expression[86]. As an example, *Appleby v. UK*[87] shows us that in order to have a legally acceptable protest, there should be a direct link between the cause of the protest and the private place[88]. There should also be non-existence of an alternative place to protest[89]. The latter would be easy to solve in the virtual world since there are no appointed public spaces on it; however, the first part is important for the virtual protests, because it would give us the reason why we should count public institutions' home pages as a public place on the internet.

The lack of public places in the virtual world could lead us to think either that we should count some of the websites as public space like the government websites or we should be able to justify hacktivist acts directly on privately-owned spaces[90]. As *Morozov* stated, "If society tolerated organizing sit-ins in the university offices and temporarily halting their work, there is nothing wrong with allowing students to organize [DDoS] attacks on university websites[91]. Hence, the author believes that governments' or public officials' home pages could be assimilated to the lobby or space in front of their buildings which in the real world would be considered as a public space and would be a possible place to protest. Internet is originally a space for discussion and exchange of thoughts thus should be considered as a public sphere and hacktivism is a vital institution in the virtual world since they are contributing to the free flow of information, use their computer know-how to make sure that people know there is an injustice[92]. Therefore, we could say that accessing webpages becomes inevitable, of course, within the boundaries of proportionality[93].

---

[84] Chris Baraniuk, Interview with Molly Sauter, 'Legalise Digital Protest' [2014] 224 New Scientist.
[85] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 4.
[86] Karagiannopoulos 47.
[87] [2003] 37 EHRR 38.
[88] Karagiannopoulos 47.
[89] Ibid. 48
[90] Ibid. 49.
[91] Morozov 228.
[92]Karagiannopoulos 49; DJNZ and the Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' [2001] 34 Leonardo 269-274, 269; Scheuerman 313.
[93] Karagiannopoulos 49.

Lastly, the author would like to state that if people would not get punished by all injustices they cause, why do we keep punishing hacktivists who tries to create a public discourse, just because the tool they are using is hacking? Those people want to reach out to the public against unfairness. Just as the rest of the people, who would try to find the best platform if they are experiencing injustice or dissent which they feel is not fair, hacktivists too, are trying to use their best tools they have got. The reason is that a person simply would not choose the weak platform if they sincerely believe that something is unjust and should be ameliorated.

E. Freedom of Expression, Freedom of Assembly and their limits

Freedom of expression is one of the most known rights among human rights[94]. Studies show that 142 countries' constitutions already regulated freedom of expression[95]. The marketplace of ideas, which is the foundation of free speech theory states that democracy would not reach its maximum level without the free flow of information[96]. In order to reach the truth, there should be an environment where there is a competition of conflicting ideas and opinions[97]. Therefore, freedom of expression could not exist without ensuring people's rights to access information. Being able to express thoughts without interference is essential for our autonomy, dignity, and self-worth[98]. Hence, restricting free speech and protest could be a type of censorship which would allow third parties, courts in our case, to decide whether your speech is worth to be heard[99].

In Europe, freedom of expression has mostly relied on the European Convention on Human Rights. The 10th article of the Convention ensures that everyone has a right to freedom of expression[100]. On the second part of the article, restrictions on the freedom of expression are regulated[101]. According to this, states may restrict those rights if the cause of the restriction is prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for

[94] Mark W. Janis, Richard S. Kay and Anthony W. Bradley, *European Human Rights Law: Text and Materials* (3rd Edition, Oxford 2008) 235.
[95] Ibid.
[96] John Stuart Mill and others, *On Liberty* (1st Edition, Yale University Press 2003) 31; Li 312; Illig 1048.
[97] Li 312
[98] David Mead, *The New Law of Peaceful Protest: Rights and Regulation in the Human Rights Act Era* (1st Edition, Hart Publishing Ltd 2010) 7.
[99] Ibid.
[100] European Convention on Human Rights 1953 (ECHR) Article 10; Bernadette Rainey, Elizabeth Wicks and Clare Ovey, *The European Convention on Human Rights* (6th Edition, Oxford, 2014) 435.
[101] ECHR Article 10; Rainey 435.

the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary[102]. ECtHR will seek whether Article 10 is engaged first or not; then, will analyze restrictions stated by the article one by one[103]. This means that the Court will evaluate and try to balance rights clashing with the freedom of expression[104].

States have some level of discretion supervised by the European Court of Human Rights to take legislative, administrative and judicial actions which is called the "margin of appreciation"[105]. The Court's duty is not to take the place of Member States and give a judgment; instead, to review under Article 10, if the nation's approach is consistent and compatible[106]. As stated in *Handyside v UK*, the margin of appreciation granted to contracting parties should be proportionate[107]. Therefore, those restrictions stated above must also be proportionate to the legitimate aim[108].

With the margin of appreciation principle, the Court will first seek the necessity of interests of the national regulation, which will depend on the state[109]. Secondly, the Court will evaluate whether governments are in touch with the vital forces of their countries to assess that necessity rather than the ECHR[110].

The United Kingdom, as a signatory state, on the other hand, implemented the "Human Rights Act" to regulate the fundamental human rights derived from the ECHR[111]. Thus, whenever there is an allegation which curtails the right to freedom of expression of a protestor, British courts should be able to apply Article 10[112].

[102] Rainey 435; ECHR Article 10, 11; D. J. Harris and others, *Law of the European Convention on Human Rights* (4th Edition, Oxford 2018) 12.
[103] Harris 631.
[104] Rainey 436.
[105] Harris 15.
[106] Rainey 440.
[107] *Handyside v United Kingdom*, (App. 5493/72) 7 December 1976, Series A No 24, 1 EHRR, 48; Rainey 437; Harris 15.
[108] Harris 12.
[109] Janis 242.
[110] Ibid.
[111] Hampson 530.
[112] ECHR Art. 10; O'Malley 148.

Article 11 of ECHR ensured that everyone has the right to freedom of assembly and freedom of association and freedom of expression is a term which includes and protects forms of protests[113]. Free speech and by extension, the right of peaceful protest might be justified or asserted as being valuable compared to others even if this does not mean that there is no superiority among fundamental human rights[114].

Regarding the topic of this study, we could state hacktivism could enjoy rights to freedom of expression and peaceful assembly because ECHR defines "peaceful protest" as the term includes "conducts which may annoy or give offense to persons opposed to the ideas or claims that it is seeking to promote"[115]. With this, the Court expands its non-violence criteria for peaceful protests.

Secondly, the guideline of Venice Commission states that this conduct should also include the ones which "temporarily hinders, impedes or obstructs the activities of third parties"[116]. In addition, according to *Handyside v. UK*[117] the information or ideas which are protected, including those that offend, shock, or disturb the State or any sector of the population[118]. In summary, we could count some forms of hacktivism, which will be analyzed later in this study, as a peaceful protest because it only damages parties temporarily and is being launched to annoy of offense people to create public discourse and present a dissent.

However, it should be noted that just because most of the forms of hacktivism is considered as an expression does not mean they all need to be legitimized[119]. Even if it could be possible to accept hacktivism under the scope of freedom of expression and freedom of assembly, these acts do still fall within the criminal law sanctions under the CMA in the UK and Convention of Cybercrime[120].

---

[113] ECHR Art. 11; Donna Gomien, *Short guide to the European Convention on Human Rights* (3rd Edition, Council of Europe Publishing 2000) 117; O'Malley 139; *Stankov and the United Macedonian Organisation Ilinden v Bulgaria* (2002) App No 29221/95 and 29225/95 para 85.

[114] Mead 7; Gomien 117.

[115] Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom, 'Draft Report on Freedom of Assembly and Association on the Internet' (30 September 2015) MSI-INT (2014) 08 rev5 para 59; *Stankov and the United Macedonian Organisation Ilinden v Bulgaria* (2002) App No 29221/95 and 29225/95 para 86; *Plattform "Ärzte für das Leben" v Austria* (1988) Series A no. 139 para 32.

[116] European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 'Guidelines on Freedom of Peaceful Assembly' (9 July 2010) para 26.

[117] *Handyside v United Kingdom,* (App. 5493/72) 7 December 1976, Series A No 24, 1 EHRR, 48.

[118] Rainey 436.

[119] Hampson 533.

[120] Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom, 'Draft Report on Freedom of Assembly and Association on the Internet' (30 September 2015) MSI-INT (2014) 08 rev5 para 59.

F. Computer Misuse Act 1990

CMA is the primary legislation of the UK for the computer crimes which was amended by the Police and Justice Act[121] . The act has three criminal offences, such as unauthorized access to computer material[122], unauthorized access to computer material with the intent to commit or facilitate further offences[123], and lastly unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.[124]

Before the CMA was drafted, rules applied to the real world would also be applied to the virtual world. This caused many problems because even if those two worlds had much in common, they had many difficulties, such as concepts of anonymity and automation[125]. After *R v. Gold*[126], Due to the deficiency and the legal gap in the virtual world, the UK wanted to establish an act to regulate the criminalization of computer abuse and misuse actions; therefore, CMA was drafted[127].

The aim of the CMA was due to the need to protect and secure computers from attacks[128]. However, apart from this need, there were other needs, such as the concept of property and tangibility of computer information, but this was not regulated[129].

Section 3 of the Act is about when a person commits an offense knowingly and intentionally, which causes an unauthorized act on a computer, any particular program, or data[130]. The sanction given for section 3 is imprisonment of up to ten years and/ or fine on indictment while up to a year and/or fine on a summary conviction in Scotland[131]. The original text of section 3 did not consider DDoS attacks as illegal because of the term "unauthorised modification." Since DDoS attacks would not modify any substances, those attacks could not be convicted[132].

---

[121] Computer Misuse Act 1990 (CMA); Police and Justice Act 2006; Beamish 1.
[122] CMA s.1
[123] CMA s.2
[124] CMA s.3
[125] Beamish 7.
[126] [1998] AC 1063.
[127] Beamish, 8; Klang, 'Civil Disobedience Online' 76.
[128] Law Commission, Criminal Law Computer Misuse (Law Com No 186, 1989) para 2.11-2.15; Neil McEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' [2008] 12 Crim. L.R. 957.
[129] Beamish 8; Neil McEwan, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' [2008] 12 Crim. L.R. 955-967, 957.
[130] CMA, s.3
[131] Karagiannopoulos151.
[132] Andrew Murray, Information Technology Law: Law and Society (3rd Edition, Oxford University Press, 2016) 378.

DPP v Lennon[133] also helped us to understand the view of legislators because courts had a hard time to apply the law to the current situation which the mail bombing program that Lennon used did not amount to a "modification" as the section sought[134]. Thus, this case influenced a change on the act, and it was generally accepted that data does not have to be modified to commit the act[135].

CMA was also not in accordance with Article 5 and 6 of the Convention of Cybercrime[136] , which states that each country must adopt national measures to protect the attacks on system interference and misuse of devices. Article 3 of the EU Framework Decision on Attacks against information systems would also refer to the same situation[137]. Article 4 of the same EU Framework Decision also criminalizes DoS attacks[138]. Therefore, the new section 3 was created according to all international treaties and applying APIG recommendations[139]. This way, DoS attacks are regulated following an amendment which came into force on 1st October 2008 according to the s.35-36 of the Police and Justice Act[140]. By this way, legislators made the actus reus principle broader[141].

In the UK, the perception of criminalizing hacktivism is more likely to be within the bounds of possibility[142]. It would be a low possibility for the UK to recognize hacktivism as an exception to the Computer Misuse Act because international treaties criminalize all unauthorized acts. Hence, with the current situation, there is no possibility to decriminalize hacktivism within the boundaries of Criminal Law unless the legislation changes.

In conclusion, the author believes that restricting unauthorized attacks for organizations who are trying to exercise their right to protest deserves a defense for hacktivists to reduce or decriminalize the act if it is proportionate and applicable to criteria which will be suggested in the next chapter. The CMA and accordingly Convention of Cybercrime has to be revised and include a defense for

[133][2006] EWHC 1201.
[134] John Worthy and Martin Fanning 'Denial of Service: Plugging the legal loopholes?' [2007] 23 Computer Law & Security Report 194-198, 194.
[135] Ibid. 195
[136] Convention on Cybercrime 2001, Art. 5,6.
[137] Karagiannopoulos 156; Murray 378; EU Council Framework Decision 2005/222/JHA On Attacks Against Information Systems Art.3.
[138] EU Council Framework Decision 2005/222/JHA On Attacks Against Information Systems Art.4; Karagiannopoulos 156.
[139] Beamish 11; Wall 61.
[140] Police and Justice Act 2006.
[141] Stefan Frederick Fafinski, 'Computer Use and Misuse: The Constellation of Control' (PhD. Thesis, The University of Leeds 2008) 76; Wall 61.
[142] Hampson 535.

justifiable forms of virtual protests so that hacktivists would enjoy their fundamental rights even if there is unauthorized access.

III. CRITERIA ON JUSTIFYING (ELECTRONIC) CIVIL DISOBEDIENCE

There are criteria offered by different scholars, who are trying to find a justification for civil disobedience. This study will carry some of those scholars' ideas, consisting of Rawls, Electrohippies, Klang, and O'Malley; to justify hacktivism in the light of those criteria. It should be noted that these criteria will not be adopted on a word-for-word basis. Instead, they will be distilled to offer a synthesis of ideas which the author later uses to classify forms of hacktivism to conclude whether they are justified or not.

A. Rawls

Rawls' definition of civil disobedience is *"public, nonviolent and conscientious yet political to the law usually done with the aim of bringing about a change in the law or policies of the government"*[143].

As the first criterion, *Rawls* stated that "civil disobedience is a public act: not only it is addressed to the public principles, it is done in public"[144]. However, as stated in the latest chapter, there are no appointed public places on the internet. Since the internet is free, open, and includes official websites, it could be said that those very spaces have the intention to become a public sphere or as we stated above, we could count official websites as public space where it is allowed to protest.

The second and the "central identifier" of civil disobedience is to have an act that is damage free[145]. "Violence is any undesirable situation which causes an offence or an inconvenience"[146]. If it is a violent hacktivist act such as seizing control of computers, modifying information and stealing data, there cannot be a justification to legalize hacktivism[147]. Therefore, it is impossible for a type of hacktivism such as information theft or DDoS attacks which utilizes involuntary botnets to be justified as a legitimate form of protest[148].

[143] Rawls 320; Bartels 50; Scheuerman 308.
[144] Rawls 321.
[145] Bartels 10.
[146] Karagiannopoulos 71.
[147] Hampson 537.
[148] Hampson 533.

Another criterion to justify civil disobedience is that there should be a conscientious belief that the situation in which protesters are disobedient about is creating an injustice[149]. Conscientiousness is the responsibility which would lead to the security of the public support: it is a criterion which would strengthen the action and establishes the sincerity and the morality of the disobedience[150]. Conscientious acts can only be legitimized if they are being done to ameliorate the rules of law by also having fidelity towards the legal system[151].

In order for us to count the act as civil disobedience, there also should be an act which disobeys the law; which means that there should be volunteerism to break the law[152]. For the concept of justifying civil disobedience, the breach of law should be regarded as a narrower meaning: the breach of law is not towards the whole legal system, but it is towards that specific legislation or situation which is seen as unjust by the disobedients[153].

One of the other criteria was the willingness to accept the possible outcomes of the act[154]. There should be an intentional acceptance of the possible punishments that protestors could receive[155]. The draft report of the Council of Europe suggests that disobedients should have the willingness to have the possible legal consequences[156]. Willingness also includes that the act of civil disobedience should also be conscientious, which means that they should have a genuine and serious belief that the current legislation of the subject of the protest creates injustice[157].

Lastly, *Rawls* states that "since civil disobedience is a last resort, we should be sure that it is necessary"[158]. Platforms should be as relevant as possible[159]. Therefore, disobedients should use the platforms which are relevant to what they are demonstrating[160].

[149] Karagiannopoulos 66.
[150] Bartels 5.
[151] Scheuerman 301.
[152] Karagiannopoulos 51.
[153] Bartels 6.
[154] Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in *Internet Security: Hacking, Counterhacking and Society* 63.
[155] Karagiannopoulos 82.
[156] Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom, 'Draft Report on Freedom of Assembly and Association on the Internet' (30 September 2015) MSI-INT (2014) 08 rev5 para 61.
[157] Bartels 5.
[158] Rawls 327.
[159] Ibid.
[160] Karagiannopoulos 82.

B. *Electrohippies*

Electrohippies suggest that if there is proportionality, openness, speech deficit, and autonomy while making a protest and therefore restraining other people's freedom of expression and causing a proportional amount of violence, then the online civil disobedience should be justified. In order to justify the act, the main goal should be to create public discourse and get attention from the public. A hacktivist attack should have a focus, and the tactics should occur regarding that focus[161].

Proportionality also should exist in a hacktivist tactic, which means that it would not be acceptable to virtually protest against an organization on a general basis[162]. If consequences of damages and restrictions on the freedom of expression are more critical than the protests of disobedients, then it would be impossible to justify civil disobedience.

C. *Klang*

Klang sets out four criteria to justify civil disobedience and asserts that if those criteria would be transferred into the digital area, there is no reason why online civil disobedience could not be justified[163]. The first criterion is "disobedience," which means that there should be a non-permitted action by the law with the desire to protest, which is very similar to *Rawls'* "breach of law" criterion[164]. In our situation, since many types of hacktivism which will be covered in the next chapter is considered as "legal," it would be apparent for us to state that hacktivism is considered as disobedience[165].

The second criterion that *Klang* presents is "civil"[166]. In order to be civil, there needs to be a publication and the public interest of the protest[167]. In online civil disobedience, however, there might be issues because of the multinational character of the internet and hence hacktivism because firstly the targeted person's acts could be considered as legal in its country and secondly the attacker could not be from the target's country which would not give the rights to have a direct demonstration[168]. Nevertheless, even if this criterion could have weakened the justification of

[161] DJNZ 272.
[162] Ibid.
[163] Klang, 'Civil Disobedience Online' 80.
[164] Ibid 79.
[165] Ibid 80.
[166] Ibid.
[167] Ibid.
[168] Ibid.

online civil disobedience, the author believes that the global character of the internet would be an important reason to tolerate these facts[169]. Therefore, this criterion will not be added to criteria which the author displays.

The third criterion in which *Klang* displays is "non-violence"[170]. There is a misconception about civil disobediences stating that there is no space for violence[171]. Naturally, in civil disobedience, violence could be included and be tolerated if it does not cause physical harm and is proportionate with the act of the protest[172]. In online civil disobediences too, the most criticized topic is the limitation of access to personal property[173]. *Illig* states that if hacktivism damages people, it should not be legitimized. It should not be forgotten that there are hacktivist acts, will be analyzed in the next chapter, which does not cause any damage, and it would not be fair to exclude them from legalizing it[174]. They should be legal as far as it does not cause disproportionate harm[175].

According to the analysis the author had while differing differences between online and offline protests, since most of the attacks would only cause a temporary disruption, it is not a severe violent act towards websites which should, of course, be evaluated on a case-by-case basis regarding proportionality[176].

The last criterion is "justification"[177]. The civil disobedience's justification is when there is a breach of law made with moral values[178]. The actions of disobedients should also constitute some willingness to face the sanctions of their actions[179]. This means that compared to *Rawls'* justification of civil disobedience, this criterion includes "conscientiousness" in the means of breaching the law and willingness.

For the online civil disobedience, however, we often see that the "willingness" is not satisfied. In response, *Electrohippies* suggests that even if hacktivists would not openly show themselves, they

[169] Ibid 81.
[170] Ibid.
[171] Ibid 80.
[172] Ibid.
[173] Ibid 81.
[174] Illig 1048.
[175] Ibid.
[176] Klang, 'Civil Disobedience Online' 81; Morozov 228.
[177] Klang, 'Civil Disobedience Online' 80.
[178] Ibid.
[179] Klang, 'Civil Disobedience Online'81; Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' *Internet Security: Hacking, Counterhacking and Society* 63.

do not hide either; the reason why they would not reveal their identity is that it would endanger their livelihoods or personal safety[180]. This approach would not go along with *Rawls*' idea of justified civil disobedience, by contrast, since online civil disobedience faces with more prejudices than civil disobedience and have more excessive sanctions which seem unfairly regulated, lack of willingness should be more tolerated[181].

D. O'Malley

According to *O'Malley,* there are certain factors which must be present for protests to be legally justifiable[182]:

First of all, justified disobediences should be non-violent[183]. Secondly, the motivation of the justified protest should be derived from injustice[184]. Thirdly, there should be a message behind the protest so it would be considered as an expression[185]. As outlined in Chapter 4, forms of hacktivism such as involuntary DDoS attacks and information theft will be outside the scope of a legal protest due to the lack of expression, justifiable political or social background and non-violence[186].

The fourth factor of a legal protest is proportionality[187]. There should be a balance between the expression and the disruption or damage given to society[188]. *O'Malley* argues that if actions such as DDoS attacks would be nothing but large-scaled, aggressive, and disproportionate then it should not be justified[189]. This approach is also similar to *Electrohippies'* idea to proportionality while putting criteria on justifying civil disobedience. *Klang*, on the other hand, evaluates proportionality under the "non-violence" criterion.

The last factor is the willingness of the attacker to face the consequences[190]. This is the hardest factor among all because hacktivists are usually anonymous, and they are often not identifiable[191].

[180] Klang, 'Civil Disobedience Online' 81.
[181] Ibid.
[182] O'Malley 156
[183] Ibid.
[184] Ibid 157.
[185] Ibid.
[186] Ibid.
[187] Ibid.
[188] Ibid.
[189] Ibid.
[190] Ibid 158.
[191] Ibid.

E. Summary

As indicated criteria created by such scholars to justify civil Disobedience, we could see that most of the ideas of scholars are based on *Rawls'* ideas. Even if there are terminological differences between them, the idea stays the same. As an example, while talking about "breach of law" criteria, *Klang* preferred to use the term "Civil" instead. Also, *O'Malley's* "injustice" criterion does contain the same information with the "conscientiousness" criterion. Overall, we see that all scholars mentioned about criteria of willingness, non-violence, proportionality, breach of the law, and conscientiousness more or less.

Since *Rawls'* ideas are from the pre-internet era, he does not have an evaluation on electronic civil disobedience. Therefore, if we compare the ideas behind justifying civil disobedience and electronic civil disobedience, we could state that there are small differences about criteria of "willingness" and "public".

While *Rawls* is talking about "public" criterion, he mentions that the act should be in public. This creates problems when we convert this idea to the virtual world, due to lack of public sphere as discussed in the previous chapter.

The author believes that the "willingness" cause problems for electronic civil disobedience because the issue of anonymity and extreme sanctions and therefore should not be included in our criteria. Although this does not mean that it will not be taken into account while evaluating forms of hacktivism.

Even if this criterion would be challenging to be applied to the virtual world, it should be stated that there should be more tolerance towards hacktivism. It is not surprising that most of the hacktivists would feel hesitant to accept the legal consequences of their acts seeing that sanctions are mostly extreme compared to offline protests as also mentioned by *Electrohippies*[192].

For this criterion, the term "anonymity" is also vital because if we do not know the person or the group who committed the act, that person could not face the circumstances[193]. Thus, it seems hard to justify hacktivism with anonymity in that sense[194]. Hacktivists can feel less intimidated by

[192] Scheuerman 308.
[193] Himma 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 74; Tom Sorell, 'Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous' [2015] 7 Journal of Human Rights Practice 391-410, 391.
[194] Knapp 263.

expressing themselves anonymously rather than publicly. Because even if this will mean that they will be seen less trustable by society, if they feel more independent, hacktivism should be allowed and would not constitute a problem[195].

F. The author's criteria

Having provided an overview of the criteria that should be taken into account to justify electronic civil disobedience, this author contends that, forms of electronic disobedience which are (i) primarily expressive (ii) which does have conscientiousness in the means of not involving unauthorized access to computers for personal or financial gain, (iii) which causes violent action only if it is not physical and is proportionate should be regarded as a legitimate form of protest[196].

Hence, types of hacktivism which are primarily expressible, non-violent, proportionate, and does not illegally access and modifies information on computers to have a financial advantage, should be protected as a type of protest[197].

1. Expressive

According to *O'Malley*, there should be a message behind the civil disobedience; therefore, civil disobedience should be primarily expressive[198]. If hacktivism has bad intentions and promotes censorship, there will not be any justification for the hacktivist act.

As the allegation that hacktivism has bad intentions and promote censorship, we could say there are hacktivists with bad intentions. We could see that from such forms of hacktivism which are being used to access and modify data. Censorship could be opposed in the eyes of hacktivists but sometimes also can be promoted or used[199]. For example, in 1997, a mail bombing attack was launched against a Spanish ISP called "IGC" due to oppositions against Euskal Herria Journal[200]. Hacktivists which held the majority in Spain, did not want the journal to be published and thus hacked into IGC which forced IGC to remove the publications[201]. This is an example where

[195] Sorell 392.
[196] Hampson 526; Karagiannopoulos 91.
[197] Hampson 532.
[198] O'Malley 157.
[199] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 52.
[200] Ibid.
[201] Ibid.

hacktivism could lead to censorship because the sole cause of ISPs to exist is to provide these services online if not, the corporation will have a high amount of damage.[202].

However, this does not prove that hacktivists do not have good intentions. The core mentality of hacktivism is to expose unjust applications of organizations, individuals, or governments and promote the free flow of information[203]. It would ideally be expected from a protestor to react against morally wrongful acts[204]. On the other hand, the strict distinction of stating hacktivism is either good or bad would be superficial for this profound concept, since hacktivism is an irreducible concept in the means of being good or bad[205].

As an excellent example to hacktivists with good intentions would be Aaron Swartz. Aaron Swartz, a hacktivist who "gave his life" to fight against human rights violations, committed suicide while he was being charged under CFAA because of his actions[206]. He was trying to make JSTOR, an academical database, articles accessible to more people, but he ended up being charged with imprisonment for 35 years and monetary fine up to one million dollars which eventually caused him to take his own life because he could not resist being charged anymore[207].

Swartz thought that students, scientists, and academicians should have the privilege to access all documents to do their research[208]. He suggested that accessing information is one of the most important fundamental rights of the human-kind which should be carefully protected and the Internet is a contemporary tool to execute this right, and yet, unfortunately, his actions were not justified[209].

Hacktivism can be considered as disruptive speech, but this does not mean that they are in denial of freedom of expression. One of the main goals of hacktivism is to promote freedom of expression and free flow of information by using their right to protest, which is also considered as a fundamental human right[210].

---

[202] Ibid.
[203] Monarch 4.
[204] Klang, 'Civil Disobedience Online' 82.
[205] Gunkel 596.
[206] Knapp 260.
[207] Scheuerman 300; Monarch 13.
[208] Monarch 13; Simpson 7.
[209] Simpson 33.
[210] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 49.

2. Conscientious

Rawls states that conscientiousness should be understood in the means of morality and sincerity[211]. The author, on the other hand, thinks that the idea of conscientiousness should be narrowed down towards the *Electrohippies'* approach, which is that the main approach of the protest should be about creating a public discourse[212].

In order to legitimize electronic civil disobedience, we should be able to prove that the act is not made to become vandals or cyberterrorists, meaning that it should be ethically and politically motivated[213]. Hence the focus of the protest should not be based on any personal or financial gain; it should be about getting the attention of the public.

3. Restrained Violence and Proportionality

As recognized, the virtual world could not harm anyone physically. Therefore, in order to imitate the non-violence criterion to the virtual world, there should be a more abstract interpretation which goes beyond physical damage or any other damage to property[214]. In order for us to make this interpretation, we have to widen the scope of violence[215].

We could say that hacktivism is disruptive because this is the nature of the actions[216]. Even if in some cases damage to property is acceptable and proportionate, violence to people is never acceptable[217]. It should be noted that to fulfill this criterion, there should be a proportional approach between the law-breaking act and the injustice in which the subject of the protest creates[218]. Thus, the author takes *Klang's* approach about this criterion and states that violence on cyberspace could be constituted as justifiable if there is no physical damage, and the damage given to the personal property is proportional and not permanent[219].

No matter the purpose of hacktivism and how horrible the subject of the protest sounds, hacktivists should take reasonable actions to be able to claim that their actions were carried with political

[211] Karagiannopoulos 66.
[212] DJNZ 272.
[213] Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in *Internet Security: Hacking, Counterhacking and Society* 63.
[214] Karagiannopoulos 74.
[215] Ibid.
[216] Thomas
[217] Bartels13.
[218] Karagiannopoulos 70.
[219] Klang, 'Civil Disobedience Online' 81; Karagiannopoulos 76.

intentions and a way of civil disobedience[220]. If their actions are disruptive, which is not equivalent to violence, yet communicative and reasonable, then there is a possibility that their actions could be justified[221].

One of the main criticisms of hacktivism is that it would curtail other people's freedom of expression[222]. *Electrohippies* suggests that if curtailing freedom of expression is because of the speech deficit of the attacking group and is only being exercised as a medium, not as the primary goal, then it should be justified[223].

As a way of free speech, hacktivism is also impermissible insofar as it could result in harming innocent third parties: it could be a variety of people such as website owners and users[224]. If it harms, it is outside the scope of proportionality.

It should be reminded that in real-world protests, we tolerate being disrupted all the time. Offline protests would usually cause disruption but the society would more likely to be borne because the people should tolerate others to protect demonstrators' fundamental rights which will, later on, affect theirs if one day they would decide to stand against something[225]. However, even if conditions are the same, virtual protests do not exercise the same rights as offline protests, which is not fair[226]. The correct way of having this idea should be exercised in both online and offline protests. As *Klang* states, "the creation of legislation with the intent of criminalizing protest under the guise of terrorism is to minimize the openness we presently enjoy in society"[227].

It would be beneficial towards society if we have the chance to use hacktivism to reveal people or nations go unheard due to their Internet restrictions[228]. More people could be able to express themselves. We have a platform, called internet which has a chance to double, even triple the amount of audience, so we should take full advantage of it, in order to bring more democracy to the world, as long as it does not seriously breach other people's lives.

---

[220] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 31.
[221] Ibid 32.
[222] Klang, 'Civil Disobedience Online' 81.
[223] Ibid.
[224] Himma, 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' 74.
[225] Klang, 'Civil Disobedience Online' 82.
[226] Hampson 540.
[227] Klang, 'Virtual Sit-Ins, Civil Disobedience and Cyberterrorism' 143.
[228] Hampson 540.

IV. TYPOLOGY OF HACKTIVISM AND WHETHER ACTIONS SHOULD BE REGARDED AS LEGITIMATE FORMS OF PROTEST

This part will give the most used types of hacktivism, by providing how they work along with examples to show whether which type should be regarded as a legitimate form of protest. Seven types of activity will be considered starting from type(s) of activity which has/ve the lowest potential to be legal to those which has/ve the highest potential to be legalized.

A typology of hacktivism developed by this author is used to categorize hacktivist activities. The red color represents the ones which could not be legitimized, yellow ones represent the ones which are unlikely to justify regarding the facts of the case, and green titles represent the ones which should be legitimized. The color change between the first green category and the second is because the latter is easier to be legitimized.

We state that forms of hacktivism such as virtual sit-in and voluntary DDoS attacks should be permissible; however, there is a high chance that they will create a financial loss to the owner of the website[229]. Even blocking a site for ten minutes could cause serious harm to the owner. Although this does not mean that those attacks should be criminalized; they still should be compensated by attackers. The details about compensating losses happened due to those attacks could be studied on a paper on private law; however, we could at least state that there is a possibility that this suggestion can be unpractical due to the anonymity of hacktivists[230]. If there is no addressee, it will become a problem to address the compensation.

[229] Hampson 539.
[230] Sorell 391.

A. Information Theft

This form of hacktivism, according to the chart, is created with the color red because there is no possibility for it to be justified. Information theft is a self-explanatory term which means to access a private network's system to either sell or reveal the information[231]. It is one of the most damaging hacktivist attacks because of the act consisting of stealing data[232].

Whether it should be considered as a type of hacktivism is questionable. First of all, information theft is usually organized towards government papers or corporate secrets which are being held digitally[233]. Although they could now be stolen by using hacking tools, before the virtual world, it was still possible to steal data physically[234]. In summary, it was always considered as "theft," and it still is.

Secondly, the motivation is also vague: the act could be arranged in to embarrass or shame the organization or to make a political point, but we also witness that the motivation of these attacks could also be derived from personal aims[235]. If the former is the case, then we could say it still

[231] Illig 1043.
[232] Ibid.
[233] Monarch 8.
[234] Ibid.
[235] Illig 1043.

could not be considered as justifiable due to the lack of proportionality. The harm caused to people or corporations by stealing data would be considered more dominant to the goal of the protest or the reason for hacktivists to get attention to convey a message.

As an example, in 2012, Anonymous hacked emails and stole information from the company "HB Gary Federal Inc." and released the information because Anonymous wanted the CEO of the company, Aaron Barr to be convicted due to his actions[236]. It was later asserted that Aaron Barr was advising his customers to use methods such as cyber-attacks, forged documents, and blackmail[237]. Even if the group revealed a piece of crucial information which would affect injured parties, it would not justify these actions as a justified protest because the means to achieve this information should not be legal at the first place[238].

Also, if the latter is the case, it would be impossible for us to consider these attacks as hacktivism because as we stated above, there should be a non-personal aim leading to a protest[239]. For example, in 2011, Lulzsec, a group from the UK which left the Anonymous and started a subgroup, hacked Sony PlayStation and stole usernames, passwords, security answers, purchase history and addresses from the company and released them online[240]. The motivation behind this attack was due to criticism and legal threats of Sony towards Anonymous, which seems to be personal rather than political[241].

First of all, there is no expression and no justifiable protest in that situation[242]. If there is no expression which led to these attacks, they could never be accepted as civil disobedience and could not benefit from right to freedom of expression[243]. Secondly, the action is motivated by a personal aim to damage Sony, which makes information theft the furthest type of hacktivism from being

[236] O'Malley 145.
[237] Ibid.
[238] Ibid.
[239] Illig 1043; O'Malley 144.
[240] O'Malley 154; Joshua Adams, 'Decriminalizing Hacktivism: Finding Space for Free Speech Protests on the Internet' [2013] <https://ssrn.com/abstract=2392945 or http://dx.doi.org/10.2139/ssrn.2392945> accessed 20 December 2018 6.
[241] O'Malley 154.
[242] Ibid.
[243] Ibid 145.

legitimized[244]. Thirdly, the acts are so disproportionate in the means of violence, the benefit which could be brought with the protest is exploited with the harm brought by the act[245].

As *Rawls* has stated, "civil disobedience cannot be grounded on self-interest"[246]. Therefore, if we count hacktivism as ECD, we should not include the ones that amount to self-interest such as information theft. In summary, information theft could be a type of hacktivism but not a type of ECD, since it is not a justifiable form which guarantees freedom of expression protection[247]. According to the author's criteria, the action is usually launched to have a financial gain; it leaks through data and damages targets violently and disproportionately; hence, it could never be justified as a form of hacktivism.

B. Website Defacement

According to our chart, website defacement is placed as the yellow color, since it could mostly not be considered as a justifiable form of hacktivism; but there is still a possibility to be justified if the criteria could be applied and if the action would not access to data.

Website defacement, which is one of the most common types of hacktivism, seeks to gain unauthorized access to a website and make modifications on that page[248]. It requires having access to one's computer and modifying or adding content to a website, either by changing the already existing data or not[249]. They are executing these actions by accessing a web server and eventually replacing or altering the content with the message they would like to forward, which consists of a political message[250]. They are very similar to graffiti on the walls of the streets[251].

The motivation of this act could either be derived from protesting a government or affecting a political decision[252]. Website defacements do not necessarily damage the targeted site; instead, they are trying to convey a message but also using technical tools, and this way, people give even more attention to those attacks, which is the goal[253].

---

[244] Ibid 155.
[245] Ibid 159.
[246] Rawls 321.
[247] O'Malley 155.
[248] Klang, 'Civil Disobedience Online' 77; Hampson 519.
[249] Karagiannopoulos 28.
[250] Illig 1040; Hampson 519.
[251] Illig 1040.
[252] Klang, 'Civil Disobedience Online' 77; Illig 1040.
[253] Hampson 520.

Despite the communicative method of website defacement, it is unlikely for web defacements to be legitimized because of the modification they are doing onto the websites by hacking them and replacing the content[254]. These activities' legality, which are the ones standing in the middle ground, should be decided on regarding the factual circumstances[255]. This means that if they are accessing third parties' data or breach their freedom of expression disproportionally and cause those sites grave harms, then these actions should not be regarded as justifiable.

As an example, one of the longest-running website defacement attacks is made in the name of #OpIsrael, where Anti-Israel campaigns are being made with website defacements[256]. In 2012, "myisrael.us" experienced a website defacement attack where the regular content is deleted and is replaced with messages including "Freedom for Gaza"[257]. In this situation, there is a protest made with a political aim, and there is a message conveyed showing that there is an expression. However, even if this was a way of exercising freedom of expression rights, the author believes that since the targeted website is on a small- scale and would be assumed that they did not have other platforms on the internet, the attack is also breaching that website owners' freedom of expression. For that reason, regarding the factual circumstances, it might not be considered as justifiable.

There also have been website defacement attacks against terrorist organizations such as ISIS, organized by Anonymous[258]. Anonymous targeted an ISIS supporting website by hacking into the website and switching the content with messages to make the website look like a pharmacy advertising the sale of drugs such as Prozac and Viagra[259]. This was an attack made with the classical mocking attitude of Anonymous to make a protest and overwhelm the terrorist organization[260]. Therefore, in this situation, no matter how disruptive the case is, the act would not be about protecting the freedom of expression of others since the content on an ISIS supporting site would not be considered as an expression due to the restriction of the national security

[254] Ibid 535.
[255] O'Malley 159; Morozov 228.
[256]Graffiti in the Digital World: How Hacktivists Use Defacement? (25 April 2018) Trend Micro <https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/> accessed on 25 July 2019.
[257] Ibid.
[258] Andrew Griffin, 'Anonymous Group Takes Down ISIS Website, Replaces it with Viagra Ad Along with Message to Calm Down' (26 November 2015) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-group-takes-down-isis-website-replaces-it-with-viagra-ad-and-message-to-calm-down-a6749486.html> accessed 27 July 2019.
[259] Ibid.
[260] Ibid.

regarding article 10(2) of ECHR[261]. The disruption caused by this hacktivist act might be considered as proportionate.

According to the criteria, even if website defacements are expressive, and is not made due to achieve a financial gain, it is still considered as violent since there is a possibility to access data of the target which causes disproportionality. Hence, unless the data is not accessed, this action should not be justified because changing content could harm the target gravely.

C. Site Redirects

Regarding the chart, site redirects are placed by using the color yellow because there might be a possibility to justify these actions; however, it is unlikely that they could ever be justified.

Site redirects concerns about getting the unauthorized access to a website by changing the address into the new one and redirect into the new URL address which the attackers created, usually containing satirical content about the targeted website[262].

It is made by accessing a server and alter the URL address, so that whenever a user wants to access that site, another site, created by hacktivists, opens instead[263]. The new site made by hacktivists consists of information or any political message that they would like to convey[264]. Often, the alternative site is critical towards the targeted website[265].

Since the message which hacktivists want to convey is not seen on the original website, it might take time for the target website controllers to understand that there is a redirect which differs site redirects from website defacements[266].

One of the interesting examples of site redirects was the one made by Lulzsec in 2011[267]. Lulzsec redirected the website of the newspaper's website "the Sun" to a URL address which was similar to the Sun's and covered a story about a false allegation of Rupert Murdoch being passed away[268]. When people clicked on the refresh button the website, readers were directed to a fake page called

[261] ECHR Article 10(2).
[262] Karagiannopoulos 28.
[263] Illig 1040.
[264] Ibid.
[265] Hampson 520.
[266] O'Malley 143.
[267] Charles Arthur, Hanna Godfrey and Ben Quinn, ' Sun Website Hacked by Lulzsec' (18 July 2011) <https://www.theguardian.com/media/2011/jul/18/sun-website-hacked-lulzsec> accessed 31 July 2019.
[268] Ibid.

"new-times.co.uk/sun"[269]. The timing of the incident shows us this was a protest against Murdoch due to phone hacking scandal happened in the UK, which led to the famous Leveson Inquiry[270].

The author believes that since there was not any harm given to the website, because instead of hacking into the original website, another website was created, we could not say there was any severe damage given to the company. The main aim of this act was to criticize Rupert Murdoch by throwing a protest against him. The content of the alternative site was also included humor because it was clear that he was not dead.

Nonetheless, this action of site redirecting means that the website is hacked and the protestors had unauthorized access into the server. This means that unlike DDoS attacks which only freezes the server from giving services, it could steal the legitimate traffic from the target and direct it into a new site which could duplicate users to reveal their personal data[271].

Hence, we could state, that since there was not any grave harm given, at least in our example, and since the first aim was to protest without stealing data but only misdirecting people for a limited time to protest, on this example there was a justified protest. This, however, does not mean that every single attack could be seen as a justifiable form, it should still be analyzed by the facts of the situation and the principle of proportionality within the non-violence criterion.

Even if the possible damage given to targets is less violent than website defacements, there still is unauthorized access to URL addresses of the target which damages the proportionality and non-violence criteria that we put. Therefore, even if the act is considered as expressive and is made to get attention, it could not be justified.

D. Denial of Service Attacks

DoS attacks are marked as dark green color on the pyramid because it is likely to justify the action as a form of hacktivism. DoS attacks, which are commonly used for online protest, detains the ability or access of a block user or an organization to reach a system's operation[272]. The action could either be towards an e-mail address or to a domain name[273].

[269] Ibid.
[270] Goode 77.
[271] Adams 9.
[272] Klang, 'Civil Disobedience Online' 78.
[273] Klang, 'Virtual Sit-Ins, Civil Disobedience and Cyberterrorism' 138.

What denial of service attacks does is "zombifying" the device by overloading the server with so much data so that the user eventually could not function the device[274]. Zombifying a device is an expression for losing the computer's control so that the attacker could manipulate the device or the server.

There are two types of denial of service attacks: Denial of Service Attacks and Distributed Denial of Service Attacks[275]. What DoS and DDoS attacks have in common is that they have the same outcome at the end. Eventually, both attacks are trying to stop access to the targeted server[276]. However, while standard DoS is made to a server by a single user, using a single Internet connection DDoS attacks are doing the opposite, they are using multiple numbers of computers to send a malicious code so that the legitimate users' service would be denied[277].

Denial of service attack is essentially started by hitting the refresh button until the website crashes[278]. However, once the technologic developments went forward and it became impossible to crash websites with these acts, hacktivists came up with software which would do the same thing[279]. Since it is hard for one computer to exhaust the targeted server, DDoS attacks are almost always being used instead[280].

DDoS attacks also have two branches: voluntary and involuntary DDoS attacks[281]. Voluntary attacks occur either when controlled computers are transferred to the central computer or when users are directly participating in the attack[282]. The party launches the act by attacking a target website with its computer server, which eventually causes the server to slow down or shutdown[283]. Unlike involuntary DDoS tactics, voluntary DDoS requires the participation of real people, which makes it closer to offline protests[284].

[274] Worthy and Fanning 194.
[275] Karanasiou 104.
[276] Beamish 3.
[277] Karanasiou 104.; Beamish 3.
[278] Baraniuk.
[279] Ibid.
[280] Lilian Edwards, 'Dawn of the Death of Distributed Denial of Service: How to Kill Zombies' [2006] 24 Cardozo Arts & Entertainment 23-62, 25.
[281] O'Malley 142.
[282] O'Malley 142; Li 307.
[283] Hampson 518; O'Malley 141.
[284] DJNZ 270.

On the other hand, involuntary DDoS attacks occur when hackers maliciously hack into computers without the consent of the host computers; they are using to launch the attack[285]. There is a large number of computers which tries to access the target website repeatedly and eventually results overwhelming the server and cut the capacity [286].

The intermediary machines which were used during a DDoS attack are called either bots, slaves, or zombies, which are a chain of computers controlled by one centralized location [287]. Using botnets can be controversial, depending on being voluntary or not[288]. If those groups of computers are being used to attack websites or devices with the consent of those very computers, then there is no problem; it will be counted as voluntary DDoS attacks[289]. However, if the group of computers which the owners did not give their consent to be a part of a botnet would undoubtedly be considered as illegal and they would be called involuntary DDoS attacks[290].

Involuntary DDoS attacks are usually not seen as hacktivism because of their malicious behavior and because it is seen as hijacking computers without the consent of their owners rather than making a political or social point; thus, are out of the scope of our work[291]. It also is conducted due to personal matters and financial reward, which is irrelevant to hacktivism.

CMA defines modification as the situation when any program or data held in the computer is added to, altered or erased[292]. On the other hand, DDoS attacks do not modify or remove anything from the targeted system, but the operation of the system is not under the control of the user[293]. While this attack continues, the legitimate user does not know about the ongoing attack; they will only see an error message whenever they will try to access the server[294].

Anonymous is one of the most famous examples of hacktivist actions throughout the world, which commonly uses DoS attacks[295]. What makes Anonymous unique is their effectiveness compared

[285] O'Malley 142.
[286] Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet' 10; Hampson 518; O'Malley 141.
[287] Edwards 26; Beamish 4.
[288] Baraniuk.
[289] Ibid.
[290] Ibid.
[291] O'Malley 142.
[292] CMA s. 17; Fafinski, 'Computer Use and Misuse: The Constellation of Control' 46; Beamish 10.
[293] Edwards 38.
[294] Worthy and Fanning 194.
[295] Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet' 41.

to other groups and their sense of senses of humor[296]. The way they mocked their targets and their visual contents related to popular culture were some of the things which made them particular[297].

Anonymous' roots are not entirely political; instead, they are mostly based on ridiculing authority[298]. The group originates all the way back from 2006 with the name of "4chan," which is a collection entitling themselves with organizing online pranks[299]. Later on, the group became more politically-oriented in 2008 with the virtual sit-in action they did to Church of Scientology[300]. Anonymous' famous slogan is "We are anonymous. We are legion. We do not forgive. We do not forget. Expect us. Knowledge is free." which shows us that they are standing for the freedom of expression and against censorship[301].

The most famous operation of Anonymous was Operation Payback, which was a series of DDoS attacks against the corporations which "turned their back" against Wikileaks[302]. In 2010, Wikileaks leaked some information which was linked to the US government consisting of 251.287 unclassified and classified diplomatic cables, copied from the closed Department of Defense network[303]. Due to the leakage "Banking Blockade" was interposed, which entailed big corporations such as Amazon, PayPal, Visa, and Mastercard to cease their donating services to Wikileaks[304]. When some corporations withdrew their services towards Wikileaks, Anonymous started to form attacks against those companies due to their intention to silence Wikileaks, which would damage the freedom of expression[305]. Therefore the "Operation Payback" started[306] , and the group commenced to bombard the websites of those companies with DDoS attacks[307].

---

[296] Ibid.
[297] Ibid 50.
[298] Goode 77.
[299] Karagiannopoulos 33; Goode 75.
[300]Gabriella E. Coleman, 'Anonymous: From the Lulz to Collective Action (6 April 2011) <http://mediacommons.org/tne/pieces/anonymous-traveling-pure-lulz-land-political-territories> accessed 21 July 2019; Karagiannopoulos 37; Mikhaylova 19; Gabriella E. Coleman , *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (1st Edition, Verso 2015) 2.
[301] Imogen Richards and Mark A. Wood, 'Hacktivists against Terrorism: A Cultural Criminological Analysis of Anonymous' Anti IS Campaigns' [2018] 12 International Journal of Cyber Criminology 187-205, 191; Knapp 286.
[302] Sauter, 'Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet' 41.
[303] Hampson 511; Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 1.
[304] Molly Sauter, The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet (1st Edition, Bloomsbury 2014) 1.
[305] Thompson; Hampson 511.
[306] Hampson 513.
[307] Ibid.

On this operation, Anonymous used the LOIC software, an example of voluntary DDoS attack, which enabled even beginner level hacktivists to join into those actions[308]. LOIC is a remotely controlled application which adopts a single central user to launch attacks without having a grave risk on the user[309]. It is also a tool to include people with no know-how on technology to the protests[310]. With LOIC now, it is enough for people to download the system and push the big button they put into the software, which makes the protest very similar to civil disobedience[311]. Therefore, we could state that there was an expression behind the attack.

What Anonymous did was to post a software for people to download it. Thereafter, when 6.000 people downloaded the software, the data blocked and caused traffic to those companies' websites[312]. Some of the sites crashed, and some of them could not be operated for an amount of time[313]. The UK charged four men due to the participation in the operation, and they were all convicted[314].

Although DoS attack is mostly considered as illegal, the author believes that the criteria for justifying hacktivists actions as civil disobedience is mostly satisfied. First of all, those attacks would be considered as "public" because of the participation of at least tens of thousands of people which guarantees the public discourse[315]. Secondly, in voluntary DDoS and DoS attacks, it is clear that the action is expressive, and there is conscientiousness since the action is formed with morality and without having any personal or financial gain.

There also should be a proportionality between the aim of the expression and the harm given to the target or third parties due to these attacks which should be decided on a case-by-case basis[316]. If there is a political or a social motive behind those attacks which would proportionally be justified, then we could say that the measures taken towards those attacks are disproportionate to the right to

[308] Hampson 519; O'Malley 142.
[309] Sauter, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* 103.
[310] Jessica L. Beyer, 'The Emergence of a Freedom of Information Movement: Anonymous, Wikileaks, the Pirate Party and Iceland' [2014] 19 Journal of Computer-Mediated Communication 141-154, 146.
[311] Ibid.
[312] Thompson.
[313] Hampson 513.
[314] R v Weatherhead, Rhodes, Gibson, and Burchall, unreported, Southwark Crown Court, 24 January 2013.
[315] DJNZ 272.
[316] Morozov 228.

freedom of expression. Lastly, we could state that the way it has a temporary nature also gives us the reason why it should be counted as proportionate in the means of violence.

Mail bombing, which will be discussed in the next part should also have the same consequences with those acts because mail bombing is a type of DoS attacks.

E. Mail bombing

Mail bombing is shown as a dark green color on the chart because it is likely to be justified as a form of hacktivism. As stated above, mail bombing is a type of DoS attack which is committed with the aid of automated devices to block target's incoming mailbox; therefore, it is impossible for the targeted person to reach legitimate e-mails[317]. Usually, a massive number of messages would be sent to the e-mail address with meaningless content, to occupy and overwhelm the mail server and bring the server down[318]. Since overwhelming the mail address would cause the mail server to deny services to the legitimate user, it is considered as a type of DoS attacks[319]. In the UK, this falls under section 3 of CMA[320] if the attacker intends to limit the users[321].

Mail bombing is being used because it is easier than the DoS attacks[322]. Instead of trying to limit the access of big mail server companies such as Google or Microsoft, with the mail-bombing, the only thing the hacktivist need would be attacking that person's or organization's mail address directly[323].

DPP v Lennon[324], is an example about an irritated employee, Lennon, who targeted his employer and launched e-mail bombings, which overall cost his ex-employer £30.000[325]. He downloaded a mail bombing software and used e-mails to overload the server as a DoS attack[326]. The Court at first instance decided that such acts constituted a modification of the e-mail account; therefore, there was a breach regarding section 3 of CMA[327]. However, after it has been decided that the

[317] Denning 268.
[318] Josh Hendrickson 'How Email Bombing Uses Spam to Hide and Attack' (29 April 2019) <https://www.howtogeek.com/412316/how-email-bombing-uses-spam-to-hide-an-attack/> accessed 24 July 2019.
[319] Fafinski, 'Computer Use and Misuse: The Constellation of Control' 66.
[320] CMA s.3.
[321] Klang, 'Civil Disobedience Online' 76.
[322] Hendrickson.
[323] Ibid.
[324] *DPP v Lennon* [2006] EWHC 1201 (Admin).
[325] Worthy and Fanning 194,5.
[326] Ibid 195.
[327] CMA s.3.

server was only built to receive e-mails so ultimately, the defendant did not exceed his authorization; which meant that the defendant's actions were authorized[328].

F. Virtual Sit-in

The given color of virtual sit-ins on the pyramid is dark green because the author believes that this form of hacktivism should be justified as a type of electronic civil disobedience. A virtual sit-in is blocking the access to the aimed website or server by conducting a paralyzing amount of data which causes that target to either crash or slow down[329].

Virtual sit-ins are one of the most familiar categories to offline protests because there should be a participation to convey a social or political message[330]. The motivation is the same as the offline sit-in, which is to get attention to the protestors by blocking or occupying the space[331]. Virtual sit-ins are also similar to DoS attacks, but the difference is the consistency of participants[332]. In virtual sit-ins, unlike DoS attacks, a large organized group of people simultaneously reload the targeted website until it becomes unfunctional[333].

What they do in these acts is to set up particular websites with automated software, and when the protestors access to that software, they simultaneously visit the targeted site and create traffic so significant that the other users cannot reach it[334]. While some virtual sit-ins are manually made by reloading the page simultaneously, the others download a special code which automates reloads to the targeted site[335].

This type of hacktivism is seen as a more democratic way to exercise freedom of expression among all forms of hacktivism[336]. Unlike any other types of hacktivism, a virtual sit-in is made by a group of people and is a reflection of justified offline protest which is protected by freedom of expression

[328] Stefan Fafinski, 'Computer Misuse: Denial-of-Service Attacks: DPP v Lennon [2006] EWHC 1201 (Admin)' [2006] 70 *The Journal of Criminal Law* <https://doi.org/10.1350/jcla.2006.70.6.474> accessed 20 June 2019 474-478, 475.
[329] Karagiannopoulos 28.
[330] Illig 1039.
[331] Denning 264.
[332] Illig 1039.
[333] Ibid.
[334] Denning 264.
[335] Hampson 520.
[336] Ibid.

in the virtual world[337]. Therefore, it is, among other forms of hacktivism, more likely and easier to be legitimized.

However, this is not seen as the same by the lawmakers. As a prominent example, in 2010, Ricardo Dominguez, who is an associate professor at the University of California, called his students to organize a virtual sit-in participated by hundreds of students due to the budget cuts and high tuitions[338]. The action was taken with a DoS attack with protestors whose names were identifiable and was very similar to offline protests due to the attendance of people[339]. Even if the main aim was to jam the university's portal to convey a message with many people participating in the act, he was still charged with criminal hacking laws in the US[340].

In summary, the only difference between a real and a virtual protest is the use of the internet as a tool[341]. Also, the draft report of Council of Europe suggests that DDoS attacks and virtual sit-ins are acceptable as a form of freedom of expression and even if it does constitute a crime, the sanction should always be given with proportionality[342]. As stated above, these actions are a way of exercising freedom of expression; plus, the given damage is done proportionally and the only reason to launch this attack is to get public's attention and create a public discourse. Therefore, they should be exempt from cybercrime legislation and be decriminalized[343].

G. Site Parodies

A site parody, as shown in the pyramid as light green color because it should be justified according to our criteria, is when a hacktivist creates a website which is almost similar to the targeted website, but the content consists of messages that hacktivists wish to give[344]. The reason behind this action is to confuse customers or users while trying to access a website and would find themselves on the website that hacktivists created so that hacktivists would make a point[345].

---

[337] O'Malley143.
[338] Illig 1039; O'Malley 151; Morozov 228.
[339] Illig 1039.
[340] Dan Goodin, '"Virtual Sit-in" tests line between DDoS and Free Speech' (9 April 2010) <https://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/> accessed 31 July 2019.
[341] O'Malley 152.
[342] Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom, 'Draft Report on Freedom of Assembly and Association on the Internet' (30 September 2015) MSI-INT (2014) 08 rev5 para 61.
[343] O'Malley 158.
[344] Illig 1041.
[345] Ibid.

As an example, the National Security Agency was mimicked by creating another website, and the content put onto the newly created website was about the Snowden controversy[346]. The creator's motivation was to create an amusing way to express free thoughts[347].

This type of hacktivism may seem very similar to site redirects due to the existence of an alternative website. However, the difference is that site parodies do not manipulate web servers; instead, they are creating a similar one. This means that the targeted site is not directly being attacked, and there is no damage given to the actual site[348]. Plus, they do not access or modify any information or security that the targeted person/organization carries, which gives us the idea that if we already accept site redirects as justifiable with exemptions, then site parodies should be accepted as a form of ECD since they are matching the criteria which the author created[349].

[346] Ibid 1042.
[347] Ibid.
[348] Ibid.
[349] Ibid.

V. CONCLUSION

Democracy is something that would lose its path from time to time, and protests could be used as a tool to put the system back on track. Hacktivism could help degenerated democratic systems as being a watchdog such as the press. The one clear argument of hacktivists is that the current system does not work; the computer age was only beneficial to large corporations, and it should be stopped[350]. People should access all the information, and they should not trust the authorities.

This study tried to justify hacktivism so that it could be legally accepted as a form of protest. In order to do that, after explaining some definitions and relative concepts about hacktivism, a criterion has been created with the help of ideas coming by various scholars to justify these acts. According to these criteria, the author concluded that if the protest is considered as an expression, if it is not made with personal or financial interests is only proportionally violent without causing any physical harm; hacktivism could be justified.

After setting criteria, the study created a typology of hacktivism, applied the criteria mentioned above, and analyzed those forms to justify these acts. In conclusion, the author suggested that information theft cannot be protected and website defacements and site redirects are unlikely to be protected because the way they interfere with data and hack into the servers which would create unauthorized access disproportionately. The study also suggested that it is possible to protect voluntary DDoS attacks and DoS attacks, mail bombings, virtual sit-ins, and site parodies because they are proportionate according to their aim, therefore, should be considered as a justifiable form of disobedience.

So far, however, we currently fall into despair because of the world's legal system and their approach to hacktivism. Even if the Lufthansa case would enlighten us and had the possibility for European courts to recognize hacktivism as a justifiable form of expression and protest, it is unlikely to apply the rule due to the obstacles of international treaties such as Convention on Cybercrime which gives little space for the interpretation of such acts being legitimized[351].

[350] Manion and Goodrum 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in *Internet Security: Hacking, Counterhacking and Society* 69.
[351] Karagiannopoulos 50; Convention on Cybercrime 2001 Art. 2,5; Klang, 'Virtual Sit-Ins, Civil Disobedience and Cyberterrorism' 143.

This study finally asserts that hacktivism is worth protecting and should not be seen as a crime[352]. It is genuinely considered as an expression and protest[353]. The only problem is that "hacktivism is not a lack of answers: it is having too many answers"[354].

In hacktivism, exercising freedom of expression by protesting is the main idea[355]. Changing mediums is only a detail in the process[356]. If a hacktivist action merely aims to convey a message, it should be legally permissible to do so[357].

[352] O'Malley 138.
[353] Ibid.
[354] Gunkel 597.
[355] Knapp 287.
[356] Knapp 287; Sorell 397.
[357] Mikhaylova 9.

TABLE OF CASES

A. UK

Brutus v. Cozens [1973] A.C. 854 (H.L.) 863 (U.K.)

DPP v. Lennon [2006] EWHC 1201

R v Jeffery, unreported, Southwark Crown Court, 13 April 2012

R v Weatherhead, Rhodes, Gibson, and Burchall, unreported, Southwark Crown Court, 24 January 2013

R v. Gold [1998] AC 1063

B. ECHR

Appleby v United Kingdom (2003) 37 EHRR 38

Eon v France App no 26118/10 (ECtHR14 March 2013)

Handyside v United Kingdom (1976) Series A No 24

Plattform “Ärzte für das Leben” v Austria (1988) Series A no. 139

Stankov and the United Macedonian Organisation Ilinden v Bulgaria (2002) App No 29221/95 and 29225/95

C. OTHERS

Oberlandesgerichts Frankfurt am Main v Thomas Vogel No.1 Ss 319/05

TABLE OF LEGISLATION

A. TREATIES

Convention on Cybercrime 2001

EU Council Framework Decision 2005/222/JHA On Attacks Against Information Systems

European Convention on Human Rights 1953

B. STATUTES

Computer Misuse Act 1990

Law Commission, Criminal Law Computer Misuse (Law Com No 186, 1989)

Police and Justice Act 2006

C. REPORTS

Council of Europe Committee of experts on cross-border flow of Internet traffic and Internet freedom, 'Draft Report on Freedom of Assembly and Association on the Internet' (30 September 2015) MSI-INT (2014) 08 rev5

European Commission for Democracy through Law (Venice Commission) and OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), 'Guidelines on Freedom of Peaceful Assembly' (9 July 2010)

BIBLIOGRAPHY

A. BOOKS

Coleman G, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (1st Edition, Verso 2015)

Gillmor D, *We the Media Grassroots Journalism by the People, for the People* (1st Edition, O'Reilly Media 2004)

Gomien D, *Short guide to the European Convention on Human Rights* (3rd Edition, Council of Europe Publishing 2000)

Harris D J and others, *Law of the European Convention on Human Rights* (4th Edition, Oxford 2018)

Himma, K E, *Internet Security: Hacking, Counterhacking and Society* (1st Edition, Jones and Bartlett Publishers, Inc 2007)

Janis, M W, Kay R S and Bradley, A W, *European Human Rights Law: Text and Materials* (3rd Edition, Oxford, 2008)

Jordan T and Taylor P A, *Hacktivism and Cyberwards: Rebels with a Cause?* (1st Edition, Routledge 2004)

Mead D, *The New Law of Peaceful Protest: Rights and Regulation in the Human Rights Act Era* (1st Edition, Hart Publishing Ltd 2010)

Mill J S, *On Liberty* (1st Edition, Yale University Press 2003)

Morozov E, *The Net Delusion: The Dark Side of Internet Freedom* (1st edition, Public Affairs 2011)

Murray A, *Information Technology Law: Law and Society* (3rd Edition, Oxford University Press 2016)

Rainey B, Wicks E and Ovey C, *The European Convention on Human Rights* (6th Edition, Oxford 2014)

Rawls J *A Theory of Justice: Revised Edition* (Oxford University Press 1999)

Sauter M, *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet* (1st Edition, Bloomsbury 2014)

Wall D S, *Cybercrime* (3rd Edition, Polity Press 2011)

B. CHAPTERS

Denning, D E, 'Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy' in John Arquilla and David Ronfeldt, *Networks and Netwars* (1st edition, RAND 2001) 239-289

Himma K E, 'Hacking as Politically Motivated Digital Civil disobedience: Is Hacktivism Morally Justified?' in Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking and Society* (1st Edition, Jones and Bartlett Publishers, Inc 2007) 73-99

Klang M, 'Virtual Sit-Ins, Civil Disobedience and Cyberterrorism' in Mathias Klang and Andrew Murray, *Human Rights in the Digital Age* (Cavendish Publishing 2004) 135-147

Manion M and Goodrum A, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' in Kenneth Einar Himma, *Internet Security: Hacking, Counterhacking and Society* (1st Edition, Jones and Bartlett Publishers, Inc 2007) 61-73

Meikle G, 'Electronic Civil Disobedience and Symbolic Power' in Athina Karatzogianni *Cyber Conflict and Global Politics* (1st Edition, Routledge 2008) <https://dspace.stir.ac.uk/bitstream/1893/6577/1/Electronic%20Civil%20Disobedience%20and%20Symbolic%20Power.pdf> accessed 21 June 2019

Vegh S, 'Classifying Forms of Online Activism: The case of Cyberprotests against the World Bank' in Martha McCaughey and Michael D. Ayers, *Cyberactivism: Online Activism in Theory and Practice* (1st edition, Routledge 2003) 71-97

C. THESIS

Bartels R, 'The Virtual Sit-in' (Master Thesis, Leiden University 2015)

Fafinski S F, 'Computer Use and Misuse: the Constellation of Control' (PhD. Thesis, The University of Leeds 2008)

Karagiannopoulous V, 'The Regulation of Hacktivism in Contemporary Society: Problems and Solutions' (PhD. Thesis, University of Strathclyde 2013)

Mikhaylova G, 'The "Anonymous" Movement: Hacktivism as an Emerging Form of Political Participation' (Master of Arts Thesis, Texas State University 2014)

Samuel A W, ‘Hacktivism and the Future of Political Participation’ (PhD. Thesis, Harvard University 2004)

Sauter M, ‘Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet’ (Master Thesis, MIT 2013)

D. ARTICLES

Adams J, ‘Decriminalizing Hacktivism: Finding Space for Free Speech Protests on the Internet' [2013] <https://ssrn.com/abstract=2392945 or http://dx.doi.org/10.2139/ssrn.2392945> accessed 20 December 2018.

Beamish C, ‘Denial of Service Attacks: Ineffective U.K. Legislative Overkill, How the Americans Do It and the Recurring Issue of Regulation’ [2012] 2 Southampton Student L. Rev. 1-24

Beyer J L, ‘The Emergence of a Freedom of Information Movement: Anonymous, Wikileaks, the Pirate Party and Iceland’ [2014] 19 Journal of Computer-Mediated Communication 141-154

DJNZ and the Action Tool Development Group of the Electrohippies Collective, ‘Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?’ [2001] 34 Leonardo 269-274

Edwards L, ‘Dawn of the Death of Distributed Denial of Service: How to Kill Zombies’ [2006] 24 Cardozo Arts & Entertainment 23-62

Fafinski S, ‘Computer Misuse: Denial-of-Service Attacks: DPP v Lennon [2006] EWHC 1201 (Admin)’ [2006] 70 *The Journal of Criminal Law* <https://doi.org/10.1350/jcla.2006.70.6.474> accessed 20 June 2019 474-478

George J J and Leidner D E, ‘From Clicktivism to Hacktivism: Understanding Digital Activism’ [2019] Information and Organization https://doi.org/10.1016/j.infoandorg.2019.04.001 accessed 21 June 2019

Goode L, ‘Anonymous and the Political Ethos of Hacktivism’ [2015] 13 Popular Communication 74-86

Gunkel D J, ‘Editorial: Introduction to Hacking and Hacktivism’ [2005] 7 New Media & Society 595-597

Hampson N C N, ‘Hacktivism: A New Breed of Protest in a Networked World’ [2012] 35 B. C. Intl’l & Comp. L. Rev 511-542

Illig A T, ‘Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists’ [2015] 119 Penn St. L. Rev 1033-1057

Karanasiou A P, 'The Changing Face of Protests in the Digital Age: on Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks' [2014] 28 International Review of Law, Computers & Technology 98-113

Klang M, 'Civil Disobedience Online' [2004] 2 Journal of Information, Communication and Ethics in Society 75-83

Knapp T M, 'Hacktivism- Political Dissent in the Final Frontier' [2015] 49 New Eng. L. Rev. 259-295

Li X, 'Hacktivism and the First Amendment: Drawing the Line Between Cyber Protest and Crime' [2013] 27 Harvard Journal of Law & Technology 301-333

Manion M and Goodrum A, 'Terrorism or Civil Disobedience: Toward a Hacktivist Ethic' [2000] 30 Computers and Society 14-19.

McEwan N, 'The Computer Misuse Act 1990: lessons from its past and predictions for its future' [2008] 12 Crim. L.R. 955-967

Milone M G, 'Hactivism: Securing the National Infrastructure' [2002] 58 Bus. Law 383-413

Monarch B, 'The Good Hacker: A Look at the Role of Hacktivism in Democracy' [2015] <http://dx.doi.org/10.2139/ssrn.2649136> accessed on 15 July 2019

Monshipouri M, 'Human Rights in the Digital Age: Opportunities and Constraints' [2017] Public Integrity 123-135

O'Leary S, 'Balancing Rights in a Digital Age' [2018] 59 Irish Jurist 59-92

O'Malley G, 'Hacktivism: Cyber Activism or Cyber Crime' [2013] 16 Trinity C. L. Rev. 137-160

Richards I and Wood M A, 'Hacktivists against Terrorism: a Cultural Criminological Analysis of Anonymous' Anti IS Campaigns' [2018] 12 International Journal of Cyber Criminology 187-205

Samuel A W, 'Digital Disobedience: Hacktivism in Political Context' ("The Internet as Agent of Change: Bridging Barriers to Cultural, Political and Activist Discourse" Panel, San Francisco, CA, September 2001)

Scheuerman W E, 'Digital Disobedience and the law' [2016] 38 New Political Science 299-314.

Seebruck R, 'A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model' [2015] 14 Digital Investigation 36-45

Simpson J D, 'Unauthorized Expression: Does "Hacktivism" Have a Viable First Amendment Defense?' [2014] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473245> accessed 15 June 2019

Sorell T 'Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous' [2015] 7 Journal of Human Rights Practice 391-410

Thomas, J L C, 'Ethics of Hacktivism' [2001] <https://www.arifyildirim.com/ilt510/julie.thomas.pdf> accessed 17 July 2019

Van Laer J and Van Aelst P, 'Internet and Social Movement Action Repertoires' [2010] 13 Information, Communication & Society 1146-1171

Worthy J and Fanning M, 'Denial of Service: Plugging the legal loopholes?' [2007] 23 Computer Law & Security Report 194-198

Wray S,

- 'Electronic Civil Disobedience and the World Wide Web of Hacktivism' [1998] <https://www.arifyildirim.com/ilt510/stefan.wray.pdf> accessed 17 July 2019
- 'On Electronic Civil Disobedience' [1999] 11 Peace Review 107-111

E. WEBSITE BLOGS

Arthur C, Godfrey H and Quinn B, 'Sun Website Hacked by Lulzsec' (18 July 2011) <https://www.theguardian.com/media/2011/jul/18/sun-website-hacked-lulzsec> accessed 31 July 2019.

Coleman G E, 'Anonymous: From the Lulz to Collective Action (6 April 2011) <http://mediacommons.org/tne/pieces/anonymous-traveling-pure-lulz-land-political-territories> accessed 21 July 2019

Cox J, 'The History of DDoS Attacks as a Tool of Protest' Motherboard (1 October 2014) <https://motherboard.vice.com/en_us/article/d734pm/history-of-the-dDoS-attack> accessed 20 December 2018

EDRI, 'Frankfurt Appellate Court Says Online Demonstration is not Coercion' (7 June 2006) https://edri.org/edrigramnumber4-11demonstration/ accessed 31 July 2019

Goodin D, '"Virtual Sit-in" tests line between DDoS and Free Speech' (9 April 2010) <https://www.theregister.co.uk/2010/04/09/virtual_protest_as_ddos/> accessed 31 July 2019.

Graffiti in the Digital World: How Hacktivists Use Defacement? (25 April 2018) Trend Micro <https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/> accessed 25 July 2019

Griffin A, 'Anonymous Group Takes Down ISIS Website, Replaces it with Viagra Ad Along with Message to Calm Down' (26 November 2015) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-group-takes-down-isis-website-replaces-it-with-viagra-ad-and-message-to-calm-down-a6749486.html> accessed 27 July 2019

Hendrickson J, 'How Email Bombing Uses Spam to Hide and Attack' (29 April 2019) <https://www.howtogeek.com/412316/how-email-bombing-uses-spam-to-hide-an-attack/> accessed 24 July 2019.

Kerr D, 'Anonymous Petitions U.S. to see DDoS attacks as legal protest' Cnet (9 January 2013) <https://www.cnet.com/news/anonymous-petitions-u-s-to-see-dDoS-attacks-as-legal-protest/> accessed 4 January 2019

Thompson C, 'Hacktivism: Civil Disobedience or Cyber Crime?' ProPublica (2013) <https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime> accessed 20 December 2018

F. INTERVIEWS

Chris Baraniuk, Interview with Molly Sauter, 'Legalise Digital Protest' [2014] 224 New Scientist