Cybercrime vs Hacktivism: Do we need a differentiated regulatory approach?

by

Francesca Farmer

First Supervisor
Alison Harcourt

Second Supervisor
Oliver James

Amended thesis submitted by Francesca Farmer, to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Politics, March 2022.

I certify that all material in this thesis which is not my own work has been identified and that any material that has previously been submitted and approved for the award of a degree by this or any other University has been acknowledged.

Tables and Charts:

Abstract

Background and aims:

Cybercrime is an issue that increases year on year, however rarely are the motivations behind these attacks investigated. More and more people are turning to the internet to protest with some scholars debating whether hacktivism is a social movement. This Dissertation uses networked social movement theory in order to establish if hacktivism is a social movement or whether it is simply a politically motivated form of cybercrime. While demonstrating hacktivism's place in the social movement landscape this Dissertation will also analyse how hacktivism is currently regulated and whether the legislative and regulatory tools are appropriate.

Methods:

This Dissertation uses a multi-method approach to establish whether hacktivism could be considered to be a social movement. The first method used is a rhetorical analysis of the Twitter accounts from active hacktivist accounts. Tweets posted by these accounts are coded using Stewart's functional approach to rhetoric used by social movements (1980) using MAXQDA's content analysis software. The second method used is a descriptive statistical analysis of a number of publicly available datasets (Zone H; the Cambridge Computer Crime Database; DCMS's Cyber Security Breaches Surveys from 2017-2021; an AnonOps Internet Relay Chat Channel; a sentiment analysis; the hack aggregator 'Hackmageddon') to establish hacktivism's similarities and differences to both cybercrime and social movements.

Results and Conclusions::

This Dissertation found that hacktivism is substantially different to cybercrime despite it being regulated as such based on the methods, targets and ideologies. Additionally, the Dissertation found that hacktivism could be considered to be a social movement based on similarities in their communications and motivations as well as the online parallels hacktivism has to social movement methods. The dissertation also found that due to the similarities hacktivism shares with traditional offline protests and hacktivism, the UK should look at the offline parallels when regulating hacktivism to ensure that the human rights of those taking part in hacktivist methods are not being quashed and are being upheld.

Declaration

Hacktivism: Do we need a differentiated regulatory approach?

Amended Thesis submitted by Francesca Farmer, to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Politics, March 2022.

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

I certify that all material in this thesis which is not my own work has been identified and that any material that has previously been submitted and approved for the award of a degree by this or any other University has been acknowledged.

Acknowledgements:

Whilst undertaking this Dissertation I have been fortunate to receive a great deal of support and guidance. I would firstly like to thank my supervisor, Professor Alison Harcourt for the support, encouragement and enthusiasm shown throughout the process of researching and writing this Dissertation. Her patience, expertise and kindness have been invaluable and she has kept me motivated and calm throughout this process. I could not have finished this without her.

I would also like to thank my second supervisor Professor Oliver James for his advice and support over the last few years. His practical guidance and helpful feedback has been greatly appreciated. I would like to thank the numerous members of staff at the University of Exeter Political Science department for their support as well as the other PGRs from my cohort. I would also like to thank Dr Andrea Calderaro and Dr Bice Maiguashca for taking the time to read my thesis. Their feedback has been incredibly useful and has resulted in many improvements. I have also been fortunate to have received guidance and support from Professor Isabelle Engeli, her persistence enabled me to undertake my research on large datasets during the global pandemic. I would also like to thank the University of Exeter IT department for their laptop loans ensuring I could work on these datasets from home.

I would like to thank the ESRC for funding this Dissertation and believing in me. I would also like to thank the ESRC funded project IntCivSoc as well as the Centre for European Governance for their employment. I must also thank the University of Exeter and my first year undergraduate students who made teaching them a joy. I would not have been able to undertake this PhD without the financial support of the above.

I would also like to extend my gratitude to those that collated and created the publicly available datasets. I would not have been able to write this without their civic-mindedness.

I am enormously grateful to my friends and family who were always there when I needed them. Thanks to my mum for your optimism and support. Thanks to Natasha, Sam, Tom and Dan for not taking things too seriously, you're the best siblings anyone could ask for. Thanks to Pete, Caitlin and Hannah for your proofreading skills. Finally, thanks to Ben for always being a calming presence and for listening to my ideas, rants and ramblings. Your enthusiasm and encouragement for my research despite not really understanding it has meant the world to me. I am so grateful for your loving, unwavering support.

Chapter 1: Introduction

1. Introduction

This Dissertation aims to establish whether hacktivism could be seen to be a social movement or whether it is cybercrime by comparing it to both phenomena. It will then establish whether the UKs regulatory approach to hacktivism is correct. This chapter will introduce key terms and themes present throughout the dissertation as a whole. It will argue that the approach taken to answer the research question is the most appropriate including the theoretical approach and the methods selected. The first section will examine the research context within which this Dissertation is positioned (2). The chapter will then introduce the theoretical framework that has been selected for the project, this is networked social movement theory (3). The research methods will then be introduced as well as subquestions (4). The scope of the project will then be detailed including the methods selected (5.1) and the limitations of the study that the project has attempted to overcome (5.2). The Dissertation as a whole will then be detailed with a brief explanation for each chapter (6). The findings of the research will then be summarised (7) before the chapter is concluded (8).

2. Research Context:

According to the Department for Culture, Media and Sport's Cyber Security Breaches Survey, 39% of businesses and 26% of charities had identified breaches or attacks in 2021.[1] Moreover 68% of business leaders feel the risks of a cyber attack are increasing.[2] The 2020 EasyJet hack is just one of the examples of how millions of people have become victims of cyberattacks. The company released a statement in May 2020 explaining that nine million customers had been affected by the data breach with email and travel details being stolen, as well as the credit card details of over 2,000 customers[3]. Neither the nature of the attack nor motivations behind it have been released. Yet, this is just one of the 65,000 attempted cyber attacks that happen every day

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021#chapter-5-incidence-and-impact-of-breaches-or-attacks Last Accessed 5 Feb 2022

[2] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 Last Accessed 1 Nov 2020

[3] http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756 Last Accessed 10 April 2021

globally.[4] The ever increasing number of cyber attacks represents a substantial burden on victims of cybercrime. Such attacks can result in a damaged reputation, loss of employee time, impaired productivity and huge financial costs. In the UK, Redcar and Cleveland Council suffered a cyber attack in February 2020 that disabled its servers for three weeks and resulted in financial loss with residents being concerned that the council's infrastructure was in danger of collapse.[5] During the ransomware attack that took the council's systems offline, staff were informed that computers, tablets and mobile devices had been disabled and instead had to rely on pen and paper reducing the services of more than 135,000 residents.[6] Yet, rarely are the motivations behind such attacks investigated academically. Indeed, greater numbers of individuals are using hacking methods to protest on a wide range of issues, from anti-globalisation to anti-capitalism.

Thomas has argued that as a result of the internet "civil society is strengthened and technology mediated new public spheres are evolving" (Thomas 2012: 294). One of these digital methods of protests is hacktivism. Hacktivism has been defined as "*The promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure's technical features, without the use of physical violence and without gaining direct economic benefits.*" (Romagna 2019: 5). In 2022, hacktivists, including the well-known collective Anonymous, worked together to hack Russian payments services, transportation, the media and government systems as a result of the Russian invasion in Ukraine. Some have even claimed that the war in Ukraine has sparked a revival of hacktivism. Threat intelligence group Flashpoint have tracked close to 50 different hacktivist groups with the majority supporting Ukraine.[7] This dissertation argues that personal and political motivation distinguishes hacktivism from other forms of hacking and aligns it more with social movements than cybercrime. Criminal hackers do not express a political or moral view, while hacktivists strive to instigate a greater moral good by raising attention to injustice with the aim of bringing about change (Himma 2007). Hampson

[4] https://www.businessleader.co.uk/how-many-cyber-attacks-are-attempted-on-uk-businesses-per-day/54688/ Last Accessed 2 Jan 2021

[5] https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attackLast Accessed 3 Jan 2021.

[6] https://www.bbc.co.uk/news/technology-51504482Last Accessed 3 Jan 2021

[7] https://www.ft.com/content/9ea0dccf-8983-4740-8e8d-82c0213512d4 Last Accessed 4 March 2022

claims that criminal forms of hacking are instead “motivated by nefarious and fraudulent aims” (2012: 516) and it is ideology and objectives that differentiate hacktivism and hacking.

In the UK, the main legislative tool used to deal with cybercrime is the 1990 Computer Misuse Act which criminalises all forms of hacking and impairment of systems (Computer Misuse Act 1990). Section 3 of the Computer Misuse Act corresponds most directly to hacktivist activities. It refers to any unauthorised act in relation to a computer with intent to impair its operation, hinder access to a program or data held, impair the operation of programs and to enable these actions.[8] This piece of legislation is used to charge those that access computer material without authorisation. Furthermore, Article 5 of the Council of Europe’s 2001 Budapest Convention, which concerns System Interference and the serious hindering of the functioning of a computer system, leaves little room for licit acts of electronic civil disobedience. The Council of Europe study on national implementation of the Budapest Convention proposed that Member States should criminalise DDoS attacks that do not necessarily cause damage in the form of serious hindering but instead act as a menace for the proper functioning of a system. Yet, Article 11 of the UK’s 1998 Human Rights Act protects the right to protest under “freedom of assembly and association” and the state has a positive obligation to take reasonable steps to facilitate the right to protest.[9] If hacktivism is a legitimate form of protest, then prosecuting hacktivists could be viewed as contrary to Article 11 of the Human Rights Act. It is worth bearing in mind that if the 2021 Police, Crime, Sentencing and Courts Bill becomes law, the right to freedom of assembly will be restricted with noisy, annoying and static protests all facing restrictions.[10] This will affect the rights offline protestors have and as a result, if online protests were afforded the same rights, it might also affect the rights of online protestors. The effect on this bill on future protests and hacktivism is unknown but should be examined if the Bill becomes law.

Numerous hacktivist protests have taken place over the last few decades, but the activity which resulted in the most arrests was #OpPayPal (2011). This originally took place in 2011 and was a response to opponents of internet copyright infringement and escalated when torrent sharing site, Pirate Bay, was shut down. This then shifted again when the US Government started scrutinising Wikileaks and the way in which supporters could donate to the site. As a result, Visa, Mastercard and PayPal were targeted and their websites were taken offline due to

[8] https://www.legislation.gov.uk/ukpga/1990/18/contents Last Accessed 18 Dec 2020
[9] https://www.legislation.gov.uk/ukpga/1998/42/contents Last Accessed 2 Jan 2019
[10] https://bills.parliament.uk/bills/2839 Last Accessed 16 April 2021

numerous DDoS attacks. After the protest, 19 members were arrested globally, four of those were based in the UK and were charged with conspiracy to impair the operation of computers under Section 3 of the Computer Misuse Act. Two of the defendants admitted to their part and received a six-month sentence, suspended for two years. While the other two pleaded not guilty, one of which was jailed for 18 months, the other was jailed for 7 months (Halliday 2013).

As stated earlier, hacktivism has been defined as "*the promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure's technical features, without the use of physical violence and without gaining direct economic benefits.*" (Romagna 2019: 5). An interesting debate that arose when undertaking this project was the split between some scholars considering it to be a tactic used by protestors while others consider it to be a political entity similar to other protest groups. This Dissertation considers hacktivism to be both a tactic and an entity. This is due to the fact that the tactic of hacking has shaped the ideology and the dynamics behind hacktivism itself. This, then provides a set of values and a specific mental approach that is embedded in the hacktivist mentality (Romagna 2019: 5). As such the Dissertation will detail what hacktivism actually is by investigating whether hacktivism is cybercrime and cyberterrorism. It will find that while technically it could be a form of cybercrime according to the literature, it is not cyberterrorism despite many claiming that the line between hacktivism and cyberterrorism is blurred. The Dissertation will then ask whether hacktivism is a political practice or whether it is a collective political entity with it establishing that it could be both in the form of both electronic civil disobedience and social movements.

Hacktivism has produced real world results. Internet campaigner and coding prodigy, Aaron Swartz, downloaded thousands of articles from JSTOR in an effort to make them accessible to all in 2011. He was arrested by the United States Federal Government in 2011 for bypassing security blocks at MIT (Amsden, 2013). Due to the prosecutors' harsh and vindictive methods, Swartz took his own life.[11] However, the principles of the Open Access Movement, which Swartz adhered to, is now becoming widely adopted, partly as a result of Swartz's activism. Indeed, his efforts fueled the op-access initiative with Montgomery stating that "2020 appears to have

[11] https://www.scientificamerican.com/article/digital-activists-suicide-casts-spotlight-on-growth-of-open-access-movement/ Last Accessed 3 Jan 2021

locked in momentum for the open access movement" (Montgomery, 2021).[12] Indeed, research funders from 11 European research funders have stated that publishers must make the papers that benefited from specific research grants free to read immediately upon publication.[13] It is clear that hacktivist actions are making a difference and as a result could be seen to be legitimate forms of protest. Wray has argued that hacktivism could be seen to be effective depending on how effectiveness is defined (1999). If the desired goal is to draw attention to an issue, it could attract media coverage ensuring it is effective. However, if the goal is to mobilise more individuals then hacktivism may not be as effective as offline protest.

3. Theoretical framework

This Dissertation will draw upon the literature on Online Social Movement studies to compare hacktivism and historical protests. According to Castells *"Movements are [...] global, [...], they learn from other experiences, and in fact they are often inspired by these experiences to engage in their own mobilisation. Furthermore, they keep an ongoing, global debate on the Internet, and sometimes they call for joint, global demonstrations in a network of local spaces in simultaneous time. They express an acute consciousness of the intertwining of issues and problems for humanity at large, and they clearly display a cosmopolitan culture, while being rooted in their specific identity"* Castells (2012: 250-251). With the internet activists are able to reach wider audiences without having to expend a great deal of resources. State control can also be bypassed while retaining editorial control over the content (Scott and Street 2000). Bennett and Segerberg argue that digital technologies are changing the traditional paradigms used to explain collective action (2012). Digital technologies demand a theory that moves away from traditional theories of resource mobilisation, rational decision-making and cost-benefit analyses and instead looks at 'connective action'. This results in large-scale personalised and digitally mediated political engagement whereby "ideas and mechanisms for organising action become more personalised than in cases where action is organised on the basis of social group identity, membership or ideology" (Bennett and Segerberg 2012: 744).

[12] https://theconversation.com/2020-locked-in-shift-to-open-access-publishing-but-australia-is-lagging-150284 Last Accessed 22 April 2021.

[13] https://www.nature.com/articles/d41586-018-06178-7 Last Accessed 12 Jan 2021.

The dominant theory of computerised social movements was put forward by Manuel Castells as digital technologies are changing the traditional paradigms used to explain collective action (2009). Castells claims that the result of the transformation of social movement networks has led to movements no longer needing an identifiable centre, formal leadership or vertical power structures to ensure their message reaches the masses. Communication has alway been crucial in social movements as people can only challenge those in power by connecting with one another. They are based on shared outrage and a feeling of togetherness. Thus movements rely on interactive networks of communication. It is through the internet and digital communication techniques that movements are able to live and grow. The internet has provided a space for leaderless movements to thrive and expand. It does so, by ensuring those in the movement can maintain communication amongst themselves and the outside world.

A criteria on what constitutes a social movement will be put forward in this Dissertation in Chapter 2 which will include how modern social movements do not need an identifiable centre, formal leadership or traditional vertical power structure in place; that social movements need to have an awareness of the intertwining issues that are affecting humanity at large; that they are predominantly triggered into life by a specific event or when their disgust at those in power reaches its peak; that movements are constantly engaging in self-reflection and stating their aims; that the main aims of the movements is to raise awareness and empower citizens to mobilise; and finally that these movements rely on interactive networks of communication. Based on this criteria, it is clear that hacktivists could consider themselves to fall under the realm of social movements.

Despite the criteria, it is evident that there is still a great deal of debate surrounding the computerisation of social movements, even more so hacktivism which does not seem to be fully explored within any of the literature surrounding social movements. Thus, this Dissertation will be using the concept of networked social movements in order to determine that hacktivist groups are an online networked social movement. This will then provide more detail into whether or not the methods of protest they use could simply be considered to be the online equivalent to traditional protests. Therefore, within the wider scope of the research project the following research questions that will be answered will form the backbone of the dissertation.

4. Research Question:

The main question of the Dissertation is: ***‘Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?’***

Sub-questions are: **Is hacktivism different to cybercrime? What are the main debates that arise when discussing hacktivism? Are the methods used by hacktivists successful and legitimate forms of protest? How are the methods used by hacktivists regulated in the UK in 2022? Should the methods used by hacktivists be regulated differently to cybercrime?**

These questions ultimately delve into the legitimacy of hacktivism and whether it can be compared to traditional offline social movements. They compare civil disobedience methods with the new electronic versions employed by hacktivists, outlining the similarities but also the issues that arise when comparing the two. The questions are attempting to establish whether or not hacktivism is different to criminally motivated, self-interested cybercrime due to it’s politically motivated stance. More broadly, a wider look at how the internet has affected protest and social movements will also be investigated. The latter two questions address the future of cybercrime decision-making and how this should take place. They will specifically focus on the 2022 regulatory framework in the UK and the impact it has had on hacktivism from 2012 onwards.

In order to answer these questions the motivations and politics of hacktivists will be analysed through both qualitative and quantitative methods and will be compared with criminally motivated hackers and social movement groups. Government publications surrounding hacktivism will also be analysed in order to understand the broader state view on hacktivism. Before analysing the impact that this project will have, its scope must first be outlined and examined.

5. Scope

This dissertation aims to establish whether or not hacktivism is different to traditional forms of cybercrime and criminally motivated hacking. If this is the case, it will then analyse whether it could be seen to be a form of social movement. It also aims to establish whether the regulatory approach that has been applied to the methods used by hacktivists in the past, and is the same as the approach applied to cybercrime, should be changed to reflect the political motives behind the methods used. This project will outline the numerous debates in order to establish whether hacktivism is a political entity or a tactic; whether the methods used are legitimate civil disobedience methods; whether hacktivism is a form of cybercrime or even cyberterrorism; and where hacktivism should be placed when discussing social movements and whether the state needs to rethink the cybercrime laws that hacktivists are prosecuted under. In order to do this, social movement theory will be reviewed and applied in order to establish whether hacktivism could fall under the banner of social movements and whether their methods of electronic civil disobedience should be regulated similarly to traditional methods of protest. This Dissertation focuses on the UK, despite hacktivism and cybercrime being global issues, it would be impossible for an examination of all of the global cybercrime laws and hacktivism to be within the scope of a PhD project. Global cyber norms as well as European cybercrime laws are summarised in Chapter 7 but the majority of the project focuses on the UK both for a practical reason and also due to the fact that the UK was one of the first nations to develop a computer crime law and, as such, could be considered to be a global example of how to implement cyber laws.

5.1. Methods:

The methods used in this dissertation are a mix of qualitative and quantitative. The first method to be used is a rhetoric analysis on a number of known hacktivist Twitter accounts. These tweets are coded using Stewart's functional approach to rhetoric. The theoretic base for a functional approach to rhetoric was first laid out by both Simons (1970) and Gronbeck (1975) as was an original list of functions. Simons et al considered three broad rhetorical functions: mobilisation, exercise of external influences and resistance to counter influence. He then established a list of functions in order to ensure that these previous broader functions were achieved: (1) Justifying the mission to its followers and external third parties; (2) Infusing the movement's mission with a sense of urgency; (3) Obtaining both material and non-material resources; (4) Organising followers into a cohesive unit; (5) Meeting the personal needs of followers; (6) imposing a program for action upon the movement; (7) Discrediting oppositions; and (8) Countering all efforts for social control. Based on these theorists, Stewart delineated specific functions of rhetoric to be used when studying the rhetoric employed by social movements (1980). These include (1) transforming perceptions of history; (2) transforming perception of society; (3) prescribing courses of action; (4) mobilising for action; and (5) sustaining the movement. This typology will then be identified within the data published by hacktivists that are the subjects of the analysis.

Secondly, the results of a statistical analysis on a number of datasets will be presented. These datasets include Hackmageddon database (01),[14] the Zone H hacktivism dataset (02),[15] Cambridge Computer Crimes database (03),[16] the UK's Department of Culture, Media and Sport's National Cyber Breach survey reports (04),[17] the AnonOps Internet Relay Chat (05)[18] and the sentiment analysis from SWGFL (06).[19] These datasets will allow for a comparison between hacktivism and cybercrime in terms of their targets, methods and ideological motivations as well as a comparison between hacktivism and social movements in terms of their campaigns, successes and public opinion. This analysis will find that there is a clear distinction between hacktivists and cybercriminals and that hacktivists have a great deal in common with social movements. It will also argue that while hacktivism has a lot in common with offline social movements, the successes of hacktivists can never reach the same heights as offline social movements, nor does the public look as favourably upon hacktivism as they might with more legitimate social movements.

5.2 Limitations:

The empirical results reported herein should be considered in the light of some limitations including issues with bias, generalisability and reliability which must be mitigated in the dissertation. For the research to be reliable, researcher bias must be overcome by constant questioning and acknowledging one's own assumptions and experiences. When undertaking the rhetoric analysis, the researcher must immerse themselves in the text that is being analysed

[14] Cyber attack timelines 2012-2019. Compiled by Paolo Passeri. Available on request at https://www.hackmageddon.com/. Downloaded on 6 August 2020. Last Accessed on 13 April 2021

[15]Zone H cybercrime archive. Available http://www.zone-h.org/archive/special=1. Downloaded on 29 Jan 2022.

[16] Cambridge Computer Crime Database. Compiled by Professor Alice Hutchings. Available at https://www.cl.cam.ac.uk/~ah793/cccd.html. Last Accessed 27 Jan 2022.

[17] DCMS Cyber Security Breaches Survey 2017-2021 https://www.gov.uk/government/collections/cyber-security-breaches-survey

[18] AZSecure-data.org. Anonops IRC channel Sep 2016-May 2018. Created by the University of Arizona (NSF #ACI-1443019), Drexel University, University of Virginia, University of Texas at Dallas, and University of Utah. Available to download from https://www.azsecure-data.org/internet-relay-chat.html. Downloaded on 6 August 2020. Last Accessed 13 April 2021.

[19] SWGfL Reputation Alerts Sentiment Analysis. Available when subscribed and logged in: https://swgfl.org.uk/login/

to ensure they can maximise the material. Furthermore, certain limitations that may occur as a result of the COVID-19 pandemic should also be considered. These issues include a lack of available computational power with large datasets requiring cleaning, processing and analysis which needed to be mitigated. Issues with access could also occur as there is a lack of personal contact with the individuals studied which could be seen to be a limitation of this dissertation. This is due to the secretive nature of hacktivists and the illegality of the methods they use. Due to the lack of contact with individual's there are very few ethical issues that could arise. However, one must be conscious that when utilising publicly available data certain issues with privacy should be considered. While privacy is difficult to define due to the fact that it can be perceived differently by many different people. Cooper and Coetzee state that "Privacy is perceived as being about protecting people's personal information, but it also includes territorial (or location) privacy, physical (or bodily or health) privacy and privacy of communications" (2020: 162). This issue will be mitigated with the researcher ensuring that there is no personal, territorial or physical information present in the datasets. Moreover, the purpose of the datasets used is to provide a general overview and identify macro trends, however the individual datasets might contain a certain degree of subjectivity. As a result a number of datasets have been analysed in order to offset this and ensure a single biassed dataset isn't used. Finally, there is no one specific dataset that could detail the information that was needed to answer the research question and while hacktivists will post online about their successes there is also no official government dataset on hacktivists. Several theorists working in both cybercrime and hacktivism, including Vasileios Karagiannopoulos, Leonie Tanczer and Alice Hutchings, were consulted with regards to their knowledge of government backed hacktivist data but were unable to offer any specific hacktivist datasets. This is in part due to the fact that hacktivism is hard to distinguish from regular cyberattacks unless the attackers claim responsibility with a very clear political agenda.

6. Project outline:

The dissertation will be divided into 8 chapters (including this introductory chapter). The second chapter will evaluate the current literature on social movement theory narrowing down to networked social movement theory before offering a criteria for establishing what an online social movement is (Chapter 2: What constitutes a social movement?). The third chapter then asks what hacktivism is and aligns it with both electronic civil disobedience and social movements (Chapter 3: What is Hacktivism?). The fourth chapter will outline the research methods to be used in dissertation including the rhetoric analysis and the different forms of quantitative analysis to be used on the six datasets mentioned above (Chapter 4: Methods). The fifth chapter will outline the results of the rhetoric analysis of the tweets posted by different hacktivism accounts including both Anonymous and non-Anonymous affiliated accounts using Stewart's functional approach to the rhetoric used by social movements (Chapter 5: The Rhetoric used by Known Hacktivists). The sixth chapter will outline the results of the work undertaken on the quantitative datasets including a look at the methods, targets, motivations, and successes of hacktivism (Chapter 6: Hacktivism - cybercrime or social movement?). The seventh chapter will outline the current regulatory approach that is used in cyber security, cybercrime and cyber terrorism. It will also investigate how this applied to hacktivism using the example of Anonymous's #OpPaypal and the legislative consequences of the protest. The messages distributed by the government will also be analysed in order to establish how the state views hacktivist activities and those that engage in them (Chapter 7: The UK's Current Regulatory Approach to Hacktivism). The final chapter will summarise the research project as a whole and will answer the research question and subquestions before concluding with the results and a discussion of the results. It will also offer future recommendations for the field of study (Chapter 8: Conclusion).

7. Findings/ Impact:

The findings of this dissertation will now be introduced before moving on to the impact the overall dissertation could have. With regards to the rhetoric analysis, the majority of the rhetorical functions set out by Stewart in the *Functional Approach to Rhetoric used by social movements* were identified in the tweets analysed. These functions include 'Transforming perceptions of history'; 'Transforming perceptions of society'; 'Prescribing courses of action'; 'Mobilising for action'; and finally 'Sustaining the movement'. The hacktivists' accounts reference the past, present and future as part of the first function. This is predominantly used for mobilisation purposes with the tweets either encouraging their followers to prevent previous atrocities from occurring again or or to prevent alternative dystopian futures. When 'transforming perceptions of society', all hacktivists will reference the self and the opposition employing an 'us vs them' dichotomy in order to distance themselves from their opposition. They will also use emotive and inflammatory language when trolling the opposition. The hacktivists will also prescribe courses for action despite the illegality of many of their methods. Nevertheless, in general the tweets that implemented this function prescribed legal courses for action such as the signing of petitions or marches. The original function outlines that when prescribing courses for action, social movements should prescribe specific tasks to specific people, this was not identified in the tweets. The fourth function ‘mobilising for action’ was employed in a myriad of ways by Anonymous including the aforementioned ‘us vs them’ dichotomy, the demonstration that the opposition is taking away personal freedoms and by the pressuring of the opposition. Finally, the hacktivists ‘sustains the movement’ by posting about their successes.

In the statistical analysis the main targets identified as the victims of attacks instigated by hacktivists are consistently governments despite the fact that the UK government considers hacktivists as being similar to cybercriminals in their communications. This is different to cybercrime who target individuals and large corporations. The main methods used by hacktivists are DDoS and web defacements both of which have offline parallels in the real world in the form of sit-ins and graffiti. While cybercriminals will predominantly use fraudulent emails and malware. The ideologies behind the operations undertaken by hacktivists are for the most part political in character with social and religious ideologies also being identified as the motivations behind some of the operations. Yet a look at the motivations behind confirmed cyberattacks undertaken by cybercriminals show a further distinction between hacktivism and cybercrime with the main motivations behind these attacks being financial, sexual or personal. It has been found that in order for a social movement to truly enact change, 3.5% of a population must engage and participate in protests which is highly unlikely with regards to hacktivist operations (Chenoweth 2011). Additionally, public opinion of hacktivism is neutral to negative. The key words analysed (‘hacktivism’, ‘hacktivist’, ‘electronic civil disobedience’ and ‘online protest’) had a neutral sentiment attached to them. Indeed, on certain days some of the key terms had a negative sentiment attached to them. These results are outlined in more detail in both chapters 5 and 6.

Overall, this dissertation could have a wide impact on different areas. Firstly, it will make a major contribution to the literature of both hacktivism and networked social movements. Existing literature on how the internet and networked communications has impacted social movements in general will also be examined. Additionally, the current legislative and regulatory processes that govern hacktivism will be outlined in order to provide a comprehensive overview of the current regulatory landscape and how these were applied to a case study. As one of the first countries to implement cybercrime legislation, the UK has been chosen as a national case study as a potential example for nations that are yet to implement cyber laws or for countries that are considering altering their approach. The dissertation also creates new and original knowledge in the form of a statistical analysis and rhetoric analysis. Moreover, this dissertation could be of interest to policy makers and those working in specific regulatory bodies such as the National Cyber Security Centre. UK Law Enforcement agencies such as GCHQ and the new National Cyber Force could use this research leading to softer prosecution of hacktivists and on the ground implementation. Additionally, scholars could use the dissertation as a building block in which to progress the ideas either in the form of a longitudinal study or a study that interacts with either hacktivists or regulators. Finally, the impact of the 2021 Police, Crime and Sentencing Bill on protests could be analysed in order to establish if, when the act becomes law, the level of internet protest increases.

8. Conclusion

Over the following chapters this Dissertation will analyse theories of online and networked social movements with reference to hacktivism. The existing literature on hacktivism will be reviewed alongside the history of hacktivism, and whether hacktivism is cybercrime, cyberterrorism, a tactic or a political entity. The research methods that will be used in order to answer the main research question will then be outlined in detail including the rhetoric analysis and the descriptive statistical analysis using the six different datasets detailed above. The results from both of the research methods and analyses will be explained with reference to existing studies and research. The current regulatory approach that is used in cyber security and cybercrime and how this applied to hacktivism using the case study of OpPayback will then be outlined. Finally, the dissertation as a whole will be detailed in the conclusion chapter with references to future recommendations for the field of study.

Chapter 2: What constitutes a social movement?

1. Introduction

Citizens throughout history have protested against those in power or taken issue with injustice. This has only increased as time has progressed (Goodwin and Jasper 2014). People organise themselves in a variety of ways in order to pursue countless goals whether it be political or social change. Social movements have been and continue to be seen as the levers of social change. They occur as a result of a social crisis that can make living unbearable for the majority of citizens (Castells 2012). Social movements offer a way to express unhappiness and distaste and this appears to have been facilitated with the invention of the world wide web and other information and communication technologies. In 2002, electronic philosopher Levy claimed that "the destiny of democracy and cyberspace are intimately linked because they both involve what is the most essential to humanity: the aspiration to freedom and the creative power of collective intelligence" (2002: 33). It is clear that the world has changed as a result of the emergence of the Internet, therefore it stands to reason that how social movements occur and are organised, as well as the ways in which protests are undertaken, would change too. Traditional theories of social movements are struggling to explain these new methods and as a result newer theories such as networked social movement theories are coming to the fore.

This chapter centres around the concept of online social movements and whether the barrier to entry for the classification of social movements has changed in order to establish if hacktivism could be classified as a social movement based on existing lierature. It will do so by detailing existing literature on online social movements and the predominant theory used in modern online social movements: Networked social movements. The aim of this chapter is to understand what constitutes a social movement, specifically an online movement where the barrier to entry appears to be lower than for offline movements. It's clear that the technological landscape in which movements are now created has altered movements as well as the methods they use and as such this chapter will allow for an examination of whether hacktivism as a concept could be considered to be a social movement. The chapter will delineate existing criterias on what constitutes a movement, with a specific view on how this has changed as a result of ICT innovations. Using the theory of Networked Social Movements and the resulting criteria the chapter will state that as a result of these innovations, hacktivism would fall under the criteria of an online social movement and as such should be treated in a similar manner to offline movements. In order to make this argument the chapter will firstly detail the concept of online social movements, how social movements have been altered as a result of the ICT technologies and the key arguments on whether the internet has facilitated social movements (2). This will then lead on to Castell's theory of networked social movements with reference to hacktivism and the decentralised, fluid and self-interrogating nature of modern movements (3), this will then feed into a criteria on what constitutes a social movement to which hacktivism will be applied (4). The chapter will then present some key definitions relating to online social movements that will be referred to throughout the Dissertation (5).

2. Social Movements Online:

Online and offline worlds are becoming increasingly interconnected and blurred (Kneip and Nieysto 2007). Calderaro states that the advent of the Internet led to a great deal of debate on how digital platforms impact on the political sphere, specifically political engagement (2018: 781). In the 1990's the Internet was "hailed as the opportunity for the realisation of the ideal of direct democracy" (Slaton 1992; White 1997; Calderaro 2018: 782). Indeed, the Internet was seen by some to be an instrument through which citizens and institutions could be linked, as a way in which to create and nurture new forms of political participation and as a new space to talk about politics (Fearon 1998; Price & Cappella 2002; Wright 2004; Calderaro 2018: 782). Indeed, some states have linked democratic principles with ICTs, for example, Estonia's groundbreaking use of technology in their election systems as well as ensuring 99 percent of public services are available online 24 hours a day[20].

When broken down, Calderaro states that the debate on how the internet affects politics can be summarised along two lines (2018: 782). There are those who argue that the internet strengthens democracies while others who put forward that instead, the internet offers very little with Margolis and Resnick describing it as 'politics as usual' (Margolis & Resnick 2000: 207). Hess et al. have argued that social movements use of the Internet is one of the few areas "where the much vaunted but rarely realised democratic promise of the Internet is at least partially borne out" (2008, 476). This is because it allows marginalised and excluded voices to be heard and allows them to participate in political debate (Dahlberg 2007: 56). Social media,

[20] https://e-estonia.com/solutions/e-governance/e-democracy/. Last Accessed 10 March 2022.

for example, is claimed to democratise participation allowing more people to express opinions and increasing the accessibility of mobilisation (Bruns 2008: 13-14). Trevisan notes that the Internet has enabled access to those who were once excluded from protest spaces due to physical disabilities (2016: 1593). Previously, offline social movement methods were exclusionary yet now the Internet acts as a facilitator for those who were physically excluded to make their voices heard. However, Breindl claims that the current debates focusing on the democratic potential of the Internet were preceded by similar debates on computerisation movements whereby computers were seen as either a tool of empowerment or a source of alienation for society (2010: 46). Powell argues that the "democratic imaginations of computer technology establish alternatives to the dominant institutional frameworks for computers" and are associated with "disruptive and oppositional political positions" (2008, 1). Jackson asserts that the ways in which activists have used old and new media technologies is nothing new (2018: 5). McKinney identified the use of online bulletin boards used by HIV/AIDs activists in the 1980s to demonstrate this (2018: 8). This links to Ganesh and Stohl's view that the ubiquity of computer mediated communications has not drastically altered activist organisation, instead it has become a vital part of the activist toolkit (2013: 3). The Internet has enabled a 'critical periphery' of individuals who would not have engaged in the same way as those taking part in offline activism (Jackson 2018: 6). Barberá et al maintain that these online spaces act as an entry into social movements with online members of a movement acting as promulgators of activist messages to new members and networks (2015). Yet, recent research recognises that digital activism is vastly different to traditional activism (Bennett and Segerberg, 2013; Selander and Jarvenpaa, 2016; Vaast, Safadi, Lapointe, and Negoita, 2017). This is due to the fact that while many online activities are reflections of offline activities, information and communication technologies offer innovative action (George and Leidner 2019: 5).

Digital activism has been defined as digitally mediated social activism (Bennett and Segerberg, 2013; Selander and Jarvenpaa, 2016). Internet-supported collective action adopts formal and informal structures. Bimber claims that "with the rise of micromedia (email, chat rooms and cell phones) and 'middle' media (websites, webzines, Internet-based communication campaigns), formal organisations, flexible decentralised organisations, networks, and even individuals now have the potential to communicate and coordinate with others in ways that until recently were feasible almost exclusively for formal organisations" (Bimber et al., 2005: 375). However, Earl and Schussman claim that ICTs reduce the incentive to join established organisations such as social movements (2003: 185). Instead, we see 'movement entrepreneurs', defined by Garrett as non professional individuals who are motivated by personal interest and rely on their own skills when undertaking movement activity (2006: 211). Hacktivists may be described as movement entrepreneurs as while they may be professionals in ICT, for example, they are not professional protestors, they also rely on these ICT skills in their protesting. Social media also offers new possibilities for more solo protest activities. Here, users can control and generate their own content. Häyhtiö and Rinne claim that "most issue-specific individually oriented political interventions differ both from the traditional social movements, as well as from the 'new social movements' in respect to their agenda, aims, temporal duration, and lines of chosen activities" (2008: 26). Thus, it is clear that there seems to be a trend whereby citizens make political connections by following personal interests rather than overarching ideologies. Breindl (2009) claims that while the fast adoption of the Internet by activists has allowed individuals to produce and publish media outside of traditional mass media systems, it does not make much sense to oppose traditional mass media through alternative media sources as both traditional and new media seems to influence one another. Based on this, an obvious strategy of activists and their networks is to impact on the information provided by traditional media sources. Castells states that these sources are vital channels for mobilising larger groups for protest actions (2007). While assisting in information diffusion, the Internet can also offer a vast array of framing opportunities (Nieysto 2007, Kavada 2009). The framing and reframing of activist struggles is an important aspect of social movements. Blogs and social media can offer activists unlimited editorial control with regards to explaining and informing specific narratives. Indeed, hacktivists themselves have both collective social media accounts and websites as well as individual social media accounts for specific hackers ensuring that they are not reliant on traditional media companies in portraying their messages and that they retain complete editorial control.

However, there are still significant knowledge and skills gaps with regards to using the internet. Lehtonen states that "apart from being able to understand and interpret media texts, citizens are expected to adopt, filter and communicate masses of information coming from various sources" (2008: 173). Media skills are key to social movements and as such issues of information overload and practices of disinformation are still issues that need to be addressed. Thus, it could be seen that to some, the Internet has a de-mobilisational aspect to it (Breindl 2010). Calderaro argues that the internet's effect in politics means that some individuals are now spreaders of information and producers of content which is much easier than it once was (2018: 785). Yet, due to the vast amount of information the risk of receiving fake information online is high (Calderaro 2018: 786). The ability to engage in political discourse is seen to be a basic right, yet if they do not have the ability to take part in this discussion aspects of their citizenship could be seen to have been removed. Moreover, Rosenbaum and Bouvier have suggested that algorithms put in place by social media companies may limit the wider reach of social movement organisations (2020). As a result, these social media companies could be identified as being ‘organising agents’ (Rosenbaum and Bouvier 2020: 121).

On the other hand, another aspect in which the Internet appears to have assisted in social movement participation is through the idea of social capital or the notion in which daily social contact would increase support the development of civic trust (Putnam 1993). Essentially meaning a functioning social network is key to increasing political participation. Many theorists have claimed that the Internet has caused a weakening in social ties (Putnam 2000). However, in their study on face to face versus computer mediated communication, Etzioni and Etzioni found that “far from finding that CMC systems cannot meet the needs of 'real' communities, we find that there are no conceptual reasons or technical ones, that CMC-based communities, especially given additional technical development, could not become fully fledged communities” (1999: 247). Kniep and Nieysto claim that the offline and online worlds have become so intertwined, it does not make sense to separate them (2007). Furthermore, Yzer and Southwell also reject “the polar choices of isolation and interconnectedness” by claiming that “new communication technologies seem at best to have interacted with human group tendencies to produce yet again a world in which loneliness is common but not universal and social networks exist but have important limits” (2008: 12). This blurring of worlds is also apparent with regards to hacktivists with collectives that would only protest issues online taking to the streets to march or organising offline activities to protect the homeless population during winter which will be seen in Chapter 5. Kobayashi, Ikeda and Miyata also believe that participation in online communities enhances and encourages social capital as online reciprocity “has a positive effect on intention to participate in online civic discussion” (2006: 582). Zuckerman found that when activists spread their messages via the main social media platforms they were less likely to be shut down (2015). Zuckerman suggests that this is due to the fact that authorities do not want to alert regular users that they might be censored and they don’t want to anger users by shutting the social media service down (2015). Additionally, 66% of social media users have posted expressing their political opinions, responded to or shared political posts, followed political groups or joined specific political groups online (Rainie, 2012).

Neumayer and Svensson have stated that studies focusing on online activism do not differentiate between the forms of participation, however, there is clearly a diversity in how the Internet is used which depends on the actors political positions and the ways in which they're willing to enact change (2016). The less radical forms of online participation include comments in discussion forums, Facebook likes, petition signing and showing solidarity on Twitter. Those involved in less radical actions also share and disseminate information and are important for the visibility and acknowledgement of activist demands. However, Nemayer and Svensson claim that these forms of participation do not fall under the banner of acts of civil disobedience (2016). This is due to the fact that they are simplistic and there is a lack of risk involved in them. However, if the activist were to carry out these actions in an authoritarian state where there is a higher level of risk, the level of risk would increase greatly. Therefore, it is not simply the form of action that is undertaken that can fall under the banner of civil disobedience but also the context within which it is undertaken. Neumayer and Svensson, then, state that "a situational and relational component determines activists' readiness to expose themselves to the risk of surveillance and punishment by potentially hostile authorities" (2016: 136).

Similarly to offline forms of activist participation, online forms of resistance vary and can include mass action and civil disobedience alongside symbolic action, performance acts and artistic expressions of resistance. During these events, social media and mobile communications are used in order to mobilise and connect individuals. Lievrouw puts forward the examples of culture jamming, artistic expression, hacking, participatory journalism and coordination of physical protest as the ways in which participants can make use of new media (2011). Yet, a debate exists on whether participants both online and offline would consider themselves to be activists, for example, those who like a Facebook page supporting protesters may not consider themselves to be aligned with radical activists and civil disobedience. Mercea found that digital participation is more extensive when participants feel they are exposed to a lower level of risk as awareness of being under surveillance by authorities will most likely decrease the readiness of individuals to use public platforms to carry out protest actions (2012: 161). Nemayer and Svensson state that although social media is important with regards to mobilisation across the political spectrum, there are structural disadvantages for radical activists who rely upon it (2016). These disadvantages can occur as a result of the fact that the data is owned by dominant economic players who are able to share this data with state authorities such as the government or police. Therefore, they claim that social media and street action are important when paired together. However, there are also protest activities that occur solely online such as hacking, information leaking, doxing and crowdsourced attacks. These loosely connected hacktivist groups have a clear political agenda and many individuals who may not identify with these groups have shown support for their forms of resistance through likes, comments and participating in protest activities that require crowdsourced online actions such as denial of service attacks. Yet, Milan asserts that as a specialised form of activism, hacktivism lacks widespread support (2015: 6). She explains that this is due to the lack of transparency it involves and their lack of accountability to the individuals they claim to serve. Moreover, hacktivist operations have at times become coercive as activists “assert their moral claims, irrespective of the legality of their protest, by using their bodies to occupy a space” (Doherty et al, 2003: 67). However, the argument does not take into account the ways in which certain hacktivist collectives will also take to the streets and take up space.

Nemayer and Svensson find that readiness to act in civil disobedience is a key dividing line with regards to how dissent is expressed (2016). As a result they differentiate between individuals who express an opinion on social media platforms as a part of identity expression and those who are prepared to act in civil disobedience and expose themselves to a higher level of risk. Similarly along this differentiation then is those who do not consider themselves activists but instead see themselves as politically engaged individuals and those who do. Therefore, it would seem that readiness to engage in civil disobedience is linked to the individual's conception of themselves as an activist as opposed to merely politically-engaged. Based on the notion of activist participation, identity and readiness to act, Nemayer and Svensson put forward four types of activist (2016). These types are the salon activist, the contentious activist, the law-abiding activist and the Ghandian activist. The salon activist views their opponent as an enemy who should be fought rather than accepted. They have an antagonistic view of their opponent and are prepared to engage politically within the legal framework but not prepared to engage in civil disobedience or any other high risk protest activities. Salon activists are likely to identify as politically active but not as an activist. However, they are likely to support activists and form a temporary unity with them against their opponent, however fear of punishment would prevent them from engaging in anything radical. The salon activist is more likely to be more visible in the present day due to social media and can be linked to the more derogatory arguments surrounding activism online as being slacktivists or armchair activists. However, Nemayer and Svensson argue that this type of activist is important in showing and making visible campaigns as well as spreading support for more contentious types of activists (2016).

The contentious activist, on the other hand, is prepared to engage in civil disobedience in order to enact change. They are aware of the risk involved in civil disobedience and they are prepared to face the punishment for law breaking. They do not see their opponent as a respectable adversary, instead they view them as a non-acceptable enemy that must be eliminated. They self-identify as activists and acting in civil disobedience is used in order to radicalise their political position and identity. Contentious activists are likely to take part in illegal occupations or property damage as well as online methods such as hacking websites, deleting web content or sending threats. They consider civil disobedience to be a necessary strategy in order to resist their opponent that they believe needs to be eliminated. They view the risk of punishment as a part of their struggle. Nemayer and Svensson (2016) claim that the biggest problem for this activist type is that they are inclined to use violent methods of protest actions. This is due to the fact that the combination of their view of their opponent as an enemy and their willingness to accept punishment for protest actions. Hacktivists would mostly likely be considered contentious activists in that their methods of protest are illegal, they certainly consider themselves to be activists and view their opponents as non-acceptable enemies.

The law-abiding activist, however, is located at the other end of the scale whereby they respect their opponent and view them as someone to be listened to and someone with whom to engage in meaningful discussions despite the fact they have differing opinions. The law-abiding activist has strong political opinions and engages in political participation, yet they are not necessarily willing to engage in civil disobedience and do not self-identify as an activist. They will, instead, engage in participatory political discourse therefore, social media can offer law-abiding activists the opportunity to explore and express their identities by participating in online campaigns or signing petitions. However, as oppressive regimes can strategically use social media to give their public a forum for debate it can support existing power structures as the space allocated for discussion is controlled and manipulated by the government (Morozov, 2009).

The final activist type is the Ghandian activist which is characterised by a readiness to act in civil disobedience in order to enact change while also viewing their opponent as someone who has the right to a political opinion and respect. They display a high level of willingness to engage in civil disobedience and as a result are ready to risk punishment for breaking the law. However, these acts of civil disobedience should remain non-violent as violence tends to be linked to the idea of the opponent as an enemy instead of an adversary. Nemayer and Svensson (2016) claim that this activist type is the ideal against which the yardstick of activist participation should be measured and is hard to find. However, the Ghandian type does not seek a consensus and they are ready to engage in conflictual struggle. With regards to their use of the Internet in undertaking protest action, social media can provide an interesting space for participation of this kind whereby discussion and conflict can take place in a radical yet non-violent manner. However, the capitalist origins of social media can lead to structural disadvantages of this type and lead to the exclusion of political opinions if not expressed in conjunction with some form of violent action. Furthermore, Ghandian activists could be overlooked in a saturated online environment if violent action isn't used. Nemayer and Svensson (2016) claim that despite the Ghandian activist being the ideal activist type, the online media often hinders the expression of radical political opinion.

Bennett and Segerberg claim that communication itself has become a new form of organisation (2012). They argue that digital technologies are changing the traditional paradigms used to explain collective action. Digital technologies demand a theory that moves away from traditional theories of resource mobilisation, rational decision-making and cost-benefit analyses and instead looks at 'connective action'. This results in large-scale personalised and digitally mediated political engagement whereby "ideas and mechanisms for organising action become more personalised than in cases where action is organised on the basis of social group identity, membership or ideology" (Bennett and Segerberg 2012: 744). Greijdanus et al state that connective action is "bottom-up mobilisation that occurs when calls to action cascade through interconnected personal networks" (2020: 49). The theory of connective action seeks to explain contentious political action that has been altered by technology. This includes a new element of organisation as well as shared mediated content that occurs on social media (George and Leidner 2019). Connective action is successful when promoting specific messages and inciting action such as in hacktivism campaigns (Anduiza, Cristancho, and Sabucedo, 2014). Moreover, connective action successfully utilises information and communications technologies to organise and communicate with one another which predominantly uses social media platforms (Vaast et al., 2017). Based on this then, communication networks allow for this kind of personalised politics. Rosenbaum and Bouvier claim that the use of technology in social movements has shifted perceptions away from the traditional view of movements as being an organised collection of actors into a continually changing network of individuals (2020: 121; Bennett and Segerberg 2012). Indeed, historically, social movements were focused on the creation of a collective identity; however, contemporary activism is predominantly focused on a group of individuals communicating and sharing ideas at the same time. Brunner describes this concept as online activism being made up of 'shifting and messy relationships' (Brunner, 2017: 669).

Based on this, it can be argued that the current landscape of online activism is not characterised by traditional views of collective action as they are no longer focused around specific social or political organisations. Rosenbaum and Bouvier hold that activism is now an individualised and technology driven pursuit rather than a well-organised, top-down endeavour (2020: 122).

The way in which a movement reports successes has also been altered as a result of information and communication technologies. Historically, the outcomes of social movement activities refer to a change of the political, cultural, and biographical domain. The political domain is that which is studied the most, success in this regard, success would be a modification in policies, legislation, institutions or regimes (Amenta, Caren, Chiarello, and Su 2010). Chenoweth found that 3.5% of the population needs to actively take part in a protest for the protest to be considered successful in the political domain (2011). The cultural domain is that which is studied the least and relates to an alteration in the values of the greater public, the development of new cultural products and practices and the creation of a collective identity (Uba and Bosi 2009: 409). Yet Uba and Bosi state that there seems to be a general agreement that social movements can have a wide range of consequences that should not be reduced to the simple terms of “success” and “failure” (Giugni 1998; Amenta and Young 1999; Jenkins and Form 2006; Uba and Bosi 2009: 409). Hussein and Howard found that digital activism is predominantly successful when protesting government as opposed to business (2013: 32). Additionally, they found that for digital activism to be successful a number of social media tools should be utilised rather than just one. With regards to hacktivism, Downing states that hacktivists “create little islands of prefigurative politics with no empirical attention to how these might ever be expanded into the rest of society” (Downing, 2001: 72). Yet Milan argues that their operations represent an example to society (2015). Quoted in Hintz a hacktivist explained that hacktivism “can be very utopian, very experimental. They don’t have the pressure to present an outcome at the end (…) As such, they might have the function of some utopian ‘guiding star’, the star that provides a fixed point of navigation for sailors, who use it for orientation without attempting to reach it” (Hintz, 2010: 252).

3. Networked Social Movements:

Now that we have examined the literature on how the Internet has changed social movement organisations and activism we can look at the dominant theory of Internet social movements, networked social movement theory. Historically, movements relied on networks formed during a movement's lifespan as well as with other movements, the media and society at large. Newer networked social movements tend to display similar characteristics however, despite the fact that movements historically have been rooted in urban spaces through occupations and street demonstrations, they have undergone a transformation as a result of technological advances and are now placed in both physical and cyber spaces. As a result, social movements are reliant even more so on networks. The Internet has only increased this by introducing the web, email and social media to further a movement's pervasiveness. Political events such as the Arab Spring protests and the Occupy Movement as well as pro-democracy protests in Hong Kong have only reinforced this idea. Diani claims that approaching movements as networks “enables us to capture their peculiarity vis-a-vis cognate forms of collective action and contentious politics better than current dominant paradigm” (2003: 301).

Networks reflect organic forms of organisation creating a structure that enables information to flow (Gonzalez-Bailon and Wang 2016: 3-4). Cammaerts states that “networks are often understood as direct and indirect connections between individuals and/or organisations in collaborative endeavours” (2013: 421). Castells claims that the result of the transformation of social movement networks has led to movements no longer needing an identifiable centre, formal leadership or vertical power structures to ensure their message reaches the masses. The decentralised nature of modern social movements also increases the chance of participation as these networks are constantly refiguring themselves according to the level of attention and involvement with the larger population. Movements are also less vulnerable to repression due to the fact there are fewer specific targets and occupied spaces as well as less vulnerable to internal power struggles and bureaucratisation. Castells states that these new movements are both local and global. Local in that they start in specific contexts, build their own networks and occupy spaces (2012). But global in that they are connected throughout the world, they learn from other experiences and ensure ongoing debate online. New social movements express “an acute consciousness of the intertwining of issues and problems from humanity at large” (Castells 2012: 251) while being rooted in their specific identity. While historically social movements relied on the printing press, the radio or television, activists are now able to use the Internet allowing information to flow to large numbers of people which can lead to a plethora of possibilities for democratic interaction (Langman 2005: 44). This has led to the creation of newer forms of activism and cyberpolitics as well as unprecedented opportunities for discussion and debate. Yet, Slavina and Brym found that “while some characteristics of the globalised activist portrayed by Castells and others apply to the demonstrators in our sample, other characteristics are not significant, do not affect protesting in the expected direction, or are moderated by national context” (2020: 216). Furthermore, they found that rather than the democratising force the Internet was claimed to be, protesting is still positively and significantly associated with some of the traditional markers of social privilege. Slavina and Brym suggest that these findings question information and communication technology’s ability to flatten cross-national differences in activism (2020). Opposing Castells’ argument that people who live in repressive regimes are now more enabled to take part in demonstrations, Slavina and Brym found that those who are most likely to trust their government are more likely to engage in protests.

Nevertheless, Langman claims that electronically mediated participation has resulted in the perfect conditions for the emergence of mobilising structures that are highly fluid and less structured allowing for a more open and participatory space and are articulated for a wide variety of issues (2005). With regards to their genesis, newer social movements are triggered by either a specific event which causes a spark or as their disgust of the actions of rulers reaches its peak. Yet, Castells claims that the source of the call to action is less relevant than the impact of the message on the readers whose emotions connect strongly with it. YouTube, for example, has been singled out as being one of the most potent mobilising tools available to a movement in its early stages. It can increase the virality of a movement as seeing and listening to protests elsewhere can inspire mobilisation and trigger hope of the possibility of change. Castells states a “condition for individual experiences to link up and form a movement is the existence of a communication process that propagates the events and the emotions attached to it. […] In our time, multimodal digital networks of horizontal communication are the fastest and most autonomous, interactive, reprogrammable and self-expanding means of communication in history. […] the networked social movements of the digital age represent a new species of social movement” (Castells, 2012: 15). Fuchs asserts that while Castells’ may be correct in stressing that protest movements require objective conditions to emerge, the role in which the Internet and social media play needs to be confirmed with empirical evidence (2012). Fuchs argues that “Castells model is simplistic: social media results in revolutions and rebellions” (2012: 781). He questions, if social movements live and spread through the Internet, then why did the Egyptian revolution survive after the Internet had been shut off on January 28th 2011?

Decision-making in these newer movements take place in assemblies and are usually leaderless due to the deep distrust most participants have in the form of a power delegation. This, Castells claims, is the result of the rejection of political representatives by those they are supposed to represent after a feeling of betrayal in their experience of politics. Castells acknowledges that while there are participants that are more vocal, influential and active in the movement this is by virtue of committing themselves full-time to the movement. These activists are only accepted in these roles as long as they do not make any big decisions by themselves. Therefore, implicit in these movements is the rule of self-government by the people in the movement. The horizontal nature of these networks supports cooperation and solidarity while removing the need for formal leadership.

Self-reflection is also a constant in these movements. They interrogate themselves about who they are as both a movement and as individuals. Ensuring that they all know what they want to achieve, which kind of democracy and society they are after and how to ensure they are successful and don't fall into the traps and pitfalls previous movements have fallen into by reproducing in themselves the mechanisms of society that they want to change, specifically politically. This is apparent in the blogs and discussions on social movements. Castells claims that one of the key themes of discussion revolves around violence as in principle these movements are non-violent engaging in peaceful civil disobedience. It is essential in order to sustain the movement by ensuring that they remain a legitimate peaceful movement juxtaposed with the violence of the system. Furthermore, due to the nature of these modern movements, the demands and motivations of those involved are unlimited. Therefore, they do not have a program based upon a specific set of goals. This Castells claims is both their strength and their weakness. It is their strength, in that it leads to wide open appeal allowing anyone to join and their weakness as it makes achieving something difficult if they have no goals to be achieved. The result is that these social movements are aimed at changing society. They are public opinion movements that can affect elections, not through seizing the state but through transforming it.

As detailed above, communication has alway been crucial in social movements as people can only challenge those in power by connecting with one another. They are based on shared outrage and a feeling of togetherness. Thus movements rely on interactive networks of communication, which currently is the Internet. It is through the Internet and digital communication techniques that movements are able to live and grow. It has provided movements a space for leaderless movements to thrive and expand. It does so by ensuring those in the movement can maintain communication amongst themselves and the outside world. Computer-proficient organisers have become skilled in the use of the Internet in enabling Internet working. Langman claims that computer mediated communication has enabled virtual public spheres as well as fluid networks, identities and newer forms of social mobilisation that can be better understood as flows rather than the traditional lens of formal organisations (2005: 46).

Castells claims that the actual goal of modern movements is to raise awareness among citizens and to empower them through participation in the movement . This is due to the fact that the ultimate battle of social change takes place in people's minds which networked communications have assisted in facilitating. Castells found that in November 2011 in 23 countries more people were favourable than unfavourable towards the Occupy movement and the majority of people agreed with the movements critique of governments, politicians and financial institutions. A critique of this, however, is that many modern day online protestors remain anonymous. Cammaerts states that anonymity is crucial for protestors who often put their careers and freedom at risk by leaking hidden information or targeting a government website (2013) . The result of this is that very weak ties are formed within the network. Friedberg and Donovan claim that "historically activists have adopted anonymisation techniques to ensure operational security when organising on open or closed networks" (2019). Yet, the rise of the Internet has created new opportunities for individuals to influence online conversations anonymously. In their study, Friedberg and Donovan found that while the tradition of anonymity online gave rise to those appropriating the style of networked social movements to a digital space such as the Occupy Movement in 2011 a new breed of inauthentic pseudo-anonymous influence operations (PIO) were occuring. PIO refers to politically motivated actors that can impersonate marginalised or vulnerable groups in order to discredit or disrupt their causes. This can weaken trust which in turn can affect the social capital of anonymous protestors online due to inauthenticity.

Furthermore, if a networked social movement has a public facing communication strategy whereby a specific political identity is articulated it could be mimicked by PIOs (Friedberg and Donovan 2019). Thus, anyone could claim to be a part of a hacktivist collective including PIOs in order to troll and sabotage members actively taking part in political discussions (Donath, 1996: 15). Greijdanus et al. suggests that anonymous online spaces liberate people from the concerns of being evaluated and the subsequent restrictions to their behaviour (2020). As a result, activism that occurs online is free from the fear of repercussions. Indeed, a misconception on anonymity in online spaces refers to the idea that when people are less personally identifiable they become deindividuated and less responsive to social norms. Rather, Greijdanus et al. posit that anonymity to outside organisations empowers individuals to behave more consistently within the norms of the inside group (2020). Therefore, if the inside group is inherently passive and non-violent, the anonymous individuals will display these norms.

Moreover, Cammaerts researched into the dynamics of the networks surrounding Wikileaks and found that the “development of strong offline ties is combined with the strength of weak mediated ties as well as with the activation of latent ties at strategic moments’” (2013: 421). Furthermore, Benkler claims that WikiLeaks represents a “vivid instance of the ways in which the networked society has disrupted traditional pathways for the exercise of power and created new dimensions of power and new degrees of freedom” (2011: 750).

4. Criteria of modern social movements

A great deal of social movement scholars have submitted that social movements need to be unique and identifiable with explicit goals (McCarthy and Zald, 1973; Snow, Soule, and Kriesi, 2004; Tilly and Wood, 2015). Tilly put forward guidelines for the success of a social movement which includes the identification of a cause, the methods and the tools a movement should use (2006). Tilly also provided an acronym for the key aspects a movement will need to succeed: WUNC - the Worthiness, Unity, Numbers and Commitment of the movement (2006). Worthiness denotes the appearance, professionalisation and seriousness of the members of an organisation and how these come across to the public. Unity refers to the depth of agreement between members and the extent to which all members are putting forward the same messaging. The concept of numbers is linked to the number of members with a larger amount of members exerting more influence than smaller groups. Finally, Commitment refers to the willingness of members to put in a great deal of effort and resources. However, George and Leidner suggest the WUNC guidelines no longer fit for digital activism (2019). Indeed, Worthiness can be replicated through professional looking websites and Unity is no longer required due to the decentralised nature of modern social movements with members working on individual content. Additionally, the numbers can be faked with the use of bots and previous online movements have shown successes with minimal numbers. Finally, commitment is irrelevant as successes can occur without the vast investment of effort and resources thanks to social movement. This idea can be linked back to the move from collective action to connective action which can promote messages and incite action (Anduiza, Cristancho, and Sabucedo, 2014).

George and Leidner outline the key differences between collective action and connective action (2019). Firstly, in collective action members are predominantly aligned with the beliefs of the movement while connective action does not seem to demonstrate this with members engaging with differing levels of commitment and beliefs (Bennett and Segerberg 2012; Bennett and Segerberg 2013; Selander and Jarvenpaa, 2016; Vaast et al., 2017: George and Leidner, 2019). Moreover, the costs associated with collective action are much higher than those associated with connective action. Information and communication technology has improved communication as well as the coproduction of content. The concept of personalisation is also a key component of connective action. Content can now be targeted and framed in ways that were not possible historically (Bennett and Segerberg: 2013; Young: 2018). George and Leidner maintain that connective action is key to digital activism. It is clear then, that the Internet has changed the activism landscape and as a result the key criteria. With the Internet altering the amount of individuals needed to result in success as well as the skills needed to organise (George and Leidner 2019: 5). George and Leidner created the below table (Table 4) outlining the changes the Internet has led to as well as what is needed to be considered a social movement (2019, 5).

Table 1: Traditional vs Digital Activism (George and Leidner 2019: 5)

	Traditional Activism	Digital Activism
How many participants are required?	Successful social movements were associated with large numbers of participants (Tilly 2006)	Digital resources provide efficiencies that allow fewer participants to have a greater impact (Bennett and Segerberg 2012)
How old are participants?	Greater participation was associated with an increase in age (Milbrath 1965)	Younger people with technology skills are more likely to engage (Rainie et al 2012).
What are success factors for the cause?	An identified cause or campaign, effort, worthiness, unity, number of participants, commitment, resources. (Zald and Asha 1966; McCarthy and Zald 1973; Snow et al 2004; Tilly 2006; Tilly and Wood 2015)	Digital skills, access to the Internet, digital technologies, large social network. (Bennett and Segerberg 2012; Rainie et al 2012; Bennett and Segerberg 2013; Agarwal and Dhar 2014; Selander and Jarvenpaa 2016; Vaast et al 2017; Young 2018).
How do participants connect?	Attending meetings and demonstrations, communications via post (mail), manned information tables.	Via social media, websites, texting, digital platforms using a variety of ICT. (Nam 2011; Vitak et al 2011; Bennett and Segerberg 2013; Agarwal and

	(Tilly 1978; Melucci 1996; Bimber 2000; Karpf 2010)	Dhar 2014; Selander and Jarvenpaa 2016; Constantinides, Henfridsson and Parker 2018)
How are marginalised groups affected?	Marginalised groups were often left on the sidelines because of a lack of resources. (Tilly 1978; Jenkins 1983; Bennett and Segerberg 2013)	Marginalised groups have more options to make their voices heard. However, a gap in digital content production still exists. (Schradie 2011; Bennett and Segerberg 2013; Agarwal and Dhar 2014; George and Leidner 2018; Schradie 2018)

This table details how the social movement landscape has been significantly altered by information and communication technologies. The result of this is that previous definitions and criteria set forward by historical social movement scholars could now be considered to be obsolete. As a result a criteria in order to establish what constitutes a social movement will take into account the above table and the changes it outlines. Rather than applying the WUNC criteria measuring the Worthiness, Unity, Numbers and Commitment of a movement, a new criteria will be based upon the Digital Activism section of the table set out by George and Leidner (2019: 5). As a result, in order to establish what constitutes a social movement within the realm of this dissertation, the success factors and the way in which participants connect will be applied. Additionally, further factors to consider in a criteria on what constitutes a social movement in the age of the Internet are put forward by Castells (2012). Firstly, a modern social movement does not need an identifiable centre, formal leadership or traditional vertical power structure in place. While some movements may have members that are more vocal or committed, these spokepeople are only permitted to act in these roles as long as any big decisions are made as a group. Secondly, social movements need to have an awareness of the intertwining issues that are affecting humanity at large. Thirdly, they are predominantly triggered into life by a specific event or when their disgust at those in power reaches its peak. Fourthly, these movements are constantly engaging in self-reflection and stating their aims. Fifth, the main aims of the movements is to raise awareness and empower citizens to mobilise. Finally, these movements rely on interactive networks of communication. Based on this criteria, it is clear that hacktivists could consider themselves to fall under the realm of social movements. Taking Anonymous as the largest and most well known hacktivist collective, The success factors of digital skills, access to the Internet, digital technologies and a large social network can certainly be identified with the collective existing solely as a result of the Internet and requiring digital skills to engage in their operations. Moreover, the participants of Anonymous connect to one another using Twitter as well as Internet relay chat channels. Additionally, using Castell's networked social movement theory, Anonymous does not have an identifiable centre, any leadership or vertical power structures. They express an awareness of the wider problems humanity faces and their specific operations are predominantly triggered into existence as a result of an event. Anonymous regularly posts reminders about who they are as a group and will engage in a large amount of awareness raising in their social media communications. As a result, it is clear then that certain hacktivists could be seen to fall under the realm of new networked social movements. The empirical chapters in this dissertation (Chapter 5 and 6) will outline this in more detail.

Karatzogianni details the different movements that make use of digital technologies and the wide range of issues that they are based around (2015: 122). These include:

- "Demanding global justice, countering capitalist crisis and austerity
- Challenging hegemony: secession, insurgency, and extremist movements
- Demanding regime change, opposition movements
- Countering the state, transparency, anti-surveillance movements
- Offering alternative socioeconomic, lifeworld, and political reforms: peer production, ecological, LGBT/queer/feminist movements." (Karatzogianni 2015; 122).

When considering how the Internet has affected social movements, Van de Donk claims that "as a means of facilitating the creation of cross-national, 'disorganized' networks for collective action on the basis of negotiated common concerns, the Internet might almost have been purpose-built for social movements" (2004: xvii). Breindl claims that the Internet is useful for social movements as it facilitates mesomobilisation, or the coordination between various movements across borders (2010). Rosenbaum and Bouvier posit that on a societal level these new technologies have the ability to counter corruption, circumvent authoritarian regimes, and contest existing power structures (2020: 121). Activists are able to reach many without having to expend a lot of resources, furthermore, state control can be bypassed while still retaining editorial control over the content (Scott and Street 2000). Caren, Andrews and Lu have identified important characteristics of the merging landscape of new technology and media forms with social movements that are different from those that occurred in earlier periods (2020: 444). The characteristics "include (a) the rapid speed of communication, (b) the ability to deliberate and coordinate activity without physical copresence, and (c) the capacity for many-to-many communication" (Shirky 2008; Earl and Kimport 2011; Caren, Andrews and Lu 2020: 444). Schradie suggests that these changes have the potential to influence the speed and scale of mobilisation as well as the ability to enhance, undercut or change the efficacy of a movement (2019). Additionally, Caren, Andrews and Lu claim that new movement technologies result in reduced costs for movements which may lead to movements that are more nimble, participatory and less dependent on media gatekeepers in their search for supporters and targets (2020). Certainly, these characteristics assisted in the introduction of hacktivists within the movement landscape with hacktivists communicating rapidly online, coordinating activities without ever having met and communicating to large audiences. Moreover, hacktivists do not rely on traditional media structures and do not require much in terms of their finances.

Moreover, Samuel distinguishes hacktivism as other forms of online political activism due to its disruptive nature. While historical social movements do use online petitions, websites, discussion lists and other electronic tools to organise, lobby and communication hacktivism stands slightly apart in its use of electronically-enabled disruption for political means (2001:8). However, she still makes the case that hacktivism should be considered a social movement in that they share a common discourse, they are outside of the world of institutionalised politics and that it is a response to collective action problems. Samuel found that hacktivists define themselves as their own movement, this can be linked to Fine's 'bundle of narratives' notion (Fine 1995: 128). Here, social movements promote shared identification and self-define which is a phenomenon many hacktivists engage in and was certainly found in Chapter 5. In Samuel's analysis of hacktivist listserv's she found that hacktivists are at least as occupied with creating group narratives as they are with hacking websites. The fact that hacktivists are also external to institutionalised politics is also important in identifying hacktivism as a social movement. Throughout the history of social movement studies, theorists have studied revolutions, protests and other non-institutionalised events (Lo 1992:225). Hacktivism would certainly fall under this view as it occurs outside of routine political channels such as campaigning and voting. Hacktivists themselves also take pride in their outside status which again is found in Chapter 5 with hacktivists calling out institutional politics for wrongdoing. It is clear then that hacktivism emerged out of an innovative solution to collective action dilemmas, by increasing individual efficacy by creating technologically enhanced one person forms of protest.

5. Definitions:

It is apparent that due to the internet the criteria for what constitutes a social movement has shifted. Based on the above section outlining the updated criteria members no longer need the same beliefs and can commit to the movement as they wish, the costs to entry are substantially lower and content can be framed and targeted without the need to traditional media companies or governments. Moreover, movements no longer need an identifiable centre, formal leadership of traditional power structures. Modern movements are aware of the complexity of modern politics, usually triggered into like by a specific event and constantly engaging with themselves. They aim to raise awareness and encourage citizens to act and rely on interactive networks of communications to communicate with these citizens. Finally, modern movements will share a common discourse and will exist outside of the world of institutional politics. This criteria would lend itself to hacktivism which could be seen to inhabit all of these qualities. Hacktivism, which has been described as "a method, a tool and a way of acting up, regardless of your political leanings" (Batz 28 October 1999 Quoted in Samuel 2001:14), will be examined in more detail in the following chapter, however, before this can be detailed, a final definition of social movements must be established as well as definitions for the key concepts to be returned to throughout the Dissertation. These were selected for their suitability to this Dissertation based on the above theories and criteria. Castell's earlier discussed networked social movement theory defines social movements as "*global, [...], they learn from other experiences,[...]. Furthermore, they keep an ongoing, global debate on the Internet, [...]. They express an acute consciousness of the intertwining of issues and problems for humanity at large,[...], while being rooted in their specific identity. They prefigure to some extent the supersession of the current split between local communal identity and global individual networking*" (Castells 2012: 250-251)[21].

Table 2: Definitions used in this Dissertation

Term	Definition used in this paper	Reference

[21] The full definition of social movements according to Castells is Social Movements are "*global, because they are connected throughout the world, they learn from other experiences, and in fact they are often inspired by these experiences to engage in their own mobilisation. Furthermore, they keep an ongoing, global debate on the Internet, and sometimes they call for joint, global demonstrations in a network of local spaces in simultaneous time. They express an acute consciousness of the intertwining of issues and problems for humanity at large, and they clearly display a cosmopolitan culture, while being rooted in their specific identity. They prefigure to some extent the supersession of the current split between local communal identity and global individual networking*" (Castells 2012: 250-251).

Social Movement	“Movements are [...] global, because they are connected throughout the world, they learn from other experiences, and in fact they are often inspired by these experiences to engage in their own mobilisation. Furthermore, they keep an ongoing, global debate on the Internet, and sometimes they call for joint, global demonstrations in a network of local spaces in simultaneous time. They express an acute consciousness of the intertwining of issues and problems for humanity at large, and they clearly display a cosmopolitan culture, while being rooted in their specific identity.”	Castells (2012: 250-251).
Digital Activism	“digitally mediated social activism”	Bennett and Segerberg, (2013); Selander and Jarvenpaa, (2016); George and Leidner, (2019)
Networked Social Movement	A movement that pursues change through informal, non-hierarchical or decentralised networks rather than through formal, centralised and hierarchical institutions.	Castells (2012)
Connective Action	“Collective action that exploits the personalised connectivity afforded by digital social networks”	Bennett and Segerberg (2012); Bennett and Segerberg (2013); George and Leidner, (2019)

The above table puts forward the definitions to be referred to throughout this dissertation of key concepts including the aforementioned connective action, digital activism and networked social movements. These definitions demonstrate that hacktivism could be a social movement. When considering Castell’s definition of social movements he details that movements are global, which hacktivism is. They learn and are inspired by the experiences of other movements, which again hacktivism is, this is evident in their language and some of their methods. Movement's engage with global debate and call for joint demonstrations, hacktivists will engage with both other hacktivists and other movements, for example their support of the Black Lives Matter movement. Finally, movements demonstrate the split between local communal identity and global individual networking, hacktivists do this through the fact that on the one hand they will work towards a specific operation while still forming part of the wider hacktivist network. Chapter 5 will empirically explore in more detail how hacktivism could be considered a social movement through comparison with other movements and the functions they employ.

6. Conclusion:

It is clear that new innovations have changed the face of social movement organisations whether they mobilise and organise online as well as offline or simply remain a virtual organisation based solely in cyberspace. Social movement's have existed throughout history, gaining attraction by scholars in the 19th century. Interest in social movements only grew with social movement scholars putting forward theories to try and explain how these movements work and understand why individuals would take part in such a movement. While some scholars would analyse the cost and benefits of a social movement (Zald and McCarthy 1987), others would investigate the socio-psychological process in order to explain why individuals would connect with movements (Goffman 1974; Snow et al 1986). Yet, over the past 20 years, scholars have become more interested in the way in which information and communication technologies have impacted on social movements. The Internet has enabled movements to connect in ways that many did not expect, movements can now cross countries without using any resources. It has impacted on the speed in which a movement can gain followers and allowed anyone with a cause to to be heard. There are still those who disagree on the level in which social movement organisations have been altered with some scholars claiming that the Internet has vastly altered the social media landscape and has, as a result, has enabled wider participation (Dahlberg 2007; Barberá et al 2015; Trevisan 2016). Whereas other scholars would consider digital activism as the same as traditional forms of activism (Foot and Schneider 2002; Lehtonen 2008; Jackson 2018). Despite this, Castells developed a new theory on social movements that only exist as a result of the Internet. He calls these 'networked social movements' and seeks to explain how digital technologies are altering the traditional paradigms used to explain collective action (2012). These networked social movements are decentralised in nature, are acutely aware of social justice issues and are triggered into life by specific events.

They engage in self-reflection, raise awareness of specific issues and rely on interactive networks of communication. Moreover, George and Leidner found significant differences in traditional forms of activism and digital activism which relies on skillful young people who connect via the Internet. When analysing this, it becomes apparent that activism has changed and those engaging in it are no longer experienced protestors with a large following. The Internet has appeared to democratise protests and what constituted a movement over 20 years ago may not be relevant in the current landscape.

There are now protestors who use their digital skills and the efficiencies that the Internet has allowed for fewer participants to engage in illicit forms of activism that were criminalised in the early 1990s. Hacking has existed since computer networks emerged and some forms of it are linked to political activism. In a similar vein to Castells, Jordan claims that power is shifting from physical locations to virtual ones. Hacktivists claim that the elites are developing and remaking the world through the use of electronic flows of power through cyberspace. As a result, hacktivists claim that power derives from information flows which should be blocked. When analysing the criteria developed in this chapter from the different social movement theorists' work, hacktivism could certainly constitute a social movement. Hacktivist organisations are decentralised, composed of young digitally skilled individuals who are acutely aware of present injustices. However, there is a gap in the literature on whether hacktivism could truly be considered a social movement which should then be afforded the same right to protest as offline movements as can be seen in the need to establish the above criteria. This dissertation aims to fill that gap. The following chapters in this dissertation will attempt to analyse this in more detail using a mix of quantitative and qualitative empirical research in order to establish if hacktivism could be considered a social movement. The next chapter will question what hacktivism as a phenomenon is asking whether hacktivism is a form of cybercrime or cyberterrorism, whether hacktivism is a form of civil disobedience and as such a tactic, whether it is a social movement, and as such a political entity, or a mix of these different concepts.

Chapter 3: What is Hacktivism?

1. Introduction

Politics has changed in recent decades as a result of globalisation and as such so have the ways in which people challenge it. Jordan argues that this globalisation alongside an increasing disappointment in political systems has led to political groups becoming dedicated to global political issues such as the economy or climate change (2002). The previous chapter detailed that hacktivism should be included in these political groups. This chapter will establish what exactly hacktivism is with scholars describing hacktivism as cybercrime, cybterrorism, electronic civil disobedience and a social movement. Indeed, the UK government sees hacktivism as a form of cybercrime and the phenomenon is legislated against under the 1990 Computer Misuse Act as a form of cybercrime. This chapter aims to demonstrate that hacktivism is a contentious subject with a great deal of conflict on what it actually is. It will argue that while some may consider hacktivism to be cybercrime, it is certainly not cyberterrorism. Moreover, while not explicitly detailed in any of the literature it is evident that some scholars view hacktivism as a method with other scholars would describe it as a political entity. This chapter will present the definitions for both cases before establishing that within this Dissertation hacktivism is considered to be both a political practice and a political entity with a definition that incorporates both aspects. For those that consider hacktivism to be a tactic, there is an explicit debate on whether hacktivism can be defined as electronic civil disobedience, both sides of this debate will be detailed. Firstly, this chapter will firstly detail the history of hacktivism and how it has evolved to become the movement that it is (2). It will then move on to the idea of hacktivism as cybercrime (3.2) and cyberterrorism (3.3). The chapter will then move on to the main crux of the argument examining whether hacktivism is a tactic (4), specifically whether it is electronic civil disobedience (4.1) and the reasons why it may or may not be considered to be so (4.1.1), or whether it is an entity (5), specifically a social movement entity (5.1). The chapter will then detail why hacktivism could be considered to be both an entity and a tactic (6) before then examining all of the above and answering the question, what is hacktivism (7) in doing so it will put forward a criteria on how hacktivism can be understood.

2. History of Hacktivism:

Hacking did not originally refer to illegal acts undertaken with computers or networks, it was originally used to refer to the habit of those working within the technology sector who would tinker with it in order to create something original or unorthodox, essentially aiming to make the technology do something that it was not originally intended to do. Hackers were predominantly interested in discovering new technological uses and assisting in the progression of knowledge by sharing their experiments with others. Jordan and Taylor suggest that modern day hackers originate from phone phreaks and programmers who developed into a subculture of people that were comfortable with new technologies instead of fearing them (2004). In 1984 journalist Steven Levy coined the term “hacker ethic” when describing the beliefs that run deep across this hacker subculture (1984). Kelly claims that this hacker ethic contained seven core tenants (2012): Firstly that access to computers should be unrestricted; secondly, that hackers should honour the “hands-on imperative”; thirdly, that information should be free; fourthly, that hackers should distrust authority and promote decentralisation; fifth, that hackers should only judge one another based on their hacking prowess and not by any educational or professional pedigree; sixth, that it is possible to create beautiful art simply by using a computer; and finally, that computers can improve a person’s life. This Kelly argues is proof that hackers have always shared a philosophical approach to their internet presence (2012). Historically, hackers have always preferred a decentralised and nonclustered meritocracy over a highly centralised close knit community. Karagiannopoulos adds to this by claiming that the hacker community is linked to the ‘resistance-facilitating potential of technology’ allowing for people to challenge established norms and standards (2018: 7).

Thus, the transition from this early vision of the hacker to the hacktivist of 2022 is an obvious one due to the belief that hacking can be inherently political. Bartlett states that hacktivism springs from the hacker tradition of theatricality and irreverence which was originally nonpolitical and confined to only those who had a deep knowledge of technology (2014). Nowadays however, according to Kelly when hacking becomes overtly political it is reframed from its philosophical underpinning to a more explicit view of gaining attention for worthy and neglected issues (2012). Kelly argues that this move from the historical philosophical hacker ethic to modern day hacktivism means that there is a more fine-tuned set of beliefs surrounding the tolerance for legal risk, scale of collective action and propensity for multinational cooperation (2012). Kelly suggests that these newer beliefs contain two important changes to the more traditional beliefs (2012). Firstly, hacktivists tend to engage predominantly in illegal rather than legal computer activity. Secondly, hacktivists tend to form collectives. This is unsurprising as they band together to target single issues.

Yet, Sorell argues contrarily that hacktivism is not necessarily a democratic process as it does not need to be backed by consensus building when directed against institutions that could be the target of conventional political opposition (2015). Furthermore, it is difficult to know how many people support a cause that is the aim of hacktivists as their methods tend to be anonymous. Thus, one hacktivist could have numerous cyber-personas. Sorell claims many hacktivists tend to be in their teens and as a result could lack political sophistication (2015). This opinion is not new, with Yar suggesting that hacktivists are perceived to be teenagers that undertake criminal behaviour by politicians, police, security experts and journalists (2005). Cultural representations also reflect these opinions, for example Hollywood films. The hacker is perceived as a "quintessentially teenage miscreant" (Yar 2005, 388). Sorell claims that hacktivists tend to espouse crude libertarian ideals and lack wide political support, despite this they can enjoy significant power as a result of their cyber-expertise (2015). Furthermore, as they are predominantly anonymous, hacktivists can be less inhibited in expressing unpopular opinions that are more impervious to criticism than those who express these opinions publicly. As a result, according to Sorell, hacktivism can appear much more shadowy than mainstream activist groups and is more frequented by fringe groups and outsiders (2015).

Karagiannopoulos claims that there were two eras of hacktivism with a shift occurring in the middle of the 2000s (2018). Prior to this shift, hacktivists were split into two groups based on their principles. In the first group were those that engaged in mass action hacktivism which mainly involved virtual sit-ins (Jordan and Taylor 2004). In the second group were hacktivists who focused more on the software side creating software that would facilitate activism. This is similar to Samuel's distinction of direct action versus digitally correct groups (2004). Karagiannopoulos splits these groups into three: The Virtual Demonstrators, the Artivists and the Information Purists (2018). The Virtual Demonstrators referred to protests undertaken by hacktivist collectives such as the Critical Art Ensemble (CAE) who focused on the importance of information in the networked world. They undertook an expansive analysis of cyberactivism tactics and their philosophies. The protests pioneered by CAE were put into practice by other groups such as the Electronic Disturbance Theatre which was a small group of activists that aimed to translate offline lives to the online world. The EDT's most famous action was supporting the Zapatista struggle in Mexico in the late 1990s. The artivists, or web artists, were also using technology to express their political opinions and share their art. Their activities ranged from sending out viruses with a political message to creating website parodies and were ideologically opposed to intellectual property restrictions and the commodification of art. The information purists would create software such as Floodnet, that was used to assist protesters in virtual sit-ins and would flood a network to disable it. This group was focused on promoting freedom of information and increasing privacy online. Unlike the previous two groups, however, the information purists were against virtual sit-ins and web defacements as they saw it as impeding free speech rights, instead they focused on information liberation. Due to these beliefs, they were seen as the digitally correct branch of hacktivism.

The second era, according to Karagiannopoulos, progressed to be an interesting blend of the methods and groups from the first era but pushed the limits even further (2018). This era is dominated by the collective Anonymous, who originally started out on 4chan, an online message board whereby users converge to discuss their interests and spread internet culture such as memes. Anonymous was formed on the b/board section of 4chan, where a large portion of the online trolling community originated from. Coleman has claimed that Anonymous has moved from a group of internet trolls to become a movement catalysed by political issues and world events (2011). This collective lacks concrete membership or ideology and is essentially an umbrella identity that can be used by anyone. This, according to Coleman, forms part of the core characteristics of Anonymous, the others being the lack of agreed mandates, the unpredictability and flexibility (2014). However, the collective does have a certain set of principles that all who use the mantle will abide by. These range from the hacker humorous deviant outlook to the use of technology. The rhetoric used by Anonymous is a lot more radical than that used by groups in the first era. Goode has suggested that the tone used by Anonymous is 'simultaneously nihilistic and idealistic, dystopian and utopian, egoistic and collectivist, and dedicated to the negative freedoms of libertarianism yet also concerned with collectivist goals of equality and justice' (2015: 79).

3. Hacktivism as Cybercrime or Cyberterrorism?

3.1. Cybersecurity

Before detailing the debates on whether hacktivism is a tactic or an entity and whether hacktivism is a social movement, it is important to firstly examine the overarching concept of cybersecurity as well as what cybercrime and cyberterrorism is with a specific focus on hacktivism as part of both. The Internet is a decentralised structure, the proper functioning of this structure depends on a series of complementary technical protocols, laws, and international regulations. (Calderaro 2020). Negotiations among different stakeholders, including those responsible for developing digital markets, policies, legal frameworks and technical standards are needed to ensure it functions as it should. Due to the vast expansion of the internet, states are increasingly focusing on cybersecurity to prevent a range of threats to the online space (Calderaro 2020). Definitions for the term cybersecurity are highly variable, context-bound, often subjective, and, at times, uninformative. Cavelty states that there are multiple interlocking discourses around the field of cybersecurity (2010). Craigen et al. have identified five dominant themes in the existing definitions of cybersecurity: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security) (2014). As well as the dominant themes, Craigan et al. also identified several conceptual categories present in existing definitions. These include asset, capability, misalign, occurrence, organisation, process, protect, resource and property right. As such, they proposed the following definition: “Cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al. 2014: 17).

Nye defines cybersecurity as “… a set of resources that relate to the creation, control, and communication of electronic and computer-based information – infrastructure, networks, software, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications" (Nye 2010: 123). Charlet and King state that cybersecurity policy is more successful when it is proactive rather than reactive and when it accounts for rapid technological change (2020: 8). They claim that there are many factors that result in the challenges policy makers face when tackling cybersecurity. For example, it is an issue that touches on technology, psychology, economics, business operations and behaviour. It also has different rules to those policy makers have become used to in the physical world, everything appears sped up in cyberspace. Cybersecurity is also a new area for policy makers and as such they’ve not yet had the time to develop the laws, policies, and practices needed.

While cybersecurity predominantly falls under the domain of governments and supranational institutions, they are not the only organisations with power online. Cyber power is one of the foremost theories of power online and is defined as “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power”(Kuehl 2009: 12). Defined behaviourally, It is essentially the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. ”Cyber power can be used to produce preferred outcomes both within and outside cyberspace (Nye 2010). Due to the man made nature of cyberspace it is unique and subject to vast technological development. This theory is relevant to hacktivism as the barriers to entry in the cyber domain are much lower than in other forms of power which results in non-state actors engaging in it, including hacktivism. Indeed, due to the low price of entry, anonymity, and ease of access has resulted in smaller actors having a greater capacity to exercise power in cyberspace than in many other traditional domains of world politics. These smaller non-state actors, such as hacktivists, use cyberspace as a tool of liberation (Nye 2010: 18). As a result some theorists argue that “even if we could stop all cyber attacks from our soil, we wouldn’t want to” in order to preserve the ability for hacktivists to use the internet to protest (Goldsmith 2010: online).

3.2. Types of Cyber Attacks

As explained above, internet crimes are wide ranging in scope and can include identity theft, fraud, phishing, child exploitation to name a few. Internet criminals could take the form of a single hacker working alone, activists, organised criminal gangs or even Nation States engaging in industrial espionage. However they take place, cyber incidents put at risk the supply of essential services such as banking. In general, Cyber attack is defined as “use of deliberate actions and operations ... to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information.” (Lin 2010: 63). This section will now define the main types of cyber attacks that are referred to throughout the Dissertation. Firstly, Phishing is the most common form of cyberattack used by cybercriminals as identified by the NCSC Cyber Breach Surveys. This is defined as “a scalable act of deception whereby impersonation is used to obtain information from a target” (Lastdrager 2014:8). The second most common form of cyber attack is a computer virus which NIST describes as “a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk."[22] The final cyber attack that is used by cybercriminals to be defined is ransomware. This has been defined by Pont et. al. as "a type of malware used to extort money from victims" whereby the "victim is typically notified through the use of a ransom note often accompanied by threatening demands and instructions on how to pay (usually via cryptocurrency such as Bitcoin). The attacker will only release the decryption key if the ransom is paid" (2019: 1). The types of actions used by hacktivists differ to those used by cybercriminals. The main methods used by hacktivists are DDoS and web defacements. Sauter defines a DDoS action as a "large number of computers attempting to access one website over and over again in a short amount of time, in the hopes of rendering it incapable of responding to legitimate requests" (2014:2). Web defacements are defined as " the unauthorised change of a Web Site or a Web Application front-end, that introduces significant modifications, with important negative impacts for the reputation and the operations of the owner organisation" (Bergadano et al. 2019: 4). Additional terms such as SQL injection will be defined later in the Dissertation (Chapter 6).

3.3. Cybercrime

Cybercrime is defined by UK police as "the use of any computer network for crime" (House of Commons E-crime report 2013). It is usually enabled and conducted through a connection to the Internet and can be committed anonymously with relative ease, sometimes without the victim knowing (Wilson 2009: 1). Cyberspace also allows cybercriminals to extend their reach beyond national borders. Due to the ease, anonymity, low probability of detection by law enforcement and the possibility of illicit profits cybercrime rises year on year. The UK Home Office uses a three-fold categorisation to divide types of cybercrime. The first is 'pure' internet crimes where a digital system is both the target and the means of the attack. The second category is 'existing' crimes that have been transformed by the internet which has allowed these crimes to be carried out on an industrial scale. The final category is the use of the internet to assist in the narcotics trade, people smuggling and other traditional forms of crime. The European Commission, similarly, proposed a threefold definition identifying cybercrime as traditional forms of crime committed using electronic networks and information systems, the publication of illegal content through electronic media, and crimes unique to electronic networks.

[22] https://csrc.nist.gov/glossary/term/virus Last Accessed 10 March 2022.

Efforts are being made by both national governments and multilateral organisations, such as the European Union, to deal with this issue. The main offences covered by existing legislation involve privacy offences such as the illegal collection of personal data, content related offences such as the distribution of pornography, economic crimes, unauthorised access and sabotage such as hacking or computer sabotage, and intellectual property offenses such as copyright.

Within the literature, at its absolute broadest, the term cybercrime has been used to refer to any type of illegal activities which results in a pecuniary loss (Jahankhani, Al-Nemrat and Hosseinian-Far 2014). Jahankhani, Al-Nemrat and Hosseinian-Far claim that in order to fully define cybercrime “we need to understand the impact of information and communication technologies on our society and how they have transformed our world” (2014: 149). Wall argued that the term ‘cybercrime’ does not actually do much more than signify the occurrence of a harmful behaviour that is somehow related to a computer, and it has no specific reference in law (2005). However, Yar has subdivided cybercrime into four areas of harmful activities: cyber-trespass; cyber-deceptions and thefts; cyber-pornongraphy and cyber-violence (2006). Hacktivism would fall under cyber-trespass in that it crosses cyber boundaries into other people’s computer systems whereby the rights of ownership have already been established resulting in damage. Donalds and Osei-Bryson established a taxonomy of cybercrime: Victim, Attacker, Objective, Tool & Tactic, Impact, Result, Relationship, Target and Offence (2014). Using this taxonomy, hacktivism could be seen as a cybercrime as it includes a victim (e.g a government who is the victim of a DDoS attack); an attacker (e.g a hacktivist collective undertaking a hack) that uses their technical skills to bypass security systems to promote their political cause; there is always an objective of a hacktivist attack, specifically a political or ideological objective. Hacktivism also includes a specific methods (e.g. using botnets for a DDoS attack); it will result in some form of impact as a direct consequence of the attackers action; it will then lead to a result, often in the case in hacktivism it can result in reputational damage. Hacktivism also includes a relationship whereby the hacktivist is linked to the victim; it also includes a target which is the object at which cybercrime is aimed. Finally, hacktivism, at present, leads to an offence as the methods that hacktivists use are legislated against in most countries, for example the 1990 Computer Misuse Act. Based on this criteria, it is clear that currently hacktivism constitutes cybercrime. Chapter 7 details the current regulatory approach to cybercrime including European and UK approaches to legislation and cybersecurity strategies, their use of both hard and soft law mechanisms, their use of agencies in attempting to tackle cybercrime and law enforcement approaches to reduce cybercrime.

3.4. Cyberterrorism

While, according to the literature hacktivism is a cybercrime, there are some scholars who would compare hacktivism to cyberterrorism and claim that there is a blurring of both concepts. Cyber terrorism is defined as “the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.” (Denning 2000; Special Oversight Panel on Terrorism). It exclusively happens in cyberspace with ICT systems forming both the weapon and the target (Kenney 2015: 121). While cybercrime is predominantly carried out for economic purposes, cyberterrorism is motivated by a specific ideology with the main aim being to shock or cause panic (Veerasamy 2020). Cyberterrorism comprises the following elements: political or ideological (e.g. social, religious or ethical) motivations; threats or actions that affect the government or public; causing harm or damage through attacks on ICT systems or infrastructure; and that the attacks are undertaken by clandestine or sub-national groups which at first glance does appear to have a great deal of similarities to hacktivism. Veerasamy offers breaching banking systems, the breakdown of energy suppliers through attacks on their ICT systems, disruption of governmental computer networks as examples of cyberterrorism. The motivations for engaging cyberterrorism reflect those of offline terrorists and will have an affiliation to one of the following causes (Nelson, Choi, Mitchell and Gagnon 1999; Flemming and Stohl 2000; Armistead 2004; Weimann 2004):

- Nationalist/Ethic whereby the terrorist aims to create a new politcal order based on their opinion of ethic dominance;
- Religious whereby the terrorist holds a strong belief in a particular religion’s views and values;
- Both left and right wing political intention to commandeer power;
- Single use which promotes a specific cause such as environmental issues.

The effects of cyberterrorist attacks will often result in detrimental impacts on civilians (Veerasamy 2020). These effects include disrupting core competencies such as health care or air travel. Cyberterrorists will target critical infrastructures to cause devastation and panic.

However, while cyber terrorism is a real threat, it has been described as limited and mostly ineffective. Cyberterrorism is more far reaching than cybercrime. It aims to create disarray, outrage and disruption on the widest possible scale whereas cybercrime is focused on stealing data or money from individuals that predominantly results in nuisance, annoyance or inconvenience (Veerasamy 2020).

While cyberterrorism and hacktivism do have similarities, they are separate entities. This is due to the fact that while web defacement and DDoS attacks may result in annoyance, they would be unlikely to threaten the lives and livelihoods of their victims. Davis elaborates on this by claiming that hacktivists are politically motivated and target institutions that oppose their political views, if a hacktivist were to target a healthcare institution for example, they would most likely search for specific patient data, intellectual property or aim to embarrass the institution (2016). Cyberterrorists on the other hand would destroy the critical infrastructure of the institution thus putting lives at risk. Moreover, the main methods used by hacktivists will only temporarily affect the target with the website being restored once the attack is finished. Cyberterrorism aims to have longer lasting effects with the aim of destroying the critical services of a nation. Indeed, while hacktivists use their knowledge of ICT systems and software tools to gain access to a computer system, they will do so to draw attention to their cause through well thought out and publicised disruptions of specific targets (Kenny 2015: 117-118). Indeed, Denning has stated that no hacktivists attacks have risen to the level of cyberterrorism as they did not result in "violence or injury to persons, although some may have intimidated their victims" (2000; Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism). Krapp has identified an alternative distinction with hacktivism and cyberterrorism which centres on their origins (2003). As detailed previously in this chapter, hacktivism originated from computer hobby-ists playing and innovating online with this spirit with its aims to create spectacles of vigilante computing (Krapp 2003: 87). Yet, at its origins cyberterrorism is essentially the transition of offline terrorist activities to cyberspace. An extension of this relates to the non-violent nature of hacktivism. Cyberterrorism will, at times, aim to harm human beings while hacktivists will, for the most part, simply engage in electronic civil disobedience and aim to cause a temporary nuisance (Samuel 2004). Samuel states that Cyberterrorism "is separated from hacktivism by its willingness to cross over into violence against actual human beings, or substantial damage to physical property" (2004: 4). Yet, Samuel states that in the post-9/11 contexts, hacktivism tends to be mis-characterised as cyberterrorism. Indeed, in analysis of major media articles the were published in the six months prior to and post 9/11 found that while there was some convergence in the two terms pre 9/11, the media blurred 97% of the coverage of digitally-enabled cyber terrorism and hacktivism after 9/11 (2003). As a result, Samuel states that the effort to distinguish hacktivism from cyber-terrorism, and the concern over who can lay claim to the title of hacktivist, indicate the importance that is attached to the hacktivist label (2004). The below table indicates the differences between hacktivism and cyberterrorism as well as general cyber-attacks and cyber-warfare. The table also demonstrates the lack of concrete definitive examples of cyberterrorism.

Table 3: Kenney's 'Necessary Attributes of Different Cyber Phenomena; (2015: 123).

Attribute	Cyber-attack	Cyber-warfare	Hacktivism	Cyberterrorism
Computer attack targeting other computers, computer systems, or the information they contain	✓	✓	✓	✓
Attack in pursuit of political, social, or religious aim		✓	✓	✓
Attack part of broader hostilities between belligerents, usually states or their proxies		✓		✓
Attack produces physical violence against persons, property or critical infrastructure				✓
Attack causes widespread fear or physical intimidation beyond immediate victims				✓
Examples	"I Love You" worm, "Slammer" denial of service attack, "Conficker" virus	Stuxnet, Russian cyber-attacks on Georgia	Anonymous attacks, "cyber jihad" against Danish newspapers	?

It is evident, based on the above, that hacktivism and cyberterrorism, while linked in their use of the internet and ICTs to undertake politically or ideologically motivated cyber attacks do have distinct differences. These include their origins, their methods, the effects that these attacks have on both the technologies they attack as well as governments and citizens. Indeed, while some of hacktivist attacks can be described as an aggressive form of contentious politics, it would appear that they fall more within the realm of civil disobedience rather than terrorism (Kenney 2015). Hacktivists will seek to communicate through disruptive techniques while cyberterrorists will do so through terror. As such it is evident that while hactivism could be considered to be a form of cybercrime by the UK government, it is not cyber terrorism. This will be examined further in Chapter 7 with a distinction between the different legislative approaches to both entities. The concept of hacktivism as both a tactic used in cyber activism and hacktivism as a political entity, specifically a social movement will now be examined.

4. Hacktivism as a tactic?

An identified gap in the literature is that some would describe hacktivism as a tactic and some would describe it as a political entity. This section will detail those that define hacktivism as purely a tactic followed with a debate on whether hacktivist techniques can be defined as electronic civil disobedience. The following section will then detail the literature on hacktivism as an entity, specifically continuing the discussion from the previous chapter on whether hacktivism is a social movement. The term Hacktivism is the conjoining of the words hacking and activism which was coined in 1996 when a member of the hacking collective ‘Cult of the Dead Cow’ sent an email using the word hacktivism to describe their behaviour and the group’s increasing political interest. The term itself has been adopted by many different groups of individuals, from groups themselves attempting to legitimise their behaviour to sensationalist media who use it for many incidents of cyber disruption. In general, Vegh (2003) and Denning (2001) have studied the wide variety of instances in which the term hacktivism was used ranging from cyberactivism to cyberterrorism and internet warfare. Denning defined hacktivism as “the marriage of hacking and activism” (2001: Online). Jordan and Taylor, on the other hand, have defined hacktivism as the “combination of grassroots political protest with computer hacking” (2004: 4). For scholars that consider hacktivism as a tactic, it “covers operations that use hacking techniques against a target’s Internet site with the intent of disrupting normal operations but not causing serious damage” (Denning 2001: 241). Similarly, Ludlow defined hacktivism as using “technology hacking to effect social change" (2013: 4). Karatzogianni has claimed that it refers to "when individuals organise through the internet to protest, or when they use networking to convey a political message" (2015: 14). Karatzogianni elaborates on this by stating that it is a "kind of civil disobedience in which activists break into governmental, corporate or organisational computer systems" (2015: 14). Furthermore, Li broke the definitions down to its simplest sense claiming that it "involves the use of technology hacking mechanisms, often in the form of cyberattacks to effect particular political and/or social change" (2013: 302). Karagiannopoulos describes hacktivism as 'the use of computer and network access and reconfiguration techniques that transgress or challenge cybercrime laws in order to produce or facilitate symbolic effects that confer a political message or protest a particular policy' (2018: 7). Moreover, civil society groups have defined hacktivism as a tactic. The Open Rights Group (ORG), a UK-based digital rights organisation, has defined hacktivism as "the use of unauthorised computer access to further an agenda, usually political or social."[23] The Brussels based European Digital Rights (EDRi) group has similarly described hacktivism as "confrontational activities like DoS attacks via automated email floods, website defacements, or the use of malicious software like viruses and worms."[24] They explain that digitally correct hacktivism as an alternative claiming that it "designs computer programs that help confirm and accomplish their political aims." The US based Electronic Frontier Foundation (EFF), on the other hand, has simply defined hacktivists as "people using computers and networks as a means of protest or action"[25] Big Brother Watch compares hacktivism alongside the democratisation of information flows and citizen journalism[26]. Some hacktivists themselves have acknowledged that hacktivism is "a method, a tool and a way of acting up, regardless of your political leanings." (Batz 28 October 1999).

According to Hampson, ideology and objectives can determine the form of hacktivism and the various methods used can be placed across a scale starting from those that transgress clear legislation, such as site defacements and distributed denial of service attacks, to methods where the legality is more blurred, such as virtual sit-ins (2012). Site defacements involve gaining access to a web page and changing the page. Site redirects entail gaining access to web servers or networks and changing the web address so that the visitor to the site will be redirected to an alternative site that is usually critical to the victim of the attack. Instead many

[23] https://zine.openrightsgroup.org/features/2012/is-hacktivism-a-genuine-form-of-protest Last Accessed 13 August 202
[24] https://edri.org/our-work/privacy-movement-dissent-protest/ Last Accessed 13 August 2020
[25] https://www.eff.org/event/who-are-hacktivistsLast Accessed 13 August 2020
[26] https://bigbrotherwatch.org.uk/about/events/Last Accessed 13 August 2020

people block access to the network through a coordinated data overload aimed at the target server which will slow it down or crash it. These data overloads can take the form of an email bomb (a large number of emails that it cannot handle), iRC jamming (overloading and internet Relay Chat) or ping storm (overwhelming the server with small data packets). The public can participate in these processes by downloading software that automates the process.

4.1. Hacktivism as Electronic Civil Disobedience?

Denning describes the techniques used by hacktivists as “electronic civil disobedience, which brings methods of civil disobedience to cyberspace” (Denning 2001:263). This corresponds to how hacktivists CAE defined electronic disobedience as the transition of traditional tactics of blockages and trespasses onto the internet. Stefan Wray, one of the founders of an early hacktivist collective, Electronic Disturbance Theatre, wrote a manifesto establishing the group’s techniques alongside those undertaken by Henry David Thoreau, the Civil Rights Movement and the Vietnam War. He claimed that as hackers become more politicised and activists gain a better understanding of computer systems, an increase in the number of hacktivists was inevitable. Their techniques, he claimed, would fall under the mantle of electronic civil disobedience whereby the same methods of traditional civil disobedience such as blockage and trespass will take place in electronic or digital form (quoted in McLaurin 2011: 239-240). This would suggest, according to O'Malley, that if a hacktivist's computer were removed, they would be no different to a protester demonstrating in the street (2013). Here, the issue lies with the computer, if the protest were carried out in real time online, it would simply be a legitimate exercise by a citizen engaging in their right to freedom of expression. Indeed, “for the hacktivist, hacktivism is an internet enabled-strategy to exercise civil disobedience” (O’Malley 2013: 140). They believe that they can make a difference to present day global society and state that “When we are strong, we possess the power to do the impossible—to make a difference, to better our world” (Anonymous 2010 quoted in Beyer 2011: 3). O’Malley compares online protests to offline protests such as strikes, which constitute a breach of employment contract, and sit-ins, which hinders businesses, to online protests as they are also technically illegal yet permitted due to the important social and political roles they have played throughout history (2013). Li suggests then that hacktivism amounts to civil disobedience as it is achieved either through the mechanism of disruption, information distribution or otherwise (2013: 304).

Zuckerman argued that a catastrophic consequence of the emerging digital public sphere is that everyone can now speak but not everyone is heard (2014). As such, protections to freedom of speech could be ineffective. In the physical world, activists demand to be heard by occupying public spaces. In the Civil Rights movement, protesters occupied lunch rooms and buses to demand equality. Yet on the internet, there is no equivalent public space, instead they are only complex private spaces nested amongst one another. While offline, activists can protest a corporation by standing on the pavement next to their headquarters, online there is no equivalent. Creating a website that no one will visit is an entirely different prospect. As such, Zuckerman concludes that, despite being problematic, occupying a corporation's website is an effective way to reach the proper audience (2014). Additionally, Sauter argues that it is important to recognise that the disruptive power of hacktivist actions is one aspect that ties them closely to traditional theories of civil disobedience (2014). This is due to the fact that the focusing power of a public disruption is considered key to these political actions whether they take place online or on the street.

Furthermore, Li has set out three ways in which hacktivism can exhibit the characteristics of offline protests (2013). Firstly, hacktivists can claim similar motivations to protestors in that they are attempting to effect political or social change - usually in response to a specific event. Secondly, hacktivists plan campaigns based on what is likely to gain the most attention. Finally, and similarly to O’Malley, the cyberattacks undertaken by hacktivists exhibit similarities to sit-ins and picketing as they exploit the attention directed at the property of the target to gain attention. O’Malley also identifies key factors that are present in these forms of lawful protest (2013). Firstly, they are non-violent, which is something they have in common with hacktivism. Secondly, the purpose behind the lawful protest is important. Political and social protests have legitimate purposes, for example the anti-war protests and the civil rights movement in the 1960s in the US. Therefore, O’Malley states that hacktivism needs to have a legitimate purpose behind it for it to be considered on the same legal footing as offline protests (2013). Himma has put forward a series of defining features typically associated with traditional methods of civil disobedience. This boils down to the notion that civil disobedience can be defined as the “open, knowing, commission of some non-violent act, that violates the law, for expressive purpose of protesting the law (or the legal system) or calling attention to its injustice” (2006: 74). Therefore, if a hacktivist operation can meet these features it could be seen to be electronic civil disobedience and be justified. Samuel put forward the below matrix comparing traditional civil disobedience to electronic civil disobedience methods in order to show similarities between the two. This allows readers to locate hacktivism along a scale of forms of protest, both on and offline. Based on this then, hacktivism can either be directed at online property (such as DDoS attacks or website defacements) or it can develop independently of the target's property (such as website parodies or software development).

Table 4: Samuel's different activist repertoires (2004, 6-7)

	Offline	Online
Conventional	Activism: Voting Electioneering Non-violent protest marches Boycotts	Online Activism: Online voting Online campaign donations Online petitions
Transgressive	Civil Disobedience: Sit-ins Barricades Political Graffiti Wildcat strikes Underground presses Political theatre Sabotage	Hacktivism: Website defacements Website redirects Denial of service attacks Information theft Site parodies Virtual sabotage Software development
Violent	Terrorism: Political bombing Political hijacking Tree spiking	Cyberterrorism: Hacking air traffic control Hacking power grid *(note: to date these examples are all purely hypothetical)*

Delmas, on the other hand, has argued that hacktivism isn't civil disobedience (2018). Few hacktivist acts are able to satisfy the majority of criteria mentioned above. Taking Himma's framework, hacktivism can only fall under electronic civil disobedience if it does not cause damage to innocent third parties, if those taking part are willing and prepared to accept authority and if it is in pursuit of a plausible political agenda (2006). Using this framework then, Himma found that hacktivist methods can only be justified if used in order to protest human rights violations. Other hacktivist operations such as those undertaken for electronic freedom and privacy issues, then cannot fall under the framework for electronic civil disobedience. Delmas claims that issues such as these arise as theorists assume that the offline world is analogous to the online world (2018). Yet, many aspects of the offline world are missing online, for example, streets, public forums, democratic authority. Speech online is always mediated and regulated by internet service providers or content providers. Thus, in order to successfully protest online, one has to digitally trespass on private property which immediately raises the stakes for protestors online.

Therefore, instead of stretching the concept of civil disobedience beyond its common meaning to incorporate forms of hacktivism, it should fall under a different framework. Delmas has entitled this framework, that of electronic resistance (2013). This designates a broad range of dissident activities that express opposition to a dominant system of values. The five types of electronic resistance put forward by Delmas are vigilantism, whistleblowing, guerilla communication, electronic humanitarianism and electronic civil disobedience. These different types all culminate to what electronic resistance should be about "a public, geeks-and-grassroots mass movement advocating the free flow of science and culture, with a coherent political platform, and that constitutes the "avant-garde of the digital publics"'(Delmas 2013, 79). McLaurin argues that the rhetoric of civil disobedience is useful for those undertaking DDoS attacks as it provides an inherently legitimate framework to the activity regardless of its legality (2011). In fact, one hacktivist has claimed that the only difference between the civil rights protests of the 1960s and Denial of Service attacks is the change of setting, the fact that they take place in cyberspace instead of a physical location (Quoted in McLaurin 2011, 241).

McLaurin has claimed that DDoS attacks negate the potential for political dialogue about the issues that motivate hacktivists (2011). This is the result of the assumption that the opposition would be unwilling to negotiate and or to respond to the presence of the protestors by standing down. Newman claims that the fact that hacktivists often live outside of the country where a specific conflict that has caught their attention can create a sense of detachment or disconnect between their activities and the local grassroots movements that are protesting on the ground (2019). Yet, hacktivists will still claim credit for victories despite the fact that the progress was potentially the result of the local protesters. Van Riper has claimed that due to the decentralised nature of hacktivist collectives, they lack the efficiency of other forms of protest (2019). He goes on to suggest that hacktivists would need to shift back to the group mentality they had during operations such as #OpPayPal.

4.1.1. Issues with Anonymity:

The main issue scholars have with hacktivism is due to it Anonymity. Hacktivists tend to be ‘stateless, elusive, sometimes lawless and almost always anonymous’ (Sorell 2015, 392). They are additionally unaccountable in states that protect freedom of speech rights and the right to privacy, or as Sorell describes them, human rights-respecting jurisdictions (2015). Due to this anonymity, hacktivists can be less inhibited in expressing hateful or abusive ideas as opposed to those who express them publicly and as such have to defend them (Sorell 2015). Many internet researchers (Kizza 2010; Aas 2007; Lessig 2006) have argued that ever since the early days of the internet, anonymity has been the norm which has led to the early internet pioneers embracing of concepts such as privacy, freedom of speech and creativity and thus it could be seen to be worth preserving. The anonymity displayed by hacktivist collective Anonymous originated on 4chan whereby anonymity was a norm for all users. It was mainly used as a feature of equality and the lack of focus on an individual’s identity. This anonymity has even moved from being simply online to offline protests organised by the collective such as the Million Mask Marches whereby protestors are encouraged to wear masks to hide their identity (Karagiannopoulos 2018).

Hacktivists have been criticised for this anonymity, this is due to the fact that traditional civil disobedience scholars see the acceptance of punishment as part of their protest. Storing claims that this is indicative of a protesters altruism and their respect for democracy and the state as well as the citizens who were affected by their law-breaking (2002). Greenawalt adds to this by stating that by eschewing anonymity protestors distinguish themselves from those engaged in covert criminal acts, confirming the morality of the protestors (1989). Thus, hacktivists could be criticised for not revealing their identities and as such a comparison could be drawn to criminal hackers with more nefarious intentions. Yet, Arendt posits that those engaged in civil disobedience will accept any punishment as that would seem as if they aren’t defending their case and thus nullifying their defendant rights (1972). Furthermore, it is well known that Gandhi stated that though he believed that accepting punishment is linked to the moral motives of the protestors, he found it unlikely that the state would accept any legitimacy of the protesters' cause.

Due to the illegality of hacktivism protestors have faced high penalties for their actions. Karagiannopoulos claims that these penalties are much higher than protestors acting offline would face for similar actions (2018). For example, vandalism or trespassing offline will usually lead to a misdemeanour charge whereas hacktivists would face felony charges. Coleman furthers this argument by using the example of Eric J Rosol who was given a two-year probation and a fine of $183,000 for engaging in a virtual sit-in organised by hacktivist collective Anonymous for 1 minute (2014). While someone charged with arson would face a substantially lower fine. Therefore, Karagiannopoulos argues that perhaps hacktivists choose to remain anonymous as they are aware of the very high penalties compared to the seriousness of their actions 2018).

However, O'Malley argues that the protester must be ready and willing to accept the consequences of their action, argue their case and potentially change the law if they win (2013). This, O'Malley claims is the moral footing for the maintenance of peaceful protest and is where hacktivism is at its most different to offline forms of protest (2013). Up until now, hacktivist collectives such as Anonymous could have satisfied all of the factors in order to be considered to be within the law. However, they are unwilling to accept personal responsibility for their actions and as a result would not be able to fulfil any of the above criteria. Oxblood Ruffian, a founding member of a hacktivist collective has claimed, however, that DDoS attacks being the online equivalent of a lunch counter sit in is an offensive thought. This is due to the fact 'implicit in the notion of civil disobedience is a willful violation of the law; deliberate arrest; and having one's day in court' (quoted in Sauter 2014: 5). This corresponds to Thoreau's original conception of civil disobedience whereby the spectacle of public disobedience is not complete without punitive reaction from the government. For Thoreau, including the state as a player in his act of civil disobedience would reveal that they are unjust. Similarly, Martin Luther King Jr stated that "one who breaks an unjust law must do so openly, lovingly and with a willingness to accept the penalty" (1963).

Contrarily, due to the harsher sentencing of hacktivists, Karagiannopoulos claims that they should not necessarily accept the punishment they are given (2018). Instead of accepting punishment, it could be argued that they accept the risk of prosecution instead of punishment. This would allow the protestor to defend their case properly and publicise the morality of their cause while allowing them to remain politically active. Thus, Karagiannopoulos suggests that the concept of acceptance should not simply be accepting a specific punishment handed down by the legislature but rather acceptance of the prospect of being faced with sanctions as a result of their protests, their need to defend themselves and the justness of the cause (2018). If this were the case, the onus would be on the state to convince the court that it has good reasons to punish the hacktivists who believe in something so much that they would risk convictions for them.

McLaurin has argued that DDoS attacks cannot be linked to traditions of civil disobedience due to the fact that hacktivists are participating in a “shallow gesture” (2011, 245). Hacktivists are hidden behind computers and the anonymity that they enjoy de-personalises their messages, requires little commitment and as a result shows a lot less conviction than a traditional act of civil disobedience whereby the protester takes responsibility and potentially faces criminal punishment. McLaurin claims that while hacktivists may feel as strongly about issues as traditional protestors, the community receiving their messages will not be able to measure their conviction other than reading what they post online and measuring how long servers are taken down.

4.1.2. Hacktivism as Too Easy

Furthering this idea is the critique that hacktivism is ‘the ideal type of activism for a lazy generation’ (Morozov 2009). Yet, Sauter claims that this slacktivism critique makes assumptions about the purposes of activism (2014). According to those who posit the slacktivist critique, the only worthwhile form of activism is that that is performed on the streets, where the activist is in physical and legal danger. Here, Sauter argues, this activism is *hard* and only a few people are able to do this (2014). If the activist is not placing themselves in peril, it is not *real* activism. But comparing young activists to those that took part in the exceptional movements of the past is reductive. This critique fails to consider that activism can have many diverging goals beyond directly trying to influence those in power. Sauter states that ‘it explicitly denies that impact on individuals and personal performative identification can be valid outcomes’ (2014: 6). It places the same lens on practices that have been used in civil disobedience for centuries as it does on a newer sphere of activism. It further sees the ease with which people can engage in these newer forms of activism as a failure. Sautner claims that as the cost of entry level activism decreases, more and more people will engage (2014). Some of these people will continue to stay involved while others will not but there must be a bottom run on the step, slacktivism could serve as this bottom step.

Karagiannopoulos argues further, stating that hacktivism could be preferable to offline protests as traditional protest methods run the risk of physical harm (2018). Physical injury would adversely impact a protest and could undermine the expressive nature of the protest. As a form of non-violent protest, hacktivism with its relatively low intensity disruptions could be used as a release valve for social tensions. These would indicate the sources of disaffection before the public can become radicalised and engage in violent outbursts. For example, a virtual sit-in could be used in order to attract attention to a cause and initiate a dialogue.

4.1.3. Hacktivism and Freedom of Expression

Klang, on the other hand, argues that new, online forms of disobedience do not conflict with the traditional theories (2004). This is because politically motivated online disobedience is actively taking part in political discourse. As a result, they are using their freedom of expression. Yet Karagiannopoulos posits that an argument against the disruptive practices employed by hacktivists is that contemporary democracies have opened up new possibilities for expression, these possibilities are particularly apparent online, with blogs and social networks enabling anyone to share their political opinions (2018). As such, dissent could be expressed without impinging on the freedom of expression on those that are being protested against. Websites contain messages that can be used to express opinions, disabling these websites could therefore infringe on the rights of those behind the targeted websites. Yet, using social networks or blogs to express an opinion means that only a small circle of peers will be exposed to them. Furthermore, relying on websites such as Facebook, means that should your messages transgress their rules of conduct, they will have the right to take down the content. As a result, minority political views could be marginalised as they are unable to reach the same audiences as popular information channels.

Governments or large corporations are most often the targets of hacktivist actions and tend to have access to large audiences through popular mainstream communication channels. This easy access to larger audiences could facilitate the influence on democratic processes and disproportionately affect political discourses and consequently steering public opinion in their favour. Samuel, therefore, posits that hacktivist tactics can intervene on the proper functioning of speech and expression (2004). Yet, they can also broaden the scope of speech and debate by offering the chance to speak in the same place as those that they target, therefore gaining similar numbers and audiences. As such, Karagiannopoulos claims that we need to evaluate each particular context with regards to the opportunities being given to each side of the conflict and the impact of the actions on the speech opportunities of the protest's target (2018). O'Malley argues that the necessity of expression rather than the conduct is a key factor. The main reason for a legitimate purpose is to communicate a clear message backed by a legitimate aim. This O'Malley argues would mean that DDoS attacks or website sabotage could too be considered a lawful protest as unauthorised access or hacking should not be considered impermissible due to the conduct that occurs while they are being undertaken (2013).

However, Solomon has argued that as hacktivism infringes on the rights of others, the argument for it as a means of defending human rights is undermined (2017: 725). The unauthorised intrusions on private networks and computers that form part of hacktivist operations amount to trespassing on their digital property which equates to trespassing on physical property. This can also include through the use of controlled slave computers involved in DDoS attacks. Solomon also argues that hacktivism tends to be censorial and as a result opposed to freedom of expression (2017: 728). This is due to the fact that the threat of a potential cyberattack silences many who would speak out against any of the causes that are adopted by hacktivists. Armstrong, however, has argued that censorship is too strong a term for hacktivist activities claiming that it is "more comparable to graffiti than book burning" (2012: Online). Additionally, McLaurin argues that while not rising to the level of physical violence, DDoS attacks could be seen to threaten the economic and social liberties of others which would disqualify it from belonging to the tradition of civil disobedience (2017). This is due to the fact that traditional protestors rely on the strength of their arguments and ensure that they identify with a greater audience in order to gather support, yet DDoS attacks drown out any persuasiveness of their arguments. Furthermore, victims of the collateral damage caused by DDoS attacks would be unlikely to search for any meaningful purpose behind their losses.

4.1.4. Hacktivism as Vigilantism:

It has been argued, however, that hacktivism brings together people who protest against matters of which legal remedies are not possible due to jurisdictional or financial reach. For example, Operation PayPal whereby Anonymous took down Visa and PayPal after they froze donations to Wikileaks. This had serious free speech complications globally yet very few people would have had the ability to have challenged this decision in court. Furthermore, by the time the court had decided Wikileaks would probably have had to have been taken down due to financial issues (Fitzpatrick 2012). This protest led to a reversal of the decision to block payments to Wikileaks. Furthermore, Karagiannopoulos argues that as hacktivism tends to be eye-catching it will often lead to a public discussion bringing an issue to the fore (2018).

Contrarily, individuals should make certain not to condone all forms of vigilantism. An important aspect to remember, however, is that with such skill and power, they are liable to make mistakes . The form of vigilante justice that hacktivists have demonstrated can make it harder for law enforcement. However, Shaw has argued that hacktivists have made mistakes by doxing the wrong person (2012). Sorell states that Anonymous are therefore guilty of a serious injustice and that this sort of exposure is unjustifiable (2015). Gross claims that Anonymous have also made it harder for law enforcement due to the fact that they might disagree with a specific investigation (2012). For example, they were involved in DDoS attacks on the Swedish Prosecutor's office as well as other Swedish organisations that were involved in the prosecution of Wikileaks founder, Julian Assange after he was alleged to have sexually assaulted numerous women. This is despite the fact that there is no record of Swedish criminal prosecutions being unjust. However, hacktivists do need to carefully consider their protests and the methods they use so as to not be seen as vigilantes. Thus, they should evaluate whether a legal method is possible, accessible and efficient and whether or not legal recourse has already been brought before engaging in an illegal method. It could be argued that the rhetoric Anonymous employs at the moment is not helpful with regards to portraying a measured approach to the public. For example, their constant declarations of war against anybody they disagree with does not portray a coherent organisation with consistent beliefs.

Milone has also argued that hacktivism could be seen as a public good in that it can aid in the defence of the National Infrastructure as it tests systems and identifies weaknesses (2003). Yet legislation as it stands, particularly in Western states, aims to secure National Infrastructures by increasing surveillance and increasing the prosecution of computer related crimes. Yet, by discouraging hacktivists and other hackers, potential flaws may not be identified. Indeed, a more preferable solution could be to "foster a sense of civic duty among groups of ethical hackers, revise existing laws to facilitate cooperation between hacktivists and law enforcement, and develop innovative programs that encourage responsible hacktivism and fuel hacktivists' innate love of a good challenge." (2003: 413).

5. Hacktivism as an Entity

While it is clear that hacktivism could be be seen to be a tactic, specifically electronic civil disobedience and indeed originated as a tactic, it appears to have moved beyond that with many members of hacktivist communities no longer possessing the skills to undertake the more traditional hacktivist activities such as DDoS attacks and web defacements. In 2020 a European organiser with Anonymous told Rosenblatt that while Anonymous is still made up of different groups with differing ideologies, this new brand of Anonymous is missing technical abilities: "I have not seen anything indicating real hacking. If it happens, they are smart enough to not do it publicly, [...] "Currently the theme is to disrupt communication of the right wing scene, take over their hashtags, make social media unusable for them. You don't need hacking for that"[27] (2020). Indeed, K-Pop fans have flooded rightwing hashtags and supported the Black Lives Matter protests in conjunction with Anonymous protests (2020)[28]. Therefore, it's clear that while hacktivism may have originated as a tactic it has now moved beyond that with many considering themselves to be a hacktivist without the skills needed. Defining hacktivism as purely a tactic may no longer be suitable in the current era.

The State appears to define hacktivism as an entity. The UK 2016-2021 National Cyber Security Strategy refers to hacktivists as decentralised and issue oriented individuals or groups stating that, “They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims.” (2016: 19). The National Cyber Security Centre also describe hacktivists as a term used to describe hackers motivated by a specific cause, for example to further political or personal agendas or in reaction to events or actions they perceive as unjust." The 2015 National Risk Register for Civil Emergencies refers to hacktivism as “The threat to the UK from politically motivated activist groups operating in cyberspace is real. Attacks orchestrated by hacktivists on public and private sector websites and online services

[27] https://www.darkreading.com/theedge/whats-anonymous-up-to-now/b/d-id/1338112 Last Accessed 21 Nov 2020

[28] https://www.forbes.com/sites/paulfroberts/2020/06/24/are-k-pop-fans-the-new-anonymous-dont-count-on-it/#3eccf18542f2 Last Accessed 21 Nov 2020

are becoming more common and aim to cause disruption and reputational and financial damage to gain publicity."

Additionally, hacktivists have a distinct culture which is based around theatricality and irreverence with a reliance on memes and internet culture. Indeed Samuels claims that they put a premium on humour with many of their activities using humour to make their point. Moreover, they will also endeavour to draw attention to their activities, either by contacting the media or by submitting a defacement to a defacement "mirror" so that it can be preserved for posterity. Wong and Brown find that hacktivism has been represented as a form of e-banditry whereby they represent "Robin Hood, resisting the power that [...] threaten the desire to keep the Internet free [...] and capitalise on the Internet and other information technologies to lead disembodied, virtual attacks against physical targets in order to encourage political change"(2013: 1015). Karagiannopoulos argues that hacktivism as a philosophy and reconfiguration of political practice is a vital part of the culture that arose as a result of cyberspace whereby anti-globalisations dissent occurs and civil liberties and democratic values are protected (2020: 78-79). As such, hacktivism is an entity with a shared culture and at times shared ideology that gather together to protest injustices.

5.1. Hacktivism as a social movement?

The phenomenon of hacktivism as a social movement has clearly reflected a shift in technology facilitated politics as a movement. The concept of hacktivism as a social movement can be found in detail in the previous chapter, however it is clear that if hacktivism as an entity would fall under the concept of social movement entity. Several authors have demonstrated that social movements, being networks of diverse groups and activists, are interested in using the Internet because of its fluid, non-hierarchical structure, which is linked to their ideological and organisational needs (Klein 2001; Bennett 2003; van de Donk, Loader, Nixon and Rucht 2004b; Van Laer and Van Aelst 2013). Moreover, the internet offers a space for democratised participation; increased access to protest spaces and easier ways to protest. Indeed, Barberá saw the internet as a means of entry to those who would have been on the periphery of offline protest actions.

As detailed in Section 2, hacktivism is thought to have originated as a result of the anti-globalisation movement and has extended beyond that into its own movement. One that has been characterised as characterised as “heroes and hustlers, freedom fighters and cyber lynch mobs, political activists and anarchists” (Klein 2015:379). Many scholars agree that a social movement needs to have an identity that makes them unique and identifiable and their goals should be explicit (McCarthy & Zald, 1973; Snow, Soule, & Kriesi, 2004; Tilly & Wood, 2015). Romagna has claimed that the hacking element, present in the majority of hacktivist activities has led to the shaping of an ideology, the development of a certain set of values and a mental approach embedded in the hacker mentality (2019: 747). Alongside this shared ideology, as detailed in the previous chapter, hacktivism does not have an identifiable centre; those that identify as hacktivists have an awareness of global political issues; they are triggered into life by specific events; they engage in self-reflection; and rely on interactive networks of communication. Samuel also makes the case that hacktivism is a social movement in that hacktivists share a common discourse, reside outside of institutionalised politics and have found a way to respond that is similar to offline forms of collective action (2001:8). Alexopoulou and Pavli claim that hacktivism is motivated by political views to perform activism in the virtual world (2021: 240). Indeed, both hacktivism has been associated with the expression of political thought, free speech and human rights (Romagna 2019: 746). Moreover, Klein has described hacktivism as a counterhegemonic movement that challenges dominant systems, including mass media (2015: 399). In hacktivist’s rejection of traditional media instruments, it is indicating how it views the media to be a part of the system it opposes. Hacktivism has adapted over 30 years, from its creation to the present, to reflect the evolution of society and technology as many other social movements that have come before it, such as feminism, have done. Further theoretical analysis on the idea of hacktivism as a social movement can be found in the previous chapter (Chapter 2). Empirical analysis on hacktivism as both cybercrime and social movement will be presented later in this Dissertation (Chapters 5 and 6).

6. So What is Hacktivism?

It is clear from the above and the previous chapter that there is a lack of consistency with regards to whether hacktivism is either a tactic or an entity. Indeed, there is a clear gap in the literature on this topic. This thesis considers hacktivism to be both a tactic and an entity. This is due to the fact that the tactic of hacking has shaped the ideology and the dynamics behind hacktivism itself. This, then provides a set of values and a specific mental approach that is embedded in the hacktivist mentality (Romagna 2019: 5). Indeed, Romagna, identified three key elements that can be found in existing studies on hacktivism: first, there is the need of supporting an ideology or cause that has its bases in socio political struggles; secondly, the Internet has been identified as a necessary infrastructure that allows the activity and as target of an attack (Milan 2015); and finally, the desire for any group or single individual to promote a sociopolitical agenda that should either lead to a change in society or to keep the status quo. As a result this Dissertation will use the following definition which combines the notion of hacktivism as being both a tactic and an entity: "*The promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure's technical features, without the use of physical violence and without gaining direct economic benefits.*" (Romagna 2019: 5). This definition is used as it identifies that hacktivism can be a technique and an ideology while acknowledging that it can form collective actions based upon a shared agenda.

The debates surrounding hacktivism are far from being resolved. As a result, it makes identifying what hacktivism is difficult. This could be the result of a lack of research that directly contacts hacktivists themselves. Due to the reclusive nature of hacktivists and their willingness to work with researchers, scholars will rely on manifestos, websites or media articles on hacktivists themselves which Samuel claims can paint an overly dramatic picture of hacktivists themselves and their agendas (2004: 29). Taylor has claimed that hacktivism engages with a new form of metapolitics "directly and, with its close ties to the politics of globalisation, marks the beginning of a significant new chapter in radical technological politics" (2005: 4). Furthermore, Ranario suggests that "as global politics continue to endure a turbulent and complex time in history, an awareness of hacktivism will continue expanding and evolving." (2008: 2). Haywood claims that if hacktivism is not purely a technological act then using the lens of the hacker ethic could present a useful notion in understanding how hacking has moved beyond the realm of computing (2018). This approach would demonstrate how hacktivism is both an entity and a tactic with a view of it not only being a form of activism and a social movement but also being a culture as well. This interprets hacking as the construct and performance of a set of ethics that moves beyond technology towards wider society. Steven Levy, one of the earliest writers looking at the hacker ethic, claimed that "to qualify as a hack, the feat must be imbued with innovation, style, and technical virtuosity" (1984: 23). Levy then goes on to summarise hacker ethics as: Sharing; Openness; Decentralisation; Free access to computers; and World improvement. The predominant ethical principles of hacking silently agreed upon by early hackers put forward by Levy are:

- Access to computers - and anything which might teach you something about the way the world really works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust authority - promote decentralisation.
- Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.[29]

These ethical principles are followed by the hacktivist collective, the Chaos Computer Club, who went on to add two further principles in the 1980's: 1. Don't litter other people's data and 2. Make public data available, protect private data. Himanen has claimed that hackers are defined by qualities such as playfulness, caring, exploration, passion, enthusiasm (2001:2009). In his view, Himanen argues that there is less of a division between work and leisure, instead hackers are motivated by the happiness and joy of their work which isn't found in many other professions. These principles are used as guidelines and a basis for discussion by hackers. As a result, in this Dissertation these principles will be used as a basis for a criteria when studying hacktivists in order to draw a line under what is hacktivism and what is cybercrime or cyberterrorism.

7. Conclusion

Hacktivism is obviously contentious, this can be seen in the different approaches used to define the phenomenon with some describing it as cybercrime, others as cyberterrorism, some as civil disobedience and others as a social movement. A consequence of these conflicting opinions results in a certain amount of difficulty in establishing what hacktivism is. This chapter has detailed that hacktivism is both electronic civil disobedience, despite the arguments against it, and a social movement. Due to the difficulties that arise as a result of the conflicting definitions, Levy's hacker ethic will be used to provide content to the concept of hacktivism. While a lot has

[29] https://www.ccc.de/en/hackerethics Last Accessed 21 Jan 2021

been written on hacktivism as electronic civil disobedience, very little work has been done on hacktivism as a social movement. Hacktivism arose as a result of other movements, uses methods that have clear offline parallels and despite the anonymity, ease of protest and vigilante quality of hacktivists, it is clear that its motivations and targets are similar to those of other social movements. As a result theoretically hacktivism could be seen to be a social movement. This suggestion will be empirically tested through the use of a rhetoric analysis and through a statistical analysis comparing hacktivism to traditional movements and cybercrime. The following chapter will detail the methods and data collection methods that this dissertation will use to empirically answer the research question: *'Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?'*

Chapter 4: Methods

1. Introduction

Following on from the theoretical section of the Dissertation, this chapter outlines the various research methods to be used in order to test the hypothesis that hacktivism is a social movement and as such should be given the same protections as offline protest movements. This chapter will detail the chosen methods as well as justify their use in this project. It will describe the types of research conducted, the data collected, the level of analysis of the data as well as the limitations and ethical considerations taken into account when undertaking the research. This chapter will set out why these data collection methods are the most appropriate methods to be used to answer the research question. Firstly, the overall research strategy will be detailed as well as a justification for the multi-method approach utilised in the research (2). The two data collection methods will then be presented. The first method to be detailed is a rhetorical analysis of known hacktivist Twitter accounts (3.1). The approach used in order to facilitate a comparison between hacktivism and social movements is Stewart's approach to the analysis of the functional rhetoric used by social movements, this will be outlined in section 3.1.1. (1980). The specific texts that will form the basis of this analysis will then be detailed (3.1.2) before the way in which these texts will be coded and analysed is explained (3.1.3). The second data collection method will then be delineated with a clarification of the statistics used in the thesis which will be used in order to establish whether hacktivism has more in common with social movements or cybercrime (3.2). The different datasets that will be used for this purpose are each explained detailing the nature of the dataset, why they have each been used and what the dataset can demonstrate (3.2.1). Finally the limitations and ethical considerations that must be taken into consideration will be assessed (4) including the potential for researcher bias, the generalisability of the study, the impact of the COVID-19 pandemic on the Dissertation and any ethical issues that may arise when using publicly available data. The methodology chapter will then be concluded (5) with an overall examination of the key sections and how this is applied in the research.

2. Research Strategy

The concept of a research strategy has been defined as “the general plan of how the researcher will go about answering the research questions” (Saunders et al 2009: 600) as well as “a general orientation to the conduct of research” (Bryman 2008: 698). The research strategy lays out the general direction of the research which includes the way in which the research is conducted. Saunders et al. have outlined how a research strategy should be selected in relation to the research questions, the objectives of the research, the extent of the previous knowledge on the specific subject area and finally the amount of time and costs available to the researcher (2009). Alternatively, Yin suggests that a research strategy should be based on the following three conditions (2003). Firstly, the type of research question. Secondly, the extent of control the researcher has on behavioural events and, finally, the degree of focus on specific events. Wedawatta et al. claim that when deciding on a research strategy, the most advantageous strategy to the specific piece of research should be the most important consideration (2011: 3). As such, the research strategy for this Dissertation was established based on how the research questions can be answered. Thus, the main aims of this Dissertation are focused around the idea of understanding more about hacktivism in order to establish whether it has similarities to historical social movements and as such be regulated in a similar manner.

Furthermore, a mix of both quantitative and qualitative methods will be used. This multi-method approach will allow for both an objective and subjective perspective when answering the research question. Many scholars recommend the use of multiple methods to study complex social phenomena of which hacktivism can certainly be identified as such (Brewer and Hunter 1989; Newman and Benz 1998; Creswell 2003). One of the reasons a multi-method approach was selected in order to answer the research question is due to the fact that it assists in obtaining a broader response to research questions and expands the robustness of the researchers' understanding (Mingers 2001). Additionally, multi-method approaches have the advantage of increasing knowledge on different aspects of the phenomenon being studied which allows for a better, more detailed explanation. These different methods focus on the different aspects of the research question which allow for a deeper understanding of the research topic (Mingers 2001: 241). The understanding can also be more meaningful by including the analytical power of both quantitative and qualitative research methods. As a result, a combination of descriptive statistics as well as a qualitative analysis of the rhetoric used by known hacktivists will be undertaken. These two methods will now be outlined in more detail.

3. Methods used in this Dissertation

3.1 - Rhetoric analysis

Willihnganz claims that a rhetorical analysis is an investigation into how a text persuades the reader. It is concerned with the way in which a text communicates, the strategies it uses to connect to an audience, how issues are framed and the ways in which it makes, supports and persuades an audience to accept a claim (2008). Leach defines rhetoric “as both the production of persuasive communication and the analysis of persuasive communication” (2011: 226). She states that it is a dialectical process between audience and representation. Corbett argues that classical rhetoricians discuss three means of persuasion: the rational, the emotional and the ethical (1974). Meanwhile, Gregg claims that the rhetorical transaction is specifically focused on a situation whereby a speaker produces a message for the purpose of affecting the beliefs and behaviours of a listener or group of listeners (1971). A successful rhetorical transaction, therefore, would be one whereby the speaker has manoeuvred the listener to agree with the claims proposed by the speaker. Kenneth Burke, defines rhetoric as "the use of language as a symbolic means of inducing cooperation in beings that by nature respond to symbols" (1950: 173). Central to his thesis is the concept of identification, whereby common interests are recognised among humans. He stated that "Wherever there is persuasion, there is rhetoric. And wherever there is 'meaning,' there is 'persuasion" (1950: 172). Burke viewed all symbolic behaviour as strategic action that is directed at defining situations but rhetoric is inherently used in order to induce cooperation. He also claimed that rhetoric preserves or changes the social order by influencing the way in which people perceive their symbolic relations.

Jensen argues that since the 1940s communication scholars have studied the rhetoric of social movements (2006). Griffin , a pioneer of social movement rhetoric, used historical events to explain the key moments that led up to movements and the stages through which these evolved (1952). In the 1960s, it was found that a lot of the rhetoric used by protestors was not rational, instead it included marches, music, chants and other non-verbal communication (Jensen, 2006). Rhetorical critics now see the “object domain” of social movement studies “as immensely rich and complex and almost coextensive with ‘discourse’ and ‘discursivity’ that calls for a flexible critical practice” (Gaonkar 2002: 411). Stewart defines rhetoric as “the process by which a social movement seeks through the manipulation of verbal and nonverbal symbols to affect the perceptions of target audiences and thus to bring about changes in their ways of thinking, feeling, and/or acting.” (1980: 301). Stewart also claims rhetoric is “the primary agency through which social movements perform necessary functions that enable them to come into existence, to meet opposition, and perhaps, to succeed in bringing about (or resisting) change” (1980: 301). The approach taken in this rhetorical analysis will be a functional approach whereby rhetoric is viewed as an agency through which social movements perform specific functions. Simons claims that movements should fulfil the same functional requirements as more formal and systemic collectivities (1970). He focuses predominantly on the leadership of these organisations claiming that they must attract, maintain and mould workers into an organised collective, they must secure adoption of their views to a wider audience and they must be prepared for resistance generated by it. Gronbeck, claimed that "Rhetorical forces function as a set of skills able to create, sustain, and terminate movements by uniting the other forces" (1973: 153). Therefore, the rhetorical analyst should pose three questions: What functions are fulfilled by rhetorical discourse?; With what substances are these then fulfilled?; And, in what form then does this substance appear? (1975: 4-7).

3.1.1 Functional Approach to Rhetoric

The approach taken in this Dissertation is based upon the above ideas. Stewart delineated specific functions of rhetoric to be used when studying the rhetoric employed by social movements (1980). These are not developed chronologically as “social movements are expansive collectivities that may contain many campaigns and a variety of organisations” (Stewart 1980: 154). This list of functions is what will be utilised in order to identify whether the communications distributed by hacktivists are similar to those published by social movements. The first function identified by Stewart and used in this study involves transforming perceptions of history. This can be broken down into altering perceptions of the past, the present and the future. He claims that audiences are not necessarily aware of problems or refuse to admit a problem exists. These beliefs are reinforced by established orders such as the government and schools. Therefore, if hacktivism is a social movement it must change the ways in which audiences perceive their chosen issues in order to persuade audiences that the issue warrants action. This function is always in flux as social movements may need to revise their versions of history and where they place within it.

The second function that will be used when analysing the tweets is focused on how movements attempt to transform perceptions of society. This can be reduced to how movements will attempt to alter perceptions of the self and as well as the opposition. The main rhetorical task of this function involves stripping the opposition of its authority and legitimacy. Movements can do this either by portraying the opposition as a powerful, demonic conspiratorial force or by contrarily portraying it as weak, disorganised and powerless. Social movements must also attempt to change the way in which the audience sees themselves. In doing so, if hacktivists form a social movement they will need to instil a sense of pride and power in their audiences ensuring they question society and help to bring about change.

The third function identified by Stewart that this Dissertation will aim to identify in the hacktivist Tweets centres around prescribing courses of action. This involves prescribing what must be done, who should do it and how it should be done to both the movement and audiences. The movement should state a list of demands and solutions that will improve a condition or prevent undesired changes. Every movement should explain, defend and prescribe its own methods for change. Furthermore social movements should prescribe who they believe is up to the task. This is to increase legitimacy by claiming that only an un-institutionalised collective is able to effect change. Social movements must identify which strategies and communication channels are the most effective as well as justifying their means. This is due to the fact that, on occasion, the tactics that are used could negatively affect everyday people and cause a backlash. Therefore, their actions must be defended to both members and outsiders.

The fourth function put forward by Stewart is based upon the idea of a movement mobilising for action which focuses on organising discontent, gaining sympathy and pressuring the opposition. These actions can be change oriented while other actions can involve gaining control of agencies of influence. Additionally some actions can seek to gain sympathy and attention or to apply pressure on the movement's opponents to gain recognition from its antagonists. However, no matter how a social movement will attempt to effect change, it is a long process that can require years of effort by numerous members. Movements must convince people that victory will happen if members commit themselves to change and maintain unity, this is what Hoffer describes as “extravagant hope” (1952).

The fifth function to be identified in the tweets analysed is that hacktivists must attempt to sustain the movement due to the longevity of these protest movements. In doing so social movements must justify setbacks, ensure the movement remains viable and maintain visibility.

Movement organisations will often be working for a number of years and regularly are affected by changing circumstances. Therefore, they have to defend setbacks and explain their gains. The audiences may perceive victories differently and opponents capitalise on delays to proclaim superiority over a movement. Thus, Stewart claims that “social movements must wage a continual battle to remain viable” and that as a result more rhetorical energy may be expended on keeping the movements profile visible than on selling ideologies (157).

However, when analysing these tweets several caveats must be considered. Firstly, social movements are considered to be organised and expansive collectivities that protest and mobilise in order to bring about change predominantly through rhetoric. Stewart claims that rhetoric is the primary agency through which social movements are able to satisfy the functions outlined above. Additionally, while social movements must perform these functions, some will be more successful than others. The aims of the social movement will affect this as revivialist social movements may seek to limit or replace norms and power distributions. The final caveat is that these functions are not chronological or linked to progressive steps. Social movements encompass many different campaigns and a variety of collectivities. Social movements are unlikely to perform a function only once and then proceed to the next step. Some functions may also dominate the energy and rhetoric of a movement at any time while still demanding attention.

3.1.2 Texts to be analysed

Now that the way in which the rhetoric to be studied and examined has been outlined, the types of texts to be analysed will now be discussed. Followed by the specific methods and coding and analysis techniques to be employed. Milliken states that a discourse analysis needs to be undertaken over multiple texts as a single source “cannot be claimed to support empirical arguments about discourse as a social background” (Milliken 1999: 233). Marsh and White claim that the most important consideration with regards to the date being used is that it provides enough useful evidence for answering the main research questions (2006). The data must also communicate some form of message from a sender to a receiver. Marsh and White state that the text should convey a coherent linguistic message that has meaning which should relate to the writers’ attitude or purpose. Those who receive the text should understand it and expect for it to be relevant and inform them of something new. Where the text was created will impact how it was produced and where it is appropriate and is related to similar texts within a genre, such as tweets.

Due to the nature of hacktivists, their methods and the ways in which they communicate with the outside world, the texts to be studied will all be taken from the internet. Wellman has claimed that the internet ‘has become embedded in the daily lives of much of the developed world'; it 'decreases', 'transforms' and 'supplements' community, and its proliferation 'is facilitating social changes that have been developing for decades in the ways that people contact, interact, and obtain resources from each other’(2003)[30]. Mautner claims that the internet can provide both opportunities and challenges when engaging in discourse analysis (2005). This is predominantly due to the size of the web and the ease of accessibility. She claims that a specific criteria of what needs to be included in the study needs to be developed and applied to the project. This can include the author of the publication, the time in which it was published, where it was published and the cultural and national origin. As a result, the Tweets to be analysed will originate from specific hacktivist operations that were identified in the datasets detailed below. The selected operations will be those that were found to last for 2 years or more and that have a Twitter account associated with it. The Twitter accounts that meet this criteria and were analysed are as follows: @MMMLondon; @OpRussia; @OpFreePalestine; @OpGreenRights; @OpIsrael; @OpKillingBay; @OpLastResort; @OpSyria; @OpLiberation. For each account a maximum of 350 tweets are analysed. Additionally, more general Twitter accounts associated with Anonymous with at least 50,000 followers will be analysed to provide a more general picture of hacktivism as a whole: @YourAnonOne; @YourAnonNews; @TheAnonMovement; @AnonOps; @YourAnonCentral. For each of these general Anonymous accounts a maximum of 500 tweets were analysed. Three Twitter accounts not linked to Anonymous have also been analysed in order to provide an alternative perspective on hacktivism as well as to provide an examination of other contemporary forms of hacktivism : @ChaosComputerClub; @BelarussianCyberPartisans; and @GhostSquadHackers. The large number of followers that these Twitter accounts have offsets the difficulty Mautner describes whereby the internet can make it hard to identify who is behind internet communications (2005). In total 3,640 tweets were analysed using Stewart’s functional approach to the rhetoric used by social movements (1980).

Moreover the ephemeral nature of the internet results in texts remaining in flux resulting in changes or the removal to the chosen analytical texts. This results in attempts to make a

[30] https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2003.tb00216.x Last Accessed 13 April 2021

dynamic website into a static document that can be relied upon for the rest of the research period. Consequently, in this Dissertation, the tweets were downloaded in the form of a Microsoft Excel file through the Google Chrome Browser plugin ‘Twlets’ that can download tweets from public facing Twitter accounts. The Twitter accounts were visited and the tweets were downloaded into an excel file and stored on an external hard drive. This resulted in a static document from which the tweets could be coded from. This document was then uploaded to the coding software.

3.1.3. Coding and Analysing.

The approach to coding the data followed multiple steps suggested by Marsh and White (2006). Firstly, the research questions guided the initial approach to the data in order to establish the big picture. Gill claims that when coding, the researcher should “start as inclusively as possible so that all borderline instances can be counted in rather than out.” (Gill 2000, 180). Secondly, key phrases and text segments were identified while interesting points were noted. The categories and constructs are compared while keeping in mind the functions outlined by Stewart (1989). In order to keep track of the developing concepts and how they relate to social movements two types of memos were used: concept memos and theory memos. Concept memos focused on emerging concepts while theory concepts were used when the concepts emerge into a workable model. The software used to code the selected tweets in this Dissertation was MAXQDA which is a software package for qualitative data analysis and mixed methods research. This software is used to code the tweets utilising Stewart’s functional approach to the rhetoric used by social movements (1980). The tweets are firstly examined in general in order to determine their suitability for this Dissertation. The functional approach to rhetoric was then used to code and categorise the texts with those tweets containing any of the five functions being highlighted with different colours. Additional categories were also be identified as being pertinent to this Dissertation, for example a category that identifies specific tweets of interest despite potentially not containing any of these five functions: ‘Transforming perceptions of history’; ‘Transforming perceptions of society’; ‘Prescribing courses of action’; ‘Mobilising for action’; and finally ‘Sustaining the movement’.

Lincoln and Guba’s four criteria for assessing the truth value of the study will be applied in this Dissertation to ensure the research is reliable. These include credibility, transferability, dependability and confirmability (1981: 146). Credibility calls for identifying the key factors in the research question and describing the ways in which they are reflected within the data. Transferability boils down to a judgement call about how one can apply the findings from one context to another, predominantly a similar theoretical paradigm. Triangulation is used in order to heighten credibility and confirmability, this is when the researcher collects, analyses and cross-checks a variety of data on a specific aspect of a research question from a variety of sources and perspectives (Buchwald 2000). Dependability refers to the idea of replicability and confirmability addresses objectivity and whether the data itself can support the conclusions found in the study. Moreover, the reliability and the validity of this research is checked by a deviant case analysis. This is a detailed analysis of those tweets that appear to deviate from an identified pattern. This analysis adds more depth to the Dissertation. The second way in which the validity and reliability of this Dissertation is examined is through its coherence. Discourse analysis is a methodology that builds over time and over research studies. Each new research checks the reliability of earlier studies (Potter 1996). Research that is coherent lends elements to future studies while those that do not are ignored and discarded.

3.2. Descriptive Statistics

The second method to be used in this Dissertation centres around descriptive statistics using categorical variables. This method is used to summarise and describe the variables for a sample of data. In this Dissertation, univariate analyses will be the predominant analytical method used to summarise one variable at a time. Larson states that most data analysis starts with the calculation of descriptive statistics on the variables included in the data (2006). Descriptive statistics summarise different aspects of the data providing information about the sampled population. Additionally, the variable's type will determine the nature of the descriptive statistical analysis taking place as well as the way in which the analysis is reported, commented on and displayed (Larson 2006[31]). The variable type within the key datasets are categorical variables, these have been defined by Spiegelhalter as "measures which can take on two or more categories which may be unordered categories [...] or ordered categories [...] or numbers that have been grouped"(2019: 27). The categorical variables identified are mostly unordered categories. Frequency statistics are the main type of descriptive statistics utilised with these

[31] https://www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.105.584474 Last Accessed 10 April 2021.

variables. These “include absolute frequencies (raw counts) for each category of the discrete variable, relative frequencies (proportions or percentages of the total number of observations), and cumulative frequencies for successive categories of ordinal variables" (Larson 2006)[32]. This method has been selected as a descriptive approach which allows for an in depth look at the phenomenon of hacktivism. Gerring states that descriptive methods are best suited to ‘what/is’ questions (2012). As the research question this Dissertation attempts to answer is *‘Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?*’ A description of hacktivists, their methods, their motives and their targets is needed in order to establish if these objects being described reflect those linked to offline social movements.

3.2.1 - Datasets used

The descriptive statistics will be applied to a number of datasets. This includes data supplied by Zone H[33]; the Cambridge Computer Crime Database[34]; DCMS’s Cyber Security Breaches Surveys from 2017-2021[35]; an AnonOps Internet Relay Chat Channel[36]; a sentiment analysis; the hack aggregator website entitled ‘Hackmageddon’[37] (see Table 5 for numbers assigned to these datasets) These datasets were selected as traces of hacktivism are difficult to access online with Kurzmeier stating that the vast majority of data linked to hacktivism is lost for research purposes (2020: 54). Indeed, Kurzmeier states that “actual hacktivist content probably occurs at a prevalence of less than 0.01” (2020: 54). As a result these databases, while not focused on hacktivism, offer information and perspectives on hacktivism, its prevalence, its targets, its methods, its ideologies and its motivations. Due to the lack of data that exists online the data may not be generalisable to the wider hacktivist landscape, however in using multiple datasets the data is not reliant solely on one source. These databases will now be explained as well as the reasons for their selection.

[32] https://www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.105.584474 Last Accessed 10 April 2021.
[33] http://www.zone-h.org/archive/special=1 Last Accessed 29 Jan 2022
[34] https://www.cl.cam.ac.uk/~ah793/cccd.html Last Accessed 1 Feb 2022
[35] https://www.gov.uk/government/collections/cyber-security-breaches-survey Last Accessed 29 Jan 2022
[36] https://www.azsecure-data.org/internet-relay-chat.html Last Accessed 13 April 2021.
[37] https://www.hackmageddon.com/ Last Accessed 13 April 2021

The Hackmageddon dataset	Dataset 01
Zone H Archive	Dataset 02
The Cambridge Computer Crime database	Dataset 03
DCMS Cyber Security Breaches Survey	Dataset 04
AnonOps Internet Relay Chat Channel	Dataset 05
Sentiment analysis from SWGFL	Dataset 06

Table 5: Datasets used and their respective numbers

The Hackmageddon dataset (Dataset 01) is compiled using the following sources: Bleeping Computer; The Record by Recorded Future; ZNET; Security Affairs; SecurityWeek; ThreatPost; Infosecurity Magazine; HelpNet Security; DarkReading; Daily Swig; The Register; Security Magazine; Ars Technica; TechCrunch; BBC News (Cybersecurity Section); Forbes (Cybersecurity Section); Graham Clubby; Krebs On Security; Naked Security; Databreaches.net; Databreachtoday.net; GovTech.com; HackRead; HealthITSecurity. These feeds are checked regularly and the information is selected a priori. The variables included in the dataset are: the attacker, the date of the attack, the method used, the target, the motivation behind the attack and a short description of the attack itself. The creator of the dataset has described it as to provide an overview of the threat landscape identifying the macro trends. Mr Paolo Passeri will collect events that have an important impact per se (for example mega breaches) or have an impact as part of a general trend (for example ransomware attacks to school or healthcare organisations). Any events included in the dataset have all been directly verified. The dataset was originally a set of different spreadsheets for each month, however, these spreadsheets have been merged and cleaned to ensure it's ready for statistical analysis. The analysis on this dataset allows for a comparison between the activities and methods of hacktivism and cybercrime as well as to provide a starting point for comparison between hacktivism and social movements from 2012 until 2019. Furthermore, the dataset allows for categorisation with the attacks having hacktivism as a motive being categorised based on their methods and their targets as well as a comparison of these categories to the wider cybercrime landscape allowing for differentiation between hacktivism and cybercrime. An additional variable was created using the short description of the hacks identifying the operation linked to the action. These operations were fact checked by the researcher to ensure the information is reliable. These operations are an important variable in any analysis of hacktivism as they allow hacktivists to combine their efforts in order to defend a specific cause aligned with their values, to promote a political agenda or social change[38]. The operation variable will enable the analysis of the length of operations, the frequency of operations and allow for a springboard for further research into the motivations, ideologies and successes of these operations.

Zone H Archive (Dataset 02) is a website defacement archive that is a freely available database that has recorded website defacements since 2001. The database is open for general consultation and includes some specific characteristics: targeted domain; attack date; attack time; attacker's nickname; operating system of the attacked website; and web server of the attacked website. Each entry into the archive is a confirmed hack and with a link to see a mirrored version of the defacement to ensure it is factual and reliable. Zone-H also features news entries that detail internal engagement with the material held in the archive. This shows that hacktivism is acknowledged as part of the collection and that efforts were made to find and describe sites hacked by hacktivists (Kurzmeier 2020: 55). This database then allows for an examination of 1250 domains targeted by hacktivists and as a result, the types of organisations that are the main target of hacktivists. This database was selected in order to see who hacktivists are targeting as well as to provide a view on the mirrored defaced sites and the information that hacktivists will leave.

The Cambridge Computer Crime database (Dataset 03) is a comprehensive list of computer crime events where the offender has been arrested, charged and/or prosecuted in the UK starting in 2010. These events have been described as high tech offences that fall under computer crime legislation such as the 1990 Computer Misuse Act and the 1998/2018 Data Protection Act. Additional crimes that use computers and are linked to high tech or computer crime are also included such as fraud and money laundering offences. The database is updated weekly. While the database is not focused on hacktivism it does include details of arrests of hacktivists that have engaged in computer crime offences, as such the database offers a comparative view of hacktivism and cybercrime by detailing the collective and the reason for the offence. It is important to note that this dataset only includes arrests that have taken place in the UK. As such it does not include the hacktivist activities that have not led to arrests in the UK and may not be representative of all hacktivist activities.

[38] https://securityboulevard.com/2020/06/analysis-of-the-top10-hacktivist-operations/ Last Accessed 3 Feb 2021.

The Department for Culture, Media and Sport's Cyber Security Breaches Surveys (Dataset 04) have also been used in this thesis to provide an official government perspective on cybercrime. While these reports do not include hacktivist activities, they do include information on one of the key methods used by hacktivists, DDoS attacks. They also offer a look at the businesses that are targeted by cybercrime. The annual survey reports have been compiled into one document in order to illustrate how cybercrime has changed over the years and starts with the first available report on the DCMS website in 2017 until the most recent report in 2021. The government details that the survey is run to "help businesses understand what other similar businesses are doing to stay cyber secure, and supports the Government to shape future policy in this area"[39]. The report contains two different data collection methods: interviews and surveys. The survey is a random probability telephone survey of 1,523 UK businesses and has been weighted to be statistically representative of the UK business population by size and included sectors. Additionally, a total of 30 in-depth interviews were undertaken to follow up with businesses that had participated in the survey and gain further qualitative insights.

These datasets allow for the analysis of frequency statistics that includes raw counts for each variable included in the dataset which can then be converted into relative frequencies. These datasets will be analysed in Microsoft Excel as the variables are all categorical in nature and do not require any software or programming languages to analyse. Frequency tables will be used in order to identify either the absolute or relative frequencies where applicable. These frequency tables will be used in order to create graphical displays.

The AnonOps Internet Relay Chat data (Dataset 05) provides background information on specific hacks. The dataset is qualitative in nature and was taken from one of the AnonOps Internet Relay Chat Channel. This dataset was made available on the https://www.azsecure-data.org/internet-relay-chat.html website. The AZ Secure Data website is linked to the Artificial Intelligence lab at the University of Arizona and describes the dataset as: "Anonops IRC channel has been affiliated with the activities of Anonymous hacktivist group through which the group discusses a variety of topics such as planning, coordinating and sometimes announcing their future attack targets. Therefore, the dataset is crucial to predictive and proactive analysis of hacktivist communities. The dataset contains 1,874,984 messages

[39] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (p4) Last Accessed 12 Feb 2022

dating from September, 2016 to May, 2018”[40]. This dataset allows for insight into the beliefs of those engaging in Anonymous operations as well as the general beliefs of those that identify as Anonymous. The AnonOps.log dataset also provides an in depth analysis of the language used by members of Anonymous and their opinions of other phenomena linked to hacktivists. Key words will be searched for in the vast dataset that are relevant to the analysis. The use of this dataset provides colour and an in depth description of hacktivism as a whole which assists in answering the question on whether hacktivism could be seen to be a politically motivated social movement as opposed to a form of self motivated cybercrime.

The final dataset to be analysed as part of the descriptive statistical analysis section focuses on the public opinion of hacktivism. The sentiment analysis programme, provided by the South West Grid for Learning, analyses data from upwards of 10 million public facing websites with a specific focus on news sites, blogs, forums and message boards, review sites and Twitter. The programme is only able to find content that is publicly available and open to everyone on the internet, meaning that private social media accounts, for example, will not provide any data to be featured in the analysis. The keywords to be analysed using the program are ‘hacktivism’, ‘hacktivist’, ‘online protest’ and ‘electronic civil disobedience’. The program searches publicly facing websites for these key terms and returns an indication of the sentiment of the overall post based on its source context. The sentiment analysis took place over two months from 1/11/2020 until 15/1/2021. The programme analyses the source content to extract positive, neutral or negative contexts, words and phrases and returns a sentiment metric. The sentiment metric returned is a number between -1 and +1 with negative values ranging between -1 to -0.33, neutral values ranging between -0.33 to 0.33 and positive values ranging between 0.33-1. These keywords were analysed using the programme provided by SWGfL in order to understand how the public talk about hacktivism, online protest and electronic civil disobedience giving an overview of public opinion on the matter. This analysis of public opinion is used in Chapter 6 in order to judge hacktivism’s legitimacy as Olsen states that a protest movement needs widespread public acceptance in order to be seen as a legitimate movement (1968). The keywords selected were chosen based on the existing literature on hacktivism. Both ‘hacktivism’ and ‘hacktivists’ are analysed in order to understand how the public feel about the phenomenon itself as well as those engaging in it. This provides a clear understanding of the sentiment many individuals feel regarding the form of protest and those protesting. Additionally, ‘electronic civil

[40] https://www.azsecure-data.org/internet-relay-chat.html Last Accessed 13 April 2021.

disobedience' is analysed as it is a key term identified in the literature on hacktivism in Chapter 3. The final keyword selected, 'online protest' was chosen as it is essentially a more approachable way of defining what both hacktivism and electronic civil disobedience is. Therefore those who may not know these terms but do share opinions on the matter can be included in the analysis.

In this Dissertation, The PPDAC problem solving cycle will be applied as described by Spiegelhalter (2019: 13-15). The cycle commences by the specification of the Problem, in this case the problem to be solved is the research question: *'Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?*' Once the problem has been defined and understood, the second stage of the cycle is linked to the need for a careful and comprehensive plan. This plan focuses on what needs to be measured, how to record the data and how to collect it. In this case the plan centres on understanding the current state of hacktivism, as well as the methods, motives and targets of hacktivists. The third stage of the cycle focuses on the collection, management and cleaning of the data. Spiegelhalter states that collecting good data requires organisational skills, specifically when that data comes from routine sources (2019). This is due to the fact that the data may need to be cleaned in order to ensure it is ready for analysis. In this case, the datasets will be cleaned and merged to ensure the analysis can take place. This leads on to the analysis stage whereby the data is sorted, tables and graphs can be constructed and patterns can be searched for. The final stage of the cycle is then the conclusion stage which centres on interpretations from the analysis stage, the conclusions that can be drawn and the new ideas and knowledge that have come to light. This stage will feature both in the analysis chapter, as well as the final chapter. Now that the datasets and methods have been outlined both methods, the limitations will now be identified.

4. Limitations of the Research Methods and Ethical Considerations

This section explains the main limitations that the Dissertation mitigates as well as any ethical considerations that need to be taken into account. Firstly, the issue of researcher bias is addressed. This particular bias is linked to the rhetoric analysis section of the Dissertation with any discourse analysis being a subjective research method that is led by the researcher's experiences. As a result, any discourse analysis should be undertaken with scepticism and an analytic mentality (Shenkein 1978) . In this Dissertation, all researcher assumptions were questioned throughout the rhetoric analysis with the researcher constantly questioning herself asking ‘why am I reading this in this way?’. Additionally, the discourse analyst must immerse themselves in the text, in this case the tweets that were analysed to ensure the maximum potential of the material was achieved. This resulted in the research question and subquestions being answered as objectively as possible. Another limitation to be considered with regards to the rhetoric analysis is the lack of reliability of the research. Again, due to the subjectivity of the method it is very difficult to replicate the results to the wider population. This limitation will be mitigated through the statistical analysis section which will ensure half of the research can be replicated. This method will not only provide some context on the state of hacktivism as it currently stands but also will also ensure that the research is less prone to bias and remains objective in nature.

A lack of personal contact with the individual’s studied could also be seen to be a limitation of this Dissertation. Hacktivists themselves are very secretive as a result of their illicit activities and very unwilling to cooperate with researchers. While some hacktivists had been contacted with interview requests very few responded. Those that did, declined to be interviewed predominantly as they had had difficult experiences with researchers in the past. Moreover, policy makers had been contacted and a plan had been set in place to meet some at conferences. However, the COVID-19 pandemic resulted in the cancellation of these conferences. As a result, the Dissertation found an alternative plan in the use of the publicly available datasets. This instead, provides a more objective look into hacktivism and the operations associated with it. An additional issue that arose as a result of the COVID-19 pandemic is linked to the vast datasets and the lack of computational power. There was a great deal of data to be cleaned, processed and analysed and due to the COVID-19 lockdowns, the available technology could not compute the amount of data. As a result, the University of Exeter loaned a powerful laptop to ensure the data analysis could still take place from the researcher's home. The COVID-19 pandemic also led to a very startling change in many individual’s situations affecting the way in which the research took place and where. This Dissertation was predominantly researched and written up from home which led to its own challenges. As a result, a strict routine was imposed to ensure a balance could be struck as well as it being finished on time.

The research in this Dissertation was approved by the Ethics Board at the University of Exeter. The ethical issues arose through the use of the datasets analysed. All of the data used in this

Dissertation is publicly available data. Cooper and Coetzee define publicly available data as data found readily (such as on the Internet) and accessed (downloaded) easily and for free (2020: 159). Many of these datasets are created and distributed by public organisations. The data used in this Dissertation is a mix of open data that is freely usable, reusable and redistributable without restrictions and data available on request. Throughout this Dissertation, one must keep in mind that datasets act as a surrogate. Indeed, Cooper and Coetzee state that the data is not the real world and acts as a surrogate for the phenomena, in this case hacktivism, in the real world that is being measured or analysed (2020:160). This can arise due to issues of cost, availability, and laws, all of which apply in this Dissertation. No matter what form the publicly available data takes, certain ethical issues can occur. These issues include considerations with regards to privacy with the possibility of moral and legal concerns occurring over the invasion of the privacy of individuals groups or organisations. Cooper and Coetzee indicate that privacy is difficult to define as it is perceived differently by many different people (2020: 162). They state that “Privacy is perceived as being about protecting people’s personal information, but it also includes territorial (or location) privacy, physical (or bodily or health) privacy and privacy of communications" (2020: 162). This issue has been offset by ensuring the dataset contains no personal, territorial or physical information with the datasets only including the pseudonyms hacktivists use in their online communications. Furthermore, hacktivists will often take credit for specific hacks and post information online regarding these which indicates that they are not concerned with the idea of being researched. Finally, there is no one specific dataset that could detail the information that was needed in this Dissertation and while hacktivists will post online about their successes there are no official government datasets on hacktivists. Several theorists working in both cybercrime and hacktivism, including Dr Vasileios Karagiannopoulos, Dr Leonie Tanczer, Dr Claudia Peersman and Professor Alice Hutchings, were consulted with regards to their knowledge of government backed hacktivist data but were unable to offer any specific hacktivist datasets. This is in part due to the fact that hacktivism is hard to distinguish from regular cyberattacks unless the attackers claim responsibility with a very clear political agenda. The purpose of these datasets is to provide a general overview and identify some macro trends, however the individual datasets might contain a certain degree of subjectivity As a result a number of datasets have been analysed in order to offset this and ensure a single biassed dataset isn’t used.

5. Conclusion

In conclusion, this chapter outlined the research design as well as two research methods that were used in the following chapters in order to answer the research question as well as the subquestions. The research design applied was exploratory in nature using a multi-method approach. This approach was based upon the type of research questions, the amount of control the researcher had on the phenomenon and the degree of focus on certain events as well as the fact that there is little existing research in this particular research subject. The multi-method approach combines both qualitative and quantitative methods in order to ensure a balance between objectivity and detail. The first research method utilised in this Dissertation is a qualitative rhetoric analysis which attempts to identify Stewart's (1980) functional approach to rhetoric used by social movements in the tweets published by known hacktivist accounts. These five functions include 'Transforming perceptions of history'; 'Transforming perceptions of society'; 'Prescribing courses of action'; 'Mobilising for action'; and finally 'Sustaining the movement'. With regards to the first function: 'Transforming perceptions of history'. This rhetoric analysis allows for a comparison between hacktivism and offline social movements. The second method to be used in the Dissertation is a descriptive statistical analysis using the multiple datasets detailed above in order to provide different perspectives on hacktivism and cybercrime including data compiled by the UK government; cybercrime theorists; cyber intelligence employees and a database of defaced websites. The variables in these datasets will be analysed in the form of frequency tables which were then used in order to create graphical displays to illustrate the results. Finally, there are various ethical issues that arose and limitations were considered. These issues included issues with bias, generalisability and reliability which must be mitigated in the Dissertation. Furthermore, certain limitations that occurred as a result of the COVID-19 pandemic were also considered. The ethical issues linked to publicly available data were also reviewed, specifically issues relating to privacy. These have been dealt with by the researcher ensuring that there is no personal, territorial or physical information present in the dataset.

Chapter 5: The Rhetoric used by Known Hacktivists

1. Introduction:

In the previous chapter, the data collection methods used in this dissertation were delineated as well as their suitability in answering the research question. This chapter presents the results of the rhetoric analysis of Twitter accounts identified as being from known hacktivists. These accounts include those of specific long-running operations identified as Anonymous Operations from the hackmageddon dataset such as OpIndia and OpGreenRights, more general Anonymous Twitter accounts such as AnonOps and YourAnonNews and active hacktivists not affiliated with Anonymous such as Chaos Computer Club and Belarussian Cyber Partisans. These Twitter accounts will be analysed and coded in reference to Stewarts *Functional Approach to Rhetoric* used by social movements which was outlined in the previous chapter (1980). In this chapter, the analysis of the Twitter accounts will take place which identifies the specific ideologies, how often the account is used and how many people are interested in their tweets to provide a grounded view of the purpose of these accounts (2). The results of the rhetoric analysis are then presented with reference to the tweets used (3).

The aim of this chapter is to establish whether the communications used by hacktivists contain the same functions identified in the communications of other social movements. This will assist in aligning hacktivism with social movements rather than cybercrime. At present, the UK government still considers hacktivism to be a form of cybercrime. By examining whether the communications used by hacktivists are similar to social movements it will provide a compelling argument as to whether the UK government should instead align it with social movements. This chapter will argue that the communications used by hacktivists to outsiders do indeed contain the same functions as those used by offline movements. As such, hacktivism could be seen to be a social movement and as a result, the methods used by hacktivists should be afforded the same rights as those used by offline social movements.

2. Analysis of Twitter accounts:

The twitter accounts used for analysis are a mixture of accounts relating to specific operations that were identified as taking place for longer than a year as well as general Anonymous accounts with at least 50,000 followers. Datasets of active hacktivist groups not linked to Anonymous were also analysed to ensure a balanced analysis. These twitter accounts were identified through desk based research as being pertinent hacktivists. The accounts analysed were @YourAnonOne; @YourAnonNews; @TheAnonMovement; @AnonOps; @YourAnonCentral; @MMMLondon; @OpRussia; @OpFreePalestine; @OpGreenRights; @OpIsrael; @OpKillingBay; @OpLastResort; @OpSyria; @OpLiberation; @GhostSquadHacks; @ChaosComputerClub; @BelarusianCyberPartisans. These 17 Twitter accounts will now be outlined before the findings of the rhetorical analysis are presented.

2.1. General Anonymous Accounts

@YourAnonOne:

This account has 470,800 followers and follows 126 accounts. It has been on Twitter since August 2018 and their biography is "We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us. News in the world in real time. Turn on notifications."[41] @YourAnonOne Tweets regularly, usually tweeting at least once a day. The account tweets mostly global news, although the tweets analysed were predominantly relating to US politics and will often retweet other accounts linked to Anonymous. Despite the fact that Anonymous claims to not follow any specific ideology or politics, their tweets seem to be predominantly linked to progressive ideology such as racial equality, aid distribution and the right to peaceful protest.

@YourAnonNews:

This account has 6.8 million followers and follows 759 accounts. The account joined Twitter in April 2011 which was around the time Anonymous as a collective began to diversify after predominantly being interested in issues focusing on the internet (Olsen 2012). The twitter bio is the same as @YourAnonOne: "We are Anonymous, we are legion, we do not forgive, we do not forget. Expect us."[42] The account tweets at least once a day usually receiving quite a lot of engagement and retweets from a wide range of global sources. Again, similarly to @YourAnonOne, their tweets focus on climate change, defunding the police, and support anti

[41] https://twitter.com/youranonone?lang=en Last Accessed 11 November 2020.

[42] https://twitter.com/YourAnonNews Last accessed 11 November 2021

institution protests and rebellions globally stating for example: “Revolution is festival of oppressed folks”[43].

@TheAnonMovement:

@TheAnonMovement has 63,100 followers and follows 38 accounts. They joined Twitter in November 2014. Their twitter bio is slightly different to the previous two accounts: “Hacktivists specializing in Anonymous operations, occupy & resistance movements, journalism, and security. We are a voice for the voiceless. #AnonOps #ExpectUs.” In their bio they outline their interests in journalistic freedom, resistance and fighting for justice for the oppressed. They tweet less regularly than the previous accounts, posting only when there is a relevant operation occurring, the most recent of which was taking part in the Black Lives Matter movement. They also predominantly retweet other accounts, the most common of these are other Anonymous affiliated accounts.

@AnonOps:

This account has 285,400 followers and only follows 6 accounts, who are all either hacktivists and whistleblowers. Their twitter bio is “We are fighters for internet freedom. News about Anonymous”[44] and they joined twitter in December 2010. They don’t tweet regularly, and indeed only tweeted once in 2018. They regularly post about other hacktivists such as Aaron Schwartz and their tweets are predominantly focused on internet freedom and security, for example: “The US government prevents its people from being spied on by China through #Tiktok, because they want to be the only ones who spy on you through Facebook / Instagram and Google”[45].

@YourAnonCentral:

This is the final non-operation specific Anonymous account to be analysed and has 5.9 million followers, following 766 accounts. They joined Twitter in September 2011 and tweets regularly, usually multiple times a day. Their Twitter bio states: “Exposing Human Rights abuses from around the world. Reporting, resistance resources, & Anonymous updates. Actions Not Nouns. We do not forgive. 🛰 #EndImpunity”[46] outlining what followers are likely to see if they follow the

[43] https://twitter.com/YourAnonNews/status/1335257796594569216 Last accessed 11 November 2021

[44] https://twitter.com/anonops?lang=en Last accessed 12 November 2020

[45] https://twitter.com/anonops/status/1307006434362753024 Last accessed 12 November 2020

[46] https://twitter.com/YourAnonCentral?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor Last accessed 11 November 2020.

account. Their pinned Tweet also lists their ideological beliefs: “We support the weak against the powerful and stand for justice. Our values are the following:

- Human rights.
- Autonomy & self-governance.
- Resistance against tyranny.
- A more humane society.
- Actions Not Nouns.”[47]

Their tweets reflect those of other Anonymous accounts and they will post about some specific operations eg #OpSafeWinter which is aimed at ending homelessness. They also post about the Black Lives Matter Movement, internet and journalistic freedom and support global resistance movements.

2.2. Operations Accounts

@MMM_London:

This twitter account is the account linked to the operation Million Mask March which is also named OpVendetta. The march is a yearly anti-establishment protest that occurs on the anniversary of Guy Fawke’s attempt to destroy the House of Lords on November the 5th. Those taking part in the march also wear a mask based on the stylised depiction of Guy Fawkes on the graphic novel and film V For Vendetta, which takes place in a dystopian neo-facist Britain whereby the main character is an anarchist inspired by Guy Fawkes[48]. The account has 1,091 followers and joined Twitter in March 2014. They don’t tweet regularly, mostly when there is an interesting news story, or to retweet another Million Mask March account. Their twitter bio mostly just points users to the hashtags linked to the yearly march: “#MMMLondon #Opvendetta #MMM2020 #MillionMaskMarchLondon #MillionMaskMarch #Anonymous #Anon Original MMMlondon twitter Account”[49]. Their tweets are mostly anti-authoritarian in nature either criticising various heads of state/the police or in support of global protest movements.

@Op_Russia:

[47] https://twitter.com/YourAnonCentral/status/1268288486857048064 Last accessed 11 November 2020

[48] https://londonist.com/london/politics/everything-you-need-to-know-about-london-s-million-mask-march Last accessed 11 November 2020

[49] https://twitter.com/mmm_london Last accessed 12 November 2020.

This account is linked to the operation OpRussia which was initially in support of Ukranian protestors during a period of civil unrest which was caused by the government choosing closer ties to Russia over the European Union.[50] These protests have been described as being "a rejection of injustice as a way of life and of the post-Soviet politics of corruption and nepotism" (Open Society Foundations). The account has 12,800 followers and has been on Twitter since February 2011 despite the Russian invasion of Ukraine in March 2022. Their twitter bio is linked to Anonymous: "We Are Anonymous, We Are Legion, We are everywhere, We are invincible, We do not forgive, We do not forget"[51]. They haven't tweeted since 2016 and seem to have last been active in their support of the protestors taking part in the Ferguson Unrest in 2014 as a result of a police shooting an unarmed black man.

@OpFreePalestine:

OpFreePalestine is an operation in support of the Palestinian people protesting Israeli forces in Gaza. This account has very few followers - only 11-, they haven't posted anything since April 2016 and have only tweeted 15 times. Their twitter bio states "Freedom for the Palestine people! Stop killing innocent humans! #Israel is about to destroy #FreePalestine."[52] The majority of their tweets are focused on Israeli forces and their abuse of the Palestinian people.

@OpGreenRights:

This account is linked to the operation 'Operation Green Rights' which was originally created in order to protest for "Human Rights and against Big Company which destroy Nature and ancient Cultures. We sustain Free Green Energy."[53] The operation claims "Operation Green Rights wants a future for our kids where a clean and civilized world is waiting for them with open arms where there is respect for nature. We don't want anymore oppression and blood to rule because of greed."[54] The account has 9,698 followers and has been on Twitter since March 2011. The account has been inactive since 2016 with the last tweet being from November 5th 2016 supporting the Million Mask March. Their twitter bio follows the majority of Anonymous linked Twitter accounts by stating the group's strapline - "We are Anonymous. We are Legion. We do

[50] https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests Last accessed 12 November 2020

[51] https://twitter.com/op_russia?lang=en Last accessed 12 November 2020.

[52] https://twitter.com/opfreepalestin3 Last accessed 12 November 2020.

[53] http://operationgreenrights.blogspot.com/search?updated-max=2013-11-06T15:31:00-08:00&max-results=8&start=32&by-date=false Last accessed 12 November 2020.

[54] https://anonitaly.blackblogs.org/2019/01/23/opgreenrights/ Last accessed 12 November 2020.

not Forgive. We do not forget. Expect Us."[55] Their twitter posts are predominantly focused on the operation, posting when they've taken a website offline or linking to the operations blog when they have an update on it. Ideologically, their posts are in line with environmental causes targeting companies accused of ecological wrongdoings.

@OpIsrael:

The OpIsrael twitter account focuses on the operation OpIsrael which is very similar in beliefs to OpFreePalestine. The account focuses on calling out Israeli human rights breaches towards Palestinian people. It has 35,100 followers and follows 258 people. The bio for OpIsrael is "#OpIsrael - #FreePalestine - #AntiZionism - #FuckIsrael - #Anonymous - Viva Operation Israel Hackers!"[56] The account has been inactive over the last few years with the last post being in 2017 with a pinned tweet from 2015 at the top of their feed: "If you have children, we urge you to teach them that Palestine exists and needs freedom. The hope of Palestine rests with their generation." They joined Twitter in January 2012 and have posted a great deal more than the @OpFreePalestine account, posting 36,300 tweets. They post quite a lot of sensitive information in the form of disturbing images that Twitter has flagged as sensitive.

@OpKillingBay:

OpKillingBay is an operation which brings attention to the hunting of whales and dolphins in Japan, the Faroe Islands and other Arctic countries.[57] They joined twitter in January 2014 and have 404 followers. However, the Twitter account doesn't seem to focus on the operation itself - their bio states: "#OpKillingBay Greetings Japan. We know your secret. We are disgusted. Allow animal/human marriage. We are Anonymous! Expect us."[58] They tweeted 47,000 times, however they were only active between Feb 23, 2019 and March 27, 2019. All of their tweets are focused on Japan outlawing animal/human marriage, specifically with dolphins with the hashtags #Tweet4Taiji and #Taiji which doesn't seem to be linked to the contents of the tweets. Taiji is a small Japanese town whereby inhabitants drive cetaceans into a small bay where they are captured and mostly killed for their meat as a part of local traditions[59].

[55] https://twitter.com/opgreenrights?lang=en Last accessed 12 November 2020.

[56] https://twitter.com/op_israel?lang=en Last accessed 12 November 2020.

[57] https://security.radware.com/ddos-threats-attacks/opkillingbay2017/ Last accessed 12 November 2020.

[58] https://twitter.com/OpKillingBay Last accessed 12 November 2020.

[59] https://www.dolphinproject.com/blog/taijis-dolphin-hunting-season-has-come-to-a-close/ Last accessed 12 November 2020.

@OpLastResort:

This account is linked to what Anonymous believes to be excessive prosecution of hacktivists. The operation is also linked to their aim of reforming computer crime laws. They joined Twitter in January 2013, potentially in response to the suicide of hacktivist Aaron Schwartz who died on 11/01/2013. They have 7,000 followers and have tweeted 1,143 times. The bio for OpLast Resort is: “This tragedy is basis for reform of computer crime laws, and the overzealous prosecutors. | http://youtube.com/watch?v=_bAMgFt9z4Q | #Anonymous #OpLastResort #AaronSwartz.”[60] They last tweeted in 2014 on the anniversary of Aaron Schwartz’s death. The majority of their tweets are focused on previous hacktivists arrests and motivational posts, for example: “You ask what is our aim? I can answer in one word: It is victory, victory at all costs victory in spite of all terror, victory, however long”[61].

@OpSyria:

OpSyria is an operation linked to the Syrian civil war, the operation started when the Syrian government prevented any outside communications by disabling the internet.[62] The hacktivists stated: *“Everything that can be done to create and disseminate the Anonymous Operation Syria Care Package has already been done. Syrian activists have prepared for months for this shut-off, and activist media centers are located in every city. So this Op will have two prongs, one: gather any and all media coming OUT of Syria and spread the info. And two: OFFENSIVE, we are going to take down EVERY Embassy in the world Assad has left, begining with his biggest and most powerful supporter nations. Thankfully, he doesn't have many left so....”*[63] The twitter account has 228 followers and joined the social networking platform in March 2011. Their last tweet was on Jul 15, 2013 so is currently inactive. The twitter bio states: “Updates from Operation Syria broadcast live via LiveWord?[64]” The account posted updates with links regarding the war in Syria with the links directing to a no longer active website hosted on Liveword.

@OpLiberation:

[60] https://twitter.com/oplastresort?lang=en Last accessed 12 November 2020.

[61] https://twitter.com/OpLastResort/status/395886970779361280 Last accessed 12 November 2020.

[62] https://www.databreaches.net/opsyria-what-is-it-and-why-is-it-being-done/ Last accessed 12 November 2020.

[63] https://pastebin.com/jKjUtsNu Last accessed 12 November 2020.

[64] https://twitter.com/opsyria Last accessed 12 November 2020.

This is the final account linked to a specific operation to be analysed. OpLiberation is aimed at raising awareness of abuse in ‘troubled teen camps’. The operation website states:

“For years, teenagers have had to suffer from countless years of torture and brainwashing in so called “troubled teen camps.” These include camps like Cross Creek in Utah, and Paradise Cove in Samoa. We will not stand for the abuse against these children, we will make sure all of the schools, and the sponsors who started these schools, the WWASP, will suffer consequences for their actions against the civil rights of the youth. The parents are persuaded by the camps to send their children into these evil institutions. The camps use excuses such as ‘poor grades, antisocial children and possible drug addiction’ to get them to turn their kids in. This is when the organizations have full control, abusing and neglecting the young people until their will breaks, leaving them unable to fend for themselves. 'Awareness of this must rise’, more people must know the evils of these places… Or we will lose a generation.”[65]

The account joined Twitter in February 2014 and has 307 followers. They have tweeted relatively recently, with their last tweet being a missing persons poster of a teenage girl who had been abducted posted on November 20th 2020. Their bio states: “#OpLiberation Voice for Children & Survivors of abuse at teen residential facilities & beyond #FreeJustina #OpPedoHunters formerly @StopLoganRiver.”[66] Their tweets are mostly informing followers of convincted sex offenders and memorials for children and young women who were killed as a result of abuse.

Based on the above, it is clear to see that there is a wide range of ideological beliefs held by members of Anonymous with some accounts focusing on a specific issue while others are more generalised and focus on global news. There seems to be an overarching link between all accounts’ ideological beliefs. The operations accounts are mostly linked to left-wing progressive ideology from ecological and animal rights movements to assisting citizens based in repressive regimes throughout the world. The more generalised Anonymous affiliated accounts are similarly progressive in their ideology. They support global movements such as the Black Lives Matter movement and they attempt to bring attention to global climate change movements.

[65] https://opliberation-blog.tumblr.com/Everything_You_Need_To_Know Last accessed 12 November 2020.

[66] https://twitter.com/opliberation?lang=en Last accessed 12 November 2020.

2.3. Non-Anonymous Affiliated Accounts

@GhostSquadHacks

This account is linked to Ghost Squad Hackers which is a politically motivated group that originated in 2016 and has conducted several campaigns against high profile entities such as governments and banks. Their Twitter bio links to their Wikipedia page which details attacks on governments and organisations including the Ku Klux Klan; the Ethiopian Government; and the European Space Agency. The Group's Wikipedia pages states that they are led by hacktivist S1ege and their focus is on anti-governmental and "organisation cyber protests within current involvements of media speculation and real life happenings in 2016 to present."[67] Ghost Squad Hackers does not follow any Twitter accounts but has 8,029. The group has tweeted 406 times, predominantly about their specific activities.

@ChaosComputerClub

The Chaos Computer Club (CCC) are a german hacktivist group and have been defined by van Haaster, Gevers and Sprengers as close to an optimal hacker group due to the fact that they have skilled members, a strong public persona and many outlets to the media (2016: 115). The group defines themselves as "Europe's largest association of hackers.'[68] For over thirty years the CCC have provided information about technical and societal issues, such as surveillance, privacy, freedom of information, and data security. The group organises campaigns, events, lobbying and publications as well as anonymising services and communication infrastructure. The group follows 226 accounts which appear to predominantly be hackers, journalists and civil society groups. They have 225,200 followers, have tweeted 7,663 times and tweet in both German and English. Their tweets are focused on issues arising due to government and corporate misuse of technology.

@Belarusian Cyber-Partisans

The Belarusian Cyber-Partisans is a hacktivist group of 25 IT experts and other activists who have undertaken a series of hacks against the Belarusian government since the protests of

[67] https://en.wikipedia.org/wiki/Ghost_Squad_Hackers Last accessed 24 January 2022.
[68] https://www.ccc.de/en/ Last accessed 24 January 2022

2020. These hacks include a raid on the servers of the Belarus Ministry of Interior Affairs, obtaining access to passport databases, secret files belonging to Belarusian KGB spies and security officials, police databases of informants, and prison CCTV networks confirming police brutality and torture.[69] Since joining Twitter in August 2021 they have tweeted 103 times, follow 4 accounts including Hacktivist academic Gabriella Coleman and have 3,301 followers. Their twitter bio has the links to their Telegram channel, their email address, the twitter account of their spokesperson Yuliana Shem and their bitcoin unicode for donations. They also describe themselves as ethical hackers in their bio. During preliminary analysis their tweets are predominantly retweets of news articles detailing their hacks as well as images proving some of their hacks against the Belarusian government and government agencies.

These three additional hacktivist groups are all currently active and should shed light on the wider hacktivist community. As Anonymous is no longer as active as it was ten years ago, it should offer an examination of contemporary forms of hacktivism.

3. Functional Approach to Rhetoric:

3.1. Transforming perceptions of history:

The first function ‘transforming perceptions of history’ is focused on whether the tweets attempt to alter perceptions of the past, present and the future, in turn, amending how the audience perceives the issue and how it affects them. This could then encourage audiences to believe that the issue warrants some action on their part. Stewart claims that this function is dynamic in that history can be revised to suit the social movements needs ensuring it is adapted to meet the successes and failures of the movement. This is one of the least identified functions potentially due to the fact that hacktivism is a relatively new phenomenon. Indeed, the technology needed for hacking was only introduced in the 1980s. Indeed, the first computer hack with an explicit political aim did not take place until 1989. The "WORMS AGAINST NUCLEAR KILLERS” hack penetrated computers at NASA and the US Energy Department displayed overtly political messages on the hacked webistes including the quote from the song "Blossom and Blood" by Midnight Oil: “You talk of times of peace for all, and then prepare for

[69] https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup Last accessed 26 January 2022

war”[70]. Therefore, their view of history and their place in it will be very different to more traditional established movements such as the women’s rights or environmental movements.

This being said, Anonymous have specifically attempting to transform audiences of their current view of a recent past by claiming:

> *For those wishing to go back to normal... normal never existed, only conformity and the privilege of apathy.*

It could be argued then, that Anonymous are both attempting to transform the past and the present in the above tweet. Although not specifically mentioning a historical event, they are subverting the idea of a normal past and as a result, subverting the idea of a normal future in an attempt to mobilise those they see as being apathetic and conforming to social norms.

The collective do also reference specific historical events, with the mention of hacktivist Aaron Schwartz, his death and the actions that need to be taken to prevent a similar event occuring:

“We decided to hack MIT again in 2014 on the anniversary with a second tribute to Aaron Swartz http://t.co/x9PqTFosPv #TheDayWefightback”
“MIT hacked by Anonymous on Aaron Swatz Passing Anniversary”
“The best tribute to #Aaron Swartz would be to keep this JSTOR torrent alive. Lasting legacy of a great prodigy”

In their tweets Anonymous also discusses Edward Snowden’s and Chelsea Manning’s whistleblowing and Wikileaks co-founder, Julian Assange, describing them as internet heroes and enemies of the deep state.

Here, they can place themselves as being on the privacy side of the ongoing debate between internet security and privacy and national security. Ghost Squad Hackers will also post their support of Julian Assange. According to US law, a person should be in charge of the information

[70] https://twitter.com/todayininfosec/status/1317085055160885250/photo/1 Last Accessed 15 March 2021.

that is collected about them and how it can be used. Anonymous, as a collective, are placing themselves in this camp as opposed to those who believe that to protect citizens, governments should be allowed to tighten security measures and reduce the amount of privacy a person is entitled to.[71]

“Aaron Schwartz (RIP)\nJulian Assange\nEdward Snowden\n\nInternet heroes and enemies of the deep state.”
Ecuador you can remove our defaces but we have access to your servers, we'll just re-deface over and over.... #FreeJulianAssange *https://t.co/0JPAaU3XUb* *https://t.co/3aj2UQwJYn* *https://t.co/IV8WnNi1XD* *-* *https://t.co/o9DUNMSoQ3* *https://t.co/FxnE9GlJci* *https://t.co/oCFeOmd1e6*

As a collective, Chaos Computer Club also firmly places itself on the privacy side of this debate by detailing how national and global governments' changes to surveillance and secrecy are restricting internet freedoms. They also post about the 2021 Pegasus Spyware scandal and specifically detail the effects of the NSO Groups Pegasus spyware on citizens, activists and human rights.

“Hacked with NSO Group’s #Pegasus spyware: Since the human rights defenders discovered the infections, they have each been living with daily anxiety and fear https://t.co/sqlysuQhlF”
Hacked with NSO Group’s #Pegasus spyware: Since the human rights defenders discovered the infections, they have each been living with daily anxiety and fear https://t.co/sqlysuQhlF
Snowden, Greenwald and Hedges discuss mass surveillance, government secrecy, how oversight hasn’t been functional for years, internet freedom and U.S. attempts to extradite and prosecute Assange https://t.co/2GykfTQEX8

[71] https://www.theperspective.com/debates/living/national-security-outweigh-right-privacy/ Last Accessed 13 March 2021.

Anonymous will reference the past by using the common hashtag #throwback to remind audiences of perceived injustices. It could be suggested that in doing so, they are attempting to inform audiences of past wrongdoings undertaken by those in positions of power ensuring that the likelihood of a similar occurrence is reduced.

> *“#Throwback to the time Kapil Sibal, who ran a media channel HTN, was accused of referring to female employees as 'kutiya'”*

> *“throwback music video featuring scenes from the LA Riots in 1992. A moment in history that should never be forgotten. There's a line that the LAPD crossed &those officers will never forget it. Protip: don't cross that line #Peace”*

Another way in which Anonymous reminds audiences of previous injustices is to use highly inflammatory historical words often describing their opponents as Nazis or a Facists mobilising audiences into perceiving that the issue they are tweeting about warrants action to ensure that history doesn’t repeat itself or potentially suggesting that the current reality is paralleling abhorrent events in history:

> *“Nazis don't get a safe space. It's important to attack these terrorists on all fronts. We will attack them relentlessly on the digital front, with our packets of digital information hammering their servers #Anonymous #OpDomesticTerrorism https://t.co/QuapkRGQXt”*

> *“NEW COMMANDMENT: Thou shalt not:*
>
> - *Be Nazi*
> - *Help Nazis*
> - *Write an adorable Nazi bio for the NY Times*
> - *Refer to Nazis as ‘fine people’*
> - *Vote for Nazi sympathizers*
>
> *I feel like this shouldn’t have to be said.”*

> *“Can't stop! Won't stop! #FascistFail https://t.co/AARHkaOVx9”*

Anonymous also uses a similar tactic when they refer to a current apartheid in Israel. The UN International Convention on the Suppression and Punishment of the Crime of Apartheid defines the Crime of Apartheid as “inhumane acts...committed in the context of an institutionalised regime of systematic oppression and domination by one racial group over any other racial group or groups and committed with the intention of maintaining that regime.”(1973)[72] In calling the situation in Israel and Palestine apartheid, Anonymous are effectively reminding audiences of a situation whereby citizens are treated differently as a result of their race or religion.

“APARTHEID ALERT! Israeli forces close off Hebron's old city, block entrance to Palestinian medical center.”
“Israel is an apartheid state bent on genocide. The IDF are terrorists and murderers. #DownWithIsrael #BoycottIsrael #FreePalestine”
“More Censoring! *Apartheid #Israel approved bill to “expel & ban the entry of #BDS activists” into Israel & Palestine* *https://t.co/Y9RfYEgxzO https://t.co/bC0JhGKoSD”*

Finally, Anonymous uses the past as a form of mobilisation through the repeated references of November 5th and Guy Fawkes night. The collective view Guy Fawkes and his infamous attempt to blow up the Houses of Parliament as an anti-establishment and anti-capitalist hero[73]. Furthermore, the character V from the graphic novel V for Vendetta who popularised the Guy Fawkes masks worn by Anonymous succeeds in taking down a tyrannical government. This character, it could be argued, inspires the collective in their efforts to remove those in power that they believe to be corrupt and tyrannical.

“Remember, remember The fifth of November The Gunpowder treason and plot I know of no reason Why the Gunpowder treason Should ever be forgot”
“Remember remember the 5th of November... let's #EndImpunity.”

[72] https://waronwant.org/israeli-apartheid-factsheet Last Accessed 12 March 2021.

[73] https://www.cnbc.com/2015/12/29/the-man-behind-the-anonymous-mask-v-for-vendettas-david-lloyd.html Last Accessed 12 March 2020

“It's November 5th! Take to the streets, and have a good, safe #MillionMaskMarch! #MillionMaskMarch2018 #Anonymous”

In addition to the hacktivist’s references to the past, some references to the future have also been identified in the Twitter accounts analysed. Stewart claims that in transforming perceptions of the past, present and future audiences could in turn alter their perceptions of a specific issue changing their views of how they fit into it. The future, especially, is particularly dynamic and by altering perceptions of the future, audiences could as a result decide that action needs to be taken to either prevent a future put forward by the social movement that they find intolerable or ensure a favourable future occurs. Both Anonymous and the Chaos Computer Club will both reference possible futures, for example the 2020 US election. This is an attempt to encourage people to participate in democracy and vote to ensure that the future that they find favourable occurs.

“Biden states he would stop giving federal subsidies to big oil. Trump derails by claiming Biden plans to destroy the oil industry, brings up China in an attempt to smear Biden. Biden states he will rejoin the Paris Accord. #Debates2020”
“If Trump goes down, these guys are next: Putin, Erdogan, Modi, Orban, Bolsonaro, Boris, Bibi, Piñera, Sisi, Lukashenko, Duterte, etc. https://t.co/nJ8Gn9d5Hh”
“The message from the UN Human Rights Council is very clear: Biden/Harris administration must prioritize reengagement with international human rights and take bold actions on day one to reverse President Trump’s harmful policies. #UPR36 #USPR”
“Grumpy leftists who argue that activism will disappear under a Biden/Harris admin ... plz consider the value of CIA-loving Dems no longer being able to call themselves “The Resistance””

References to fictionalised dystopian futures have also been identified within the tweets posted by Anonymous and Chaos Computer Club, suggesting that if those in government go unchecked, futures that people find abhorrent could occur which could be seen to be a mobilising force. However, the dystopian futures mentioned aren’t all specific to a piece of literary fiction with some of the language describing an apocalypse if action is not taken.

“Prince Charles says global change is needed because we are literally at the last hour before the climate apocalypse hits humanity. (Reuters) *And he’s right. Sooner or later the climate apocalypse will come.”*
“Israel approves bill to ban #BDS activists #ThoughtControl”
“#FreePalestine *The future is what is done, now.Peace is everywhere,but if your present is war,the future will be too https://t.co/l6WFktHujJ”*
Without net neutrality, people’s ability to share their ideas with many will be severely restricted by the imposition of charges for data delivery. Open Letter against the world’s first law mandating paid prioritization https://t.co/0YKko0vizW #SquidGame

However, not all possible futures the hacktivists put forward are dystopian and fear inducing, one tweet states that ‘A better future is possible’ inspiring audiences to continue in their efforts to demand justice for protesters jailed for demonstrating against police brutality in Nigeria and encouraging the continuation of these protests[74]:

Don’t lose focus. A better future is possible. #EndSARS #EndBadGoveranceInNigeria https://t.co/8qROWwl672

As well as references to the past, the Belarusian Cyber Partisans also reference the present detailing the events in Belarus as and when they occur in order to garner support to their cause.

@CyberScoopNews described growing cooperation between Russian and Belarusian security services in the cyber field. We proved how miserable Lukashenko's regime has been in protecting gov data. The regime endangers not only Belarusians but foreign countries. https://t.co/sw1LYODIzt
Info on those who break into apartments of peaceful #belarusians without any lawful warrants became public. Punishers take people from their homes just for their comments on the

[74] https://www.bbc.co.uk/news/topics/cezwd6k5k6vt/endsars-protests Last Accessed 12 March 2021.

> *Internet in order to intimidate and suppress the will of free #belarusians. Let them feel unsafe too. https://t.co/v7OjiCGKfa*

It can be argued then, despite there being very few references to the past, those that the different hacktivist collectives do use, they do so for specific purposes. Anonymous and Chaos Computer Club predominantly uses references to historical and possible future events to mobilise and encourage audiences to take action, pressure the opposition and as a means to induce fear into audiences ensuring that they are made aware of the consequences not taking action could have. They reference ‘heroes’ both alive and dead such as Aaron Schwartz, Guy Fawkes and Julian Assange as well transgressive historical events that they find heroic to raise awareness of certain issues, such as internet privacy and the historical anti-establishment protests, ensuring that the movement survives. Anonymous also references darker issues, such as police brutality and apartheid, which they believe to still be relevant in the current political climate and as a result pressuring their current opponents from engaging in activities similar to those that occurred in the past. The collectives have also used possible futures using language which could be described as both fear-inducing and inspirational as a form of mobilisation ensuring audiences are aware that an issue warrants action. Finally, the Belarusian Cyber Partisans will refer to present events in order to educate their followers and increase public sympathy for their efforts. As a result, it would appear that the hacktivists predominantly will use history, the present and the future for mobilisation purposes.

3.2. Transforming Perceptions of Society:

The second function identified by Stewart is based around how social movements will attempt to transform the audience’s perception of society. This can include altering both the perceptions of the self as well as the movement's opposition. In doing so, the movement must strip their opposition of authority and legitimacy by using different rhetorical tools, either by portraying them as weak, clumsy and powerless or demonic and conspiratorial. The way in which the audience views themselves can also be transformed, ensuring that they have enough self-belief in order to take action and achieve what needs to be done. The rhetorical tool here would be to instil a sense of agency in the audience as well as by othering the opposition leading to an ‘us/them’ dynamic and instilling the audience with urgency. This function is the most frequent function identified.

Firstly, Anonymous, Belarusian Cyber Partisan and the Chaos Computer Club post a lot of information on their various Twitter accounts in the style of news and information based bulletins alerting audiences to specific issues globally. In doing so, they could be seen to be transforming their perceptions of global societies that audiences may not be aware of. Ensuring more people are aware of the global issues the hacktivists take issue with. Some of the information based tweets also use flagrant and violent words and imagery ensuring audiences feel outrage and respond to the issue emotionally. In some of their tweets it could be suggested that Anonymous are attempting to create a form of moral shock, outraging audiences in such a way to ensure that they take notice of the issues being mentioned and either spread the information themselves or decide to act. The Chaos Computer Club, on the other hand, tweet information in a similar way to civil society groups through the form of campaigns.

Overall, the majority of the different accounts use this method to transform the audience's perception of society, including the general Anonymous accounts, the specific operations accounts, the Belarusian Cyber Partisans, the Chaos Computer Club and the Ghost Squad Hackers.

“The whole world must know what happened in Belgium. Sanda Dia is a Belgian student who was murdered by 17 other students while he wanted to join their circle of student. He was tortured and his killers only had do to some community service and write an essay. #JusticeForSanda”
“#Brazil: President Jair Bolsonaro’s eldest son, Flávio Bolsonaro, has been formally accused of embezzlement, money laundering, misappropriation of funds and directing organized crime. Report: https://t.co/Me8q9FQqLg https://t.co/vGtIzhIxrl”
“Great idea: making forced-laborers with criminal histories do data entry for Central Accounts Payable http://208.118.246.130/lolturnover.png”
“Desperate to censor Palestinians on social media, #Israel arrests 28 Palestinian women over @facebook posts! #BDS”
“Asaduddin Owaisi flays the Congress party, says their leaders are ‘politically impotent’ to take on the BJP

https://t.co/Uw2DX4Jldn”
“Yesterday, the country of freedom made another attempt of a private armed invasion in Latin America. 2020, nothing changes.”
@balticjam,thanks for sharing the news. You can listen to the whole recording we obtained from the MVD's internal communication network. The so-called policemen were sharing their experiences of dealing with Belarusians defending their rights. Crazy staff. *https://t.co/6AEwUFVT6t https://t.co/NkcVEX8yXV*
Ecuador you can remove our defaces but we have access to your servers, we'll just re-deface over and over.... #FreeJulianAssange *https://t.co/0JPAaU3XUb* *https://t.co/3aj2UQwJYn* *https://t.co/IV8WnNi1XD* *-* *https://t.co/o9DUNMSoQ3* *https://t.co/FxnE9GlJci* *https://t.co/oCFeOmd1e6*

As well as the highly emotive language used by hacktivists in order to trigger audiences into taking action, Anonymous, the Chaos Computer Club and the Belarusian Cyber Partisans will also regularly use an ‘us vs them’ dichotomy. In their tweets they will explicitly state their opposition. This ensures the audience knows who they need to direct their anger and dissatisfaction to and in doing so, could bond the audience into believing that they have a collective identity that can rise up and put an end to their perceived injustices. As a result, they are giving the audience an enemy. Additionally, as can be seen below, the opposition is predominantly either a powerful individual/organisation or a world government.

“Palestinian teen succumbs to wounds weeks after being shot by ***Israeli forces*** *https://t.co/ConuB35yFZ”*
*“***Federal Slavery Industries*** celebrates 20 years of cozying up to the* ***DoD****: http://208.118.246.130/cozywiththedod.png #plantationelectronics”*

“Survivors from the residential facility ***New Horizons*** *discuss the torture they experienced witnessed https://t.co/1qHnUmVlqu #OpLiberation”*
“Update #OpSyria « http://t.co/evC9yCn » (08.12.2011) Has | Idlib | Protesters calling for the fall of ***Bashar*** *– free Syria #syria #mar15”*
*“**Trump** signs sweeping tax bill into law* *https://t.co/BUJ6arFM0y* *~ Ⓥ https://t.co/2snSKXJ8DT”*
UK is spending £500k on a PR campaign demonising end-to-end encryption. So far we've got a pisspoor video and... er, that's it. https://t.co/pJpoLrhKr2
End-to-end encryption obviously protects communication contents. UK gov says that's no longer acceptable https://t.co/obRZZn0OLc

However, while the Chaos Computer Club and Anonymous both have general enemies, the Belarusian Cyber Partisans have much more specific opposition in the form of the Belarusian government and President Lukashenko.

Lukashenka in the @BBCSteveR interview admitted that protesters were beaten up in the detention center. He then said that his people were also attacked.🤔 *It's a LIE. We have proofs that generals from MIA couldn't find any policeman seriously injured* 👇 *https://t.co/7gua3RhDPH*
👏*Belarusian @cpartisans claim that they identified one of #Lukashenka security officer who blinded Polish*🇵🇱 *border guards w. green laser.* *It turned out to be Vasiliev Valery Vladimirovich, born on 17.07.1980 in Kurilovka village, Kharkiv reg., Ukraine*🇺🇦 *https://t.co/pk2Wb8lwOg https://t.co/CTiZm3vtuw*

While the hacktivists in general will explicitly name their opposition, Anonymous will also occasionally attempt to create a collective identity in their tweets by including the audience as a member of Anonymous. In order to do so, they use plural pronouns such as ‘we’, ‘us’ and ‘everyone’ ensuring followers and audiences feel included and are encouraged to take part in future Anonymous campaigns and operations.

“How many #Anonymous are there? ***We are more than you think. We are more than anybody thinks. We are many. We are legion. We are absolute. And you are now one of us.*** *Resistance is existence. “*
“#Anonymous #AnonOps ***We are everywhere. We are Global****. Thanks to people in the world! Expect Us! &gt;&gt; http://t.co/MSqNlTS7”*
“Raise your voice loud and clear. ***We are legion****. https://t.co/bCUBTdVifb”*
“#Anonymous ***We are united*** *& we are not leaving EXPECT US!”*
“The Internet Strikes Back. ***We are #Anonymous****. Thanks everybody for the support! #Megaupload”*
*“****We are a global movement*** *that is reclaiming our humanity and our future. #OccupyWallStreet EXPECT US!”*
“We can’t prove them wrong. They are correct: #Anonymous threatens the establishment. ***We will not*** *take this shit anymore, and neither do you.”*

A specific example can be found in certain tweets whereby they claim that Anonymous is the 99% with the powerful elites being the 1%. This slogan is based on the anti-capitalist Occupy Movement that Anonymous supported, and their outrage at income inequality: “Occupiers were angry at the state of the world in the wake of the 2008 financial crisis. They rejected the deep inequalities that capitalism had fostered.”[75] Occupy claims that the political slogan, we are the 99% decries “the concentration of wealth and power in the hands of a few at the expense of the

[75] https://www.occupy.com/article/we-are-still-99-percent Last Accessed 1 March 2021.

many.”[76] This ideology links back to the claim that Anonymous are fighting against corrupt systems of power and wealth.

*“@Anon_Central @anonops **We are the stone in theirs shoes and there are 99% of stones and 1% of shoes in this world.** #FuckACTA #FuckSOPA”*
*“200K FOLLOWERS! THANKS EVERYBODY! **You are #Anonymous. We are Anonymous – We are the 99%**”*
*“**WE ARE THE 99% - WE ARE #ANONYMOUS** – YOU SHOULD HAVE EXPECTED US! #Megaupload”*
*“**We are the 99%** we will no longer be silent! Find a #creditunion &gt;&gt; http://t.co/swxr6qdm WITHDRAW YOUR CASH FROM BIG BANKS! #OpCashBack”*

Additionally, by claiming that Anonymous is the 99%, the collective could be seen to be demonstrating the fluid membership base. Audiences could be encouraged to take part simply by seeing how little commitment it takes to join in and how easy it is to leave. As a result, the ease in which it takes to join Anonymous could suggest that collective action is an easy activity and increase participation numbers.

Another way in which Anonymous transforms perceptions of society through their various twitter accounts is through regular reminders stating who they are and what they stand for. In doing so, the collective are transforming perceptions of the self. They will often clarify points of contention, for example their specific ideologies, their membership, or. They will regularly tweet that “Anonymous does not mean unanimous”. The result of this is that they are changing the narrative from the traditional teenage hacker alone in his bedroom, hacking for fun to politically motivated individuals who come together to undertake specific operations.

> *“Something that needs to be addressed. To be clear, #Anonymous does not mean unanimous. Our collective as a whole do not always agree nor collaborate in all operations.*

[76] https://www.occupy.com/article/we-are-still-99-percent Last Accessed 1 March 2021.

However, it is imperative that our most influential voices and outlets are not sharing conflicting messages.”
“Anonymous exists in perpetual puberty, constantly reinventing itself. With each update, pundits claim new accounts are not the ‘real’ Anonymous. All Anon accounts are “fake” to a personality-driven world as they are set up around ideas, movements, and resistance, not individuals.”
“We are interventionist. We are hacktivist. We are journalist. We are activist. We are justice. We are legion. Expect us. We are from the internet. We are #Anonymous. We are everywhere.”
“Remember, #Anonymous isn’t unanimous. Most Anons don’t know the identity of others. We are Anonymous for a reason, after all. We don’t agree on everything other members of Anonymous say/do. I not how this works. Important to remember we are all human beings too. Or are we? 👽”
“Anyone“can” "be“ or "”claim" actions in the name of Anonymous. Whether or not those who claim membership agree’, it's part of the big picture.”
“It is not time to stop, fight for: free society, free healthcare, free education, justice and equality will continue https://t.co/Qudf2P7o69”
“There's people trying to divide us based on what twitter account is the "real" Anonymous. There is no official Anonymous twitter account. If you're against corruption and for the free flow of information and pro human rights, you too are Anonymous.”
“#Anonymous is and will always be antifascist. We're against oppression and will continue to fight it in all forms.”

They have also distanced themselves from others that originated from the same message boards and at around the same time but have diverged in their ideology.

“@Hexpatriot @JoeBiden As much of the dumb f*ckery that existed in the hacker scene from wannabe libertarians, not equating that to now. It's gone full fascist. If some of our old friends are there and want an excuse to be butthurt, here's“the "f*ck off and”die."”

> *“@Hexpatriot @JoeBiden Except, this admin didn't. Never been interested in cults. Our colleagues who went right wing bat sh*t? Not really a concern. Their choice. They want to feel attacked by a call for justice? So be it. Good riddance.”*

Interestingly, some of the accounts will outline their ideologies specifically claiming that other Anonymous accounts may not agree with them but that their account specifically stands for certain ideals:

> *“We are Anonymous not unanimous, if you see other 'Anonymous' accounts posting unsubstantiated conspiracies, empty threats, vague calls for violence, race baiting, or in general trashposting it has nothing to do with @YourAnonCentral; it's on the user/or account that posted it. 📝 https://t.co/rvS0XEivSt”*

They will also offer advice on how to make sure the audience is following a reliable Anonymous account ensuring any disinformation posted by other non-reliable Anonymous accounts are discredited:

> *“There are no official Anonymous accounts, however, some are more reliable than others. A common practice to verify if someone is reliable is to search through their stream for consistency, see the date of creation, number of followers &amp; if the followers are authentic or reliable. https://t.co/GaYGX8B8bh”*

> *“You can follow us or other Anonymous accounts we follow, we work based on trust networks. If we do not follow an account, it isn't part of our trust network.”*

> *“For the record: We don't tweet news without searching.”*

In a similar vein, the Belarusian Cyber Partisans will retweet news and expert tweets praising their activities in order to promote their activities and ensure they are seen positively by followers.

> *One of the feistiest, well-organized and accomplished hacktivist groups are the Cyber Partisans (@cpartisans) from Belarus. A few of us hosted them yesterday and you can see a*

recording of the event--2 short talks and a long Q&amp;A with them--here https://t.co/ePXmqg7fbl
@vmyths Not a single person got injured from our attacks. This attack is not even terrorising anyone.. its goal is to release ill political prisoners and prevent a war

While the hacktivists will transform their perceptions of the self, Anonymous will also transform perceptions of their opposition. They do this predominantly in two ways. Firstly, they will portray their opposition as demonic, evil and conspiratorial using highly descriptive and emotive language to ensure audiences take notice.

“This is a police state. NO FREEDOM”
“Saturday: A woman suffering from a seizure was handcuffed by police and deprived of medical attention”
“Yaquis: The Story of a People's War and a Genocide in Mexico https://t.co/Snm04cFpAF via @intentlcry”
“Israeli forces violently raid Palestinian home before razing it to the ground”
“#LeyFayad is the most authoritarian anti-dissent law in America to be proposed to date. Thanks to this pendejo who wrote it-- ;@omarfayad”

The second way Anonymous do this is by trolling their opposition. Trolling is described as “to antagonise (others) online by deliberately posting inflammatory, irrelevant, or offensive comments or other disruptive content.”[77] This tool has been used by Anonymous from their inception on the b/board section of 4Chan. This is one of the places that trolling on the internet originated from with users trying to lambast each other in increasingly epic proportions. Tech magazine gizmodo states that “In early internet usenet forums, they were the people being assholes simply for the sheer joy of being an asshole”[78]. In an interview with CNN, a member of Anonymous described their use of trolling as: “Instead of gunpowder, Anonymous uses the

[77] https://www.merriam-webster.com/dictionary/troll Last Accessed 2 Dec 2021.
[78] https://gizmodo.com/the-first-internet-troll-1652485292 Last Accessed 1 March 2021.

internet. Anonymous attacks its targets by flooding and crashing corporate and government websites or digging up and publicising highly embarrassing information. It's called trolling. They troll targets out of genuine outrage but also just for fun."[79] Contrarily, Coleman stated that Anonymous were no longer internet trolls and had instead become a collective form of action catalysed by political issues and world events (2011). Based on the tweets, however, it seems as though Anonymous use trolling for ideological purposes ensuring the audience sees the opposition as weak, clumsy and powerless. Indeed, they have even explained that their opposition cannot grasp the concept of trolling for political purposes:

"*Seriously, the right wingwill never get trolling. The idiots involved in that ideology, and the clueless lazy media, has confused merely posting obviously offensive, but ultimately banal, comments as "trolling.""*
"Hey dumbass, global warming doesn't only mean extreme heat; it means extreme weather. Hot and cold. Maybe buy a thermometer and shove it up your ass. https://t.co/wdO0t0nPiY"
".@realDonaldTrump, you are embarrassing our country and the millions of Americans who fought and died to defeat Nazism."
"Let the message be clear. This is a big fuck you to #ISIS and all #Daesh RT to support the cause. #OpParis #OpISIS https://t.co/bPDGCvZn1I"
"You are fired @RealDonaldTrump. Joe Biden has been elected the 46th President of the United States of America. And Trump is going to prison. https://t.co/aPgwaUTMn9"
"So, @realdonaldtrump and @RudyGiuliani walk into a bar. Bar tender asks "what'll you have?" The Donald says "I don't drink." Rudolph says "Sex on the beach" to which The Donald replies, "bar tender, you don't sell 15 year old Kazakhs here, do you?"""

Using all of the evidence above, it is clear that the different hacktivists do use various rhetorical mechanisms to alter their audience's perception of society and themselves. They post information style bulletins and reports on their Twitter accounts in an attempt to garner support for their various causes and also in an effort to encourage audiences to inform themselves

[79] https://www.youtube.com/watch?v=4EVMRH8S7OA Last Accessed 12 March 2021.

surrounding specific topics that the collective find unacceptable. Additionally, they will employ rhetoric that supports the idea of an ‘us vs them’ dichotomy ensuring the audience feels included and are aware of who the enemy is. They will regularly name their various opponents in their tweets including Lukashenko, President Trump and Israeli forces. Moreover Anonymous, who use this function more so than the other accounts, will use plural pronouns and call themselves the 99% in an effort to recruit and empower their audiences. The different hacktivist collectives will also use multiple methods to transform the audience's perception of themselves and their opposition. Methods used in altering perceptions of the self include stating the aims of the collective, correcting false narratives surrounding them, reposting their praise and by clarifying points of contention. The methods they use to transform the audience’s perceptions of their enemies revolve around using highly emotive and violent language when discussing the perceived transgressions of their enemies and ‘trolling’ or belittling their opponent which in turn takes their power authority away from them and encourages audiences to engage in collective action.

3.3. Prescribing Courses of Action:

The third function that social movements will employ in their rhetoric as suggested by Stewart revolves around the idea of how the movement wants to affect change, and prescribe and defend these ideas. Social movements should lay out demands and solutions that relate to the movement’s goals while specifically assigning tasks to people. In doing so, the social movement can demonstrate that despite being a non institutionalised collective they still have the ability and the personnel needed to affect change. The social movement analysed should also detail the communication channels that should be used and explain why they have selected them. These choices need to be justified to both members and external audiences.

Hacktivists, however, are not the same as more traditional social movements. This is due to a variety of reasons including the illegality of the methods they use, the anonymity they maintain at all times and the decentralised nature of the different collectives. The result of this is that they are less likely to allocate specific tasks to specific people. Furthermore, the majority of specific operations are planned on a decentralised level whereby individuals will volunteer to take action as opposed to being assigned tasks. As Chaos Computer Collective, Belarusian Cyber Partisans and Anonymous are all leaderless networks and as such do not follow traditional hierarchies while Ghost Squad Hackers are led by hacktivist S1ege. For leaderless collectives, a member might put forward a specific operation which, if it interests enough members may then proceed. However, with regards to Anonymous Olson has claimed that it is not as leaderless as they try to project (2013). Rather, there is a core number of hacktivists who will meet in secret IRC channels and plan operations. These plans are then spread to the wider network. Additionally, it could be argued that those who are tasked with managing the social media accounts of the hacktivists could be seen to be leaders as they ask their followers for specific tasks. These tasks will very rarely ask followers to engage in explicitly illegal tasks on a public platform such as Twitter. However, they do prescribe a few different types of actions to followers without specific tasks being allocated. There is a mix of tasks that occur offline and those that occur online.

Firstly, Anonymous have used their various twitter accounts to ask their followers to engage in both illegal and legally dubious methods. There are a few instances of the collective asking for information in order to DOX certain individuals they believe to be wrongdoers. They have also asked their followers to illegally download JSTOR articles to ensure the torrent started by Aaron Swartz remains active and they have called for followers to engage in DDoS attacks. Additionally, the Ghost Squad Hackers will also ask their followers to download frameworks and spread leaked data.

“The best tribute to #Aaron Swartz would be to keep this JSTOR torrent alive. Lasting legacy of a great prodigy - https://t.co/6FQcFQtSao …”
“If you recognize any of the Nazis marching in #Charlottesville, send me their names/profiles and I'll make them famous #GoodNightAltRight https://t.co/2tA9xliFVU”
“Shutdown!!! http://t.co/MvxbN6SfpP #TMTshutdown #DDoS #WeAreMaunaKea #ProtectMaunaKea #MaunaKea http://t.co/6asGJV6GBX”
“#DDoS against site of #Hawaii government https://t.co/tlqkwaOBSL\nSTOP ecocide and native rights abuses #WeAreMaunaKea http://t.co/Oh1MOq9Y5N”
RedGhost, a new #Linux post exploitation framework is now available in Github, designed to assist red teams in gaining persistence, reconnaissance and leaving no trace. *https://t.co/fe2zhYbbTm https://t.co/exZq09g8JP*

Re-Upload of #OpDecryptIsis Leak:

-&gt; https://t.co/yNJtg25XOv &lt;-

Download and re-upload on other platforms to help spread the data on these admins. Isis is trying very hard to prevent this data from becoming public. https://t.co/g1MvB4lkJ9

The majority of each of the accounts calls to action are mostly focused on legal methods of collective action. Anonymous regularly posts symbolic calls to action asking followers to ‘raise their voice’, ‘fight for freedom’ and to ‘take a stand’. One could argue that in prescribing symbolic courses of action then the collective may not actually be asking their followers and members to engage in any tasks. However, they often ask followers to educate themselves and to then plan their own action.

“We hope this is the beginning of a real change. Raise your voice loud and clear. We are legion. #anonymous”

“Raise your voice for freedom #FreeMartyG #savemartyg #saveArash #SaveAli #FreeLauri”

“This November 5th remember the countless reasons to stand up

#FightForFreedom #RiseUp

#RevolutionNow #MMM2020 #MMMLondon #anonymousnews #Anonymiss #NoWarOnIran #FreeAssange #freechelsea #anon”

“Stand with human rights defender #IssaAmro -- facing Israeli military court for nonviolent resistance”

Another way in which both Anonymous and Chaos Computer Club will ask followers to inform themselves is by posting specific advice on how they can protect their privacy and themselves online by outlining companies that may not see user privacy as one of their main objectives and by posting advice articles on their websites and linking to these on their Twitter accounts.

“Cant understand the scandal now about BigData. We have known it for years! A tip: #deletefacebook and staying on others Social Networks is hypocritical/quite stupid. All provide data to influence your decisions. Do whatever you want, but do not let the media tell you what to do.”
“Drop whatsapp. Use Signal. Protect your privacy”
“Ultimate Guide for #Anonymous and Secure Internet Usage v1 http://t.co/qNj7Z7F6 #newfag #info”
“#OpSingleGateway Guide on how to use TOR even if it's blocked by your Gov. (English/Thai) https://t.co/VUNDUnReWG https://t.co/526L3ISDZu”
“Dear Twitter user, Please do not: Click on strange web links. -Discuss with fake accounts or strangers who offer you things. -Download very suspicious software or documents. -Disclose your private information to strangers or fake accounts.”

Additionally, Anonymous, Chaos Computer Club and Belarusian Cyber Partisans have asked followers to engage in low stakes efforts to engage in a specific operation or to support different social movements that they support. This can involve signing petitions, reading open letters both of which will relate to their operations or campaigns. They will also ask followers to watch specific videos or to find out about projects that the collective supports.

*“**URGENT**nPlease Sign Important Petition Solidarity with Palestinian #HumanRights defender #IssaAmro #FreePalestine”*
“WE WANT #JusticeForCornelius Shut Sequel Down! PETITION: https://t.co/wnGkP2qGZa”
“Sign this petition to demand an end #InstitutionalizedAbuse #FreeMartyG https://t.co/CpSIu67JTr https://t.co/TtIQTFSLxs”

“MUST WATCH 💔 Australian film 'Stone Cold Justice' on Israels torture of Palestinian children #Vimeo https://t.co/CPfaVgPjIW Zionism = Hell”
“Watch all of this. https://t.co/YHq0QhXrnw https://video.twimg.com/ext_tw_video/1267945429213167616/pu/vid/720x1280/hsXuIyWmIe-7epsB.mp4?tag=10”
Our friends started to release videos about #belarusian punishers [❗ Eng subtitles]. Via the link below you can see who threw hundreds of people in prisons for fake reasons. They cannot be called "your Honor" and will be prosecuted when the time comes. *https://t.co/naiUY5eJYd*
If you want to learn more about our work and thoughts on politics and future of #Belarus watch the conference hosted by @Harvard and @Yale. Now with Russian subtitles. Thanks to all organizers for their interest and support. Long live Belarus✊ *#hacktivism* *https://t.co/qxuFJAEuRU*
Biometric mass surveillance in Germany, the Netherlands, Poland. What can you do? Your voice can help: #ReclaimYourFace https://t.co/O2qCCpRrlx

Anonymous will instigate Twitter Storms in an effort to raise awareness of an issue and increase the chance a hashtag might go viral. This type of Twitterstorm has been defined as: “in its purest form, this is a story that sparks a very significant volume of messages on Twitter but is largely of interest only to a specific group and receives little or no interest from mainstream media.“[80] It could be argued that these organised Twitterstorms are most in line with the function of prescribing courses of action as they are referring to a specific activity, at a specific time in a specific virtual location.

[80] https://www.theguardian.com/media/greenslade/2011/dec/09/twitter-social-media Last Accessed 14 April 2021

“Twitterstorm: 5/17 Sunday 2:00 pm EST. Be ready. #LoraxLives #OpCyberPrivacy #CyberFail #Privacy http://t.co/eKCfFNukjY”
“Support #LoraxLives Twitter Storm 5-17-15 2pm EST =-= https://t.co/Lvj85XwJbP =-= http://t.co/Rxx4h0r43W #FreeAnons http://t.co/uWB3SYE3Bh”
“Online hactivists #Anonymous escalate Twitter war against #ISIS: http://t.co/P1LcUMm0AM http://t.co/vLL3n85GMD”
“Get ready for todays twitterstorm re Turkey's invasion in Kurdistan with the hashtag below. 10pm Kurdistan 9pm Europe 8pm London 3pm New York https://t.co/ttvLJrwz5d, http://pbs.twimg.com/media/EbnLWaGXYAI6YEU.jpg”

These efforts link back to the critiques of slacktivism, as detailed in Chapter 3, with regards to online protest efforts with some theorists detailing how far removed these actions are from the actions of past social movement efforts such as the civil rights movement. Yet, Sauter argues that the comparison with traditional movements and online movements is reductive and unnecessary (2014). Anonymous has acknowledged the slacktivism critiques in a few of their tweets and explained why it’s important to engage in low stakes activities and what can be achieved.

“wHaTs SiGnIng a PeTiTioN goNnA dO” https://t.co/v6Y6B5NFB8”
“It's a small Step to sign a Petition but maybe a Important one. https://t.co/efezC8Dhdq”

Another way in which Anonymous prescribes online courses for action on Twitter is by asking followers to support members of the collective that have been arrested and are serving prison sentences.

“@anonops one of the Anonymous arrested in Spain has been released. But about the others I can't say nothing. I WANT THEM FREE RIGHT NOW!”
“Join us! Demand justice for jailed activist Marty Gottesfeld! https://t.co/UD7hqSRhBg #FreeMartyG #CFAA #Anonymous https://t.co/Hxz3HNzWHX”
“Tomorrow I'll launch a campaign for a jailed activist facing Computer Fraud & Abuse Act #CFAA charges for allegedly working with #Anonymous”
“Our co-founder has been in federal prison for the last 6 months. Find out why! https://t.co/bLjbPqVLIj @FreeMartyG https://t.co/YeiOBy5txP”
“\u25baDOWNLOAD ORIGINAL FREE #ANARCHAOS http://t.co/JxiqorXWMg #Anonymous #J20ForJeremy #FreeJeremy http://t.co/tI8VmgJc88 @OpGreenRights”
“If you've wanted to write #FreeLorax but not sure your message will get there, cross my heart #FreeAnons delivers https://t.co/sL0lRTYUnT”
#MattDeHart needs mail! Show him some love! Matthew Paul DeHart #164682, Warren County Regional Jail, 920 Kentucky St, Bowling Green, KY 42101

Although the majority of Anonymous’s requests refer to activities that can be undertaken online such as following an account or even the more legally dubious methods they use, the collective as well as the other hacktivist accounts will occasionally call for more traditional offline protest efforts. These can include calls to join specific organised protest marches such as the Million Mask March or marches relating to Operation Green Rights (also known as Operation Monsanto). They will also ask followers to join marches relating to other social movements such as the Black Lives Matter marches. They also released guidance on how to behave during the marches.

“BLACK MARCH - JOIN US! & EXPECT US! info &gt;&gt; http://t.co/hPMfAbFW”
“March to #TahrirSquare from Giza on the one year anniversary of Egyptian Revolution LIVE NOW &gt;&gt; http://t.co/4NxNivfK”
“#OccupyLondon We march to fight government funding cuts and a massive hike in tuition fee. We do it NOW. We are on time! JOIN US!”
“#MarchAgainstMonsanto Official Press Release http://t.co/ETWC0hYBHU\nWorldwide Online Event:http://t.co/JJ1QEjlbTF http://t.co/jqzaR86w65”
“There are a lot of women's marches going on across the globe. Find one and join! #WomensMarch https://t.co/BnTPwK82a4”
“If you're attending the #MillionMaskMarch you need to know: 1. You do not need to answer police questions. 2. You don't have to give personal details under stop and search powers. 3. Ask "under what power?" to challenge a police officer telling you to obey instructions. https://t.co/tO9x4z40UT”

The Chaos Computer Club will also ask followers to join in their events, workshops and hackathons that occur both online and in person.

December 27-30 online and in your local hackspace: Remote Chaos Experience #rC3 – Baut eure eigenen Welten. Werdet kreativ! https://t.co/fnFxgicwmU
Save the date! 25. bis 31. Oktober: Die #pw21 findet noch einmal vollständig online statt. Das Team der #PrivacyWeek freut sich über tatkräftige Unterstützung: Engel werden! https://t.co/bZd9IC4uWC
Workshop on Wednesday, March 24th, at 18:00 CET, will take about three hours, held online via Jitsi: Symbolic execution with #angr – for code verification, bug hunting, and reverse engineering https://t.co/7QUQRfsQWU

Anonymous has also called for followers to boycott specific organisations or governments and to organise their own protests regarding a specific issue. Moreover, throughout 2020 Anonymous repeatedly called for their followers to wear face masks or coverings and have offered advice on how to male them to ensure a reduction of the spread of Covid19.

“This is horrific! https://t.co/sCAd9tqxLS #BoycottIsrael #BDS”
“How to help Nigeria #EndImpunity 1 Organize protests at nearest Nigeria embassy. 2 Present evidence of crimes by Nigeria government to your politicians &amp; media. 3 Pressure your government to demand answers from the Nigeria government. #BuhariResign”
“Please don't forget to wear masks as you protest or vote. Wash your hands, practice social distancing, and let's end global tyranny and #COVID19 Together. Instructions on how to make a #COVID19 mask safely and quickly. #Masks4All: https://t.co/Gx5uSe7MEe”
“Wear a mask https://t.co/pFWUNiwdNH”

Interestingly, the Anonymous Operation #OpSafeWinter calls for predominantly offline methods. #OpSafeWinter is a long running campaign whose aim is to “ get Anons and “civilians” out into the streets all over the world to save lives by giving the homeless and the critically poor the tools they need to survive at least one more season.”[81] In the original call to action posted by Anonymous in 2013 they asked for members to “list the current homeless count in alphabetical order by town/City Country” and to then “coordinate with anons and others willing to participate in the execution/distribution of services we are able to provide. Whether its transport, collection of donations etc.”[82] Despite the fact that #OpSafeWinter is a long-running operation, it was not included in the Hackmageddon dataset due to the fact that it is a predominantly offline effort which has not resulted in any hacks that were written about in the media. In the tweets analysed that use the hashtag #OpSafeWinter, the collective calls for donations and asks their followers to volunteer in homeless shelters and soup kitchens.

[81] https://www.dailydot.com/unclick/op-safe-winter-anonymous/ Last accessed 1 March 2021.

[82] https://pastebin.com/Hp772vVW Last Accessed 2 March 2020.

“There are no words, please help where you can, please #OpSafeWinter https://t.co/AreJLApk06”
“Unite in every town/city to help the homeless. Get involved in your local soup kitchen or #OpSafeWinter if u don't have one near start one. Winters here it's freezing out u may save a life, councils aren't. #NoMoreDeathsOnOurStreets Follow @streetskitchen”
“As winter grows near, keep the homeless in mind. Any thing you can do to help makes a difference. #OpSafeWinter is back in full-effect.”

After having identified numerous tweets that prescribe courses of action, it is clear that this function is used by all of the different hacktivist accounts in their communications to their followers. However, they will never prescribe a task to a specific person due to both the anonymous and decentralised nature of the different collectives. Rather, those that manage the accounts will address their followers and anyone interested in specific operations to engage in collective action. All of the hacktivists ask their followers to predominantly take action via legal means. These methods can vary starting from actions that can only be taken on Twitter such as Twitterstorms or following specific accounts to asking followers to sign petitions and outlining how this can help. They offer guidelines followers should adhere to in order to remain safe online and post symbolic messages asking their followers to take notice and rise up. However, they don’t simply prescribe online courses for action, they also ask followers to engage in offline collective action. This includes taking part in their yearly Million Mask March and taking to the streets to ask followers to donate and volunteer in order to assist homeless people over the winter months and asking their followers to take part in their workshops and events. As a result, although not adhering to each of the guidelines laid out in this specific rhetorical function such as outlining who should undertake a task, the different collectives’ methods for change are outlined.

3.4. Mobilising for Action:

The fourth function identified by Stewart that movements should include in their rhetoric to followers and the outside world is focused on mobilising for action. This can be broken down into organising discontent, gaining sympathy and attention or to apply pressure on the movement's opponents to gain recognition from its antagonists. This function is predominantly used as a way of uniting and organising their followers and members into engaging in specific change-oriented actions or by engaging with agencies of influence. The function can be utilised by the movement in order to gain sympathy, provoke attention and outrage or to apply pressure on the opposition. Social movements need to convince followers that a victory will occur and is close as long as followers are committed to the hard work needed to effect change and remain united in their goals. This is what Hoffer describes as “extravagant hope” (1952).

As mentioned in the various functions above, the different hacktivists use a variety of methods in order to mobilise their followers for action. Anonymous unite their followers with the use of plural pronouns in their tweets, through the use of an ‘us vs them’ dichotomy and by using stirring rhetoric in order to inspire followers to take action. They also use trolling as a way of pressuring the opposition as well as specifically tagging them in their tweets to ensure it gets their attention. Additionally, they have previously engaged with agencies of influence, in particular other global social movements. They use visceral language and post sensitive images and videos in order to gain sympathy and provoke outrage. The Chaos Computer club, on the other hand, will regularly post about cases and judgements questioning whether the right decision was made and will ask their followers questions in order for them to learn more. The Belarusian Cyber Partisans predominantly pressure the opposition with a list of demands.

Firstly, as outlined in the ‘Transforming perceptions of society’ function, Anonymous will use the ‘us vs them’ dichotomy in order to bond their followers and separate them from the enemy. In doing so, the audience is united in a cause and more likely to mobilise themselves to take part. Moreover, in using the plural pronouns to unite their followers, they will more often than not follow it with mobilising rhetoric as below with the collective encouraging their audience to feelin involved and take action.

“Raise your voice loud and clear. We are legion.”
“We remember when kings preceded their armies, when today they hide in holes. #Anonymus #Anonymous”
“We are one #MilionMaskMarch #MMM2018 Barcelona”

> *“Repression of peace and love for nature will not be tolerated. We are ready to take revenge. #Paris #ClimateMarch https://t.co/1pbt7fiv9j”*

Again, as with the second function outlined by Stewart, Anonymous and the Belarusian Cyber Partisans will also unite their followers by naming their opposition ensuring their audiences can unite against a common enemy.

> *“@OpGreenRights these guys, Cobble Hill Holdings and South Island Resource Management. Shawnigan water bad guys https://t.co/UHtuFIz3rU”*

> *“If you don’t want @BorisJohnson &amp; @MattHancock to get away with yet another one of their scams RT this to the country”*

> *“@Stratfor: "We will not be victimized twice by submitting to questioning about them." Sorry, but you can not avoid your responsibility.”*

> *“Do you remember Judge Adams beating daughter for using the internet? http://t.co/RS0CqnSk He made $49K during first 4 months of suspension”*

> *We #Hacked another database: we know who and when crosses the border of #Belarus including Lukashenko's personnel and dictator himself.*
>
> *We are checking ALL KGB officers who went abroad on operational assignments. No one will escape us, no one can hide.*✊
>
> *https://t.co/Ehb6jaGCVF https://t.co/cReGuLmd3q*

Both collectives will also attempt to show how their enemies are restricting freedoms and transgressing common norms in order to dehumanise them.

“They use the hatred toward nature for their dirty money and after force against people who seek love #cop21”
“The UN said that Bradley Manning's treatment was Cruel and inhuman. Will the United States of Arrogance give a shit? That's up to each of us”
“@anonops Irish government passed SOPA without vote! 80,000 signatures oppose and Irish music industry for .Democracy dying at its finest”
@Farnakyboy @TadeuszGiczan @bneeditor Such actions are a response to lukashenko torturing and killing belarusian people.

As well as uniting their followers against a common named enemy, both Anonymous and Belarusian Cyber Partisans will also provoke the enemy by trolling them and oftentimes including their Twitter handle in the tweet to ensure the opposition is notified of the tweet.

“So which prison are we sending @realDonaldTrump &amp; company to?”
“Don't donate. Just let @realDonaldTrump declare bankruptcy here as well. He knows how to do it. LOL! https://t.co/7wTcLoDPRI”
“.@ChiefMI6 When does it become politically 'unacceptable' for the UK government to continue its close support for Turkey's President Erdogan, a leader known to have supported the Islamic State and who is guilty of war crimes against the Kurds, as documented by the United Nations? https://t.co/yjCYqiQATy”
“We can think of no more fitting portrait of @realDonaldTrump to go up in the White House. https://t.co/3eLi9Eelxp http://pbs.twimg.com/media/EmRLUsoWMAAnSEq.jpg”
#Hacking of the internal mail system of the Belarusian MIA continues.♨

Yes, we are still reading your mail, and there is nothing you can do about it.🤷‍♂️😎 *You have been hiding your crimes for 27 years - the time has come to find out the truth.*

#cpartisans #suprativ #Resistance https://t.co/6DGh48o1rO

All of the hacktivist's enemies are always either people in positions of power, governments or multinational corporations they deem guilty. The accounts linked to specific operations tend to focus on one enemy, for example OpIsrael predominantly states the Israeli government and defence forces as their opposition. Alternatively, the more general Anonymous accounts will find enemies in many different national governments and multinational corporations depending on the issues at the time.

Operations Twitter Accounts:

OpIsrael - *"Only 68 years of land theft, murder and ethnic cleansing by #Israel apartheid regime!"*

OpRussia - "*New "rallies law" destroys freedom of assembly in Russia and banned our masks. #faq #Anonymous #Russia"*

OpLastResort - "*Anonymous video message to Gen. Michael Hayden and his coterie of capital cunts: http://t.co/s2kqkLISVY Study carefully; contains warnings."*

General Anonymous and non-Anonymous Affiliated Twitter Accounts:

TheAnonMovement - "*A #CivilWar is now inevitable in the United States. Trump has declared war against his own people. This will not sit well with the extremes of either side, and will irrefutably incite further and harsher violence. The #Dictatorship is now in full effect."*

YourAnonCentral - "*Trump is cancelled, no immunity and no impunity. LOCK HIM UP. #EndImpunity https://t.co/96BbOYNmRE"*

YourAnonOne - “*#US: Police in West Hollywood, California brutally beat and repress anti-police impunity protestors, pedestrians, and drag motorists out of their cars. In latest series of human rights abuses. (📹@PplsCityCouncil) #JusticeForBreonnaTaylor #BlackLivesMatter*”
Chaos Computer Club - *Kidnapping and other extreme measures: U.S. intelligence secret plans against #WikiLeaks https://t.co/03ZItHZbCR #Vault7*
Ghost Squad Hackers - *#GhostSquadHackers is tired of the war crimes* *Bashar al-Assad is getting away with we declare all out war on the Syrian Government #OpSyria*

While the hacktivist accounts provoke their opposition in a variety of different ways, another way in which Anonymous mobilises for action is by engaging with different agencies of influence in the form of other more established social movements that are predominantly based offline. Indeed, in the early days of Anonymous when they rose to prominence, they engaged a great deal with the Occupy movement. News outlet, the Fast Company, wrote in 2011 that “Anonymous has caught the attention of the media–and even Homeland Security–with its biggest contribution to Occupy Wall Street: hype.” However, Anonymous had engaged with the precursor to the Occupy Movement by collaborating with the founder of the 99 percent movement after their website had been taken down by hackers. Anonymous are still engaging with other movements at present by taking part in the Black Lives Matter movement and global climate protests, albeit in a mostly online manner.

“Big #Occupy protest in #NYC right now. Cops are out in droves barricading Union Square #OWS”
“#OurPolls OCCUPY THE VOTE - ELECTION SEASON 2012 - Your politicians have been bought (via @OurPolls)”
“Hyde Park for Black Lives Matter protest #BlackLivesMattter #blacklifematters #LondonBLM #londonprotests #LondonTogether https://t.co/Vy6CCkSwfo”

“Black Lives Matter, keep the movement going”
“In August, 43 black ppl were killed by police including Mike Brown. That's the most ever recorded. Protests ignited. http://t.co/TcY5rHoQJM”
“#ClimateMarch amazing picture from #wien in #Austria #systemchangenotclimatechange! https://t.co/zC5cEvImTD”
“People power in Madrid with the #ClimateMarch @greenpeace_esp https://t.co/Yce4n8Sq1j”
To all the racists, especially those in positions of political power. This is for you. #Anonymous will boost the #BlackLivesMatter movement to a unprecedented level. This time, it will not go unanswered. Changes are coming, and rest will not be had until they’re here. #ExpectUs https://t.co/1yotvNtVc0”

By engaging with other social movements of influence over the 2020 Black Lives Matter (BLM) protests, Anonymous saw a large surge in support.[83] The collective saw millions of new followers on its Twitter profiles as well as a vast number of people sharing their posts as a result of some of the collectives most followed accounts posting pledging their support to BLM protesters against police brutality and racism that occured after the death of George Floyd in Minneapolis. As a result Anonymous posted *"Ok. We don't know why we got 3.5 million new followers, putting us at 5 million - but if you're new to our feed, and you're not a bot we can be pretty gruff. We don't mince words, we tell it like it is and when we want lulz, it upsets many people. Welcome aboard."*

The Chaos Computer Club have also engaged with other organisations, however rather than protest movements they will engage with civil society organisations such as the Electronic Frontier Foundation. By engaging with these organisations they are asserting that they should also be seen to be an established movement.

[83] https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-activists-online-george-floyd-protests-black-lives-matter-a9544261.html Last Accessed 5 March 2021

Open letter of 20 user rights organisations on #Article17 and #Uploadfilter published today https://t.co/T4MqySYcdk
Amnesty gagged in #spyware case: Closed-door hearings in Amnesty International's legal bid to stop #NSOGroup exporting surveillance software https://t.co/BB7nho5LY1

An alternative way Anonymous attempts to mobilise their audience for action is based on the type of rhetoric they use. In the tweets analysed they will often use visceral and shocking language as well as images and videos depicting sensitive topics in an attempt to provoke outrage in their audiences increasing the likelihood that they will mobilise themselves and join in in future protest activities. This is a function that Belarusian Cyber Partisans also employ. Jasper has claimed that inducing anxieties can help recruit people to new forms of action, including protest (2011). Indeed, Jasper states that "one way that activists try to recruit others is by creating or taking advantage of moral shocks, information or events that [...] suggest to people that the world is not as they had thought. Their visceral unease occasionally leads to political action as a form of redress (Jasper 1997)"[84]. As a result, it could be argued that Anonymous are indeed inducing anxieties and taking advantage of moral shocks in order to increase the likelihood that their audience will engage in political action.

"#IOF assaulted the Palestinian young man Firas Jarjour, from Bab Hatta neighborhood in #Jerusalem #Palestine"
"Hey #USGov, remember when you "involuntarily reassigned" some of us to prison? Because we do... http://208.118.246.130/involuntary.png!"
"Survivors from the residential facility New Horizons discuss the torture they experienced witnessed https://t.co/1qHnUmVIqu #OpLiberation"
"U.S. security forces brutally beat 16-year-old child Jahmel Leach (now has his jaw wired shut), tased him in the temple, stripped him (abused him), and then threw him in an adult cell while refusing him medical attention or his parents. #BlackLivesMatter https://t.co/HAxaTJYyzb"

[84] https://canvas.harvard.edu/files/3747722/download?download_frd=1 Last accessed 14 April 2021

“The mass rape raises concerns about the safety of women on flights connecting through Doha and the suitability of Qatar hosting the 2022 world cup. Qatar refuses to acknowledge any wrongdoing or apoloize. https://t.co/PxKzYAnUTy”

However, the language used when members are communicating to one another in the public AnonOps Webchat is very different to that used on Twitter. This is more in line with Coleman’s analysis of their language whereby she claimed that Historically, Anonymous would communicate in “a language that seems to have reduced English to a bevy of vicious epithets, sneers, and text-message abbreviations. This may be shocking to outsiders, but for insiders it is the normal state of affairs, and one of 4chan’s defining and most endearing qualities.”[85] This could be due to the fact that the collective needs outsiders to take notice and as a result can no longer use the language that they had originally used on 4Chan when communicating to the outside world. Indeed, as opposed to the aforementioned tweets in support of the Black Lives Matter movement, below is an extract from the AnonOps Chat Log whereby the Black Lives Matter Movement and racism as a whole is discussed. As mentioned by Coleman, this extract features a combination of ‘vicious epithets, sneers, and text-message abbreviations’.

```
“03:24 < sirWCA> colmustard: how do you feel about the black lives matter movement
03:24 < ColMustard> that is crony capitalism, as are the endless regulations  that harm small businesses in  favor of larger ones, and several other things.  it is not real capitalsim, it is not the free market.
03:24 < Skyy> words of wiseman donald trump
03:24 < Skyy> â€œI will build a great wall â€“ and nobody builds walls better than me, believe me â€“ and Iâ€™ll build them very inexpensively. I will build a great, great wall on our southern border, and I will make Mexico pay for that wall. Mark my words.â€  Read more at http://www.marieclaire.co.uk/blogs/550112/donald-trump-quotes.html#3cwe583L3fITCILj.99
Read more at http://www.marieclaire.co.uk/blogs/550112/donald-trump-quotes.html#O6wV8Opj49zlopEr.99
03:24 <+Meow> Title: 24 Of The Most Outrageous Donald Trump Quotes  | Marie Claire (co.uk)
03:24 < cryptomillz> meow
03:24 < ColMustard> sirWCA: I think they are detrimental to what the masses want.  I think that it is a well funded top down not grassroots movement
03:24 < Skyy> â€œI will build a great wall â€“ and nobody builds walls better than me, believe me â€“ and Iâ€™ll build them very inexpensively. I will build a great, great wall on our southern border, and I will make Mexico pay for that wall. Mark my words.â€
```

[85] https://www.canopycanopycanopy.com/issues/15/contents/our_weirdness_is_free Last Accessed 3 March 2021.

```
03:25 < ColMustard> the soros leaked documents prove that it is top down.
03:25  * Dzl grabs popcorn
03:25 < sirWCA> im not sure if sky quoting donald trump is worse than the singing that came before
03:25 < sirWCA> still want to kill myself
03:25 < Skyy> i sing great
03:25 < Skyy> shhh
03:25 < ColMustard> when they make claims of racism and it turns out that there is no racism it diminishes any legitimate claims of racism.  people stop listening because they have already discovered at least some false claims.
03:26 < rocket> like CNN and pepe
03:26 < cryptomillz> racism
03:26 -!- squared [squared@quadratus.anon] has quit [Quit: after walking the plank, squared now patrols the water in a yellow submarine.]
03:26 < cryptomillz> can we talk about racism
03:26 < Dzl> Nigger.
03:26 < zu> its for the stupid
03:27 < cryptomillz> damn the hard "r"
03:27 < Dzl> Yes everyone knows white is the master race.
03:27 < rocket> moon crickets :D
03:27 < cryptomillz> lmao”
```

If the collective were to use this language in their tweets to outsiders they would not garner the sympathy needed from outsiders to support their causes and could provoke outrage aimed at Anonymous themselves rather than the opposition.

The final way in which Anonymous attempts to mobilise action from their audiences is through their use of stirring and inspirational speeches with occasional claims that victory is near. In these tweets, they will claim that change is possible and should occur soon. However, they don’t necessarily state what that change is keeping the victories vague and as such ensuring that they cannot be contradicted.

RT if you support #Anonymous. The system has failed and it’s time for change. The corrupt fear us. The honest support us. The heroic join us. #BlackLivesMatter #OpDeathEaters #GeorgeFloyd #ICantBreathe #ShutItDown #OccupyEverything https://t.co/kRbMzZdAJR

“We hope this is the beginning of a real change. Raise your voice loud and clear. We are legion. #anonymous”

“We can create a better world together. The obstacles we face, we face together. GLOBALLY everyone is coming together to face tyranny. We support all movements that push for a better society and turn away from authoritarian rule. We are Anonymous.”
“You can’t arrest an idea. You cannot kill an idea. Ideas are bulletproof. People are not. A handful of people do not represent Anonymous as a whole. Anonymous will be here long after we are all dead. It doesn’t end with them or any number of people. We are legion, we are endless. https://t.co/H7fwGSGMx4”

In addition to Anonymous’s methods for mobilisation, both the Chaos Computer Club and Belarusian Cyber Partisans will use methods to mobilise that are not used by Anonymous. Firstly, Chaos Computer Club will pose questions to their followers in order to encourage them to educate themselves and question the decisions being made by those in power.

Biometric mass surveillance in Germany, the Netherlands, Poland. What can you do? Your voice can help: #ReclaimYourFace https://t.co/O2qCCpRrlx
Biometric mass surveillance in Germany, the Netherlands, Poland. What can you do? Your voice can help: #ReclaimYourFace https://t.co/O2qCCpRrlx

The Belarusian Cyber Partisans will post tweets containing a list of demands in order to pressure the opposition and thus mobilise their followers into acting.

We have encryption keys, and we are ready to return Belarusian Railroad's systems to normal mode. Our conditions: *🔺 Release of the 50 political prisoners who are most in need of medical assistance.* *🔺Preventing the presence of Russian troops on the territory of #Belarus.* *https://t.co/QBf0vtcNbK*
Our friends #Busly Latsyats dumped a container with an incendiary mixture to the base of Internal Troops. Goals of the action: *✔ damage the infrastructure* *✔ remind that all crimes commited by the regime will not go unnoticed.* *#Belarus #Resistance* *https://t.co/nA4BDutkmk*

After having analysed the tweets in order to identify the mobilising for action function outlined by Stewart as one of the rhetorical functions utilised by social movements it is clear that all of the hacktivist Twitter accounts utilise this function. They do so in numerous ways, firstly, they will employ the use of an 'us vs them' dichotomy ensuring their audience feels a part of the collective and as a result will be more likely to mobilise in future political action organised by the hacktivists. Another way in which the collectives mobilise for action is through the use of explicitly stating how their enemies are restricting personal freedoms and transgressing societal norms in order to benefit the few instead of the many. As well as utilising this tool, Anonymous will also pressure the opposition by trolling them and also by including their twitter handle in their tweets ensuring the enemy is notified once the tweets are published. A further way in which both Anonymous and Chaos Computer Club increase the likelihood of audience mobilisation is through the use of engaging with agencies of influence. Both collectives have engaged with both longstanding civil action groups such as Greenpeace and Amnesty International and newer but influential global movements such as the Black Lives Matter movement which has benefitted them, increasing their follower count and as a result their level of influence. The rhetoric used by both Anonymous and Belarusian Cyber Partisans can also be visceral which can induce moral panics and sympathy in their audiences and consequently can increase the likelihood of political action from them. However, the language used by the collective differs greatly depending on whether they are talking to outsiders in public fora or whether they are talking to insiders in their webchat. Anonymous will also utilise stirring and emotive language in order to inspire their audiences into taking action. The Chaos Computer Club use questioning language to encourage their readers to educate themselves whereas the Belarusian Cyber Partisans will pressure the opposition with a list of demands. It is clear that this function is fully utilised by the different hacktivists in order to ensure their audiences are more likely to engage with them politically and take action.

3.5. Sustaining the Movement.

The final function utilised by social movements in their rhetoric identified by Stewart is 'sustaining the movement' as a result of the longevity of some movements. This function revolves around the idea of justifying setbacks, explaining their gains, ensuring the movement is viable and maintaining visibility. This function is vital as the most successful social movements can last for many years and are constantly affected by changing circumstances. Audiences can oftentimes perceive victories differently to the movement themselves. Furthemore, the opposition can capitalise on delays in order to affirm their superiority. Thus, Stewart claims that "social movements must wage a continual battle to remain viable" and the result of this is that more rhetorical energy may be expended on keeping the movements profile visible to audiences rather than on selling their ideologies (1980: 157).

The hacktivists do fulfil this function in some ways, they will post about their successes and they ensure they remain visible by tweeting regularly. However due to the nature of the collectives, they may not necessarily need to justify and explain their successes, setbacks and viability.

Firstly, certain active Anonymous accounts will regularly post about their successes by using the hashtag #TangoDown along with the link to the website they have either defaced or taken offline and usually hashtags explaining the reason for attacking these websites in particular. This relates to the military slang whereby a soldier will announce Tango Down when an enemy has been defeated[86]. This statement is also used when playing video games, specifically first person shooter games, when players are speaking to their team members over audio.

"http://t.co/gJaW2vwT TANGO DOWN II 404 Interpol, #Anonymous is not a criminal organization."
"http://t.co/gJaW2vwT TANGO DOWN &gt;&gt; FREE INTERNATIONAL ANONS! #Anonymous"
"https://t.co/ewTtmZBlVy is #down #TangoDown #SaveShawniganWater"
"http://t.co/vKNVQoCTGD &amp; http://t.co/mgB8IDLInq #TangoDown #Brazil We stand with Brazilian natives in opposition of #hydropower development."
"@AnonOpsSweden double #CA #ACAB http://t.co/YU9wEasH #tangodown by #Anonymous over http://t.co/MMFc7T9B"

[86] https://www.dictionary.com/e/slang/tango-down/ Last Accessed 3 March 2021.

“https://t.co/QjB7m5EehG is now offline. #Anonymous #TangoDown”

As well as the tweets using the hashtag Tango Down, all of the hacktivists will post about other online civil disobedience victories and will retweet other accounts that have posted about their victories. Indeed this is the predominant style of tweet that Ghost Squad Hackers post in order to demonstrate their prowess and spread their message.

“IBtimes: "#Anonymous Hacks Porn Site, Reveals 82 Government Employee Subscribers"”
“Newsroom: Vatican confirms second Anonymous hack - ZDnet (En) 03/2012 &gt;&gt; http://t.co/InxG46Nm”
“#Anonymous hacks Hungarian court website, rewrites new Constitution \xbb http://t.co/ekjusze9”
“HACKED PandaSecurity, used by feds to investigate #Anonymous \”
Belarusian group claims hack on railway system after Russian troop moves https://t.co/vxcQDvM6Ak
This week's hack of Belarus's state train company by @cpartisans raised a serious issue of cyber attacks and retaliation by both sides. Ukraine, dissident groups, even the US and EU intel services won't ignore Russia's legendarily lousy op-sec *https://t.co/55Fmc4qSPq*
Government Legislation Center of Poland hacked *https://t.co/9MQipXCbEg* *https://t.co/0Uu8wVg0f1*

#GSH / #GhostSquadHackers https://t.co/E75v75cpR9
Sub domain of Washington DC hacked with #FreeJulianAssange message \!/ *https://t.co/TFyjiu7e2P* *https://t.co/uJJVK17TL6* *#GSH / #GhostSquadHackers https://t.co/v9r2dFVnvL*

Along with the tweets stating their victories online, Anonymous specifically will also publish tweets when they have achieved offline successes such as the pardoning of hacktivist Chelsea Manning, the vast numbers of protestors that took part in their Million Mask March and other marches they have engaged in.

“Assange: "Thank you to everyone who campaigned for Chelsea Manning's clemency. Your courage &amp; determination made the impossible possible."”
“#Anonymous speak out at #SXSW panel- Topics: Sabu, Documentary, Leaders &amp; Last Actions &gt;&gt; http://t.co/1n3dtp43”
“#ClimateMarch amazing picture from #wien in #Austria #systemchangenotclimatechange!”
“And the activists from #MillionMaskMarchLondon were also out on the streets of London in their 'V for Vendetta' Guy Fawkes masks. #MillionMaskMarch Pics @ShutterstockNow and @AlamyNews”

Alongside their own successes, Anonymous will also post about the successes of their allies and with other social movements they have been involved with and assisted. In doing so it could be argued that Anonymous could be seen to be sustaining their movement by engaging with other movements in order to spread their name. As was seen earlier in this Chapter, Anonymous received millions of new followers after joining in with the Black Lives Matter movement over the summer of 2020.

“Thousands of #BlackLivesMatters protesters marched peacefully through Los Angeles on Sunday.#JusticeForGeorge #JusticeForAhmaud Stop #PoliceBrutality #BlackLivesMatter #LosAngeles”
“The month after Mike Brown was killed, the # of black ppl killed by police dropped 56% nationwide. Protests matter. http://t.co/TcY5rH7fSe”
“#OWS celebrates its 6th month anniversary in #NYC- Congratulations to all Occupiers worldwide!”
“People power in Madrid with the #ClimateMarch @greenpeace_esp”

As well as posting about their successful online and offline activities, another milestone that Anonymous will celebrate and tweet about is their follower count increasing. In doing so, they are celebrating the fact that they have more reach when it comes to spreading their ideological messages and can also claim to have more informal members as there is no formal membership process with regards to joining the collective. Therefore, it could be argued that with the number of followers increasing their reach, membership and engagement are also increasing. Indeed, in some of the tweets, they tell their new followers that they too are Anonymous ensuring that they feel a part of the collective.

“Congratulations to @Anonops for reaching 300,000 followers! Job well done!! http://t.co/hh59f9EG”
“300K Followers! Thanks everybody! It's an Honor! Tell us, where are you from? #Anonymous #AnonOps”

“200K FOLLOWERS! THANKS EVERYBODY! You are #Anonymous. We are Anonymous - We are the 99%”
“100.000 Followers. More than 4 million visits! Thank you all! Tell us where are you from &gt;&gt; http://t.co/Qa2KiKiW”

An interesting observation with regards to how Anonymous sustains their movement is that they will deride other hacktivists’. Diani claims social movements are linked through cooperation and mutual recognition which leads to a bond that moves beyond a specific act of protest (2003). As a result they put forward a series of conditions which they claim can explain the social movement dynamic with the first condition being that actors are often engaged in social conflict. This conflict promotes initiatives that damage other actors that are denying them resources or taking resources away from them. Based on this condition, then, it could be argued that both collectives are promoting initiatives that damage other hacktivists as they could either deny them resources or take away their resources as skilled computer programmers are a finite resource. By deriding other hacktivist collectives they could be ensuring that politically motivated computer programmers would be more likely to join them ensuring their movement sustains itself. Anonymous’s specific rival in this regard is Lulzsec who were once part of Anonymous but broke away to work on their own political activities. In celebrating their losses and deriding them, Anonymous are ensuring that their resources remain untouched. Ghost Squad Hackers, on the other hand, will regularly post about Anonymous’s successes in order to align themselves with the largest hacktivist collective in recent years and as such, in doing so could be seen to be sustaining their movement.

“#LulzSec was part of a #FBI play against Julian Assange”
“Like @YourAnonNews said... #LulzSec was a group, but #Anonymous is a movement. Groups come and go, ideas remain.”
“Lulzsec hackers' arrested in international swoop &gt;&gt; http://t.co/kZGwKinr”
#OpRussia Anonymous Hacks Roskomnadzor Federal Agency for Interational Cooperation

for government censorship of encrypted communication applications and networks/VPNS. https://t.co/WAoxqhkfZv
BREAKING: Anonymous Hacks ISIS Accounts Finds Attacks Planned for US, Bomb-Making Plans Thanks to @__s1ege for the great work. Hopefully, this prevents an attack. *https://t.co/jxeFM7NoNm*

However, it could also be argued that these hacktivist collectives are different to traditional social movements as they don’t require the same level of resources. Breindl states that thanks to the internet, activists no longer need to expend a lot of resources unlike traditional social movements (2010). Instead the internet facilitates movements across borders and can bypass state control ensuring they keep editorial control of their content. This could be that while traditional movements may have to justify their setbacks and explain in detail their successes in order to remain viable, Anonymous do not. Indeed, in the tweets analysed they never posted about any of their setbacks besides the incarceration of members and allies. These tweets are seen to be more mobilising in tone than justifying. The collective seems to see these incarcerations as proof that more work is needed and encourages their audience to participate in it.

“Our co-founder has been in federal prison for the last 6 months. Find out why! https://t.co/bLjbPqVLIj @FreeMartyG https://t.co/YeiOBy5txP”
“The imprisonment of #JulianAssange is an intimidation tactic to journalists worldwide. A journalist should never face jailtime for reporting the truth. We are all #Assange now.”
“Join us! Demand justice for jailed activist Marty Gottesfeld! https://t.co/UD7hqSRhBg #FreeMartyG #CFAA #Anonymous https://t.co/Hxz3HNzWHX”
“Tomorrow I'll launch a campaign for a jailed activist facing Computer Fraud &amp; Abuse Act #CFAA charges for allegedly working with #Anonymous”
“#FreeAssange #FreeAssangeNOW #FreeChelseaManning #FreeJeremy #Whistleblowers #Anonymous #Anon #Anonymiss #opvendetta #Nov5th #5thNov https://t.co/Rq3w1WO69r “

Furthermore, the loose membership structure of the collectives could be the reason that the different hacktivist collectives will rarely discuss their setbacks and explain their successes. There is no one leader that will be held accountable if an operation fails and as such, they are less inclined to follow the traditional movement's lead in justifying their setbacks. This occurs even with Ghost Squad Hackers despite S1ege being assigned as the leader of the group.

The final way that the hacktivists will sustain their movements is through remaining visible by posting regularly on their social media. Although some Twitter accounts, as mentioned earlier in the chapter, are not regularly updated, those with the largest following are. In posting regularly, the groups are reminding audiences that they are still active. While the imprisonment of some members seemed to impact the collectives in that the number of their civil disobedience activities reduced, some members were still actively posting. Furthermore, by posting in support of other movements, the collective are ensuring they remain relevant and visible. Indeed, over the summer of 2020 and throughout 2021 a number of news outlets posted about the 'return of Anonymous' and hacktivism in general including security company Stratfor; TechMoniter and an article in the Conversation published by Dr Vasileios Karagiannopoulos. This has only increased as a result of the 2022 Russian invasion of the Ukraine and the resulting increased hacktivist activity.[87] Indeed, below is an article from the Independent detailing how Anonymous are returning:

> *"Those aligning themselves with Anonymous were once one of the largest activist forces on the internet, using both online and real-world events and disruption to protest a wide variety of causes. In recent years, however, their media profile and the apparently number of people identifying with the group has reduced. In the wake of the ongoing protests across the US, however, a range of posts offering support for the protests and using the Anonymous name have spread across social media."*[88]

Based on the above, it is clear that this function has been at least partially fulfilled. The hacktivists sustain their movements by posting about their successful online protests such as

[87] https://www.ft.com/content/9ea0dccf-8983-4740-8e8d-82c0213512d4 Last Accessed 10 March 2022.

[88] https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-george-floyd-black-lives-matter-facebook-twitter-video-k-pop-a9542666.html Last Accessed 5 March 2021.

the tweets containing the #tangodown hashtag as well as tweets explaining other successful hacks. They will also post about their successful offline operations such as the release of Chelsea Manning from prison and the large turnout for their Million Mask Marches. Anonymous celebrates when they pass milestones with regards to their follower count as their audience is growing and as such higher levels of engagement could follow. As such, their visibility is always growing. Interestingly, some will deride other hacktivist collectives in order to preserve their resources ensuring the longevity of the movement as well as support more prominent hacktivist groups while others celebrate the successes of other hacktivists. However, all of the collectives will avoid posting anything that refers to any issues or complications which could be in part due to the fact that they do not require as many resources as traditional movements and as such do not need to justify their setbacks. Furthermore, its unconventional hierarchical structure can also be part of the reason why the collective does not post about its setbacks as it will not be held accountable.

4. Conclusion

It is clear that both Anonymous and Chaos Computer Club fulfil, if not all then the majority of the rhetorical functions set out by Stewart. Moreover, Ghost Squad Hackers and Belarussian Cyber Partisans partially fulfil the functions individually. Combined the different groups have referenced the past, present and possible futures in order to transform the audience’s perception of history. Both Anonymous and Chaos Computer Club reference the recent past, which could be in part due to the relative novelty of hacktivism. Anonymous will also use language that originated in the past in order to remind audiences that it the horrors of the past can be repeated are in fact currently occurring globally (eg Nazi and apartheid). They also use Guy Fawkes as an emblem of their anti-establishment ideologies. Both Anonymous and Chaos Computer Club reference possible futures both in contexts of fear and inspiration. They will discuss the possible futures that could occur based on election results and also discuss potential dystopian futures from fiction that could materialise. Belarusian Cyber Partisans, on the other hand, reference the present, specifically political events in Belarus as a way to gather support. As such, it seems that the majority of references to both the past, present and future posted by all of the collectives are used for mobilisation purposes encouraging their audiences to participate either to prevent the past from recurring, to prevent dystopian futures or to assist in the future that they would like. Therefore, this rhetorical function has been fulfilled by the hacktivists.

The second rhetorical function has similarly been fulfilled. The ‘transforming perceptions of society’ function is predominantly based around transforming perceptions of the self and the opposition. The rhetorical mechanisms that the hacktivists use in order to fulfil this function include posting information and report style bulletins in order to inform their audiences and garner support for their activities and spread their ideologies. Anonymous, Chaos Computer Club and Belarusian Cyber Partisan employ an ‘us vs them’ dichotomy in order to accumulate followers and distance their opposition. Furthermore they will use highly emotive and visceral language when discussing their opposition and will often troll or belittle their opponent ensuring their power decreases encouraging audiences to take part in collective action. Finally, in transforming perceptions of the self Anonymous will outline who the group is, their various ideologies and political leanings explaining that as a collective they are ‘anonymous not unanimous’. The Belarusian Cyber Partisans will regularly retweet news praising their activities in order to be seen positively. Thus, it can be argued that both the Anonymous accounts as well as the non-Anonymous affiliated groups have fulfilled the ‘transforming perceptions of society’ function in their rhetoric.

The third rhetorical function, ‘prescribing courses for action’ has also been identified in the collective’s tweets despite the fact that a large part of their methods are illegal in most countries. The majority of the tweets that contain this rhetorical function are prescribing legal courses for action such as twittestorms and petitions. Anonymous and Chaos Computer Club will ask followers to be aware of internet privacy issues ensuring they’re protected online. They will also defend these legal methods by outlining the ways in which petitions can lead to successes. Both Anonymous and Chaos Computer Club will also ask followers to take part in offline actions such as workshops, marches or helping the homeless. There are a few instances of Anonymous asking followers to take part in illegal online methods such as DDoS attacks and Doxing. It is apparent, then, that the collectives lay out their methods for change and defend these to their audience.

The fourth function outlined by Stewart, ‘mobilising for action’ has been identified in the tweets analysed in various ways. Firstly, as in the second function, an ‘us vs them’ dichotomy is employed in order for the collective’s audience to feel a part of the movement and mobilise themselves. Both Anonymous and Belarusian Cyber Partisans will portray their opposition as those in power who are taking away personal freedoms from those not in power and will name them specifically. The Belarusian Cyber Partisans will also regularly tweet lists of demands in order to pressure the opposition. All of the accounts analysed have people in power as their opposition. Anonymous specifically will engage with influential global social movements and Chaos Computer Club engage with civil society organisations in order to increase their following and their level of influence. Another way in which both Anonymous and Belarusian Cyber Partisans fulfil the fourth function is through the visceral and emotive language used in order to induce moral panics and sympathy ensuring political action will follow. Chaos Computer Club will also ask questions to their audience encouraging them to educate themselves. It is apparent then, that this function is fully utilised by the collectives in their communications to wider audiences which will ensure their audiences engage with them ideologically and mobilise themselves.

The final rhetorical function, ‘sustaining the movement’ has also been partially identified in the tweets analysed. The movements are being sustained in numerous ways. Firstly, Anonymous post about their successes by either using the military slang #tangodown in their tweets. They will also post about their online successes more generally. They celebrate milestones in their follower count as the more followers they have, the more visible they will be ensuring the movement lives on. They will also acknowledge and celebrate their offline successes, for example, the number of people that attended their offline marches. A way in which Anonymous ensures the movement remains viable is through the derision of rival hacktivist groups such as Lulzsec which could be seen to be a way in which Anonymous retains their resources and doesn't lose out to other groups while Ghost Squad Hackers will post about Anonymous’s successes. Anonymous very rarely posts about their setbacks, however, which could be due to the fact that, unlike offline social movements, the hacktivists require very few resources meaning they don’t have donors and will not have to justify setbacks. Additionally, the fluid membership and unconventional hierarchical structure of the groups could result in a lack of accountability and as such don’t need to explain their setbacks.

In conclusion, the majority of the rhetorical functions have been identified in the tweets analysed. As such, it could be argued that hacktivism is a social movement and should be afforded the same leniency in some of their protest activities. The following chapter will add to the comparison of hacktivism and social movements as well as empirically examine the similarities and differences of hacktivism and cybercrime.

Chapter 6: Hacktivism - cybercrime or social movement?

1. Introduction

Following on from the presentation of the rhetoric analysis results, this chapter will present the findings from the analysis of various datasets detailed in the methods chapter (Chapter 4) including the Hackmageddon database[89] (01), the Zone H hacktivism dataset[90] (02), Cambridge Computer Crimes database[91] (03), the UK's Department of Culture, Media and Sport's National Cyber Breach survey reports[92] (04), the AnonOps Internet Relay Chat[93] (05) and the sentiment analysis from SWGFL[94] (06). The aim of this chapter is to empirically compare hacktivism to both cybercrime and social movements in order to establish definitively whether it falls under the category of social movement or cybercrime. This will then allow the Dissertation to state whether the UK government's approach to the methods used by hacktivists should be re-examined. The chapter is split into two parts. Firstly it will compare hacktivism to other forms of cybercrime by examining its targets (2.1) and methods (2.2). The second part will then add to the comparison of hacktivism to social movements from the previous chapter (Chapter 5) by analysing the operations (3.1), ideologies (3.2), successes (3.3) and public opinion of hacktivism (3.4). This chapter will argue that there is a clear distinction between hacktivists and cybercriminals both through their specified targets, their motivations and the methods they use. It will also argue that hacktivists have a great deal in common with social movements with similar ideologies motivating their actions. However, it will also argue that while hacktivism has a great deal in common with offline social movements, the successes of hacktivists can never

[89] Cyber attack timelines 2012-2019. Compiled by Paolo Passeri. Available on request at https://www.hackmageddon.com/. Downloaded on 6 August 2020. Last Accessed on 13 April 2021

[90]Zone H cybercrime archive. Available http://www.zone-h.org/archive/special=1. Downloaded on 29 Jan 2022.

[91] Cambridge Computer Crime Database. Compiled by Professor Alice Hutchings. Available at https://www.cl.cam.ac.uk/~ah793/cccd.html. Last Accessed 27 Jan 2022.

[92] DCMS Cyber Security Breaches Survey 2017-2021 https://www.gov.uk/government/collections/cyber-security-breaches-survey

[93] AZSecure-data.org. Anonops IRC channel Sep 2016-May 2018. Created by the University of Arizona (NSF #ACI-1443019), Drexel University, University of Virginia, University of Texas at Dallas, and University of Utah. Available to download from https://www.azsecure-data.org/internet-relay-chat.html. Downloaded on 6 August 2020. Last Accessed 13 April 2021.

[94] SWGfL Reputation Alerts Sentiment Analysis. Available when subscribed and logged in: https://swgfl.org.uk/login/

reach the same heights as offline social movements, nor does the public look as favourably upon hacktivism as they might with more legitimate social movements. This chapter then, will ascertain whether hacktivism has more in common with social movements as opposed to cybercrime in order to answer the research questions ***'Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?'***

2. Is Hacktivism Distinct from Cybercrime?

2.1. Hacktivism Targets

When analysing the Cambridge Computer Crime Database (03), The Zone H Dataset (02) and Hackmageddon dataset (01) the most common target for hacktivists is consistently governments and government organisations. Based on the Zone H dataset (02), 73.52% of the web defacements analysed were targeting government domain names. This would suggest that the overwhelming majority of their targets were government organisations. Moreover, the Cambridge Computer Crime Database (03) shows that the majority of those that were arrested for computer crimes resulting from hacktivist techniques had the websites of governments, police and public officials as their targets. Additionally, according to the hackmageddon database at hacktivism's peak in 2013, 46% of hacks were directed at government organisations. In 2019 when hacktivist motivations contributed to only 1.53% of hacks, government and defence was the most common target with 39% of the hacks being directed at them. This would contradict the idea that the UK government put forward in hinting that hacktivists are to be feared in the same vein as cyber terrorists and gang members. In government messages, hacktivism is usually defined alongside cybercriminals and terrorists ensuring readers are aware that individuals see hacktivists as a threat to public safety. The Centre for the Protection of National Infrastructure has filed hacktivism under a section that outlines National Security Threats and lists hacktivist groups under its list of hostile actors. Furthermore, in a 2020 report published by the NCSC the UK government defines hacktivists as those "who wish to attack companies for political or ideological motives."[95] Yet, their most

[95] https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact#downloads Last Accessed 22 Nov 2020.

common target is consistently the government themselves and not companies or the general public. The UK government has also stated that "the threat to the UK from politically motivated activist groups operating in cyberspace is real. Attacks orchestrated by hacktivists on public and private sector websites and online services are becoming more common and aim to cause disruption and reputational and financial damage to gain publicity."[96] While it is true that hacktivists will post about their successes as was seen in the previous chapter it is not true that they simply engage in hacktivist techniques in order to gain publicity. Furthermore, the statement does not acknowledge that government websites were the main targets. This would suggest then, that the UK government is again attempting to frame hacktivism as a threat to national and public safety.

Moreover, the DCMS Cyber Security Breaches Survey (04) shows that from the start of the survey in 2017 until the most recent survey in 2021, large firms were overall the most targeted type, followed by medium and small firms (Chart 1). This survey is completed by UK businesses in order to understand the UK cyber landscape. However, as the data resulting from these surveys is supplied by businesses the survey results do not include any information on the proportion of UK government websites. The yearly survey does not distinguish between hacktivism and other forms of cybercrime. Indeed, hacktivism is not included in the survey or the results reported at all. However, the results do offer an insight into cybercrime in the UK and the predominant industries that are targeted by cybercriminals.

[96] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf Last Accessed 13 April 2021.

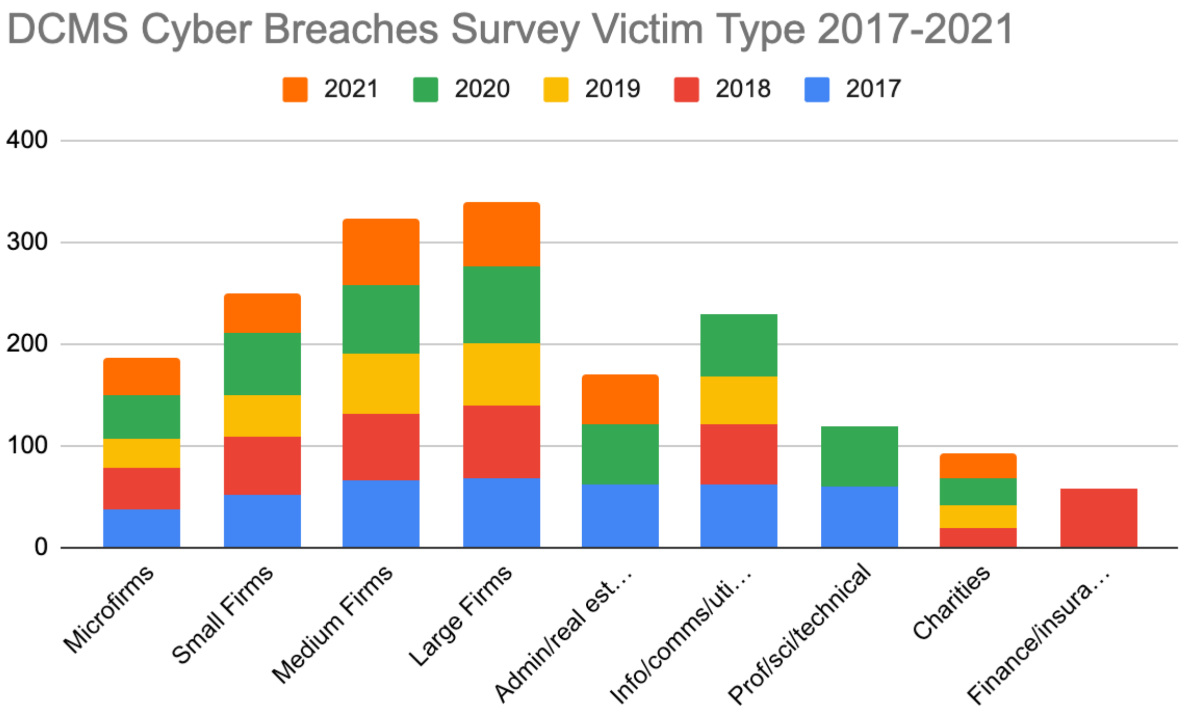


Chart 1: DCMS Cyber Breaches Survey 2017-2021 Victim Type

Additionally, according to the Hackmageddon dataset (01), the main target of cybercrime in 2019 was Multiple Industries (19%) followed by individuals (18%). Public administration, defence and compulsory social security only made up 9% of the hacks. During 2013 when hacktivism was at its peak, according to the dataset, the government was not the main target of cybercriminals. Indeed, Information and Communication was the most common target (23%) followed by Public administration, defence and compulsory social security (18%). Based on the Cambridge Computer Crimes database the majority of victims of computer crimes are individuals as a result of financial fraud, child sexual abuse material, illegal online market places and transgressions of the Data Protection Act 1998/2018. Based on both databases, it would appear that cybercriminals and hacktivists do not have the same targets and as such may have more in common with social movements cybercrime

2.3. Hacktivism Methods:

The methods used by hacktivists also appear to differ from cybercriminals. Desk based research has shown the key methods used by hacktivists are account hijacking, DDoS, defacement, SQL injection and leaking sensitive information. Account hijacking has been described as “a process through which an individual’s email account, computer account or any other account associated with a computing device or service is stolen or hijacked by a hacker.”[97] SQL injection vulnerabilities “allow an attacker to inject malicious input into an SQL statement.”[98] It originated when websites started storing user input and content in databases. This method has been described as one of the most dangerous issues for data confidentiality and integrity when it comes to web applications. Web defacements involve penetrating a website and replacing the existing content with their own messages. With regards to hacktivism, these messages can be political or religious in tone, however they can be used more generally to embarrass website owners. Distributed Denial of Service (DDoS) attacks are attempts to disrupt the normal traffic of a specific website or server by overwhelming the targets infrastructure with an exceptional amount of internet traffic[99]. Leaking sensitive information is the method predominantly linked to the Wikileaks site whereby a hacktivist will access sensitive information usually related to the state and post it online. All of these methods included in the dataset are all legislated against in the UK and most would fall under transgressions of the Computer Misuse Act 1990. It is clear therefore, that hacktivists have no interest in obeying the law.

[97] https://www.techopedia.com/definition/24632/account-hijacking Last Accessed 13 April 2021.
[98]https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/#WhatIsAnSQLInjectionVulnerability Last Accessed 13 April 2021.
[99] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ Last Accessed 13 April 2021.

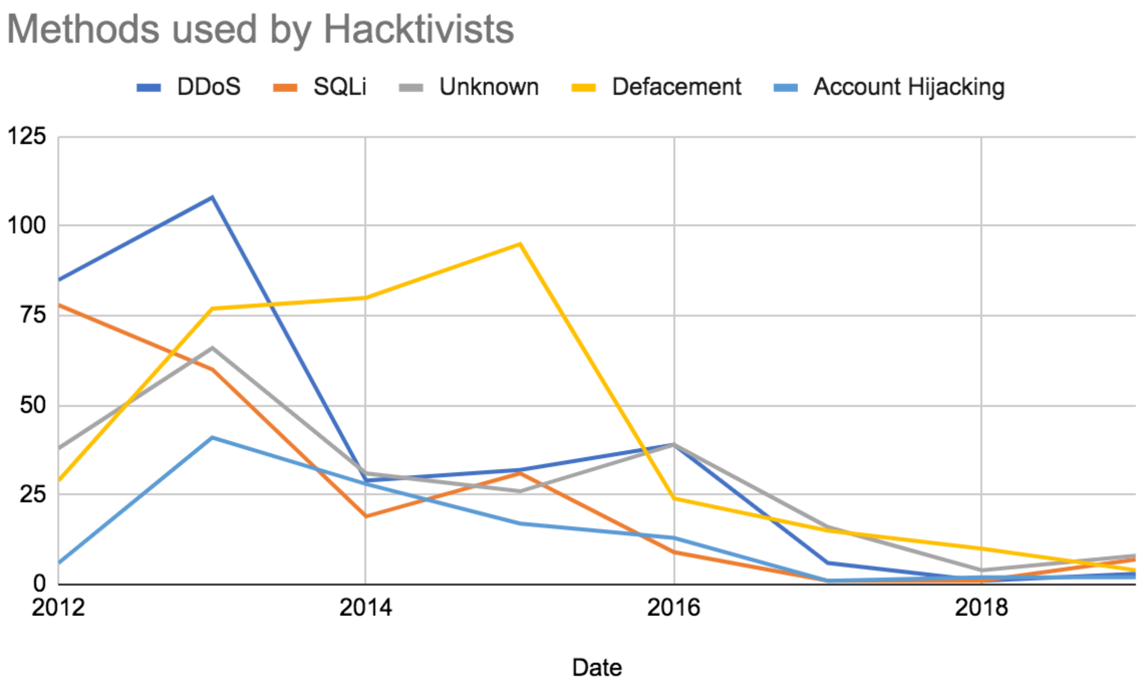


Chart 2: Hackmageddon 2012-2019 methods used by hacktivists

The Hackmageddon dataset (01) shows that the most common methods used by hacktivists are consistently DDoS and web defacement (Chart 2). In 2012 and 2013 when hacktivism was at its peak DDoS was the most common method (36% and 28%). While in 2014 and 2015 web defacements took over as the most common method (42% and 48%). In 2016 DDoS again took over as being the most common. However, from 2017 onwards defacement was again the most common method of attack. This is interesting as in the literature, DDoS attacks are consistently mentioned as the most common type of attack. Yet, the data suggests that this isn't necessarily the case with web defacements alternating for the most common method. One potential reason for this could be that web defacements are more visible than DDoS attacks and, as a result, defacements may be reported more than DDoS attacks, resulting in DDoS attacks being unreported. Indeed, the National Cyber Security Centre states: "The DDoS attacks that most people have heard about are those launched against high profile websites, since these are frequently reported by the media. However, attacks on any type of system, including industrial control systems which support critical processes, can result in a denial of service."[100] Yet the Cambridge Computer Crime database (03) consistently demonstrates that since the start of the database in 2010, any arrests that have taken place and are linked to hacktivists were done so

[100] https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection Last Accessed 10 April 2021

due to DDoS attacks on predominantly government websites. This could suggest that the UK government is more concerned with DDoS attacks rather than defacements despite their visibility.

TrendMicro have found that defacers will leave contact information directing visitors to their social media as well as messages that advertise their political beliefs.[101] Furthermore, they found that 32% of defacements link to either a streaming provider or audio file. Based on this then, it could be seen that defacements are used as a way of promoting their causes, and as such are being used specifically for their visibility. When looking at the mirrored sites that are posted on Zone H (02) many have contact details and links through to other media. Maggi et al have found that web defacers work in teams: “Especially if driven by strong ideologies, defacers are not lone wolves, but their modus operandi resemble that of well-organised cyber gangs acting in a coordinated fashion” (2018: 4). An explanation for why the UK government may be focusing on DDoS attacks rather than web defacements could be linked to cost. The estimated cost of 1,250 defacements uploaded to the Zone H database (02) and observed between 2007 and 2015 was approximately £1.6 million to the Government and industry targets involved[102]. While in its sample of 250 professionals, Neustar found that 22% of the companies that had suffered from a DDoS attack reported losses between £50,000 and £99,999 per hour for revenue losses due to outages at peak times (2015) . Moreover 16% reported that their losses per hour were less than £30,000; 12% reported losses between £30,000 and £49,999; 16% between £100,000 and £299,999; 11% between £300,000 and £600,000; 12% greater than £600,000; and 11% did not know what their outages cost them[103]. It is clear then that financially, the cost of DDoS attacks to the government over a long period of time is greater than the cost of defacements.

When searching for the terms in the AnonOps Internet Relay Chat, DDoS also appears to be the method most discussed with the term being mentioned 3375 times. These mentions include individuals asking the forum whether they know how to DDoS and whether they can teach them how,as well as posting news articles on recent DDoS attacks and users suggesting potential DDoS targets such as Donald Trump and Hillary Clinton. The second most discussed method in

[101] https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf Last Accessed 10 April 2021

[102]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf Last Accessed 31 Jan 2022

[103]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf Last Accessed 31 Jan 2022

the AnonOps IRC database is SQL Injection which is mentioned 1201 times with many users asking for advice on how to learn SQL and which software to use. Finally web defacements are only mentioned 311 times. Similarly to the other two methods mentioned in the chat, there are users posting for advice on how to deface a website as well as news articles on web defacements that have taken place. Interestingly, the chat that is focused on web defacements also offers more of a commentary on the method itself with some disparaging it stating that it is only for those seeking fame. This might explain why DDoS attacks are considered the default method used by hacktivists.

The DCMS Cyber Security Breaches Survey (04) shows that the methods used by cybercriminals in general differ to hacktivists specifically (Chart 3). Between 2017-2021 the main method used by cybercriminals is consistently phishing attacks by a large majority, specifically fraudulent emails and messages. The NCSC defines phishing as 'when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.'[104] This can be conducted via text, social media, phone and, more commonly, email. These emails can reach millions of users and can lead to attackers installing malware, sabotage systems on their hardware and can also lead to theft of both intellectual property and money. The second type of attack is viruses and malware, followed by impersonation. The survey does include DDoS attacks but this is the seventh most common form of cybercrime. The survey does not include defacements however, which is again evidence that the UK government is more concerned with DDoS than web defacements.

[104] https://www.ncsc.gov.uk/guidance/phishing#:~:text=Phishing%20is%20when%20attackers%20attempt,them%20to%20a%20dodgy%20website.&text=Phishing%20emails%20can%20hit%20an%20organisation%20of%20any%20size%20and%20type. Last Accessed 31 Jan 2022

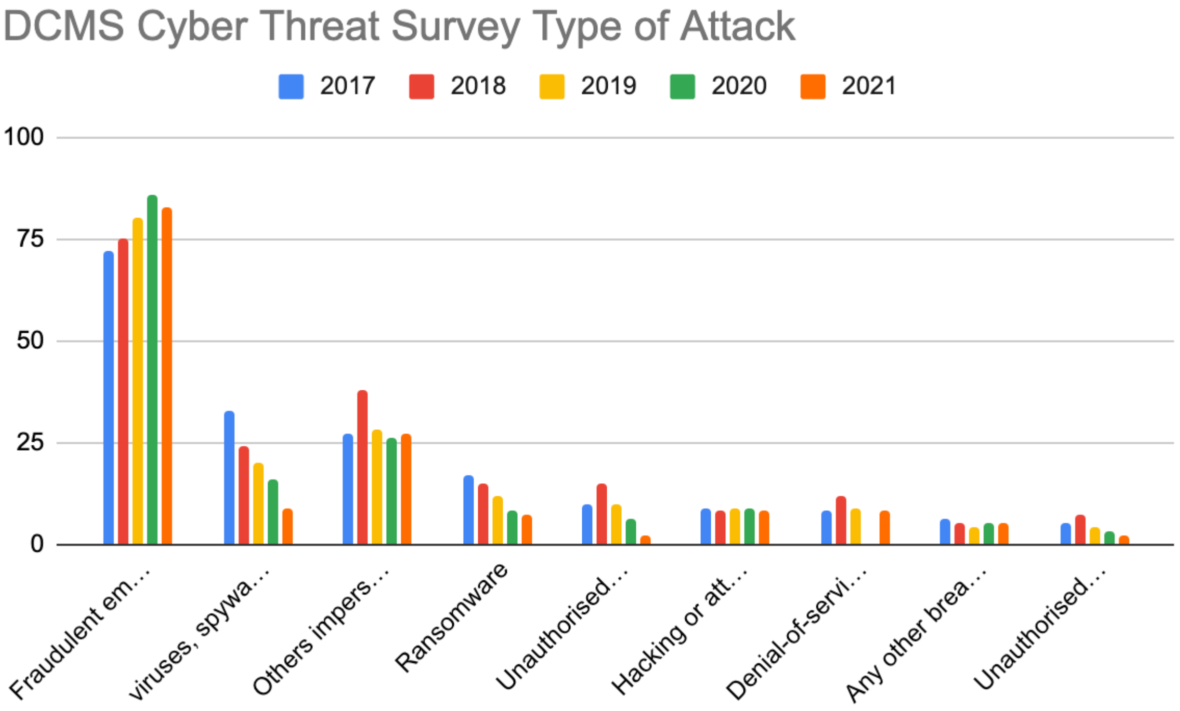


Chart 3: DCMS Cyber Breaches Survey 2017-2021 Attack Type

While many computer crimes have offline parallels, including fraud, both DDoS attacks and web defacements have offline parallels that are used by social movements in the form of sit-ins and graffiti. This would suggest that hacktivists are simply online reflections of non-violent offline protestors and as such should be afforded the same rights under the UK Human Rights Act as them. This will be explored further in the following chapter (Chapter 7).

3. Is Hacktivism Similar to Social Movements?

3.1. Hacktivist Operations

Hacktivists will regularly launch campaigns which they call operations in order to protest a specific injustice. In the Hackmageddon dataset (01) 140 different operations were undertaken throughout the 7 years that the dataset was analysed. These were all fact checked by the researcher to ensure they did take place. Based on the data, 2012 had the largest amount of individual operations (49) followed by 2013 (45), 2016 saw 25 different operations, 2015 saw 23, 2017 saw 7, 2019 saw 5 and 2018 saw 2. Interestingly the dataset showed only 4 different operations in 2014.

Out of the 140 total unique operations throughout the life of the hackmageddon dataset, 15% (21) of those last multiple years. This correlates to Bernard's views that while there are a few smaller operations that occur (for example OpDomesticTerrorism) these rarely last longer than a month and aren't adopted by the wider membership (2018). Bernard claims that "without a cause, members are likely to move on". When interviewed about hacktivist collective Cult of the Dead Cow, Oxblood Ruffin claimed that in the 1980s mostly 15 to year olds would hack the US military network until they got bored and moved on to more interesting security projects[105]. It could be suggested that the reason 85% of the different operations included in the dataset lasting for less than a year is that members become bored of that cause and move on to something else more fulfilling. OpGreenRights and OpIsrael lasted the longest with both featuring over 6 years, followed by OpUSA which occured in 4 of the years included in the dataset. OpGreenRights is a campaign that was initiated against companies that Anonymous consider to be responsible for 'destroying nature and ancient cultures'[106]. An example of this is from a hack in 2013 on Anglo American, a multinational mining company. Anonymous claimed:

> *"Anglo American Platinum filed SLAPPs (Strategic Lawsuit Against Public Participation) against a South African (public interest) lawyer Richard Spoor, who represented indigenous communities affected by platinum mining on tribal land. In August 2007, British charity War on Want published a report accusing Anglo American Platinum's parent company Anglo American of profiting from the abuse of people in the (developing) countries in which the company operates. [...] Great multinationals use "greenwashing" in order to avert human rights complaints. So large firms raise funds from people declaring to protect mining war-areas and they use this money in order to get a better control of public opinion and*

[105] https://www.rferl.org/a/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html. Last Accessed 12 April 2021.

[106] https://news.softpedia.com/news/Website-of-AngloAmerican-Mining-Company-Hacked-By-Anonymous-for-OpGreenRights-335092.shtml Last Accessed 12 April 2021.

mining areas. We say enough to all of this, We refuse this great lie which sounds like the Nazi propaganda of the 30s."[107]

Operation	2012	2013	2014	2015	2016	2017	2018	2019
#Op_Russia	1	0	0	0	0	1	0	0
#MMM	1	1	0	0	0	0	0	0
#OpGreenRights	5	3	1	2	1	0	0	3
#OpLiberation	1	2	0	0	0	0	0	0
#OpIndia	2	1	0	1	0	0	0	0
OpFreePalestine	3	1	0	0	2	0	0	0
#OpIsrael	1	3	0	5	1	2	1	0
#FuckTheSystem	2	1	0	0	0	0	0	0
#Nov5	5	0	0	0	0	0	0	2
#OpUkraine	4	1	0	0	0	0	0	0
Operation Syria	1	3	0	0	0	0	0	0
#OpEgypt	1	4	0	0	0	0	0	0
OpFuckMohammad	1	8	0	0	0	0	0	0
Operation Ababil	3	26	0	0	0	0	0	0
#OpLastResort	0	0	1	0	0	0	0	0
#OpUSA	0	2	0	1	0	1	1	0
#OpKillingBay	0	3	0	1	2	0	0	0
#OpSingleGateway	0	0	0	2	3	3	0	0
#OpSaudi	0	1	0	3	1	0	0	0
#OpTurkey	0	7	0	0	1	0	0	0
#OpBigBrother	1	1	0	0	0	0	0	0

Table 6: Longest lasting operations.

OpIsrael is an annual series of cyberattacks by a number of hacktivist collectives against Israeli targets that takes place on Holocaust Memorial Day. Anonymous have claimed that OpIsrael is the result of 'the barbaric, brutal and despicable treatment of the Palestinian people in the so called 'Occupied territories' by the Israeli Defense Force[108]. However, throughout the years it has failed to draw much traction. Ben Yisrael from Israel's National Cyber Bureau said in 2013:

[107] http://operationgreenrights.blogspot.com/2013/03/anglo-american-we-shame-you.html Last Accessed 13 April 2021.

[108] http://anonopsofficial.blogspot.com/2012/11/anonymous-attacked-40-sites-government.html Last Accessed 13 April 2021.

"Anonymous doesn't have the skills to damage the country's vital infrastructure. And if that was its intention, then it wouldn't have announced the attack ahead of time. It wants to create noise in the media about issues that are close to its heart[109]". Other hacking groups have taken part in OpIsrael throughout the years however, again, they had failed to cause much disruption. The operation was outlined in the Internet Security Threat Report 2014 published by Symantec as a key event in 2013.[110] Based on the data, one could assume that an operation doesn’t have to be a success in order to be repeated throughout the year. Instead, it could be suggested that instead of a hack resulting in success, it is in fact the ideals behind the attack that results in its duration over a number of years.

OpUSA was an collaborative operation between Anonymous, AnonGhost Team, @Charafanons, Mauritania Attacker, X-BLACKERS INC., Islamic Ghost, Tunisian Hacker Team, Sir Abdou, Shadow Haxor, Indonesia Security Down, and Anonymous Algeria. The operation is also outlined in the Internet Security Threat Report 2014 published by Symantec[111]. The operation was a follow up to OpIsrael and has been described as a rebuke to the US for what the hackers consider to be their sins:

> *“Anonymous will make sure that this May 7th will be a day to remember. On that day Anonymous will start phase one of operation USA. America you have committed multiple war crimes in Iraq, Afghanistan, Pakistan, and recently you have committed war crimes in your own country… You have killed hundreds of innocent children and families with drones, guns, and now bombs. America you have hit thousands of people where it hurts them, now it is our time for our Lulz. For this you shall pay…Obama you have seen the over three billion dollars’ worth of damage we have done to Israel in operation Israel. It hasn’t even been a few weeks and the Anonymous collective has gotten stronger since then. Therefore we will not tread lightly as you have not treaded lightly.*[112]”

[109] https://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites Last Accessed 13 April 2021.
[110] https://docs.broadcom.com/doc/istr-14-april-volume-19-en Accessed 31 Jan 2022
[111] https://docs.broadcom.com/doc/istr-14-april-volume-19-en Accessed 31 Jan 2022
[112] https://www.eteknix.com/anonymous-starting-opusa-want-to-send-a-message-to-president-obama/ Accessed 10 April 2021

Yet, Cisco has claimed that the majority of the attacks were against small businesses and personal vanity domains.[113] The only successful government centred attack was a short-lived defacement of an Ohio Election Assistance Commission site. Cisco have claimed that publicly announced cyberattacks such as this, often have highly volatile credibility whereby announcements only exist to gain notoriety. OpUSA has also been criticised for lacking coherent focus which as a result meant that it didn't get sufficient numbers and as such fizzled out.[114]. Van Riper has suggested that hacktivist groups lack the efficiency of traditional forms of protest as a result of their decentralised nature (2019). In order to return to the level of popularity and success they reached during the early part of the 2010s, hacktivists will need to shift back to the mentality they had during their earlier operations.

The operations that have the most cyberattacks linked to them are mostly linked to real world events. In fact 76% of these attacks are linked to events that occurred offline. For example, OpFreeAssange which had 8 attacks linked to it in 2012 was linked to the UK government's statement claiming that it would arrest and extradite, Wikileaks founder, Julian Assange if he left Ecuador's embassy in London over allegations of sexual assault.[115] The US have also claimed that Mr Assange had done a great deal of damage to the internal and external security of the United States and as a result could be extradited and incarcerated. This led to an unknown hacktivist hacking into the Hertfordshire Police's website and publishing login details and passwords for dozens of police officers which led to Hertfordhsire Constabulary taking down the website as a precaution. Anonymous also took down two official websites of the Australian Attorney General via DDoS attacks which caused them to be offline for several hours.[116] Another example is OpAbabil that had 26 cyberattacks linked to it in 2013. Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the operation that disrupted several major banks including Bank of America and Wells Fargo. Operation Ababil appears to be the only operation undertaken by Izz ad-Din al-Qassam Cyber Fighters in retaliation for the film *'The Innocence of Muslims'* which was claimed to contain content offensive to the Muslim community. It is clear that, again, this operation occurred as a result of offline activities and tensions:

[113] https://blogs.cisco.com/security/the-effects-of-opusa Accessed 10 April 2021
[114] https://www.thecybersecurityexpert.com/anonymous-opusa-goes-without-a-bang/ Accessed 10 April 2021
[115] https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-19432487 Last Accessed 13 April 2021.
[116] https://www.hackread.com/australian-attorney-general-websites-taken-down-for-opfreeassange/ Last Accessed 13 April 2021.

> *“Dear Muslim youths, Muslims Nations and are noblemen*
>
> *When Arab nations rose against their corrupt regimes (those who support Zionist regime) at the other hand when, Crucify infidels are terrified and they are no more supporting human rights. United States of America with the help of Zionist Regime made a Sacrilegious movie insulting all the religions not only Islam.*
>
> *All the Muslims worldwide must unify and Stand against the action, Muslims must do whatever is necessary to stop spreading this movie. We will attack them for this insult with all we have.*
> *All the Muslim youths who are active in the Cyber world will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult [...]*
>
> *Down with modern infidels.”*[117]

Furthermore, the operations that are linked to offline, real world events are often political and contentious. Badiou has suggested that activism has lost the concreteness that it had before hacktivism (2005). Instead, it now takes the form of fluid collectives that hold diverse ideological leanings that come together to protest a specific cause which has been assisted by technology which has collapsed the traditional borders of time and space. Mansfield-Devine has claimed that hacktivists’s ambitions tend to use the language of revolution and state that they are uncovering corruption and fighting oppression (2011). While their activities are seen to be juvenile stunts or vandalism, the authenticity of their motivations or feelings should not be questioned. Furthermore Delmas has argued that
“I don’t think it misconstrues their activities to call them protective of human rights, insofar as they effectively empower dissidents and pro-democracy activists. For a domestic example of electronic humanitarianism, hacktivists have manufactured and provided free social media tools to uphold civil liberties and monitor against officials’ violations” (2018: 49). Coleman has found that Anonymous lacks concrete membership and ideology and the name can be used by anyone.. It is apparent, therefore, that hacktivism, in essence, centres on political beliefs and ideologies as opposed to mischief and vandalism (2011).

[117] https://pastebin.com/mCHia4W5 Last Accessed 13 April 2021.

3.2. Hacktivist Ideologies

Many of the definitions of hacktivism in academic literature and used by governments state that it is a form of politically motivated online protest, indeed the definition used in this dissertation defines hacktivism as *“the promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure’s technical features, without the use of physical violence and without gaining direct economic benefits.”* (Romagna 2019: 5). However, when looking at different hacktivist operations, it seems that these definitions could be too narrow in their scope as they do not all occur as a result of political policies. Even amongst the most popular and frequently cited operations a range of motivations can be identified.

Cyber-security corporation, Panda Security, instead describes hacktivism as “a form of non-violent digital activism where the motive is not, primarily, personal financial gain. Instead, hacktivist campaigns aim to achieve political, social, or religious justice in line with the group’s cause.”[118] While over half of the operations analysed (66%) have either a national or global government system as their perceived opposition, this definition is more in line with the results of the data analysis. Panda Security put forward four different types of hacktivism, these include agendas that lead to hacktivism as for political lean, social justice, religious intent or anarchy. Hacks that fall under the political category use hacktivism as a form of political mobilisation whereby it attempts to sway the population to the hacktivist’s political agenda. For those hacks that fall under the social category, hacktivists see hacktivism as a way to bring about societal change. The religious category is predominantly focused around using hacktivist techniques for a religious agenda in order to either recruit or disavow a religious entity. The final category is anarchist whereby hackers would have an anarchist agenda when accessing or controlling civil infrastructure, military equipment or the population. When looking at the longest running operations, the first three categories can be identified at the motivations behind hacks linked to the operation. While the last category hasn’t been identified as being a specific ideological motivation for the operations, it could be argued that hacktivism as a whole subscribes to the ideals of anarchy. Collister claims that “hacktivism is [...] rooted in the defacing, disruption or

[118] https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism/ Last Accessed 13 April 2021.

destruction of technology developed, operated or appropriated by capitalism" (2010).[119] Furthermore, there is a subgroup within Anonymous entitled Anonymous Anarchist Action (A(A)A) that works inside Anonymous's decentralised and open structure, focusing on anti-capitalist targets and solidarity initiatives. The group states the popularity of Anonymous has pushed it to move beyond the decentralised collective movement it once was and "*This is why we, as members of Anonymous and anarchists, have decided to start an autonomous group to help spread the ideas of anarchism, anti-capitalism, anti-racism and self-organization within it. We want to provide the skills, tools and experience of direct action in the streets, and take advantage of the new resources and techniques of hacktivism."*[120]

Firstly, the most common category is the political category with 66.7% of operations having political aims. This includes operations such as #OpIndia, #OpFreePalestine, #OpIsrael and #OpUSA. These operations have broad aims and are predominantly aimed at national governments, however some operations such as the Million Mask March and Nov5 are even more broad in their aims and are focused on global governments with their general aim being simply to promote the ideals of their anti-establishment belief systems. As mentioned earlier, the broadness of these campaigns and the lack of a concrete ideological stance could be behind the decline in hacktivism. Indeed, during the Million Mask March in 2020 which has taken place historically as a form of anti-government protest anti-lockdown protestors co-opted the event. Hundreds of new recruits took part in order to show their unhappiness over the government's handling of the Covid19 pandemic and over 100 people were arrested for breaking coronavirus restrictions. However, based on the main Twitter accounts linked to Anonymous, they appear mostly to be in favour of the public safety message being put forward and encourage their followers to wear face coverings. It is clear that due to the broadness of the protest event, new followers can join and warp the political message that they aim to convey.[121] Only two of the operations categorised as being political are focused on narrow political aims such as specific policies, these are OpSingleGateway and OpLastResort. OpSingleGateway was focused on Thailand's plans to implement a single gateway internet server which would be under the government's control with many citizen's fearing Chinese-level internet censorship which would

[119] http://www.ephemerajournal.org/contribution/abstract-hacktivism-model-postanarchist-organizing Last Accessed 12 April 2021.

[120] https://libcom.org/news/anonymous-anarchist-action-hacktivist-group-founded-10032011 Last Accessed 12 April 2021.

[121] https://www.independent.co.uk/news/uk/home-news/million-mask-march-lockdown-arrests-london-police-b1626808.html Last Accessed 12 April 2021.

affect digital rights and freedom of expression online.[122] OpLast resort, on the other hand, was aimed at the United States Sentencing Commission due to what Anonymous saw as their disproportionate sentencing of hackers—specifically Aaron Swartz. However, not long after OpLastResort was announced it was denounced by other members of Anonymous with one stating "ALL credible sources/anon cells to date have no idea who is running this operation. It came out of thin air and is using old anon operations data claiming it's new."[123] Hopkins claims that regardless of the motivations for OpLastResort and despite the fact that anonymity is one of the main tenets of the collective, it is very unusual "to find no one in the net of acquaintances who can speak to the identity and reliability of whomever was behind Operation Last Resort"(2020).[124] Nevertheless, regardless of who was behind the operation, it's aims are still political in nature and aiming to sway the population to the hacktivist's political agenda.

The second most common category over the duration from 2012-2019 is social with 23.8% of operations having this as their motivation. Here, the operations use hacktivism as a tool to bring about societal change. These operations include Operation Green Rights, Op Liberation, Op Killing Bay and Op Big Brother. Operation Green Rights is aimed at bringing about an end to climate change by alerting audiences to the most pollutant global corporations. Op Liberation is focused on the for-profit "Troubled Teen Industry" and aims to be a voice for young people who have suffered abuse at teen residential facilities and beyond. Op Killing Bay is an Anonymous operation that aims to end the hunting of dolphins and whales. In a press release Anonymous states "We have been receiving disturbing reports of dolphin slaughter in the village of Taiji in Japan. Innocent and fun loving dolphins are being lured into traps laid out by the Taiji butchers, and are ultimately either captured and transported to marine parks worldwide, or are killed, and their flesh is sold as whale meat by companies."[125] Finally, Op Big Brother is focused on ending global surveillance systems such as facial recognition software utilised by government agencies. In a press release focused on a surveillance system called 'TrapWire' Anonymous states "The software is billed as a method by which to prevent terrorism, but can of course also be used to provide unprecedented surveillance and data-mining capabilities to governments and corporations - including many with a history of using new technologies to violate the rights of

[122] https://news.softpedia.com/news/anonymous-hacks-thai-telecom-firm-to-protest-internet-censorship-plans-495289.shtml Last Accessed 12 April 2021.

[123] https://www.dailydot.com/unclick/anonymous-operation-last-resort-hoax/ Last Accessed 12 April 2021.

[124] Ibid.

[125] https://pastebin.com/2rtHP8Ax Last Accessed 12 April 2021.

citizens. TrapWire is already used in New York, Los Angeles, Las Vegas, Texas, DC, London, and other locales around the USA."[126] it is clear then, that these four operations all aim to bring about societal change in some form. While they will hack governments when protesting, the changes that these operations are advocating for are not specifically political. Indeed, two are focused on animal and ecological rights while the other two are focused more on human rights issues.

The final category identified is religious. Only two or 9.5% of the most frequent operations can be considered to have religious motivations whereby a religious agenda aims to recruit or disavow a religious entity. In this case, both operations aim to disavow an entire belief system. Firstly, OpFuckMohammad which was the personal operation of a hacker named th3inf1d3l who describes themself as a US patriot devoted to the American flag and virtual IED maker who is "unskilled but possessing enough knowledge to wreak havoc." This operation is aimed at the Islamic faith. On a page detailing the operation, th3inf1d3l states "*I am just as offended by the burning of the American Flag as Muslims say they are by media portraying Mohammad poorly. If Muslims can indiscriminately attack, riot and kill and the World says it is justified because we have to respect their beliefs than so can I. To that extent I have started #OpF***Mohammad and will publish any vulnerabilities I find in any Islam related site or server. The world must turn a blind eye to me and call my actions reasonable.*"[127] This operation lasted two years with th3inf1d3l claiming to have affected 250 sites containing vulnerabilities in any Islam related site. It's clear then, that this operation is aiming to disavow Islam. The second religiously motivated hacktivism operation is slightly more complicated, OpAbabil, undertaken by Izz ad-Din al-Qassam Cyber Fighters, occurred as a result of the film 'The Innocence of Muslims' being published online. The operation went through multiple phases with the hacktivist collective claiming that "the United States must still pay because of the insult"[128]. In a post on pastebin they state *"the Operation Ababil is performed because of widespread and organized offends to Islamic spirituals and holy issues, especially the great prophet of Islam(PBUH) and if the offended film is eliminated from the Internet, the related attacks also will be stopped*."[129] As opposed to OpFuckMohammed, Op Ababil is less about disavowing an alternative religion and instead disavowing the United States as a nation while also promoting their religion.

[126] https://pastebin.com/fkzhxLf9 Last Accessed 12 April 2021.

[127] https://th3m0squ3.wordpress.com/opmohammad/ Last Accessed 12 April 2021.

[128] https://pastebin.com/22WJ6m9U Last Accessed 12 April 2021.

[129] https://pastebin.com/22WJ6m9U Last Accessed 12 April 2021.

While the operations analysed all have either a social, political or religious ideology, the computer crimes included in the Cambridge Computer Crime database all appear to have different motivations. The majority of the individuals arrested in the UK under the relevant computer crime legislation all appear to have their own interests as the main motivation. The most common interest is finance with individuals either inserting malware into ATM machines and computers in order to steal money and stealing credit card details; there were also arrests under the Data Protection Act with individuals selling on confidential data or accessing data for purposes other than those which they are intended for. Another motivation for those arrested under the computer crime laws was sexual with many indviduals having been arrested for accessing child sexual abuse material and voyeurism by inserting malware into computers in order to hack into webcams and watch women without their knowledge. It is clear then, that the motivations of hacktivists are vastly different to those undertaking other computer crimes with the motivations of hacktivists being more in line with protestors than cybercriminals.

3.3. Hacktivist Successes

When attempting to understand whether hacktivism could be seen to be a legitimate and successful form of protest rather than a form of cybercrime, the successes of the different operations could be used. Chenoweth found that civil disobedience methods are the most powerful way of shaping world politics (2011). She claims that nonviolent methods are twice as likely to be successful in terms of their stated goals as opposed to violent methods.[130] When looking at the longest running operations outlined earlier there are certainly some successes. For example, with regards to OpSingleGateway the plans for the intended “Great Firewall of Thailand" were rolled back after the planned single gateway internet in Thailand proved to be highly unpopular with citizens.[131] Anonymous coordinated a series of attacks including an attack on state-owned telecom firm, CAT Telecom Pcl, and leaked some data allegedly stolen from the Telco company website[132]. These virtual civil disobedience methods coupled with other forms of resistance led to this success. Another example of a hacktivits’s successes is the rise of Open Access Movement, which was advocated by hacktivist Aaron Swartz before he died. His work

[130] https://www.hks.harvard.edu/faculty-research/policy-topics/advocacy-social-movements/paths-resistance-erica-chenoweths-research Last Accessed 15 April 2021.

[131] https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015 Last Accessed 15 April 2021.

[132] https://www.hackread.com/anonymous-targets-thai-govt-telecom-firm/ Last Accessed 15 April 2021.

led to the op-access initiative whereby research funders across Europe have detailed plans whereby publishers are forced to make papers with a legitimate public interest free to read upon publication if those research projects benefitted from their funding. Furthermore, hacktivists constantly advocate to free other hacktivists that have been imprisoned. Anonymous would repeatedly demand for Chelsea Manning's release after she was imprisoned for downloading and leaking 750,000 classified and sensitive documents to Wikileaks. As a result she was sentenced to 35 years in prison and Anonymous would repeatedly claim "Jail The Criminals Not The Whistleblowers!"[133] However, she was released after only 7 years as President Barack Obama commuted most of the remainder of her sentence before he left office without detailing his reasoning.[134] Moreover, In Canada, the government acted on information that was leaked by a hacktivist. During the Canadian convoy protest as a result of Covid19 vaccine mandates a hacktivist linked to Anonymous hacked the crowdfunding site GiveSendGo and found that more than half of donations to the protest were donated from outside Canada and was found to have funded "extremism" in the country.[135] Based on this information the Canadian prime minister invoked emergency powers in a bid to end protests which included bringing crowdfunding platforms under terror-finance oversight.[136] It could be argued that hacktivism is at times a successful form of protest whether it is working with or against governments.

Yet contrarily, Chenoweth defines success as a movement that has "fully achieved its goals both within a year of its peak engagement and as a direct result of its activities" (2011).[137] She also states that there are four key dynamics for a successful nonviolent resistance campaign. Firstly, the campaign should have a large and diverse population of participants that should be sustained over time. Secondly, the movement needs to be able to create loyalty shifts among business elites, the media and security elites who support the regime. Thirdly, the movement needs to be creative and imaginative in its approach to civil disobedience and should move

[133] https://h4x0r3d.tumblr.com/post/7579913669/message-from-anonymous-operation-manning-by/amp Last Accessed 15 April 2021.

[134] https://www.nytimes.com/2020/03/12/us/politics/chelsea-manning-released-jail.html Last Accessed 15 April 2021.

[135] https://www.theguardian.com/world/2022/feb/14/foreign-money-funding-extremism-in-canada-says-hacker?CMP=Share_AndroidApp_Other 15 February 2022.

[136] https://www.reuters.com/world/americas/canada-police-response-protests-spotlight-after-key-bridge-us-cleared-2022-02-14/ 15 February 2022

[137] https://www.bbc.com/future/article/20190513-it-only-takes-35-of-people-to-change-the-world Last Accessed 15 April 2021.

beyond just mass protests. Finally, the movement needs to be disciplined enough to face direct repression without opting for violence or disbanding. She claims that the last two dynamics are the most important and least understood. This is due to the fact that traditional protests that occur on the street can lead to violent repression and the response from protestors can make or break a social movement. However, while the internet can organise large numbers of people, those in power have also learned to use it for their own advantage. As a result Chenoweth states “My sense is that regimes have basically caught up to whatever advantage there was to the internet for activists,” she says. “The internet provides lots of opportunity for more narrow, discriminating repression that’s more effective than the blunt, brute force that would take place in the streets.” Based on this, it is clear that under this definition of success and using these dynamics, the methods used by hacktivists could be seen to be unsuccessful.

Chenoweth found that for nonviolent protest methods to be successful, 3.5% of the population should actively take part in the protest in order for it to succeed and ensure political change (2011). According to the Office of National Statistics, only 3% of the working population are employed in ICT and telecommunications in the UK which would suggest very few people have the skills needed to take part in a hacktivist campaign. Moreover, in a study between 1983 and 2011 Statista found that at its peak only 11% of the population took part in a protest[138]. Therefore, it would be highly implausible for 3.5% of a population to take part in an act of online civil disobedience. Based on these odds, any successes that have arisen as a result of hacktivist activities could be seen to be exceptional.

Wray, on the other hand, has argued that hacktivism could be seen to be successful and effective in certain circumstances (1999). If the desired goal is to draw global attention to an issue, hacktivism does tend to attract media coverage which could ensure the campaign is effective. Each of the hacks included in the hackmageddon dataset was included in some form of news or online media article detailing the attack and the dataset found 1324 instances of hacktivism over a period of 8 years. Furthermore, Newman argues that hacktivists have large platforms in which to push their ideals (2019). Indeed, the biggest Twitter account that was linked to Anonymous had almost half a million Twitter followers. Moreover, other prominent hacktivist groups also have many spinoff accounts on Twitter as well as accounts across

[138] https://www.statista.com/statistics/285863/protesting-political-engagement-in-great-britain-gb/ Last Accessed 15 April 2021.

different social media platforms.[139] The success of hacktivists was also analysed in part in Chapter 5 where hacktivists post about their successes in order to sustain their movement. While these successes do not correspond to those Chenoweth outlines these could be seen to be successes in the eyes of the hacktivists with many of the Twitter accounts analysed posting about the websites they'd hacked and news articles that had written about their hacks (2011). Additionally, therefore, it would seem that depending on the aims of the hacktivist campaign, they could be seen to be effective.

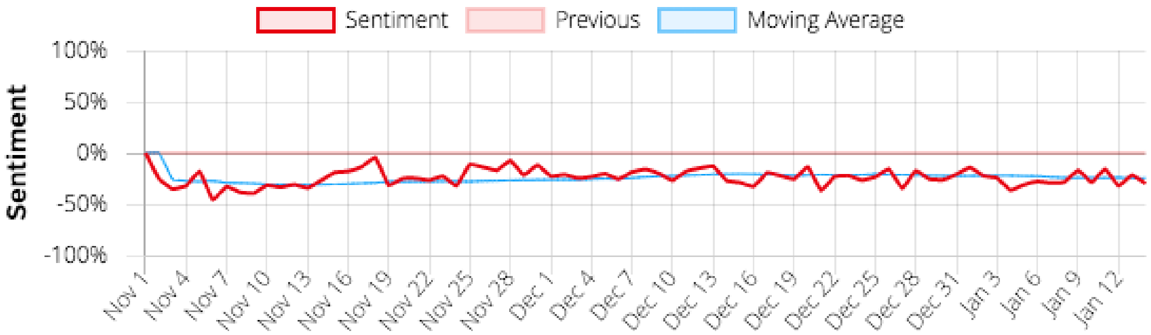
3.4. Public Opinion of Hacktivism

While hacktivists may be featured in news articles and have hundreds of thousands of social media followers, another interesting measurement of the legitimacy of a movement is that of public opinion. Giugni claimed that public support for a movement can be a valuable resource for activists (1998). This is due to the fact that social movements aim to address their messages to both powerholders and the general public. They press those in power for recognition and to get their demands met while also attempting to gain public support and sensitise the public to their cause. While social movements are attempting to gather public support, legislators and those in power will also be paying particular attention to public opinion and where it lies (Giugni 1980: 380). Based on this, it's clear that public opinion could be seen to be an important external factor in the effectiveness and success of social movements. In order to establish the public opinion of hacktivism a sentiment analysis of four key words: 'hacktivism', 'hacktivist', 'electronic civil disobedience' and 'online protest' took place. These words were selected based on the existing literature and to encompass hacktivism as both a tactic and an entity. All four of the key terms' captured content came back as 'Neutral'. This analysis showed the key terms to be more or less neutral throughout the entirety of the analysis with the occasional day where it scored a 'negative' score. The sentiment value is recorded as a score between -1 and 1 and in order to score a positive rating the score needs to be between 0.33 and 1, neutral scores fall between -0.33 and 0.33 and negative scores fall between -1 and 0.33. The four terms placed between 0% and 50% on every day that was analysed suggesting that on the days it scored 'neutral' it was usually at the lower end of the neutral rating. There were no instances of the key terms rising above 0% on the scale throughout the 2 and ½ month analysis. This would suggest that public opinion of hacktivism is somewhat low however, negative sentiment scores may not

[139] https://www.wired.com/story/hacktivism-sudan-ddos-protest/ Last Accessed 15 April 2021.

occur as a result of low public opinion and could, for example, be linked to a post whereby the tone is negative regarding a certain issue that occurs while including the key words.

Chart 4: Screenshot of sentiment analysis results



This overall analysis corresponds to the results from the 2016 CIGI-Ipsos Global Survey on Internet Security and Trust, undertaken by the Centre for International Governance Innovation (CIGI).[140] This survey found that public opinion was split on whether hacktivists have a legitimate place in society. The survey asked 24,143 respondents four questions regarding hacktivists. The first question asked "When it comes to exposing the confidential information of various groups, do you agree or disagree with the following: [Hacktivist groups are breaking the law and should be stopped]." For this first question, 66% of respondents agreed with the statement which is broken down with 35% saying that they strongly agreed and 31% saying that they somewhat agreed. Furthermore, the second questions asked respondents: "When it comes to exposing the confidential information of various groups, do you agree or disagree with the following: [Hacktivist groups are a nuisance and provide no real value]". The majority of respondents agreed with the statement with 26% strongly agreeing and 30% somewhat agreeing. However, the third question asked respondents "When it comes to exposing the confidential information of various groups, do you agree or disagree with the following: [Hacktivist groups play an important role in holding people accountable]" and the majority agreed (58%) that 'hacktivist' groups play an important role in holding people accountable (21% strongly agreed with 27% somewhat agreeing). Moreover, the final question asked "When it comes to exposing the confidential information of various groups, do you agree or disagree with the following: [If nobody else will keep someone accountable, hacktivist groups should step in and do the job]" with just over half of respondents (52%) agreeing with the statements. It is clear that the conflicting results from these questions with over half of respondents thinking that

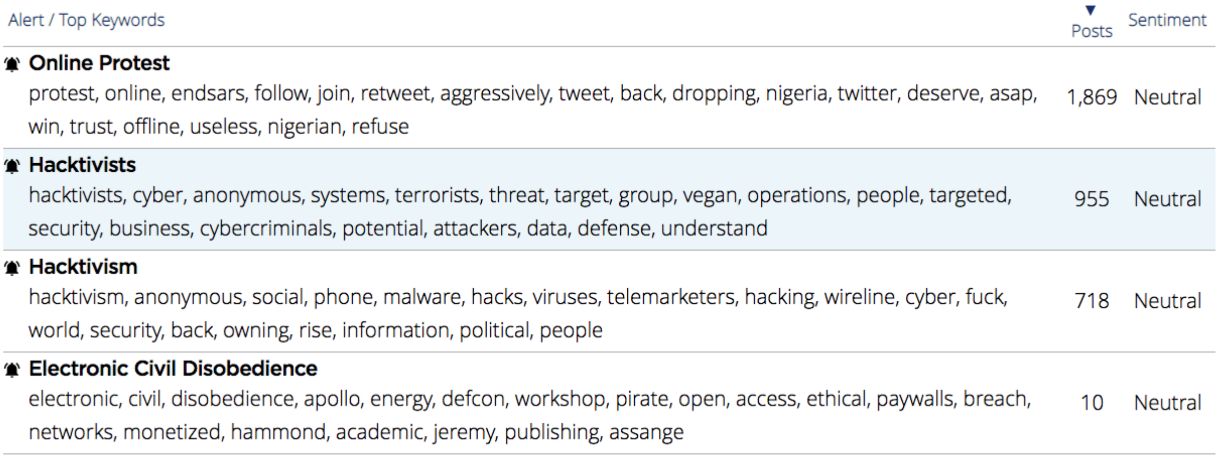
[140] https://www.cigionline.org/internet-survey-2016 Last Accessed 20 Dec 2020.

hacktivism is a nuisance while 58% of respondents also believe that hacktivism plays an important role in society. These results demonstrate that it is difficult to determine whether hacktivism can be seen to have public support, in order for it to be taken seriously as a legitimate form of protest by both the public and those in power.

The term that was analysed with the most posts was ‘online protest’. The key terms that accompanied it in posts most frequently were: ‘protest’, ‘online’, ‘endsars’, ‘follow’, ‘join’, ‘retweet’, ‘aggressively’, ‘tweet’, ‘back’, ‘dropping’, ‘nigeria’, ‘twitter’, ‘deserve’, ‘asap’, ‘win’, ‘trust’, ‘offline’, ‘useless’, ‘nigerian’, ‘refuse’. Three of these key terms can be linked to the #EndSARS protest movement that occurred in Nigeria after a video went viral of a man being killed by the Nigerian Special Anti-Robbery Squad (SARS). This is evidence that at least some of the 1,869 posts analysed featured some level of political ideology and is linked to an existing social movement. The second most common term was ‘hacktivists’ with 955 posts and the accompanying key words being: ‘hacktivists’, ‘cyber’, ‘anonymous’, ‘systems’, ‘terrorists’, ‘threat’, ‘target’, ‘group’, ‘vegan’, ‘operations’, ‘people’, ‘targeted’, ‘security’, ‘business’, ‘cybercriminals’, ‘potential’, ‘attackers’, ‘data’, ‘defense’, ‘understand’. Unlike the ‘online protest’ keywords, these words seem to be more in line with the majority of the world’s government approach to hactivism comparing those who take part to terrorists and cybercriminals despite the literature analysis in Chapter 3 as well as a further examination on the blurring of hacktivism and cyberterrorism in Chapter 7. None of the keywords linked to hacktivism have any political or social movement connotations. Therefore, how these protests are described can greatly affect how they are perceived by the public.

The third most common term in the posts analysed were ‘hacktivists’, identified in 718 posts. The key words associated with this term are ‘hacktivism’, ‘anonymous’, ‘social’, ‘phone’, ‘malware’, ‘hacks’, ‘viruses’, ‘telemarketers’, ‘hacking’, ‘wireline’, ‘cyber’, ‘fuck’, ‘world’, ‘security’, ‘back’, ‘owning’, ‘rise’, ‘information’, ‘political’, ‘people’. The words reflect those that were most common for the previous key word. Negative terms such as ‘malware’, ‘hacks’, ’viruses’ are common despite the overall sentiment being neutral. However ‘political’ was also one of the key terms that accompanied ‘hacktivists’ ensuring that the public understands the concept and how it can be linked to specific ideologies. The final term, ‘electronic civil disobedience’ was only used in 10 posts which suggests that as a term it is much less common and the public may not know what it is. The most common key terms that accompany it are: ‘electronic’, ‘civil’, ‘disobedience’, ‘apollo’, ‘energy’, ‘defcon’, ‘workshop’, ‘pirate’, ‘open’, ‘access’, ‘ethical’, ‘paywalls’, ‘breach’, ‘networks’, ‘monetized’, ‘hammond’, ‘academic’, ‘jeremy’, ‘publishing’, ‘assange’. Unlike the other key words, this one features specific individuals who are known hacktivists. Furthermore, the more negative terms that featured alongside ‘hacktivism’ and ‘hacktivists’ do not feature in this list. Based on these results, it is clear that in order to gain more sympathy from the public, the words in which those undertaking online protests use to frame their activities could be altered to reflect those that take place offline. In doing so, the public may not assume online protestors to be cybercriminals and terrorists and rather consider them to be politically engaged individuals who use technology to protest.

Chart 5: Screenshot of keyword results



Alert / Top Keywords	▼ Posts	Sentiment
Online Protest protest, online, endsars, follow, join, retweet, aggressively, tweet, back, dropping, nigeria, twitter, deserve, asap, win, trust, offline, useless, nigerian, refuse	1,869	Neutral
Hacktivists hacktivists, cyber, anonymous, systems, terrorists, threat, target, group, vegan, operations, people, targeted, security, business, cybercriminals, potential, attackers, data, defense, understand	955	Neutral
Hacktivism hacktivism, anonymous, social, phone, malware, hacks, viruses, telemarketers, hacking, wireline, cyber, fuck, world, security, back, owning, rise, information, political, people	718	Neutral
Electronic Civil Disobedience electronic, civil, disobedience, apollo, energy, defcon, workshop, pirate, open, access, ethical, paywalls, breach, networks, monetized, hammond, academic, jeremy, publishing, assange	10	Neutral

4. Conclusion:

The results of data analysis undertaken on the different databases provide both an examination on the similarities and differences of hacktivism on cybercrime as well as an extension on Chapter 5’s analysis on the similarities of hacktivism and social movements. An analysis of the different datasets linked to hacktivism and cybercrime is useful in regards to answering the research question as it delves into the legitimacy of hacktivism by looking at their targets, the collectives themselves and the methods. It also looks at the longevity of operations that are used to protest. Firstly a comparison between the targets of hacktivists and other forms of cybercrime illustrate a distinction between the two. The targets mostly hit by hacktivists are consistently government organisations, police and political actors which contradicts the UK Governments communications to civilians and companies. Furthermore, cybercriminals were more likely to target private companies and individuals. Moreover, the methods used by both groups show a further distinction with hacktivists using web defacement and DDoS attacks, both of which have been argued to be online versions of traditional non-violent methods of protest: graffiti and sit-ins. Other cybercriminals overwhelmingly rely on fraudulent emails and malware which again shows a distinction with hacktivism. One could argue that governments ought to consider hacktivism as a reflection of offline protest rather than a form of cybercrime. This leads on to the motivations and ideologies of hacktivists that occur in the longest running operations, these range from political, social and religious. Which conflicts with the majority of definitions of hacktivism being solely politically motivated. Rather it would appear that hacktivism could occur for a variety of ideological reasons. These ideologies may have a role to play in the successes and failures of hacktivism. For example, some of the operations aims are very broad and as such could result in a lack of cohesion and conflict. Yet a look at the motivations behind confirmed cyberattacks undertaken by cybercriminals show a further distinction between hacktivism and cybercrime.

A parallel with offline social movements can be found in their use of operations which further distances hacktivism to cybercrime. The most common operations are linked to real world political and contentious events which has led to the conclusion that in essence, hacktivism is indeed based on political beliefs and ideologies. Some successes have occurred as a result of the collective’s different operations however, many of Anonymous’s successes, tend to piggyback off the successes of offline protest groups such as the Black Lives Matter movement. Another way that movements can be successful is by gaining public support for their operations. With regards to hacktivism as a concept, the sentiment analysis found in 3,513 posts was mostly on the lower end of neutral, suggesting that the public do not have a high opinion of hacktivists. Furthermore, the public predominantly find the ideas of hacktivism and hacktivists as threatening linking the terms with cybercriminals, terrorists and attackers. This could be the result of a government campaign that assigns hacktivists with this categorisation. Contrarily, ‘online protest’ and ‘electronic civil disobedience’ as terms were mostly linked to specific protests and hacktivists themselves suggesting that the public are not necessarily opposed to the methods used by hacktivists.

This data analysis has provided a clear picture with regards to the research questions ***'Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?'*** Hacktivism is different to cybercrime both in regards to their targets, their methods and their ideologies. Indeed, it would seem that hacktivists have more in common with traditional social movements than cybercriminals in this regard. The following chapter will examine the legislation in place for cybercrime as a whole in both the UK, Europe and globally before detailing how this legislation is applied to hacktivism specifically.

Chapter 7: The UK's Current Regulatory Approach to Hacktivism

1. Introduction

Following on from the previous theoretical and empirical chapters that answered the first part of the research question, the various legal approaches to hacktivism will be detailed in order answer the second half on whether the currently UK legislative approach is the correct legal approach, or whether greater leniency is required due to the similarities to the methods used by other offline social movements. The aim of this chapter is to understand the current approach the UK takes in dealing with hacktivism which falls predominantly under cybercrime. This is despite the fact that the motivations behind hacktivism are clearly different to those engaging in generic cybercrime, which the previous chapter found appears to be predominantly motivated by financial gain and sexual gratification. Moreover, there are clear parallels between the methods used by hacktivists and social movements which will be elaborated upon further in this chapter. The argument running through this chapter is that the current legal approach to hacktivism needs adjusting to reflect the similarities of hacktivism to social movements. This has been demonstrated throughout this Dissertation both theoretically and empirically with hacktivism being positioned much closer to social movements than cybercrime. The chapter will also show that despite the UK government comparing hacktivism to cyberterrorism, the legislative approach is vastly different and more reflective of offline terrorism.

In order to make this argument, the chapter will firstly examine international shared principles and norms in cybersecurity in order to understand the global approach taken (2). This chapter will then define key concepts including cybercrime, cyberattack and cyberterrorism in order to understand the crimes with which the UK government currently considers hacktivism to be aligned with (3). The soft law mechanisms in both Europe and the UK are analysed (4), as well as the use of agencies to understand the cybercrime landscape and assist in catching cybercriminals (5). The hard law mechanisms in the UK will then be detailed, including the Crown Prosecution Service's approach to hacktivism (6). The ways in which cybercrime legislation is enforced by both the courts and the Police is then outlined (7). The analysis of these mechanisms will allow for a greater understanding of the government's legislative aims with regards to cybercrime, and by extension hacktivism. It will also provide much needed clarity on how hacktivism is currently legislated in order to understand whether it needs to change or whether it is suitable. A content analysis of various government definitions and communications with regards to their language on hacktivism will take place (8). This will illuminate the UK Government's general view of hacktivism as a phenomenon more aligned with cyberterrorism than social movements despite the similarities. The different legislative mechanism will then be analysed specifically with regards to hacktivism (9), whether this is the correct approach and the legislation that has been applied to the methods used by offline social movements in the past. An examination of the legislation that is applied to cyberterrorism will then take place (10) which will demonstrate that while the UK government's communications seem to apply similarities to cyberterrorism, the legislation used to both phenomena are clearly different and as such cannot be considered to be the same entity. Finally, a case study of a well known hacktivist operation that resulted in the arrests of multiple hacktivists will provide context to the legal mechanisms and processes detailed below as well as the reactions of hacktivists (11).

2. International Shared Principles and Norms of Cybersecurity

Before cybercrime can be defined, an understanding of the concept of cybersecurity as well as the global norms and policies that are adopted by states must first take place. This is needed in order to understand the UK's strategy with regards to cybercrime as well as the broader European approach, to gain an understanding of where hacktivism falls within these norms and whether there is any room for adjustment. Clark, Berson and Lin define cybersecurity as "the technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (2014: 2). Due to the increasing nature of cyber related incursions globally there has been an increasing need for nation states to pursue complementary strategies to ensure resilience within the cyber ecosystem (Christou and Raska 2021: 209). As such, many states have affirmed their commitment to ensure "an open, secure, stable, accessible and peaceful ICT [information and communications technology] environment consistent with applicable international and domestic laws" (EEAS 2019a). Many stakeholders have turned to cyber norms, which can be described as the expectations of appropriate behaviour in cyberspace in order to regulate state behaviour and limit damages from malicious online activity (Finnemore and Hollis 2016). As a result, a number of different multi-stakeholder and cross border initiatives have been proposed by the UN, industry coalitions and multi-stakeholder collectives (Calderaro and Marzouki 2022: 2).

Both the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) and the Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (OEWG) are examples of these initiatives. The GGE is US sponsored and mandated to address the applicability of international law, norms, rules and principles to cyberspace and comprises experts from 25 member states. GGE reports are adopted by the UN General Assembly and as such they have no binding power, however their normative influence is significant (Ponta 2021: 1). Working alongside the GGE, the Russian sposored OEWG is a parallel process that occurred as the result of an impasse in the GGE over international humanitarian law and the right to self-defence in cyberspace. The OEWG is open to all interested states and its final report was adopted by all of the 68 participating states in March 2021, which made it the first report on this scale on cybersecurity with direct government participation. It discussed issues on existing and potential threats in cyberspace such as attacks on public infrastructure; international law with members agreeing that the UN Charter is applicable to cyberspace; and the rules, norms and principles of cyberspace which emphasises the need for norms on protecting the public core of the internet. The 2021 GGE report overlaps greatly with the OEWG report, however the GGE report recognises the need for more work on the qualification of key terms in cyberspace and the need for states to take action to determine the nature of due diligence obligations to ensure the cyber infrastructure under their control is not used in ways that could affect the rights of other states. Moreover, differences become evident when considering the sponsorship of the processes. The US backed GGE has an open and free environment in cyberspace as a key goal while the Russian backed OEWG focuses on reaching consensus regarding cyberspace sovereignty and non-interference in states' political affairs (Kiyan 2021: Online). Kiyan states that this "clash between establishing a free internet and controlling cyberspace presents a fork in the road of whether the UN will ultimately play a key role in establishing cyber norms, or whether this split will simply lead to further splintering on this issue" (2021: Online). An additional measure put forward by the NATO Cooperative Cyber Defence Centre of Excellence is the Tallinn Manual which has been described as an essential tool for policy and legal experts on how international law applies to cyber operations.[141] It is a non-legally binding scholarly work that provides an objective restatement of international cyber laws. The Tallinn Manual is currently in its second iteration with work being undertaken for its third iteration to ensure it is up to date with the latest laws and technologies.

[141] https://ccdcoe.org/research/tallinn-manual/ Last Accessed 14 Feb 2022.

Ruhl et al. highlight a number of barriers to the introduction of global cyber norms, including a lack of transparency of state behaviour online, the low barrier to entry of the internet, a dearth of great power cooperation and a lack of incentives for internalising cyber norms (2020:1). Indeed, the internet is still a new innovation and is inherently complex to navigate which can recreate significant hurdles in creating norms (2020: 19). One potential solution is reliant on technical solutions and involves instantiating cyber norms within computer code itself. Yet, there is a need to calibrate expectations for cyber norms as when examining the different paths that the EU, JCROK and ASEAN states have taken for cybersecurity purposes it's clear that there is a level of divergence in the norms of cyberspace. Christou and Raska have claimed that this is in part due to competing interests from certain states that promote an alternative to the Western liberal model of the internet and security (2021: 226). However, they expressed optimism with regards to cooperation between the EU, Japan and the ROK due to their like-mindedness on internet governance, security and data protection. Moreover, Christou and Raska have found that cooperation between the EU and ASEAN countries could currently be considered stagnant but with potential for an upward trajectory, specifically in terms of capacity-building and the possibility of these countries ratifying the Budapest Convention which will be detailed further in this chapter (see Table 7).

	Declining	Stagnant	Upward
ASEAN		X →	
CHINA		X	
JAPAN			X
ROK			X

Table 7 'Future developments: cooperation trajectories with the EU' (Christou and Raska 2021: 225).

It is clear then, that while certain states such as EU members and the US have shared norms and these may improve over time, these are not currently held by all states. It has also been argued that unless there is a catastrophic event that could shock the political system, no great powers would change its behaviour in cyberspace. Ruhl et al. describe this possible event as a 'cyber Hiroshima' and claim that this would lead to a greater understanding on the true costs of cyber operations (2020:19). Currently though, there is a clear fragmentation of cyber norms, with Western states seemingly cooperating but other large powers such as China refusing to engage or implement Western norms. A potential way in which progress could be measured in order to investigate whether any cyber norms are developing is the Carnegie Cyber Norms Index which tracks and compares important milestones in the development of norms in cyberspace.

The nature of hacktivism specifically and its place within the global cyberspace ecosystem does not yet appear to feature in any proposed global principles and norms, and as such nation states aren't guided by any international norms in how they legislate it. While states could indeed take the view that hacktivism is a form of protest and as such leniency should be shown Karagiannopoulos claims that normatively, cybercrime tends to be dealt with through the more traditional, criminal-law based command and control approach whereby states use legal rules backed by criminal sanctions (2018: 92). Palfrey argues that states have increased their regulatory initiatives not only towards state-to-individual interactions but also private entities (2010: 981) (this will be detailed further in section 5). Schmitt and Watts argued that with regards to non-state actors, such as hacktivists, they "are fully subject to states' exercises of sovereignty" such that international organisations are not permitted to take countermeasures for self-defence because "such measures are a response reserved to states" (2016: 2). As hacktivists are non-state actors, even if global cyber norms were more developed and harmonious they still would not apply to them. However, Black has identified a number of problems for state based regulations (2002). They can be poorly targeted or too unsophisticated to deal with complex problems. There can also be insufficient knowledge on behalf of the state actors that are involved in establishing the causes of issues and generating solutions or identifying non-compliance. Finally, they can lead to inadequate implementation of the designated measures. Despite these issues, states can legislate at will to prevent or punish hacktivists. However, they could theoretically increase their tolerance for hacktivism. The different cybersecurity legislative tools implemented both by the European Union, the UK and at times the US that are currently applied to hacktivists will be examined throughout this chapter; however, firstly, the key terms will be delineated.

3. Cyber Definitions

While cybercrime refers to crimes related to a computer, no global cohesive definition exists (Jakobi, 2016). Sexton argues that cybercrime is portrayed as an "existential threat to society, the economy and national security in the UK" (2016: 223). However, Clarke and Knake have noted that attacks that fall under the overarching cybercrime umbrella are over-hyped and have not yet occurred (2010). Instead it is based on 'possibilistic thinking' based on speculative attacks (Furedi 2007: 67-68). The result of the catastrophic discourse surrounding cybercrime is that it implies the need for military and intelligence solutions. Burton argues that cybersecurity is such a broad concept that it requires different legal mechanisms (2015: 299-301). Essentially, cybercrime can be split into two different distinctions. Firstly, there are crimes in which the computer is the tool. These include fraud and dissemination of illegal information. Secondly, there are crimes in which a computer is the target, these include intrusion to networks and computers and attacks on systems. Furthermore, crimes can be split into whether they are 'traditional crimes' that use a computer or whether they are new crimes that could not exist without cyberspace (Brenner and Clarke 2005). Brenner and Clarke argue that these different types of crimes all require different types of legislative approaches (2005: 666). In fact, the National Cyber Security Strategy defines the different types of cybercrime as 1. Cyber-dependent crimes: "crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime" and 2. Cyber-enabled crimes: "traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT."[142] Cyber attack has been defined as "use of deliberate actions and operations ... to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information." (Lin 2010: 63). Additionally, while Chapter 3 detailed the difference between hacktivism and cyberterrorism, it is also important to define cyberterrorism in the context of cybercrime. Saul and Heath define cyberterrorism "as computer-based or electronic or digital means are employed to perpetrate a terrorist act, whether by harming computer systems themselves or using them as a conduit to attack dependent physical infrastructure in the 'real' world" (2021: 206). The legislative differences between hacktivism and cyberterrorism will be examined further in this chapter. Before examining the legislative tools used specifically for hacktivism, the legislative tools and regulations with regards to cybercrime more generally must firstly be detailed in order to understand the context in which hacktivism is regulated, controlled and punished. Once these instruments are delineated it will enable an examination of whether these are the most appropriate tools used for hacktivism or whether leniency should be employed due to its similarities with offline social movements.

[142] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf Last Accessed 4 Dec 2020.

4. Soft Law Mechanisms

Cybercrime, and by extension hacktivism, follows on from a long tradition of trans-border crimes that bodies such as the UN focus on. The response to these crimes tend to be through bilateral and multilateral agreements such as the United Nations Convention against Transnational Organised Crime and its subsequent protocols. These agreements and protocols tend to offer practical solutions for cross-border crimes and the difficulties in dealing with it. Moreover, international cooperation comes with specific needs that aren't reflected in the more traditional legal instruments, such as the need to increase the pace of cooperation for cybercrime cases. The traditional mechanisms in place can lead to handling times that hinder cybercrime investigations. This is due to the fact that the data needed for tracking the offences can be deleted within a short space of time.

Additionally, more traditional crimes predominantly come under the purview of national jurisdictions, which is the result of traditional history and culture influencing criminal law. Thus, criminal law and policies will differ between states. Yet, the internet is unlike any technological innovation that came before it. It is based on global technical standards and any country that ignores these protocols would risk being disconnected from global services. It would stand to reason that the legislation in place regulating it would also need to factor in the globality of the internet. The concept of 'dual criminality' is evidence of these countries being limited to crimes that are criminalised in all cooperating countries. If a country is lacking in legislative tools based on international best practices, they would essentially be prevented from cooperating on an international level and could result in the state becoming an unwitting safe haven. Calderaro details that some cyberthreats are considered to be attacks on the sovereignty of nations and due to this states are taking control of the governance of cybersecurity (2021).[143] Nation states are moving away from the early approach to internet governance that involved external stakeholders such as civil society and industry. Instead, intergovernmental bilateral agreements are coming to the fore (Calderaro 2021).

[143] Calderaro, A.. 2021. "Diplomacy and Responsibilities in the Transnational Governance of the Cyber Domain." In The Routledge Handbook of Responsibility in World Politics, eds. Hannes Hansen-Magnusson and Antje Vetterlein. London; New York: Routledge.

These agreements include the 2001 Council of Europe's Convention on Cybercrime or Budapest Convention which has 67 signatories and suggests that they should establish certain types of conduct as criminal offences in domestic legislation. It was created in order to address the jurisdictional issues that were created by the global internet - the first international treaty that dealt specifically with internet and computer crime and, by extension, hacktivism. The convention was opened for signature on 23 November 2001 by both member states of the Council of Europe and for accession by other non-member States (Council of Europe 2017). It is a negotiated and formally adopted international agreement, as well as a legal framework for cooperation between signatories. It is open for accession by any country that is willing to implement the protocols and cooperate with existing parties. Its aims are to harmonise cybercrime laws and to assist in the successful prosecution of cyber criminals. The convention was developed "in response to a growing concern about the adequacy of legislation criminalising certain activities occurring over computer networks" (Weber 2003: 428-429). It is a multilateral agreement aimed at facilitating international cooperation in the prosecution of cyber criminals. The offences covered by the Convention include those against data and systems such as illegal access, data and system interferences. The Convention also includes offences by means of a computer, however any crime at present could involve a computer system. Thus, the Convention focuses on specific conduct that acquires a new quality when committed using a computer, which reflects the aforementioned second type of cybercrime which would also include hacktivism. The Budapest Convention provides States with a list of methods to be criminalised that assist in the attack of a computer, procedural law tools to assist in the investigation of cybercrime and international police and judicial cooperation suggestions. The Global Forum on Cyber Expertise claims that 15 years after the introduction of the Budapest Convention, it is still the most relevant international agreement on cybercrime[144]. The Budapest Convention is also backed up by additional tools, guidelines and good practice frameworks. The Council of Europe has expanded on the Convention by creating tools focused on law enforcement/service provider cooperation, judicial training, training strategies and specialised services. As well as the Budapest Convention, the transnational European Union Agency for Cybersecurity (ENISA) is the European Union's agency dedicated to improving cybersecurity levels across Europe which lists hacktivism as a threat on emerging technologies.[145]

[144] https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/ Last Accessed 8 Dec 2020.

[145] https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/@@download/fullReport Last Accessed 14 Feb 2022

While a number of standards, norms and good practice frameworks are being developed to meet the challenge of cybercrime, they are not sufficiently implemented across the globe as outlined earlier in this chapter. As such, the Budapest Convention is still the de facto reference for cybercrime legislation globally, even for those states that aren't interested in becoming signatories. The Internet Society has claimed that the Budapest Convention acts as a 'template that most countries, particularly members of the OECD and the Commonwealth, can use to develop cybercrime laws'.[146]

Alongside the Council of Europe Budapest Convention, the European Union has a number of regulatory and policy statements that govern the cyber resilience of member states. These include:

- The 2020 European Strategy for Cyber Security which sets out the EU's approach to how best to prevent and respond to cyber attacks (The EU's Cybersecurity Strategy for the Digital Decade 2020). This increases entities' resilience and as such would reduce the amount of companies that could be impacted by hacktivist campaigns.
- 2013 Directive of Attacks against Information Systems which is a legal framework to approximate the criminal law of the EU Member States in dealing with cyberattacks (Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA). This piece of legislation may have led to the criminalisation of hacktivism throughout European Member States, as the EU considers DDoS to be a form of cyberattack.
- 2016 Network and Information Security (NIS) Directive which is employed to improve Member States' national cybersecurity capabilities (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union). As well as the 2021 NIS2 Directive Proposal which aims to replace the 2016 NIS Directive as a result of the growing threats online and the surge in cyberattacks. The proposed expansion would oblige more entities and sectors to take measures and assist in increasing the level of cybersecurity in Europe into the future. This proposal has been mandated to enter into interinstitutional negotiations (EPRS 2021; PE 689.33). DDoS

[146] https://www.internetsociety.org/blog/2011/09/of-cybercrime-and-cybersecurity/ Last Accessed 23 May 2020.

and similar hacktivist activities would fall under the EU categorisation of cyber attacks, and as such this law would both improve the resilience of companies while ensuring hacktivists are criminalised rather than shown similar treatment to other social movement networks.

As part of these regulatory instruments, the European Union Agency for Network and Information Security (ENISA) mandated that Member States need to implement a National Cyber Security Strategy (NCSS). These strategies are the main documents of nation states to put forward their strategic principles, guidelines, and objectives in order to mitigate the risks associated with cyber security. They act as a roadmap for States in the fight against cybercrime, setting out clear plans to ensure that each State is confident, capable and resilient with regards to the digital world. These strategies are constantly developing alongside technology and the possibilities of cybercrime. All Member States have a National Cyber Security Strategy as a key policy feature that sets out a plan of actions designed to improve the security and resilience of infrastructure and services.

The UK National Cyber Security Strategy (NCSS) is currently in its third iteration. The first Strategy was released in 2011 to cover the period until 2015, the second Strategy currently covered from 2016-2021. It tackled cybersecurity risks, built on collaboration and encouraged skills growth. The 2016-2021 UK NCSS vision for 2021 was that the UK was "secure and resilient to cyber threats, prosperous and confident in the digital world."[147] The most recent strategy only appears to cover 2022 and states that its objectives are "to ensure that the UK remains confident, capable and resilient in this fast-moving digital world; and that we continue to adapt, innovate and invest in order to protect and promote our interests in cyberspace."[148] However, Levi argues that "the wrong terminology encourages us to adopt unsuccessful strategies" (2015: 9). Sexton would agree with this statement and elaborates, stating that this could be an issue for the UK NCSS as State communications all reflect a political decision in securitising cybersecurity by using the general term 'cyberattack' in order to cover a wide range of activities taking place in cyberspace (2016). This, Sexton argues, makes it hard to establish what the strategy is attempting to defend against (2016). It could also lead to a skewering of

[147] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf Last Accessed 4 Dec 2020.

[148] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 Last Accessed 20 Feb 2022.

priorities and thus, mistaken resource allocation. Furthermore, instead of the large scale threats that the NCSS seems to prophesise, the reality is that modern cyberspace is afflicted with small scale hazards that can be avoided relatively easily, as long as users take precautions such as phishing attacks. Sexton, however, was discussing the 2011-2016 cybersecurity strategy (2016). The subsequent strategies have included the growth of cyber skills as well as changing public and business behaviours featured in the UK action plan. The second iteration of the NCSS also briefly defined hacktivism, suggesting it was an issue on the government's radar, however, it is not included in the 2022 strategy which would suggest that the government does not consider it the threat it once did. This may result in some leniency with regards to enforcement, prosecution and sentencing, however, this is something future research could analyse.

5. The Government Use of Agencies

5.1. Delegation to Private Actors

National governments and supranational bodies are not alone in working to tackle cybercrime. Private actors, too, are also working to ensure the web is a safe place (Jakobi, 2013). An example of this is by providing the data needed in investigating and prosecuting offences that the state alone would have struggled to collect. In fact, non-state actors play a vital part in the governance of cybercrime, and by extension hacktivism. Firstly, they are the main addressees of cybercrime regulation. Governments regularly delegate tasks to private businesses when regulating cybercrime, specifically ISPs. This can be seen in the Online Safety Bill that is aimed at ISPs and delegates the task of regulation to Ofcom. However, the legislation used to tackle hacktivism is aimed at the individual rather than large agencies.

At present, the UK response to cybercrime focuses on increasing the reporting of cybercrime, supporting the victims and encouraging the take-up of protective security. It is also aiming to make the UK a high-risk country for criminals to perpetuate internet and computer crimes, as well as identifying the most significant criminals worldwide, degrading the criminal marketplace and undermining the profitability of the business model used by cybercriminals. This would affect hacktivism, as the UK government considers hacktivists to be cybercriminals rather than protestors, despite their similarities. Saunders states that, at present, cybercrime is under-reported because victims believe that there is little that law enforcement can do (2017). However, this is a misconception; even if the criminal is unknown, they are often dependent on facilitators closer to the victim. It has been argued, contrarily, that governments should not be the sole actors in tackling cybercrime. Choucri et al. identify an institutional ecosystem that involves national, international and private organisations (2014). This is due to the fact cyberspace was constructed by the private sector and state involvement in it is a relatively new development. Yet, the wide variety of organisations that exist, such as the International Telecommunication Union (ITU), hold little regulatory power, and there is little evidence of institutional coordination. Contrarily, Choucri et al. claim that the existence of such organisations is “an excellent indication that the international community is taking serious steps to control a cyber threat of epidemic proportions” (Choucri et al. 2014: 28). This, they argue, could lead to more forms of lateral intergovernmental collaboration.

5.2. Information Gathering

When it comes to gathering information from the private sector, policy makers use a diverse range of evidence to propose changes to current policies and to make judgements on threat and risks, as well as mitigation and consequences with regards to cybersecurity. They assist in shaping the national regulatory landscape, as well as public and private sector initiatives. Yet, the evidence that informs policy makers has been criticised. Hussain et al. have suggested that some of the evidence that is provided for decision-makers is contradictory and can carry particular agendas that could impact on its reliability and rigour (2018). They state that the ‘politicisation’ of cyber security evidence is problematic, as they prioritise evidence provided within their states rather than rely on the quality of the evidence. A further issue identified by Hussain et al is that it is difficult to attribute cyber attacks, and to quantify the costs that are the result of insecure computer systems (2018). The result of this knowledge gap is that it makes developing sound responses challenging; without clarity on how and why communities perpetrate cyber attacks, as well as the financial implications, the policy alternatives can be disconnected from the real threat and consequently may target communities that are not malicious actors. Therefore, evidence can only support decision makers to a certain extent.

Moreover, technology progresses rapidly and spans issues such as national security, human rights, infrastructure and industry. This results in policy advisors having to balance a range of conflicting interests that are constantly competing for attention. The concept of cyber security differs depending on different policy communities, making it difficult for a unified response to emerge. These limitations have led to a divergence to traditional policy methods. In the UK the evidence supplied to cyber security policy makers takes the form of expert knowledge, published research, existing statistics, stakeholder consultations, policy evaluations and outputs from economic and statistical modelling (Hussain et al. 2018). In fact, Hussain et al. found that a wide variety of sources are used as potential evidence, including research into trends, open source material, news articles, newsletters, threat intelligence reports, academic research, and intelligence reports from both within the UK and from sister organisations overseas (2018). Crime survey data is also used, as well as existing cyber security breaches and ONS data sources. Many industry technology companies such as BAE Systems, IBM, Microsoft and Cisco supply the government with threat intelligence reports and case studies.

Hussain et al. have also analysed these sources of evidence in order to identify which options genuinely assist in policy making (2018). The first source of evidence is data. Here, they found that both technical and survey data is used, but that the scope of the data collection is not necessarily perfect. A particular case where this can be seen is the use of industry sources for threat intelligence and technological trends, as these magnify the commercial advantage of the data collection. Furthermore, analysis of this data is also abstract and can be highly open to interpretation, though bodies associated with national data collection, such as the Office of National Statistics, have been signposted to be a reliable source of data due to objectivity. The second source of evidence analysed was human evidence. Expert human knowledge is also liable to be biassed, thus objective analysis from human sources needs to be sensitive to the credibility of the entity that collected the information. An additional issue is the heightened interest that cybersecurity attracts, which lends itself to hype and a lack of balanced knowledge to assist in policy making. In fact, it has been argued that ‘cynical and overstated reports ultimately lower the quality of bureaucratic procedures and decision-making’ (Lee and Rid 2014: 2014). The final source analysed is that of providers. This refers to the industry that has emerged over the last few years that is dedicated to cyber security intelligence. It is a mix of major IT and telecommunication companies, which has become a major source of information for the government and used to make better policy. However, geopolitical affiliations can affect the credibility of such sources. For example, Kapersky Labs is a Russian company and despite its highly credible technical reputation, threat intelligence supplied by the company has been discredited. Government agencies also fall under this source, with the National Cyber Security Centre (NCSC) providing guidance and advice to official and private stakeholders. NCSC also provides advice to the wider public through a weekly briefing and data-driven guidance, such as the analysis on an Assessment of the Active Cyber Defence policy. Although it would appear that no source of evidence to assist policy makers is completely credible, the UK CSS 2016-2021 suggests that the government will continue to work with partners, to ensure that the UK is secure and resilient to cyber threats.

5.3. ISPs and Content Providers

The legislative initiatives from governments have impacted on Internet service providers, as well as those that provide content, which is, in essence, transforming them into policy enforcers (Karagiannopoulos 2018) through the extensive information exchanges between the state and corporations. An example of this was evident in Part 4 of the UK's Investigatory Powers Act, whereby broadband internet service providers and mobile operators were forced to log comparatively detailed internet activity of all of their customers for up to 12 months which could then be supplied to a valid authority, irrespective of whether they have a warrant and even if you are not suspected of a crime. This section of the IPA was ruled unlawful by the High Court of Justice in 2018 and consequently had to be amended.[149] It now stands that the authorities can only collect data if they think this person is undertaking a serious crime. A further example of this link between governments and corporations is through Australia's introduction of unprecedented legislation that will allow the government to force encrypted messaging provider WhatsApp to remove encrypted protection for people under investigation[150]. Based on these examples, it is clear that online activists would be unable to rely on the support of private actors to protect their privacy when faced with government requests.

Controversial political statements or a group that is considered to be of interest to the state or law enforcement could be removed online by internet companies to ensure that they are not seen to be contributing to or supporting the messages or groups. Moreover, large internet corporations have consistently refused to host advertisements made by controversial political groups containing contentious content (Nunziato 2005). Thus, these groups are essentially censored due to the market dominance of these Search Engines or websites. An example of this is the removal of Anonymous' accounts on Facebook and Twitter. Twitter has also blocked

[149] https://www.judiciary.uk/wp-content/uploads/2018/04/liberty-v-home-office-judgment.pdf Last Accessed 13 April 2021

[150] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption#:~:text=The%20Australian%20Government%20supports%20cyber,or%20shopping%2C%20can%20occur%20securely. Last Accessed 13 April 2021

the hashtag *#Anonymous*. Karagiannopoulos claims that legislation encourages these infringements on free speech and privacy in order to avoid liability (2018). FinTech companies such as PayPal and Visa have also shown that they are willing to succumb to political pressure, such as when online money processing companies refused to process donations to Wikileaks despite the fact that no criminal charges had been brought against Wikileaks at that time. This will be analysed in detail further in the chapter.

6. Hard Law Mechanisms

6.1 Legislation

In this section, the UK legislative instruments will be outlined for both cyber-enabled and cyber-dependent cases. The legislative instruments used in cyber-enabled cases are a lot more varied and numerous. These include the 1949 Registered Designs Act, the 1959 Obscene Publications Act, the 1960 Indecency with Children Act, the 1968 Theft Act, the 1968 Firearms Act, the 1971 Misuse of Drugs Act, the 1977 Criminal Law Act, the 1978 Protection of Children Act, the 1978 Theft Act, the 1981 Counterfeiting and Forgery Act, the 1988 Copyright Designs and Patents Act, the 1988 Malicious Communications Act, the 1990 Computer Misuse Act, the 1994 Trade Marks Act, the 2002 Proceeds of Crime Act, the 2006 Fraud Act, 2003 Sexual Offences Act, 2003 Communications Act, 2007 Serious Crime Act, 2010 Video Recordings Act, and the 2015 Criminal Justice and Courts Act.

When looking at cyber-dependent crimes, under which hacktivism falls, the legislative instruments used in tackling cybercrime are the 1990 Computer Misuse Act (CMA), the 2000 Regulation of Investigatory Powers Act (RIPA) and the 2018 Data Protection Act. The CMA is the main piece of British legislation that regulates offences or attacks against computer systems. The CMA does not define what a computer is in order to allow for technological development. Instead, a computer is defined by Lord Hoffman in DPP v McKeown and CPP v Jones as “a device for storing, processing and retrieving information”[151]. Thus, this definition can refer to smartphones, tablets and personal computers (PCs). This definition may need to be expanded

[151] https://publications.parliament.uk/pa/ld199697/ldjudgmt/jd970220/mcke02.htm#:~:text=A%20computer%20is%20a%20device,stores%20and%20processes%20that%20information. Last Accessed 12 April 2021

upon to allow for the recent influx of Internet of Things devices. The Crown Prosecution Service has jurisdiction to prosecute any offence covered by the CMA if there 'is at least one significant link with the domestic jurisdiction' (England and Wales) within the case.

The 1990 CMA makes the following acts illegal[152]:

- S.1 Unauthorised access to computer material
- S.2 Unauthorised access with intent to commit or facilitate commission of further offences
- S.3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer
- S.3ZA Unauthorised acts causing, or creating risk of serious damage
- S.3A Making supplying or obtaining articles for use in another CMA offence[153]

Cyber-criminals who have been arrested for breaking into a computer system to impair it or to steal data are predominantly charged with the 1990 CMA. The piece of legislation was deemed necessary after the 1984 Regina v Gold and Schifreen case, whereby journalists Steve Gold and Robert Schifreen hacked into BT's Prestel Viewdata service and accessed the personal message box of Prince Philip. The journalists state that this incident occurred as the result of a number of attempts to shock BT into improving their cybersecurity, after the company showed no signs of increasing the security of its system. Gold and Schifreen were charged and convicted of offences under the 1981 Forgery and Counterfeiting Act, as no computer laws were in place at the time. The specific forgery that the journalists were charged with related to the forging of the password to gain System Administrator privileges, and as a result causing the disruption[154]. Gold and Schifreen were later acquitted when a High Court appeal ruled that no crime had been committed as no data had been stolen. This result caused widespread alarm, due to the lack of legislation at the time which could adequately deal with crime of this sort. It was decided, therefore, that a new act would be introduced to deter criminals from accessing computer systems without authorisation.

[152] https://www.legislation.gov.uk/ukpga/1990/18 Last accessed 13 April 2021

[153] http://www.nationalcrimeagency.gov.uk/publications/760-a-guide-to-the-computer-misuse-act/file Last Accessed 18 Dec 2019

[154] https://www.theregister.co.uk/2015/03/26/prestel_hack_anniversary_prince_philip_computer_misuse/ Last Accessed May 25 2020.

Since its inception, the CMA has been revised a number of times in order to maintain relevance with the changes that have occured in technology and its use. The main update was when it was altered to adhere to the 2015 Serious Crime Act, which referred to how the search and seizure of computer equipment is undertaken. There are three levels of penalty if prosecuted under the CMA, which are dependent on the crime, and severity of the act. The lowest level penalty is up to two years in prison and a £5,000 fine, and is applied if found guilty of unauthorised access to a computer. The next level is applied if found guilty of gaining access to a computer without permission in order to steal data, and the sentence is up to 10 years in prison as well as a fine of unlimited amounts, depending on the severity of the act and damage. The highest level refers to modifying the content of a computer, or providing the tools to do so, and can result in up to life in prison if the damage caused extends to putting human life or national security in danger.[155] This law criminalises DDoS, web defacements and a number of other tools used by hacktivists, despite some of the activities' similarity to the methods used by offline protestors and the clear distinction between hacktivists and cybercriminals detailed in Chapter 6. The number of prosecutions under the terms of the 1990 CMA in 2017 was only 47. This decreased 18% from the previous year, yet law firm RPC have claimed that the threat of cybercrimes is growing and have estimated that there were 1.7 million cyber related crimes between 2016 and 2017. Richard Brevington from RPC claims that the lack of prosecutions is the result of inadequate police resources and as such criminals are able to escape punishment without a thorough investigation[156] . In 2021 the UK government sent out a call for information in order to establish whether law enforcement have the necessary powers to investigate and take action against cyberattacks and their perpetrators, and whether the legislation is still fit for use following the technological advances that have occurred since the introduction of the act 30 years ago. The call also asked for information on how the response to cyber dependent crimes, which would currently include hacktivism, could be strengthened within the legislative context.[157] The responses are not yet public, however, it may be that the UK government's approach to hacktivism will be altered and potentially include a level of leniency to reflect the phenomenon's practice with social movements.

[155] https://www.itpro.co.uk/it-legislation/28174/what-is-the-computer-misuse-act Last Accessed 20 May 2020.

[156] https://www.rpc.co.uk/press-and-media/hacking-prosecutions-fall-for-a-further-year-despite-the-threat-of-cyber-crime/ Last Accessed 18 May 2020.

[157] https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information Last Accessed 10 March 2022

The second piece of legislation is the 2000 Regulation of Investigatory Powers Act (RIPA). RIPA outlaws communication interception on any public or private telecommunication system at any place in the UK without lawful authority. This means that the piece of legislation could be used in hacking cases whereby content was unlawfully intercepted through cyber-enabled means. RIPA would usually be used in prosecuting if the material was unlawfully intercepted while being transmitted, while the CMA would be used when material is acquired through the unauthorised use of a computer. This law may be more aimed at cyber terrorists than hacktkvists, this will be analysed further in the chapter as the legislative tools used to deal with hacktivism are different to cyberterrorist activities. As such, it would appear the government does not equate hacktivism with cyberterrorism and may consider it to be closer on the spectrum to social movement than cyberterrorism. The third and final piece of legislation is the 2018 Data Protection Act which criminalises obtaining or disclosing personal data, procuring the disclosure of personal data, selling or offering to sell personal data. An example used to demonstrate this by the Crown Prosecution Service is that trojans can seem like legitimate computer programs but in fact facilitate illegal access to a computer in order to steal data without the user's knowledge. This could be linked to whistleblowing activities depending on the data that is leaked. These three pieces of legislation all criminalise the activities of hacktivism despite the phenomenon's similarity to offline protests, with the key methods used by hacktivists having clear parallels to methods used by social movements. While hacktivism may cause damage to online property, this is mostly to websites with government domain names and will predominantly not cause a great deal of financial loss. As a result, it would seem that classifying hacktivism as cybercrime within the legislation may not be the best approach and it may need a more tailored solution taking into account the motivation and damage.

6.2 Courts and Prosecution

With regards to the jurisdiction of the courts, the location of the server, its intended audience, the material posted, the nationality of the webmaster and where the information was created and downloaded are taken into consideration by the courts. The ‘substantial measure’ principle set out in R v Smith is also applied, stating that “The English Courts...seek...to apply the English criminal law where a substantial measure of activities constituting the crime take place in England, and restricts its application in such circumstances solely where it can be seriously argued on a reasonable view that these activities should on the basis of international comity not be dealt with by another country" (2004).[158] This measure was further applied in R v Sheppard and Whittle, whereby racially inflammatory material was posted to a website registered in the owner's name and operated by them, with the server based in California (2010). The court came to the conclusion that despite the server being based in California, everything in the case related to England and Wales.

When dealing with the transnational aspect of cybercrime, prosecutors are encouraged to consider Joint Investigation Teams (JIT). This is due to the fact that prosecutors need to be able to co-ordinate their approach and respond quickly to developments and opportunities to prevent illegal activity. A JIT is a team set up between two or more Member States in order to investigate serious cross-border crime with legal duration. This is based on Article 13 of the EU Convention on Mutual Legal Assistance in Criminal Matters. The aim of these JITs is to encourage cooperation between the judiciary and law enforcement in Member States. Prosecutors are also able to refer to the Global Prosecutors E-Crime Network (GPEN), an initiative of the CPS launched in 2008, which aims to assist states in establishing a secure online environment by ensuring prosecutors are able to effectively deal with cybercrime. GPEN provides a database of e-crime prosecutors around the world, a forum for exchange, a collection of e-crime prosecution resource material, a virtual Global E-Crime Prosecutors College and a global community of e-crime prosecutors sharing experiences. The CPS does describe hacktivists as being highly skilled with low criminal intent.[159] This could suggest that currently, the organisation does not have hacktivism as a high priority with regards to prosecution as main the intention of hacktivism is not to break the law but to raise awareness of perceived injustices.

7. Enforcement

Law enforcement efforts and the judiciaries handling cybercrime and those that engage with it will now be evaluated. Leppanen puts forward the suggestion that cybercrimes challenge law enforcement at several levels (2016). Firstly, traditional crimes that occur in the physical world usually involve one location, where the perpetrator is exposed to public view and as a result could be identified by witnesses. However, cybercrimes are only visible to professionals, and

[158] https://publications.parliament.uk/pa/ld200405/ldjudgmt/jd050216/smith-2.htm Last Accessed 12 April 2021

[159] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance Last Accessed 15 Feb 2022

both perpetrators and victims can be based in several different jurisdictions. Furthermore, cybercrimes don't lack likely offenders - perpetrators can work alone, in groups or even on behalf of the state. Thomas suggests that the police need to increase their flexibility in terms of recruitment, and should consider the cumulative skills of its people to ensure that they can deal with the continuing threat (2018). The traditional skills needed by law enforcement no longer apply, and consequently the police should target people in their late teens or early 20s, potentially even hacktivists. They should also consider recruiting cybercrime and financial experts whose skills can be used immediately, as opposed to relying on the traditional model of training recruits broadly, before allowing them to specialise in cybercrime.

Ely claims that, although prosecutors are not substitutes for the law, they do have a certain amount of freedom with regards to the legislation, and can also have an influence on the length of sentences (2004). Greenawalt suggests that prosecutors are seen as law enforcers predominantly, but also as creative agents who can interpret the law and facilitate policy processes (1989). According to the Crown Prosecution Service in the UK, prosecutors decide if there is sufficient, credible evidence to ensure a conviction, as well as making sure that there is a public interest in punishing the offender.[160] However, Reynolds has argued that this prosecutorial discretion can create serious concerns for the balance of power between those involved in the criminal justice system (2013). This power has been further increased as a result of more and more activities being considered as criminal offences, giving prosecutors more power in deciding who to convict.

Generally, the recent trend of criminalising certain behaviours in order to reduce risk, Karagiannopoulos claims, has also increased the tolerance of abuses of power from law enforcement and public officials, undertaken under the veil of public security (2018). Thus, for cases that are likely to attract high levels of media attention, such as those undertaken by hacktivists towards large corporations and the state, leniency will not be an option. This is to ensure that law enforcement or prosecutors do not appear irresponsible or inconsiderate towards public safety. An example of this is the Aaron Swartz case, whereby the campaigner who downloaded large numbers of journals from JSTOR was arrested and pursued by prosecutors on a charge that carried a potential 35 year prison sentence; the subsequent pressure he received by the state led to his suicide. Tim Wu, a law professor at Columbia claimed that it was a harmless act, stating that "There was no actual physical harm, nor actual

[160] https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance Last Accessed 12 April 2021

economic harm. The leak was found and plugged; JSTOR suffered no actual economic loss. It did not press charges. Like a pie in the face, Swartz's act was annoying to its victim but of no lasting consequence."[161] Additionally, the prosecution of the PayPal 14 in the US, whereby about 1,000 computers were used to take down the PayPal site after the corporation withdrew donations to the whistleblower site, Wikileaks, yet only 14 people were charged. Karagiannopoulos claims that the selectiveness over who to prosecute highlights concerns over the fairness and attribution of justice (2018). This overzealous prosecutorial trend in the US has resulted in a polarisation of online activists and prosecutors and thus, it could be argued that the prosecutorial process needs altering with regards to how hacktivists are treated to reflect the practice's similarities to social movements.

Assessing the role that courts play is also crucial in understanding how legislative policies are enforced with regards to hacktivism. Cohen states that courts shape sentencing decisions based on moral implications, as well as how the offence has affected society (1966). However, the majority of hacktivism cases have not progressed to a full court hearing, as they are mostly resolved before this stage with offenders pleading guilty and deals being made. This would affect the attribution of justice from the courts as it should be - instead, judges' capacities are weakened, and powers are given to the prosecutors or the executive. For the cases that do progress to a full hearing, Real and Irwin found that in crimes considered anti-social, the dominant moral rationales influence decisions in a discriminatory way (2010). Therefore, the current trend in mitigating risks and responding to moral panics will influence how judges perceive actions that generate risk, such as the activities pursued by hacktivists. Judges can also be influenced by the social and political norms that form, suggesting that the trend for overly punitive sentencing could influence a judge's decision-making. Moreover, the portrayal of hacktivists as criminals could also impact on the sentencing choices, thus making it harder for a judge to remain impartial.

A further issue that could arise is the ideological influences from the predominantly high socio-economic background of the judges that are trying the cases, meaning that they may not understand or accept radical protests against the status quo. With hacktivist techniques belonging to the ever more common civil disobedience tactics that are available to a greater number of individuals, the judges could have an unconscious bias. Additionally, the techniques

[161] https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy Last Accessed 10 May 2020.

used can be highly technologically advanced, and only those who engage in this technology are able to justify the use of these techniques. Cross found that a judge's cognitive background is important when justifying their ruling (2003). Thus, if they lack the understanding of the technologies and the opportunities they present for online forms of protest, there may be a certain level of prejudice against hacktivists. Using the example of the PayPal 14, the judge imposed a Twitter ban as a bail condition for those that were charged, despite the fact that Anonymous uses many different channels to communicate. This lack of understanding can result in broad interpretations of cybercrime law, which could ultimately lead to unjust judicial decisions.

8. Government Communications on Hacktivism

It is important to examine how the state specifically communicates to the public about hacktivism more broadly. The Government's main communication regarding cybercrime is the UK National Cyber Security Strategy 2016-2021 (NCSS). In the NCSS, the UK government set out their plan for tackling the ever-growing problem of cybercrime, stating their plan to invest £1.9 billion in defending computer systems and infrastructure, improve digital skills in every profession and they set up a National Cyber Security Centre in 2016. The vision of the strategy was that 'the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.'[162] The stated goals were to defend the UK against cyber threats, deter cyber criminals from targeting the UK by taking offensive action in cyberspace, to develop skills needed to ensure that UK citizens are not easy targets and ensure that the UK becomes a digital hub in the future.

The UK National Cyber Security Strategy 2016-2021 refers to hacktivists as decentralised and issue oritientated, stating that, "They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims." (NCSS 2016: 19). This section describing hacktivism is placed alongside terrorists and their methods of targeting information systems and data. The NCSS does not put forward how it plans to tackle hacktivism, leading the

[162] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf Last Accessed 4 Dec 2020.

reader to believe that they will be prosecuted under the 1990 Computer Misuse Act in a similar manner to those undertaking more generic cybercrime. The way in which the description of hacktivism is written in the NCSS also adheres to the idea that the state is pushing the conversation of hacktivism towards public safety and national security messages, despite the acknowledgement that the majority of hacktivists use non-violent and minimally harmful web defacements and DDoS attacks. They state that more able hacktivists are able to inflict great and long-lasting damage to their victims, ensuring that the public fear online activists. The strategy also reduces the impact of the causes hacktivists engage in, by describing them as 'perceived grievances', and does not acknowledge that hacktivism could be considered a social movement. Based on the above, it is clear that the government is using the strategy as a form of moral panic - sharing these messages causes the public to view their safety as being threatened and ensures that hacktivism is not seen favourably,, meaning the government are able to prosecute without any backlash or contradiction. While the UK government has since released its 2022 Cybersecurity Strategy, it does not include any language on hacktivists.

The National Cyber Security Centre, which was formed under the GCHQ umbrella, mentions hacktivism a number of times. In its 2018 Annual Review it simply states that "the threat from criminals, hacktivists and nation states continues to increase and evolve" (National Cyber Security Annual Review, 2018: 6). Again, placing hacktivism alongside criminals and nation states with harmful agendas ensures that those with little knowledge of hacktivism assume that it is something to fear, equatable to criminals, despite the fact that hacktivists are not interested in attacking lay people's systems or data. When searching for hacktivists on the National Cyber Security Centre website, 9 results appear, the first being the speech given by NCSC Chief Executive Ciaran Martin describing the UK's approach to cybersecurity, which again places hacktivists alongside terrorists and criminal gangs.[163] The next result focuses on mitigating denial of service attacks, and refers to hacktivists when explaining the motivation of DDoS attackers, stating that "A group of 'hacktivists' will use their hacking skills for social or political goals, for example launching a DDoS campaign against a company which carry out activities they do not agree with. The attackers are unlikely to be determined in this scenario and the attack likely to be short-lived. The attack is usually a DDoS attack on publicly facing websites, although some groups may attempt "web defacement" of poorly protected servers."[164] This definition appears to be more understanding of the concept of hacktivism, explaining that online

[163] https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk Last Accessed 13 April 2021
[164] https://www.ncsc.gov.uk/guidance/understanding-denial-service-dos-attacks Last Accessed 13 April 2021

activists launch campaigns against companies, that it is short lived and that it occurs as a result of society or politics. However, it is still placed alongside definitions of organised criminals and high capability attackers with state sponsorship, ensuring once again that the public view hacktivists in the same vein as individuals whose goals are to attack public safety and national security.

The only other definition available on the NCSC website is on an advice page to thwart devastating cyber attacks on charities stating that:

- "Hacktivist is a term used to describe hackers motivated by a specific cause, for example to further political or personal agendas or in reaction to events or actions they perceive as unjust.
- Hacktivists have successfully used DDoS attacks to disrupt websites, or have exploited weak security to access and deface them.
- The NCSC considers that the charity sector is not a priority target for hacktivists, but even a limited website takedown or defacement could have financial, operational or reputational implications."[165]

This definition appears to be an expansion on the previous definition. Though it acknowledges that the charity sector is not a target for hacktivists, and explains that hacktivists are motivated by politics, it still uses the same language the state has used in other examples. This definition is similar to the one used in the National Cyber Security Strategy, as it explains hacktivism as a concept and then discusses the threats that they pose, despite stating that charities are not a target. In fact, some hacktivists have shown support for charities. In 2011, Anonymous diverted $500,000 from clients of Stratfor, a security analysis company, to charities including the Red Cross, CARE and Save the Children.[166] Again, the language plays into the discourse surrounding hacktivism as a threat to public safety and national security.

9. Regulatory Approaches to Hacktivist Techniques:

[165] https://www.ncsc.gov.uk/news/advice-thwart-devastating-cyber-attacks-small-charities Last Accessed 13 April 2021.

[166] https://www.theguardian.com/technology/2011/dec/27/security-stratfor-hackers-credit-cards Last Accessed 13 April 2021

Now that the government language around hacktivism has been reviewed, and as such an understanding of the view the UK government takes on hacktivism has been ascertained, the legislative tools detailed above used to tackle cybercrime will be examined with a focus on hacktivism. Firstly, the Budapest Convention is obscure on the issue of hacktivism. Bussolati claims that Article 5 of the Budapest Convention, which concerns System Interference and the serious hindering without right of the functioning of a computer system, leave little room for licit acts of electronic civil disobedience (2017). In fact, the Council of Europe study on national implementation of the Budapest Convention proposed that Member States should criminalise DDoS attacks that do not necessarily cause damage in the form of serious hindering but instead act as a menace for the proper functioning of a system. Therefore, the minimum criminalisation standard set by the Budapest Convention covers DDoS attacks irrespective of the motivations, the type of attack and the amount of damage it creates.

In UK legislation, the updated Section 3 of the CMA, which was updated as result of Article 5 of the 2001 Budapest Convention, corresponds most directly to hacktivist activities, as it refers to any unauthorised act in relation to a computer with intent to impair its operation, hinder access to a program or data held, impair the operation of programs and to enable these actions. The scope of Section 3, specifically in its regards to recklessness which was included with the 2016 Serious Crimes Act, is quite far reaching and could range from someone targeting a hospital power system, resulting in loss of life due to reckless behaviour, to organising a virtual sit-in that targets a network and recklessly takes down the functionality of a wider system. Walker-Osbourne and McLeod have expressed concern regarding the scope of this section, and the acts to which it could apply, claiming that it could target less serious cyber acts that fall within the scope of the Act (2015). MacEwan argues that the extension of liability to include reckless behaviour could lead to questionable prosecutions as a result of the vagueness, specifically as ‘recklessness’ was not suggested by the Budapest Convention and was inserted into the CMA at a time where public scrutiny was not required (2008). The result of this is that hacktivists without a great deal of technical ability would not be able to foresee the amount of disruption that their protest may result in, and consequently could accidentally compromise thousands of computers. Thus, even minor offences could be criminalised and punished due to the expanded Section 3 of the CMA. The upcoming 2021 Online Harms Bill will not include any references to hacktivism. The Online Harms White Paper states: “In line with the position set out in the White Paper, a number of harms will be excluded from scope where there are existing legislative, regulatory and other governmental initiatives in place. The following will be excluded from scope: [...] Harms resulting from cyber security breaches or hacking"[167]. DCMS then elaborate on this by stating "The online harms regulatory framework will not aim to tackle harm occurring through the dark web. A law enforcement response to tackle criminal activity on the dark web is more suitable than a regulatory approach."[168] This, then, would suggest that the Online Harms Bill will not be used for hacktivist activities and, instead, the 1990 Computer Misuse Act will remain the predominant piece of legislation dealing with hacktivism.

When looking at hacktivism, an individual could be liable regardless of the extent of the damage or the duration of the impairment; despite the fact that the 2005 EU Framework Decision (Art.3) stated that minor system interferences should not be criminalised, it was not included in the recent amendments to the 1990 Computer Misuse Act.[169] Furthermore, Articles 4-5 of the Budapest Convention suggest that, although intentional and serious impairment of a system should be criminalised, less serious compromises to computers or data should be excluded from criminal liability, and the Directive 2013/40/EC explicitly states that minor cases should not be criminalised by European Union member states. The CMA neglects to include any language based on the seriousness of attacks, and does not follow any of the suggestions put forth by the European Union. Instead it appears to criminalise all interference regardless of the level of damage it could cause. Thus, it appears that the CMA would punish hacktivists regardless of the outcomes of their civil disobedience, whether positive or negative, suggesting that it is unbalanced and biassed. As the level of damage required for criminal liability seems to be very low with few mitigating circumstances, hacktivists could be less incentivised to take on moral safeguards when organising their actions as, at present in the UK, they are at risk of liability no matter their activities. In fact, Hess and Martin have argued that a lack of tolerance and a high level of punitive provisions can result in more radicalised protests that occur more frequently, often as a form of backlash (2006). This is due to the fact that the punitive measures are considered disproportionate to the actions, and are seen as illegitimate.

Additionally, Maurushat has claimed that the deterrent effect of law and sentencing on hacktivists is limited (2012). Instead hacktivists are driven by higher loyalties and the morality of

[167] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response Last Accessed 12 April 2021

[168] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response Last Accessed 12 April 2021

[169] https://www.legislation.gov.uk/ukpga/1990/18 Last Accessed 13 April 2021

what they claim to be right and just. Tomblin has noted that hacktivists use a political identity in order to justify their illicit activities (2016). However, as with the majority of individual identities, whether political or not, these identities shift and as a result, Tomblin argues that criminal justice systems should not react with harsh punitiveness as these identities are subject to change over time (2016). Furthermore, research has shown that hacktivist collectives tend to be made up of young, tech savvy individuals and Maurushat has found that in many cases, young offenders tend to cease illicit activity upon conviction, therefore using excessive sanctions may be needless (2012).

While the main focus of this chapter is the UK's approach to hacktivism, the US approach will briefly be summarised. Under the domestic regime in the US, at least forty different federal statutes govern computer crimes. The main statute that applies to hacktivism is the Computer Fraud and Abuse Act of 2006, the fifth subsection of which is directed specifically at hacking. This act is the US equivalent of the 1990 Computer Misuse Act. The most appropriate section of the Computer Fraud and Abuse Act of 2006 for prosecuting hacktivists is Section 1030(a)(5)(A), which deals with "knowingly causing a transmission of a program, information, code, or command, which results in intentionally causing damage without authorisation to a 'protected computer." (Karagiannopoulos 2018: 103-104). Two additional offences are included which deal with intentional unauthorised access to a protected computer that results in reckless damage (Section 1030(a)(5)(B)) or damage and loss (Section 1030(a)(5)(C)). The majority of hacktivist tactics that entail manipulating, impairing, suppressing access and availability of information, or compromising the integrity of websites would fall within the scope of these provisions. It would appear then that the US and the UK take a very similar approach to hacktivism and its techniques. Karagiannopoulos states that the US and UK approach of criminalising hacktivism is part of a "knee-jerk reaction despite its rigidity and documented inadequacies eventually intimidates moral protesters or radicalises the more determined ones and essentially generates concerns for the legitimacy of those prosecutions" (2018: 124).

9.1. Regulatory approaches to offline parallels

Now that the current legislative approach has been examined, the possible legislative approach to the offline parallels should be reviewed. Firstly, when comparing hacktivism to other social movements that use offline forms of protest one needs to consider the 1998 Human Rights Act.

The rights that those who undertake the offline protests have are currently different to those who undertake online protests, despite parallels between the two. There are currently two types of human rights obligations that the states must uphold, these are positive and negative obligations. With regards to a positive obligation, states must undertake preventive or protective actions to secure rights under the European Court of Human Rights. This could be assisting counter protests whereby two different protests are taking place in the same location. A positive obligation can require that states protect individuals from the actions of other private parties such as companies. A negative obligation on the other hand, states must refrain from taking specific actions such as placing unnecessary obstacles in the way of protestors.

With regards to the offline parallels of virtual sit-ins, the seventh report from the Joint Committee of Human Rights (2008-2009) states that “The right to freedom of assembly encompasses participation in private and public meetings, processions, mass actions, demonstrations, pickets and rallies. It does not include participation in violent protests but includes, for example, a sit-down protest on a public road even though traffic is disrupted as a result (this may change with the 2021 Police, Crime and Sentencing Bill). To determine whether a demonstration is peaceful, the courts will look at the intention of the organisers” (4)[170]. However, it also states that “SOCPA criminalises protests, whether static or moving, which take place within the vicinity of Parliament or other designated areas without prior notification to, and authorisation by the police.”[171] In addition, the Act makes it a criminal offence to trespass on certain protected sites. These sites include nuclear facilities and certain other facilities which are designated by the Home Secretary if “it appears to the Secretary of State that it is appropriate to designate the site in the interests of national security.” To date, this provision has mainly been used in relation to military facilities” (9). Based on the above legislative acts, it could be argued that DDoS attacks could fall under the right to freedom of assembly as long as the attack is taking place on a government website, unless it is the Parliament’s website (https://www.parliament.uk/), websites linked to nuclear facilities and those designated by the Home Secretary as appropriate to designate in the interests of national security. The state may have a negative obligation to protect them on state websites. Additionally, The European Court of Human Rights states that “In a case in which a demonstration was opposed by the authorities on the basis of disruption to public order, the Court has also made clear that: Where demonstrators do not engage in acts of violence, it is important for the public authorities to show a certain degree of tolerance towards

[170] https://publications.parliament.uk/pa/jt200809/jtselect/jtrights/47/47i.pdf Last Accessed 10 March 2022
[171] Ibid

peaceful gatherings if the freedom of assembly guaranteed by Article 11 of the Convention is not to be deprived of all substance."[172] Moreover, the seventh report from the Joint Committee of Human Rights (2008-2009) also states that "Where, however, the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights"(4).[173] Based on this, in certain circumstances the state has a positive obligation to protect DDoS protests.

When looking at web defacements, the right to freedom of expression could be seen to be applied. The Equality and Human Rights Commission states that Article 10 of the 1998 Human Rights act includes the right to express views allowed or through articles, books or leaflets, television and radio, art, the internet and social media.[174] These rights "may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial disorder or crime, for the protection of health or morals, for the protection of 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." Despite this, however, graffiti has historically been criminalised under the 1971 Criminal Damage Act for destroying or damaging private property[175]. The Department for Environment, Food and Rural Affairs (DEFRA) has defined the term "damage" as "[a]ny informal or illegal marks, drawings or paintings that have been deliberately made by a person or persons on any physical element comprising the outdoor environment, with a view to communicating some message or symbol etc. to others."[176] Additionally, the 2003 Anti-Social Behaviour Act provides penalty notices for graffiti which is usually a small fine. If the graffiti might be considered offensive, the court may impose an antisocial behaviour order.[177] Based on the above, it is clear that the UK government does not see graffiti as an art form protected by

[172] Oya Ataman v Turkey. App no 74552/01. 5 December 2006 paras 41-42.
[173] https://publications.parliament.uk/pa/jt200809/jtselect/jtrights/47/47i.pdf Last Accessed 10 March 2022
[174] https://www.equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression Last Accessed 9 April 2021.
[175] http://eprints.lse.ac.uk/64564/1/limiting%20law%20art%20%20ini%20the%20street%20street%20in%20the%20art.pdf Last Accessed 12 April 2021
[176] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/218806/cop-litter.pdf. accessed 12 April 2021.
[177] https://www.rbkc.gov.uk/parking-transport-and-streets/your-streets/street-cleaning/graffiti-and-fly-posting/graffiti-and-law#:~:text=Penalties%20for%20graffiti,of%20up%20to%2024%20months. Last Accessed 12 April 2021

freedom of expression. Nevertheless, the European Court of Justice puts forward that the right to protest and freedom of expression does not only cover quiet and bland protest, stating that "the freedom only to speak inoffensively is not worth having"[178], while claiming conflictingly that the right to freedom of expression can be interfered with if prescribed by national law.[179]

The above, however, will be affected by the 2021 Police, Crime, Sentencing and Courts Bill if it becomes law. A Home Office fact sheet detailing how the Bill affects the right to protest states:

> “Protests are an important part of our vibrant and tolerant democracy. Under human rights law, we all have the right to gather and express our views. But these rights are not absolute rights. That fact raises important questions for the police and wider society to consider about how much disruption is tolerable, and how to deal with protesters who break the law. A fair balance should be struck between individual rights and the general interests of the community. Having reviewed the evidence, our conclusion is that the police do not strike the right balance on every occasion. The balance may tip too readily in favour of protesters when – as is often the case – the police do not accurately assess the level of disruption caused, or likely to be caused, by a protest. These and other observations led us to conclude that a modest reset of the scales is needed.”[180]

The Bill will restrict protests affecting both the positive and negative obligations outlined above. This tightening of the right to freedom of assembly would suggest that if applied to hacktivism, certain restrictions would then be imposed. While some of these restrictions would not work with regards to hacktivism, such as restrictions on noise, others could apply, such as obstructing access to government buildings. However, the Home Office fact sheet also claims that the UK Police must act in a compatible manner with human rights in relations to Articles 9, 10 and 11 of the European Convention on Human Rights[181]. Moreover, a possible result of the 2021 Police, Crime, Sentencing and Courts Bill could be the expansion of internet protests and, as a result, hacktivism, with individuals assuming they may be less likely to be arrested for taking part in a protest movement. This is an area that could be investigated if the Bill becomes law.

[178] https://www.theguardian.com/law/2012/may/01/five-law-protestors-should-know Last Accessed 12 April 2021

[179] https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814 Last Accessed 12 April 2021

[180] https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-protest-powers-factsheet Last Accessed 12 April 2021

[181] https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-protest-powers-factsheet Last Accessed 12 April 2021

Karagiannopoulos has claimed that there “have already been activities that indicate hacktivism may be becoming a side-tactic for groups such as Extinction Rebellion, which has been reconsidering its future tactics in light of restrictions and preemptive arrests.”[182]

For comparison, the US approach to protecting protest is focused on the distinction between permissible protest and impermissible disruption which has been a subject of controversy for generations (Hampson 2012: 526). According to the U.S. Supreme Court, “the right to engage in peaceful and orderly political demonstrations is, under appropriate conditions, a fundamental aspect of ‘liberty’ protected by the Fourteenth Amendment.”[183] Even protests that inconvenience the audience or that are potentially disruptive to civic peace are generally protected as long as they are not “directed to inciting or producing imminent lawless action and [are not] likely to incite or produce such action.”[184] However, the US government is able to limit protest by imposing reasonable time, place, and manner restrictions on speech; however, with regards to hacktivism it is unclear what form a permissible time, place and manner restriction can take. This is due to the fact that the Supreme Court has yet to address the question of time, place, and manner restrictions on Internet conduct. However, due to the critical importance of certain websites as a source of necessary information, restrictions on otherwise permissible cyberprotests are likely in many circumstances. For example, a virtual sit-in that takes down a political office holder could normally be protected unless it takes place in the period leading to an election. With regards to the idea of web defacements as free speech, in the US, if hacktivism causes damage or involves the manipulation of hijacked private property it will not be considered to be a form of freedom of expression (Hampson 2012: 533). However, Hampson claims that based on the above, the US may be more lenient than the UK in restricting hacktivism (2012: 534).

10. Regulatory Approach to Cyberterrorism

Due to the UK government defining hacktivism alongside terrorism, as was seen in Section 8, it is important to understand whether this similarity is extended at the legislative level. Correia defines cyberterrorism as “cyber enabled activity which intends to advance political, social, or religious ideologies against the public, and cyber dependent activity which further intends to

[182] https://theconversation.com/a-decade-since-the-year-of-the-hacktivist-online-protests-look-set-to-return-163329 Last Accessed 10 March 2022.

[183] Shuttlesworth v. City of Birmingham, 394 U.S. 147, 161 (1969)

[184] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969)

threaten or facilitate damage against the public, properties, and/or systems. Cyber terrorism has the potential to coincide with traditional terrorism" (2021: 17). It encompasses a wide range of illicit behaviours including hacking, sharing online propaganda and radicalising and recruiting individuals. According to the Crown Prosecution Service there needs to be evidence of terrorist motivations for an action to qualify as terrorism.[185] The legislation used to counter the threat of terrorism, and by extension cyberterrorism, in the UK are The Terrorism Act 2000; The Terrorism Act 2006; The Counter-Terrorism Act 2008; and The Counter-Terrorism and Border Security Act 2019. These acts are different to the above mentioned texts that the UK government uses on hacktivists. Yet, there have been questions on whether these acts are the most appropriate tools to tackle cyberterrorism, with Correia offering up the example of the offence of attending a place for terrorist training which is a challenge when applying it to online terrorist training as there is no geographic location. As such, pinpointing the virtual location of training and the location of the IP addresses of each individual taking part in the training would be unfeasible.

However, the draft Online Safety Bill would include sections dedicated to tackling online terrorist activity and content.[186] This Bill is directed at platforms to ensure content is removed, rather than the terrorists themselves. The UK government also released a statement detailing their proposals on driving up security standards in outsourced IT services, which again places the burden on platforms rather than on cyberterrorists. When attempting to deal with cyberterrorists themselves, the UK government have included cyberterrorism in their 2022 National Cyber Security Strategy whereby they state they will be investing in the National Cyber Force which was established in 2020 and "is responsible for operating in and through cyberspace to counter, disrupt, degrade and contest those who would do harm to the UK or its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad."[187] Moreover the National Cyber Force is charged with countering threats from terrorists, criminals and hostile states using cyberspace to operate across borders with the aim of doing harm to the UK and allies. The National Cyber Force's operations are conducted in line with the Intelligence Services Act 1994 and the Investigatory Powers Act 2016. Based on the above legislative and regulatory approach to cyberterrorism, it does appear that the UK government considers hacktivism and cyberterrorism to be distinct phenomena, with hacktivism appearing to be much

[185] https://www.cps.gov.uk/crime-info/terrorism Last Accessed 14 Feb 2022

[186] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf Last Accessed 14 Feb 2022

[187] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-force Last Accessed Feb 14 2022

less of a threat than cyberterrorism. This corresponds to the literature in Chapter 3 whereby there is a confusion regarding the two but they are clearly distinct concepts as hacktivists use web defacements and DDoS attacks as a means to spread political or ideological messages, which may have an intimidatory effect. Yet while terrorists also have a political agenda and send an ideological message, they may intend to be intimidating and their main tools are violence and physical intimidation (Willems 2019: 52). As such, while there may be a blurring of concepts at times when the UK government publishes communications on both concepts, they do not consider the different activities to be similar in terms of the legislation used to tackle them. Therefore, while the government may consider hacktivism and cybercrime to be identical in terms of legislation, they do not see cyberterrorism as falling under this category of crime. The following section will indicate how the legislative landscape is applied in cases of hacktivism with the aforementioned Operation PayPal case study.

11. Case Study - Operation PayPal

A case study will now be used in order to provide context to the above hard and soft law mechanisms and the ways in which they're applied to offences related to hacktivism. The case study has been chosen as it is, to date, the only coordinated hacktivist activity that has resulted in such a vast number of arrests both in the UK and elsewhere. It allows for an in depth concrete analysis on how the above legislative tools are employed with regards to hacktivists rather than simply speculation. Operation PayPal was a series of coordinated attacks by Anonymous. It was originally in response to opponents of Internet copyright infringement. It began in 2010 when Bollywood companies hired a web company to launch DDoS attacks on websites that didn't remove content that infringed copyright legislation from their servers. Anonymous retaliated by attempting to take down the web company's servers. Additional attacks then took place against the Motion Picture Association of America, the International Federation of the Phonographic Industry, the Recording Industry Association of America, the British Phonographic Industry and various intellectual property lawyer websites. The attack then escalated in retaliation for the shutdown of Pirate Bay, the torrent search engine. Anonymous members went on to attack the websites of critics of Wikileaks, Visa, Mastercard and PayPal, as they had stopped payments to Wikileaks as it was being scrutinised by the US government after it had leaked sensitive diplomatic cables[188]. This series of attacks was coordinated on Internet Relay Chat channels as well as Facebook and Twitter. In a statement released at the time, Anonymous claimed that ‘Julian Assange deifies everything we hold dear’ and urged people to ‘spread the current leaked cables’ and even to vote for Assange on TIME’s Person of the Year list in 2010.

A spokesperson for Anonymous went on to tell the Guardian:

“*We’re against corporations and government interfering on the internet. We believe it should be open and free for everyone. Governments shouldn’t try to censor because they don’t agree with it.*

“Anonymous is supporting WikiLeaks not because we agree or disagree with the data that is being sent out, but we disagree with any form of censorship on the internet. If we let WikiLeaks fall without a fight then governments will think they can just take down any sites they wish or disagree with.”[189]

The Guardian was then told by the spokesperson that the collective were planning to move on from DDoS attacks and instead focus on how they could support Wikileaks through mirroring their site. They then went on the claim that “There is no doubt in [Anonymous members’] mind that they are breaking [the] law … but they feel that there’s safety in numbers.”[190] This is after claiming that over a thousand people took part in Operation PayPal.

This was not the case, only 19 people in total were arrested for taking part in Operation PayPal: two people in the Netherlands, 13 people in the United States and four people in the UK. The UK arrests are the focus of this case study. Christopher ‘Nerdo’ Weatherhead, 22, Ashley Rhodes, 27, Peter Gibson, 24, and Jake Birchall, 18, were all arrested relating to offences under the 1990 Computer Misuse Act. The attacks used the Low Orbit Ion Canon, or LOIC, packet-flooding tool, in order to undertake the DDoS attacks. The software does not hide the IP

[188] https://www.cbsnews.com/news/13-members-of-hacking-group-anonymous-indicted-over-operation-payback/Last Accessed 11 May 2020.

[189] https://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypalLast Accessed 11 May 2020.

[190] https://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypalLast Accessed 11 May 2020.

addresses of those taking part in the attacks. Nate Anderson claimed that Anonymous is divided into two groups: Those tech-savvy users who are able to remain anonymous and those who are 'shepherded' by those with technical ability and who tend to get caught by law enforcement officials. However, in this case it wasn't the LOIC software that resulted in the arrests, instead it was an analysis of public IRC logs. These logs were identified and several weeks' worth of chat were captured. Keyword searching took place and the authorities identified that Christopher Weatherhead had used the name 'Nerdo' in online games for quite a while.[191]

The Metropolitan Police chose to focus on organisers and facilitators instead of the 'foot soldiers' (Christopher Weatherhead was an administrator of an AnonOps IRC channel, his case was covered by all major news outlets). The US, on the other hand, targeted participants who had no part in selecting or planning campaigns as well as administrators. Ray Massie who led the investigation in the UK claimed that although Anonymous as a whole appears to be leaderless, the IRC channels that Anonymous used had a power structure and hierarchy. Those at the top of the hierarchy also used private IRC channels, the details of which came to light when suspects were arrested. In these chats users were careless and would provide clues about their location which as a result tied online identities to offline identities. Once these links took place, traditional methods of policing took over with suspects being surveilled and arrested. The suspects were then charged with conspiracy to impair the operation of computers under Section 3 of the 1990 Computer Misuse Act. Weatherhead claimed that the computer belonged to his sister, which corresponds to a piece of advice on the AnonNews website's FAQ page whereby the answer to the question 'Will I get caught/arrested for using it?' when referring to LOIC software was 'Chances are next to zero. Just blame you have a virus or simply deny any knowledge of it.'[192]

The CPS prosecutor of one of the cases claimed that Operation PayPal was a "persistent campaign designed to cause damage, financial losses and press exposure.[193]" Sandip Patel, another prosecutor stated that "this case, simply put, is about hackers who used the internet to attack and disable computer systems - colloquially described as cyber attackers or vandals."[194]

[191] https://www.theregister.co.uk/2012/12/14/uk_anon_investigation/ Last Accessed 13 May 2020.

[192] http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/Dagdelen2.pdf Last Accessed 5 May 2020.

[193] https://www.bbc.co.uk/news/uk-21187632Last Accessed 17 January 2021.

[194] https://www.bbc.co.uk/news/uk-20449474 Last Accessed 6 January 2021.

Both Gibson and Birchall admitted to their part and received a six-month sentence, suspended for two years, while Weatherhead and Rhodes pleaded not guilty to conspiring to impair the operation of a computer. The former was jailed for 18 months and the latter, seven months, after both were found guilty. When handing down sentences, the judge, Judge Peter Testar, claimed that the accused had “got themselves into a bit of an ideological twizzle”[195] further stating that ‘It is intolerable that when an individual or a group disagrees with a particular entity’s activities, they should be free to curtail that activity by means of attacks such as those which took place in this case.’

Coleman posted a snippet of an IRC chat that took place after those involved in Operation PayPal were arrested (2014). In the chat, members of Anonymous displayed sadness and disbelief over the arrests while also acknowledging that it was not unexpected. Coleman described the below correspondence as an “incisive and soulful lament about the hypocrisy of state power” (2004: 194):

“a> Hey folks
a> I presume you’ve all heard the news? :(
b> yes
b>this is a sad day in my mind
b> a new low for governments
a> Sad indeed
a> But, in fairness, not unexpected.
b> well kinda true
a> Yeah
b> but they still have dick all for evidence
a> It’s amazing the way they’re pursuing us all so thoroughly
a> Whilst the actual criminals named in the leaked wikileaks cables are being defended by their respective governments
a> There’s something so sick about that
b> I agree
a> I mean whatever they say about us, we’ve never actually been party to torture or murder
a> Yet they’re spending what must be a shitload of money to get people to come after us

[195] https://www.bbc.co.uk/news/uk-21187632 Last Accessed 17 January 2021.

a> Whilst offering those who have committed the most serious of crimes, diplomatic immunity and all that shite" (quoted in Coleman 2014: 193-194).

These arrests kickstarted a series of arrests across the globe. Coleman claims these arrests are historically exceptional (2014). Weatherhead responded to his arrest by calling out the hypocrisy of the British government who had DDoSed activists tweeting "My Government used a DDoS attack against servers I owned and then convicted me of conducting DDoS attacks. Seriously what the fucking fuck."[196] This case study provides clarity on the cyber regulation currently in place in the UK and how it affects hacktivist activities.

12. Conclusion:

Cybercrime is constantly evolving and growing, with cyber criminals becoming more technically proficient and aggressive over time (Saunders 2017). Interpol have stated that "more and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual" (Interpol 2018). However, Hampson has argued that those methods that do not involve obtaining or exploiting illegal access to a computer or network, that has a primarily expressive motive and that causes little or no permanent damage, should be considered a legitimate form of protest (2012). This would require the same level of tolerance to be shown to offline civil demonstrations as for the methods used by hacktivism. Therefore, as hacktivism has offline parallels with different protest methods, one could suggest that it should not fall under the remit of traditional cybercrime, and should in itself have a different regulatory process.

Despite this, it is clear that the UK government considers hacktivism to be very similar, if not completely equitable, to traditional forms of cybercrime. The 1990 Computer Misuse Act is the legislative effort used to tackle both cybercrime and hacktivism. The National Cyber Security Strategy includes hacktivism in its list of threats to cybersecurity. Both the police and the judicial system place it within the same context as cybercrime, and agencies and private corporations are used to assist the government in its battle with both cybercrime and hacktivism. The state has a number of mechanisms in place to deal with cybercrime, and by extension hacktivism, a few of which were used in the investigation and prosecution of those involved in Operation PayPal. In the following chapter, the Dissertation as a whole will be concluded with the

[196] https://twitter.com/cjfweatherhead/status/431059633071878144 Last Accessed 18 February 2021.

Dissertation being summarised, the research questions being answered, and potential research directions being indicated.

Chapter 8 - Conclusion

1. Introduction

This chapter centres around the main research question and answers it throughout. This chapter will argue that hacktivism is a social movement and as such, the methods used by hacktivists should be legislated differently. It will state that the research methods used and the literature analysed both enabled for the research question and sub questions to be answered definitively. The aim of this chapter is to offer a conclusion to the thesis as a whole and justify its use of literature and its research methods before stating its impact. The first section details both the main research question and the sub-questions. These questions will be answered in detail referencing the existing literature included in this Dissertation as well as the original empirical analyses (2). The chapter will then offer a synopsis of the Dissertation as a whole (3). Following on from this section, this chapter will then explain in greater detail the empirical chapters of the Dissertation, analysing and discussing the results from chapters 6 and 7 (4). The potential research impact of this Dissertation (5) will be detailed, as well as the limitations that were overcome and where this Dissertation could lead to in terms of future research (6) before concluding the Dissertation (7).

Throughout this chapter, the Dissertation's major contributions to knowledge will be returned to. Predominantly, the major contribution to knowledge resulting from this Dissertation is a concrete empirical difference between cybercriminals and hacktivists. Their methods, motivations and their targets differ. Additionally, the discovery from this Dissertation that the majority of operations that hacktivists organise and take part in are linked to offline events are also an important contribution. Both the statistical analysis in Chapter 6 and the rhetoric analysis of the tweets posted by known hacktivists using Stewart's (1980) functional approach to rhetoric used by social movements in Chapter 5 are original contributions to the literature on hacktivism as well as on networked social movements. A secondary contribution to knowledge is the identification within the literature on hacktivism as to whether it is described as a tactic used by protestors or whether it is described as an entity in itself. This chapter concludes that hacktivism is both, having started out as a tactic and then moved beyond that to become an entity as well (outlined in Chapter 3). Moreover, the current regulatory processes that concern hacktivists and the protections in place for offline protestors detailed in Chapter 7 offer an original contribution to the literature on hacktivism.

2. Answering the research questions:

In this section, the key research question and sub-questions will be furthered in reference to the previous literature included in Chapters 2 and 3 and existing regulations explained in Chapter 7, as well as the original research methods employed in the Dissertation in Chapters 5 and 6.

2.1 Is Hacktivism a Social Movement?

Based on the rhetorical analysis, this Dissertation has found that hacktivism should be seen to be a social movement. Castells asserts that taking part in social movements involves engagement in collective action outside of the prescribed channels in order to change the rules (2012). Those engaging in hacktivism are demonstrably taking part in collective action in order to change certain rules. Castells definition makes it clear that hacktivism should be considered a social movement "*Movements are [...] global, because they are connected throughout the world, they learn from other experiences, and in fact they are often inspired by these experiences to engage in their own mobilisation.*" Hacktivists are from all over the globe but connect through the internet specifically for ideological and protest purposes. *"Furthermore, they keep an ongoing, global debate on the Internet, and sometimes they call for joint, global demonstrations in a network of local spaces [...]"* (2012: 250-251). Hacktivists use the internet for debate but using the example of Anonymous's Million Mask Marches they also will gather in local spaces. *"They express an acute consciousness of the intertwining of issues and problems for humanity at large, and they clearly display a cosmopolitan culture, while being rooted in their specific identity."* Hacktivists have a range of ideological motivations as detailed in Chapter 6 and are acutely aware of global issues such as climate change or human rights abuses. Moreover, when returning to the criteria set out in Chapter 2 power dimensions are currently in flux with a shift from physical locations to virtual ones. Hacktivists are able to utilise Internet technologies which allow for the free flow of information to large numbers of people, leading to a vast amount of possibilities for democratic interaction. Langman has outlined how newer social movements are triggered by either a specific event, which causes a spark, or the disgust of the actions of rulers which reaches a peak (2005). This can clearly be identified in the operations analysed with either disgust at rulers (for example, OpUSA) or a specific event triggering the operation into existence (for example, OpSingleGateway). Additionally, Castells states that decision-making in online movements is usually leaderless as a result of the deep distrust most members have in traditional power dynamics. This is certainly apparent in the collectives identified in this thesis. Castells also adds that self-reflection is a constant in new social movements. The organisations frequently interrogate themselves about who they are and what they stand for. This was additionally identified in the rhetoric analysis in Chapter 5 whereby the different hacktivist collectives would regularly state who they are, what their purpose is and what they stand for. Moreover, communication is a key component in all movements, both new and old. This is due to the fact that power can only be challenged if people are willing to communicate. Members must feel shared outrage and togetherness relying on interactive networks of communication. Again, the movements analysed were all focused on communication via Twitter. A great deal of outrage was identified as well as togetherness, predominantly in the form of an ‘us vs them’ dynamic. Finally, according to Castells, newer movements are predominantly motivated by awareness raising and the mobilisation of others, and thus their main aim is used to inform. This was also identified during the rhetoric analysis of the Twitter accounts of key operations. The majority of the movements would most frequently post articles and other bulletin-style tweets in order to allow their followers to both inform and mobilise themselves. It is clear then, that hacktivism as a political entity could be seen to be a social movement, not only as a result of the rhetoric analysis undertaken on the Twitter accounts, but also when examining the nature of the methods, targets and motivations of hacktivism as a whole, and specific campaigns, and comparing it to those outlined in the literature on new social movements.

Is hacktivism different to cybercrime? - This sub-question is answered throughout the Dissertation with the review of the existing literature on hacktivism, the history of hacktivism, the literature of cybercrime and cyberterrorism and in Chapter 6 when comparing the methods, targets and motivations of hacktivism as opposed to cybercrime. The methods used by hacktivists should be considered as separate to historic forms of cybercrime despite the fact that the UK includes hacktivism as a threat in their National Cyber Security Strategy (NCSS) (2016-2021). When outlining cybercriminals as a threat, the NCSS states that “Much of the most serious cyber crime – mainly fraud, theft and extortion against the UK continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries" (2016: 17). Yet, it defines hacktivists as “decentralised and issue-oriented. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to inflict greater and lasting damage on their victims" (2016: 19). Additionally, while the UK government seems to consider hacktivism and cyberterrorism as similar phenomena in their communications to the public, when examining the legislative approaches to both it is evident that the laws applying to both differ greatly. This would suggest that the UK Government sees hacktivists, cybercriminals and cyberterrorists as separate entities.

Furthermore, the key definition drawn upon in this Dissertation states that it is *"the promotion of a sociopolitical agenda usually linked (but not limited) to ideologies typical of traditional activism and applied in cyberspace through individual and collective actions, using illegal or legally ambiguous computer hacking techniques that exploit, hinder, and disrupt the ICT infrastructure's technical features, without the use of physical violence and without gaining direct economic benefits.*" (Romagna 2019: 5). This definition makes it clear that hacktivism is similar to historic offline movements linking it to traditional activism. It also is evident in the definition that there is a sociopolitical agenda linked to the different practices hacktivists use. These motivations are clearly vastly different to cybercriminals whose main motivations were found to be predominantly based around the financial accumulation, sexual gratification and protecting their own interests as found in Chapter 6. Thus, this Dissertation identifies a clear disparity between the motivations behind hacktivism and cybercrime.

What are the main debates that arise when discussing hacktivism? - This Dissertation contributed to the key debates that divide many academics and legislators with regards to hacktivism. Firstly, there was a clear distinction in that some scholars will define hacktivism as a tactic (Denning 2001; Vegh 2003; Jordan and Taylor; 2004; Hampson 2012; Karatzogianni 2015) while others, including the UK government, define it as a political entity (Samuels 2001; Wong and Brown 2013; Romagna 2019). Within this dissertation, hacktivism is considered to be both a tactic and a political entity whereby hacktivism is both a technique and an ideology in that it can form collective actions based upon a shared agenda. This is an original contribution to the literature. Moreover, while hacktivism may have originated as a technique, a culture of hacktivism has grown to a place whereby it could be seen to be a social movement that must be imbued with innovation, style, and technical virtuosity. An additional debate examined within this Dissertation is whether, hacktivism as a tactic could be seen to be a form of civil disobedience or whether it is simply a criminal act. The anonymity of most hacktivists is a sub-debate, with historical civil disobedience scholars stating that, by remaining anonymous, hacktivists are not sacrificing their freedom or accepting the consequences of their actions. While other scholars argue that hacktivists are simply remaining anonymous due to the very high penalties they face that those taking part in offline protests do not (Coleman, 2014; Sauter, 2014; Karagiannopoulos, 2018). Freedom of expression is another key debate with regards to hacktivism. Some online civil disobedience scholars state that those engaging in digital activism are taking part in political discourse and as such are using their right to freedom of expression (Klang, 2004; Karagiannopoulos, 2018; Samuel, 2004). While others on the other side of the debate, including Solomon (2017); Armstrong (2012); McLaurin (2017) suggest that hacktivists that flood websites and deface them are in fact taking away the freedom of expression of others. Furthermore, many individuals contend that hacktivism is simply a form of vigilantism which in turn makes it harder for law enforcement to do their jobs. Yet, some would maintain that hacktivists are simply protesting matters whereby legal options are not possible due to either financial or jurisdictional reach. This thesis has found that the majority of hacktivist operations do not engage in vigilantism, and as such this argument cannot be applied to the phenomena of hacktivism as a whole. The majority of hacktivists will either deface or take down websites, rather than attempt to solve crimes that may impede on law enforcement work. Those engaging in online protests more generally have also been described as lazy and being far removed from the types of protest that occurred during the civil rights era. Yet, this Dissertation concludes that the techniques used by hacktivism is difficult and only a small number of individuals possess the skills needed to successfully engage in electronic civil disobedience.

Are the methods used by hacktivists successful and legitimate forms of protest? - This sub-question was answered in the analysis of the success of hacktivist operations in Chapter 6, as well as the subsequent analysis of public opinion. While the success rate of the operations analysed was low, with very few operations making a significant difference, it should not delegitimise hacktivism as both a practice and a political entity. Rather, the methods used by hacktivists require a specific skill set that most people do not have. As a result, any successes that occur as a result of hacktivist techniques should be acknowledged. Furthermore, the aims of certain operations are too broad for overall successes to be viable. OpIsrael, for example, is focused on bringing down the Israeli government. Bringing down a government as an aim for a protest group will very rarely lead to successes. Furthermore, for this broad aim to be achieved, over 3.5% of a population needs to engage according to Chenoweth (2011). This is highly unlikely with the majority of a population not having the skills, nor the inclination to involve themselves in hacktivism. Furthermore Sterlin has suggested that protests can oftentimes look like a failure in the short-term, despite the fact that most of the power of protests occurs in the long-term effects on society as well as the protestors themselves (2020)[197]. Hacktivism as a form of protest is still in its infancy when compared to more traditional forms of protest such as marches, pamphlets and sit-ins. A key conclusion of this Dissertation is that the lack of short-term successes should not delegitimise hacktivism, rather, time will tell on whether hacktivism is a successful form of protest. With regards to the legitimacy of protest, Olsen states that a protest movement must gain widespread public acceptance in order to be seen as legitimate (1968). The sentiment analysis in Chapter 6 found, however, that overall public opinion towards the key words: hacktivism, hacktivists, online protest and electronic civil disobedience were predominantly neutral verging on negative. While this could be the result of a negative tone in the post analysed as opposed to the public having a neutral to negative sentiment, the words most used in these posts are predominantly associated with criminals and terrorists despite the fact that earlier in the thesis it is clear that while public discourse surrounding hacktivism and cyberterrorism blurs the boundary between both phenomena, the are clearly distinct. It could be seen then that hacktivism is not yet considered a legitimate form of protest by the wider public. However, this may be changing, the invasion of Russia on Ukraine led to the Ukrainian government asking for volunteers of a cyber army to undertake the methods traditionally used by hacktivists.[198] If governments are sanctioning the use of DDoS attacks it could be that hacktivism may be on the way to becoming a legitimate social movement in the eyes of the public.

2.2 If so, Could the Methods used by Hacktivists be Protected by the Same Measures as Offline Protests?

The sub-question: **Should the methods used by hacktivists be regulated differently to cybercrime?** relates back to the analysis of the different regulatory and legislative tools used to deal with hacktivism in Chapter 7, as well as the empirical chapters (Chapters 5 and 6). This question is focused mostly on those methods used by hacktivists that have an offline parallel to the methods used by social movements. These methods are DDoS and web defacements which have a straightforward offline parallel in the form of sit-ins and protest graffiti. With

[197] https://www.theatlantic.com/technology/archive/2020/06/why-protests-work/613420/ Last Accessed 15 Feb 2021

[198] https://abcnews.go.com/Politics/wireStory/ukraine-digital-army-brews-cyberattacks-intel-infowar-83265880 Last Accessed 5 March 2022.

regards to DDoS protests, their offline equivalent, sit-ins, are afforded specific obligations under the Human Rights Act to ensure that a protestor's right to assembly is not being infringed upon. This applies whether the property is public or private, with the state having a positive obligation for sit-ins on private property and a negative obligation on public property. This right, however, may be affected in the future as a result of the 2021 Police, Crime, Sentencing and Courts Bill. Applying the rights that offline protestors receive for political graffiti is somewhat more contentious, as while it could be argued that graffiti should be protected under freedom of expression, it is still regulated against by the government. There are multiple legal mechanisms in order to prevent graffiti, which as a result can lead to punishments that include a small fixed penalty notice and anti-social behaviour orders. Nevertheless, these punishments are much less far reaching than for protestors that deface websites and are charged under the 1990 Computer Misuse Act. While hacktivism is a highly controversial phenomenon, due to the similarities it shares with traditional offline protests and hacktivism, the UK should look at the offline parallels when regulating the techniques used by hacktivism to ensure that the human rights of those taking part in electronic civil disobedience methods are being upheld.

How are the methods used by hacktivists regulated in the UK in 2021? - Hacktivism is regulated by a mix of both soft and hard laws outlined in the previous chapter (Chapter 7). These were introduced over the last 30 years in a bid to reduce the growing global problem of cybercrime. The chief legislative tools the UK government uses to prosecute hacktivists are:

- The 2001 Council of Europe Budapest Convention, which concerns System Interference and the serious hindering without right of the functioning of a computer system.
- The 1990 Computer Misuse Act which refers to any unauthorised act in relation to a computer with intent to impair its operation, hinder access to a program or data held, impair the operation of programs and to enable these actions.

Articles 4-5 of the Council of Europe Budapest Convention outline that, although intentional and serious impairment of a system should be criminalised, those compromises to computers or data that aren't serious should be excluded from criminal liability. Moreover, the EU Directive 2013/40/EC explicitly states that minor cases should not be criminalised by European Union member states. These EU decisions were not included in the amendments that took place with the 1990 Computer Misuse Act, with the UK instead seeking to continue to criminalise less serious offences. The example of Operation PayPal was referred to throughout this Dissertation, with the operation allowing for an examination of the techniques used by prosecutors, the legislative tools used to charge the hacktivists and the judgements from the court cases. Four people were arrested in the UK for taking part in the operation and the suspects were then charged with conspiracy to impair the operation of computers under Section 3 of the 1990 Computer Misuse Act. The case study provided clarity on the murky cyber regulation currently in place to deal with hacktivism. As the research sub-questions have now been answered, the following sections will examine the impact that the Dissertation could have, the limitations that occurred, how these limitations were overcome, and how this Dissertation could be useful in future research.

3. Dissertation Synopsis

Crimes occurring on the Internet are constantly increasing. The number of offences referred to the UK National Fraud Intelligence Bureau increased 35% during the year ending in June 2020 from the previous year. The hacking of social media and email saw a 58% augmentation, while computer viruses and malware saw a 55% expansion[199]. The surge correlates with the amount of large scale data breaches that have occurred throughout the world. In December 2020, network tools specialist SolarWinds announced a breach in its flagship software Orion. The company offers computer network management tools to a wide range of companies, including British accountancy firm Deloitte, and claims that the breach was used in order to penetrate US government networks[200]. The US National Security Adviser Robert O'Brien at the time stated: "It's clearly a sophisticated intelligence operation and no doubt was done by a state actor. And we'll get around to attribution of that at a time and place of our choosing."[201] This breach is just one of tens of thousands of daily cyber attacks that occur globally. However, while it is clear that the majority of these breaches and attacks are the result of malicious intentions, this Dissertation has focused on the hacks that are politically motivated and are instigated by hacktivists. The motivations behind these hacks can include activist motivations such as religious disputes, environmental concerns and anti-globalisation. Furthermore, those that engage in these hacks don't necessarily consider themselves to be cybercriminals. Instead, they would consider themselves to be protestors who engage in "a form of non-violent digital

[199] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020#computer-misuse Last Accessed 28 Feb 2021
[200] https://www.bbc.co.uk/news/technology-55442732 Last Accessed 28 Feb 2021
[201] https://www.bbc.co.uk/news/technology-55442732 Last Accessed 28 Feb 2021

activism where the motive is not, primarily, personal financial gain. Instead, hacktivist campaigns aim to achieve political, social, or religious justice in line with the group's cause."[202]

The illegal methods used by hacktivists are legislated against under the 1990 Computer Misuse Act, which criminalises all forms of hacking and system impairment. The main section used to prosecute hacktivists is Section 3, which refers to any unauthorised act in relation to a computer with intent to impair its operation, hinder access to a program or data held, impair the operation of programs and to enable these actions[203]. However, rather than prosecuting hacktivists under Section 3 of the 1990 Computer Misuse Act, instead perhaps Article 11 of the UK Human Rights Act should be enacted. This article protects the right to protest while also ensuring that the state must take reasonable steps to facilitate the rights to protest. However, the 2021 Police, Crime, Sentencing and Courts Bill may restrict these rights if the Bill becomes law, with static protests, noisy protests and those that cause a nuisance all facing restrictions. As a result, while still having greater rights than online protests, offline protests may soon face harsher legislation, prosecution and punishments.

While Social Movement studies have existed since the 19th century as a result of periods of unrest, applying these theories to Internet mediated communications is a recent phenomenon due to the increasing amount of protests that occur online, and within the context of this Dissertation specifically, hacktivists. Bennett and Segerberg posit that these new technologies mean that traditional theories of collective action no longer fit the ways in which protests are understood. Instead, theories should move away from theories of resource mobilisation, decision making and cost-benefit analyses towards theories of connective action (Bennett and Segerberg 2013). Here, the ways in which protests occur are more personalised than in traditional protests whereby action is organised based on membership or ideology (Bennett and Segerberg 2013:744). However, it has also been argued that Internet activism has not changed the issues that occur as a result of traditional power structures. Indeed, Vromen held that online mobilisation does not rally those who were not already engaged (2008: 81). Nevertheless, Castells' theory of network power, which is the predominant lens through which hacktivism is viewed, puts forward the idea that the move towards digital social movements has resulted in a lack of identifiable centre, formal leadership and vertical power structure (Castells, 2009).

[202] https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism/ Last Accessed 28 Feb 2021

[203] https://www.legislation.gov.uk/ukpga/1990/18/contents Last Accessed 18 Dec 2020.

Castells affirms that “power is based on the control of communication and information, be it the macro-power of the state and media corporations or the micro-power of organisations of all sorts” (2009: 3). Communication is key in social movements, allowing protestors to connect with one another and share their feelings. These Internet mediated communications enable movements to live and grow by providing them with a space to communicate amongst themselves and the outside world. Furthermore, Castells’ theory of networked social movements reflects the idea of the Hacker Ethic which was put forward by Steven Levy in his book Hackers: Heroes of the Computer Revolution and was silently agreed upon by early hackers (1984). This ethic states that:

- ”Access to computers - and anything which might teach you something about the way the world really works - should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better. (1984: 26-36).”

As a result of this ethic, the communications of contentious hacktivist collectives were a key focus of analysis in this Dissertation. Furthermore, other forms of communication are also referred to and analysed including a log from an Anonymous web chat that spans two years. This theory provides a useful backbone throughout this Dissertation as it provides some clarity on modern social movements and whether hacktivism might be classed as a ‘networked social movement’.

It is evident that hacktivism is a contentious subject with myriad debates from scholars, industry and governments. As a result, how it is regulated has also become highly complex. Key to understanding how hacktivism should be regulated is to first establish how it should be legally classified. Therefore, the central research question of this Dissertation was: ‘*Is Hacktivism a social movement? If so, should the methods used by hacktivists be protected by the same measures as those engaging in offline protests?’*

In answering this central question, the following sub-questions were posed: *Is hacktivism different to cybercrime? What are the main debates that arise when discussing hacktivism? Are* *the methods used by hacktivists successful and legitimate forms of protest? How are the methods used by hacktivists regulated in the UK in 2022? Should the methods used by hacktivists be regulated differently to cybercrime?* These questions were answered earlier in this chapter based upon both the existing literature and the empirical research gathered in this Dissertation. The empirical research methods chosen to answer these questions included the following: a statistical analysis of a number of datasets including the Hackmageddon database[204] (01), the Zone H hacktivism dataset[205] (02), Cambridge Computer Crimes database[206] (03), the UK's Department of Culture, Media and Sport's National Cyber Breach survey reports[207] (04), the AnonOps Internet Relay Chat[208] (05) and the sentiment analysis from SWGFL[209] (06) as well as an analysis of the rhetoric used by known and active hacktivist collectives: Anonymous, Chaos Computer Club, Ghost Squad Hackers and Belarussian Cyber Warriors in their different Twitter accounts. Stewart's functional approach was applied to the rhetoric analysis to assess whether the language used by known hacktivists contains the functions of a social movement (1980). This allows for a comparison between hacktivists and offline social movements more generally. These methods were chosen because they offer both an objective look at hacktivism, the methods used by hacktivists, the targets of hacktivists and the motivations of hacktivists and a subjective approach to the language and tools hacktivists use in their communications. The methods utilised investigated the legitimacy and successes of hacktivism assisting in a comparison between hacktivism and cybercrime as well as a comparison to offline movements. These research methods also assisted in establishing how the Internet has altered the protest and social movement landscape. In this context, the UK's current regulatory framework and the impact it has on hacktivism was analysed. The UK as a case study was selected, as the UK was one of the first nation states to implement a cybercrime law (The 1990 CMA). As such, it has led the way in how it manages and deals with cybercrime. Using a national case with an established regulatory process for cybercrime could act as a

[204] Cyber attack timelines 2012-2019. Compiled by Paolo Passeri. Available on request at https://www.hackmageddon.com/. Downloaded on 6 August 2020. Last Accessed on 13 April 2021

[205]Zone H cybercrime archive. Available http://www.zone-h.org/archive/special=1. Downloaded on 29 Jan 2022.

[206] Cambridge Computer Crime Database. Compiled by Professor Alice Hutchings. Available at https://www.cl.cam.ac.uk/~ah793/cccd.html. Last Accessed 27 Jan 2022.

[207] DCMS Cyber Security Breaches Survey 2017-2021 https://www.gov.uk/government/collections/cyber-security-breaches-survey

[208] AZSecure-data.org. Anonops IRC channel Sep 2016-May 2018. Created by the University of Arizona (NSF #ACI-1443019), Drexel University, University of Virginia, University of Texas at Dallas, and University of Utah. Available to download from https://www.azsecure-data.org/internet-relay-chat.html. Downloaded on 6 August 2020. Last Accessed 13 April 2021.

[209] SWGfL Reputation Alerts Sentiment Analysis. Available when subscribed and logged in: https://swgfl.org.uk/login/

potential example for those nations newer to the implementation of cybersecurity regulations and enable them to learn from pitfalls that the UK had to navigate. The datasets utilised in the statistical analysis enabled an in depth investigation into the fact checked operations undertaken by hacktivists and classification of hacktivist ideologies as opposed to those of cybercriminals. The success of these operations were also investigated. A short sentiment analysis of four key terms was undertaken: ‘hacktivism, hacktivists, online protest and electronic civil disobedience’. These were analysed to establish whether the public views hacktivism in a positive or negative light. The keywords were analysed by a software program that analysed the contexts of posts containing the terms. These posts were then assigned either positive, neutral or negative scores.

These methods allow for the research question to be answered as they enable a comparison between not only hacktivists and cybercriminals but social movement members as well. The descriptive analysis allowed for a differentiation between hacktivists and cybercriminals, showing how the current regulatory approach in the UK is unsuitable, while both the statistical analysis and the rhetoric analysis show how hacktivism is similar to social movements. Based on this comparison, the Dissertation then concludes that depending on the methods used and their targets, hacktivists should be protected in the same vein as offline protestors as long as their methods have offline parallels. This research project is different to existing studies on the phenomena of hacktivism and its associated regulatory processes as it offers a holistic approach, studying not only hacktivism as a concept but hacktivists themselves. It also attempts to categorise scholars who view hacktivists as a political practice and those who view it as a political entity, which to the writer's knowledge is the first time this has been undertaken. Using both qualitative and quantitative methods, this Dissertation details how hacktivists use the same language as that used by offline movements. It outlines the methods and targets used by hacktivists and explains how, based on this information, they are fundamentally different to cybercriminals despite the UK government stating otherwise. It also uses previous literature and an examination of the legislation to distinguish it from cyberterrorism. Furthermore, the Dissertation expands on this by showing the similarities hacktivists have with traditional social movements. The key factors included in this Dissertation are the targets, methods of hacktivists, the motivations of the operations and hacks, the successes of operations and the keywords from the sentiment analysis. A look at alternative variables could have resulted in a different result, for example an analysis of different keywords utilised in the sentiment analysis may have resulted in a positive sentiment. Moreover, the Twitter accounts analysed as part of the rhetorical analysis and the functions that were identified as being those used by social movements were also key factors present in the research. Using less prominent Twitter accounts or applying a different set of functions from an alternative social movement scholar could also have resulted in a different result. Yet, the variables selected were chosen based on their suitability in answering the research question, as well as their ability to provide a balance between an objective quantitative method and a subjective qualitative method. The use of the six different datasets were used specifically to ensure a more objective approach to the statistical analysis ensuring the results do not rely solely on one source of data. The results of the research will now be discussed.

3. Results

4.1 Rhetoric analysis results

The majority of the rhetorical functions set out by Stewart in the *Functional Approach to Rhetoric* used by social movements were identified in the tweets analysed in the different hacktivist accounts (1980). These overall functions include ‘Transforming perceptions of history’; ‘Transforming perceptions of society’; ‘Prescribing courses of action’; ‘Mobilising for action’; and finally ‘Sustaining the movement’. With regards to the first function, the hacktivists would reference the past, present and future at times, with the recent past being the most common. It used key terms linked to the past through the use of the ‘throwback’ hashtag and discussion of a return of Nazism and fascism. These references to the past, present and future are predominantly used for mobilisation purposes either through encouraging their followers to work to prevent previous atrocities from occurring again, or to prevent alternative dystopian futures.

The second function, ‘transforming perceptions of society’, was also identified wherein the self and the opposition were key features. The hacktivists did this by informing followers of specific situations in the style of news bulletins, while also employing an ‘us vs them’ dichotomy in order to distance its opposition whether this is a more generalised enemy or a specific one as identified in the tweets of the Belarusian Cyber Partisans. The language used in these tweets was at times emotive and inflammatory in order to motivate followers to troll the opposition to remove their power. The Chaos Computer Club would tweet information in a similar way to civil society groups through the form of campaigns. Specifically with the Anonymous affiliated accounts when outlining who hacktivists are, they will regularly explain that even though they are Anonymous, they are not unanimous and that there are many different ideologies present within the Anonymous membership.

The third function ‘prescribing courses for action’ was also employed by the hacktivists even though some of their protest methods are not legal, as outlined in Chapter 7. However, in general, the tweets that implemented this function prescribed legal courses for action such as the signing of petitions. The Chaos Computer Club would ask followers to sign open letters. Anonymous would offer guidance in order for their followers to remain safe online. Marches and volunteering were some of the offline courses of action that both Anonymous and Chaos Computer Club prescribed. There were instances of some accounts asking their followers to take part in illegal methods of electronic civil disobedience such as doxing or DDoS attacks. While the original function outlined that, when prescribing courses for action movements should prescribe specific tasks to specific people, this was not identified. This could be due to the fact that remaining anonymous is inherent to most hacktivists. Furthermore, as mentioned earlier, hacktivists are predominantly decentralised and leaderless collectives. Finally, it might be that specific tasks are allocated elsewhere in a less public space. Nevertheless, this function is evidently employed by the different hacktivists in the fact that they will prescribe specific courses for action and they have at times defended these.

The fourth function ‘mobilising for action’ was employed in multiple ways by the different hacktivist accounts. It did this by utilising an ‘us vs them’ dichotomy, by demonstrating that the opposition is taking away personal freedoms, and by pressuring the opposition. In doing this, all of the accounts would name and often include its oppositions’ Twitter handles, ensuring its opposition will see the Tweets. This Dissertation has found that Anonymous has also united with other offline social movements such as the Black Lives Matter movement which, as mentioned earlier, enhances their likelihood of successes while also increasing their follower count and level of influence. Moreover, Ghost Squad Hackers will praise Anonymous for their efforts. The inflammatory language is another way in which both Anonymous and Ghost Squad Hackers mobilise for action. This can induce moral panic and improve sympathy levels, which could lead to a surge in engagement leading to greater influence. While at times visceral language is used, so too is stirring and inspirational language which could be seen as another tactic in which hacktivists expand their influence and the likelihood of successful political action. This function is evidently used in order to strengthen ideological engagement, resulting in the mobilisation for political action.

The final function employed by both the Anonymous affiliated accounts and the non-affiliated accounts as identified by Stewart is ‘sustaining the movement’. This is employed in various ways, the first being that, after having successfully taken down the opposition’s website, Anonymous will post #TangoDown as well as posting about its successes when it comes to other methods of electronic civil disobedience more generally. Belarussian Cyber Warriors will retweet other accounts that post about their successes as a means to reinforce their wins. Anonymous celebrates increases in its follower count which enhances its influence and longevity. Moreover, its offline successes are also celebrated, such as the number of people that participate in the global Million Mask March each year. Another way in which Anonymous sustains its movement is by deriding rival hacktivist groups, ensuring the collective can retain their resources. This is unlike Ghost Squad Hackers who praise Anonymous. While the original function outlined that movements will also explain their setbacks, the hacktivists very rarely posts about their own setbacks. This could be due to the fact that hacktivist collectives need fewer resources to traditional movements and do not have donors. Moreover, the non-traditional membership structure results in a lack of accountability.

4.2 Statistical Data analysis

The statistical data analysis of the six datastest empirically demonstrates that hacktivism is different to cybercrime and similar to offline social movements. A key observation from the literature is that hacktivists’ main targets are consistently governments. This is despite the fact that the UK government defines hacktivists in the same category as cybercriminals and cyberterrorists in that the assumption is that they will attack companies. Karagiannopoulos has suggested that the driving force behind the definitions/categorisations used by the UK government appears to be framing hacktivists as something for laypeople to fear, resulting in a conversational shift towards public safety and national security and away from protest (2018). The main targets of cybercrime motivated hacks in statistical analysis were consistently large firms between 2017-2021 according to the DCMS Cyber Breaches survey. This demonstrates a clear difference between hacktivists and cybercriminals, which would suggest that they should be treated differently by the state both in how they should be legislated against and prosecuted. Additionally, the methods used by hacktivists also illustrate a difference between hacktivists and cybercriminals. The methods used by hacktivists identified in the analysis of the Hackmageddon dataset and the Cambridge Computer Crime database are predominantly DDoS and web defacements rather than fraudulent emails and malware. Both DDoS and web defacement have offline parallels in the form of sit-ins and graffiti. In the case of web defacements, it is argued here that hacktivists use these as a calling card, as they direct users to their websites or social media. Both of these methods demonstrate that hacktivists have more in common with offline protestors which again, can be used to justify a shift in the regulation and prosecution of hacktivists towards those who undertake these activities offline. A key recommendation of this thesis is for the current regulatory processes to be reviewed with regards to how they are used to prosecute hacktivists.

A detailed analysis of the specific operations exercised by hacktivists shows that 15% of the operations identified throughout 2012 until 2019 did occur in at least 2 years, with some taking place over a period of 5 years, which indicates a commitment to specific causes and contradicts Security Intelligence's claims that key hacktivists are struggling to find an ideological focus. These causes were found in this Dissertation to be predominantly linked to offline events which then triggered the operation into existence, for example ecological damage or anti-Israel and pro-Palestine sentiment. These events are frequently political and contentious, with Delmas admitting these hacktivists are protective of human rights (2018). They empower dissidents and those who engage in pro-democracy protests. This Dissertation has shown that this is evident in their support of the Black Lives Matter movement in 2020, with Anonymous hacking the Minneapolis Police Department as well as supporting the movement on social media, attending offline rallies and broadcasting it out to their followers. The ideologies linked to these operations are for the most part political in nature with social and religious ideologies included. While an analysis of the Cambridge Computer Crime database shows that the motivations of cybercriminals are financial reward, sexual gratification or personal interest which illustrates further the difference between hacktivism and cybercrime. However, despite the political character of these operations, they are substantially broad in outlook. Entire operations will be dedicated to one nation or simply to the idea of anti-establishmentism and anti-capitalism. This has led to the co-opting of certain operations. This Dissertation has observed that the broadness of these operations could also be linked to the lack of concrete successes. While it could certainly be said that hacktivists have successfully attacked and taken down websites, these protest activities will very rarely result in the overall success of a movement. While some hacktivists have engaged in global movements that have contributed to certain successes, such as the proposed single gateway Internet plans in Thailand, the majority of hacktivist operations will rarely result in concrete successes. This, however, could be due to the idea that in order for a social movement to truly enact change, 3.5% of a population will need to engage and take to the streets (Chenoweth, 2011). It is highly unlikely that 3.5% of a nation will engage in an act of illegal electronic civil disobedience, which could explain the lack of overall successes.

Finally, the public support for a movement is a valuable resource for activists. The results from a sentiment analysis that took place over 2.5 months (1/11/2020 to 15/1/2021) found that the public predominantly views hacktivists in a neutral to negative light. The key words analysed were 'hacktivism', 'hacktivist', 'electronic civil disobedience' and 'online protest' and all words had a neutral sentiment attached. Moreover, on certain days some of the key terms had negative sentiments attached to them - a further analysis could go into detail on why the sentiment dropped on certain days. There were no instances where these key terms had positive sentiments attached to them. However, it is worth explaining that even if a key term has a negative sentiment, it is not necessarily true to say public opinion is definitively negative. It could, instead, be the result of the post as a whole containing some negative sentiment. This could explain some of the negative sentiment towards the key words as hacktivists and hacktivism is focused on specific issues that they are attempting to improve. The posts themselves could be describing negative situations, as opposed to being directly negative towards hacktivists. 'Online protest' and 'electronic civil disobedience' are linked to vastly different results to 'hacktivism' and 'hacktivists'. Both online protest and civil disobedience are linked to specific protests and protestors, while hacktivism and hacktivists are linked to more negative terms such as 'malware', 'hacks', 'viruses', 'terrorists' and 'cybercriminals'. These negative terms associated with 'hacktivist' and 'hacktivism' could potentially explain the neutral to negative sentiment scores in the overall sentiment analysis. The conclusion from the data analysis is that it's apparent that hacktivism is vastly different to cybercrime and can be considered to have a great deal more in common with social movements. The targets, methods and ideologies are similar to social movements and despite their difference in origin and the various debates that arise when discussing hacktivism, one should certainly look to the regulation of the methods used by offline social movements when legislating against the methods used by hacktivists.

5. Impact

This Dissertation answered the research question detailing that hacktivism is considered to be both a tactic and an entity and as a result is a social movement according to the different definitions used to categorise hacktivism. It contributed to this debate by detailing the definitions of those who see hacktivism as purely one or the other before establishing that it should be considered to be both as a result of the natural evolution of hacktivism as being originally a technique to it now becoming a unified culture with its own set of norms. The Dissertation then ascertained that hacktivists use the same rhetorical functions in their communications to outsiders as social movements have historically used, outlined by Stewart (1980). In this way, the collectives were identified as social movements according to the criteria identified by Stewart. The Dissertation then analysed statistics on the methods, targets and ideologies behind hacktivism, with specific investigations of key operations undertaken during the period of 2012 to 2019. The Dissertation then assessed cyber norms globally before detailing the current UK based regulatory processes for cybercrime and cyberterrorism, which includes those pertinent to hacktivism as well as offline protests. These key points present an original contribution to the field, with a specific focus on the functional analysis of the rhetoric used by Anonymous, as well as the descriptive statistical analysis. This Dissertation could be relevant for a variety of different areas of study. Firstly, the UK Government is cracking down on different and creative forms of protest. UK counter terrorism police designated Extinction Rebellion as being among a list of extremist ideologies that should be reported to authorities[210], it would appear that the research could be applied to other such criminalised protest groups. It has also been argued that hacktivism is having a resurgence as a result of the Ukrainian invasion and the country's use of IT professionals in defending their cyber borders and hacking the websites and servers of Russian websites. As a result, hacktivism is now being openly discussed as a possible means for Ukraine to defend themselves.[211] Those working in legal research could find this Dissertation relevant in its description of the different legal mechanisms applied to cybercriminals and specifically hacktivists. Furthermore, this Dissertation provides a more nuanced examination of Internet crimes. Alternatively, those working in sociology and psychology could find this Dissertation relevant in its examination of the motivations and ideologies behind hacktivism, protest groups and other online subcultures.

[210] https://www.theguardian.com/uk-news/2020/jan/10/xr-extinction-rebellion-listed-extremist-ideology-police-prevent-scheme-guidance Last accessed 9 March 2021

[211] https://www.ft.com/content/9ea0dccf-8983-4740-8e8d-82c0213512d4 Last Accessed 10 March 2022.

This Dissertation is of interest to a number of professionals in the UK, including civil servants working for regulatory bodies such as the National Cyber Security Centre, The Department for Culture, Media and Sport, Minister of State for Media and Data, Minister of State for Digital and Culture, and Parliamentary Under Secretary of State for Civil Society in updating their guidance on hacktivism, UK Law Enforcement agencies with regards to softer prosecution of hacktivists, as well as categorisations and implementation on the ground. Third sector groups and digital activist groups such as the Open Rights Group, Article 19 and Big Brother Watch could also be interested in this Dissertation, along with journalists working in both technology and human rights. Finally, scholars working in the field could find this Dissertation to be of interest in its ability to inform them on the issues covered throughout and build upon this research. This Dissertation will also feed into a policy briefing document summarising the key points and offering recommendations to those working in cybersecurity legislation. Academic articles will also be written based on key sections of this Dissertation, including an article on the different regulatory processes in place with regards to hacktivism and a detailed analysis on why hacktivism and cybercrime are fundamentally different.

6. Limitations and Areas for Future Research

There are important considerations and limitations to take into account when evaluating the usefulness of this Dissertation with regards to the wider political discussion of hacktivism. This section explores the main limitations of the Dissertation that include issues with access, issues that arose as a result of the global Covid-19 pandemic and potential researcher bias. Firstly, hacktivists were unwilling to be interviewed to provide context to the research. A potential explanation for their unwillingness is the intricate legal system that surrounds hacktivist activities. Hacktivists don’t want to risk incarceration, while the controversial nature of hacktivism could prevent those in positions of power from honestly answering the interview questions. In addition, while policy makers had been contacted, the Covid-19 pandemic hit as events with stakeholders were supposed to take place, which resulted in the events being cancelled. As a result of this, the datasets were found to provide context to hacktivism as well as original and significant research. An additional limitation of this Dissertation is focused on research bias and generalisability, with the rhetoric analysis being a subjective research method that is impacted by individual life experience. As a result, the discourse analysis in this

Dissertation was undertaken with scepticism and an analytic mentality on the accounts of different known hacktivist collectives, ensuring that all assumptions about the results were questioned. This was further offset with the inclusion of more generalisable research in the form of descriptive statistical analysis on a number of datasets. This not only provided much needed context to the state of hacktivism as it stands, but also provided an alternative method that is less prone to bias to ensure the research questions were answered as objectively as possible. Additionally, the Covid-19 pandemic as a whole led to a very startling change in many individual situations, including how research takes place and where. This Dissertation was predominantly researched and written up from home, which led to its own challenges. As a result, a strict routine was imposed to ensure a balance could be struck, as well as it being finished on time. Future research could go into more depth, with a longitudinal study taking place using an ethnographic approach on the forums used by hacktivists. Furthermore, established researchers with large networks could potentially be more likely to access stakeholders in order to find out where they stand on hacktivism and the legislative tools in place that criminalise certain activities. This could provide interesting results that could explain the reasoning behind why hacktivism is managed as it is. Additionally, the effects of the 2021 Police, Crime, Sentencing and Courts Bill on hacktivism as part of the wider right to protest could also be researched, with individuals researching whether hacktivism will increase as a result of the bill with more protests turning to anonymised online methods to avoid prosecution.

7. Conclusion

Despite the limitations outlined above, this Dissertation still proves to be a source of original and valuable research on a little-known topic that those in the field find to be highly contentious. The purpose of this Dissertation was to understand what hacktivism is, whether it is a social movement, the current regulatory landscape that criminalises it, and how this could be improved. The research question and sub-questions were answered using the research methods. The research identified how hacktivism is different to cybercrime despite it being regulated as such, it identified and outlined the main debates argued by scholars and established that hacktivism is a social movement. The six different datasets used allowed for an examination on hacktivism, its methods, targets and ideologies to take place, as well as an in-depth analysis of the operations, including hacktivism's successes and legitimacy. Furthermore, the current legislative tools were outlined, as well as analysis of whether hacktivism should be regulated differently to cybercrime. The rights that offline protestors received were explained. Consequently, this Dissertation has made an important contribution in understanding what hacktivism is, the legislative tools that criminalise it and whether they should be altered to reflect hacktivism’s offline parallels.

References

Bibliography:

@TH3INF1D3L (2013). OPF***MOHAMMAD. Available at https://th3m0squ3.wordpress.com/opmohammad/. Last Accessed 8 Dec 2020.
fz
Aas, K.F. (2007) *Globalization and Crime*. London: Sage Publications.

Accenture Security (2019). The Cost of Cybercrime. Available at https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50. Last Accessed 1 Nov 2020.

Agarwal, R. and Dhar, V. (2014). Editorial—Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research. *Information Systems Research*. 25(3): 443-448

Alexopoulou, S and Pavli A (2021) 'Beneath This Mask There is More Than Flesh, Beneath This Mask There is an Idea': Anonymous as the (Super)heroes of the Internet? *International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique volume* 34:237–264

Amenta, E, and Young, M. (1999). "Making an Impact: Conceptual and Methodological Implications of the Collective Goods Criterion." In: Giugni, M., McAdam, D. and Tilly, C (Eds) *How Social Movements Matter.* Minneapolis: University of Minnesota Press, 22-41.

Amenta, E, and Caren, N. (2004). The Legislative, Organizational, and Beneficiary Consequences of State Oriented Challengers. In Snow, D., Soule, S. & Kriesi, H. (eds) *The Blackwell Companion to Social Movements*. Oxford: Blackwell.461-89.

Amenta, E., Caren, N., Chiarello, E. and Su Y (2010). The Political Consequences of Social Movements. *Annual Review of Sociology.* 36(1):287-307

Amsden, D. (2013). The Brilliant Life and Tragic Death of Aaron Swartz. Available at https://www.rollingstone.com/culture/culture-news/the-brilliant-life-and-tragic-death-of-aaron-swartz-177191/. Last Accessed 12 April 2021.

Anderson, N (2010). "Operation Payback" attacks to go on until "we stop being angry". Available at https://arstechnica.com/tech-policy/2010/09/operation-payback-attacks-continue-until-we-stop-being-angry/. Last Accessed 12 May 2020.

Anduiza, E., Cristancho, C. and Sabucedo J.M (2014). Mobilization through online social networks: The political protest of the indignados in Spain. *Information, Communication & Society*. 17(6): 750-764,

Anon2world (2020). Ideas are Bulletproof Episode 1: What is Anonymous?. Available at https://www.youtube.com/watch?v=enqfZCRueOo. Last Accessed 13 March 2021.

AnonOps Communications (2012). Anonymous attacked 40 sites the government of Israel! #OpIsrael. Available at http://anonopsofficial.blogspot.com/2012/11/anonymous-attacked-40-sites-government.html. Last Accessed 5 Dec 2020.

Anonymous (2011). “Open Letter from Anonymous to the UK Government”. Available at: https://www.indymedia.org.uk/en/2011/01/472905.html. Last Accessed 7 Nov 2019.

Anonymous (2012). Anonymous - Operation Trapwire has Begun. Available at https://pastebin.com/fkzhxLf9. Last Accessed 7 Dec 2020.

Anonymous (2013). #OpKillingBay- Message From Anonymous. Available at https://pastebin.com/2rtHP8Ax. Last Accessed 7 Dec 2020.

Anonymous (2013). Anonymous #OPSafeWinter Engaged. Available at https://pastebin.com/Hp772vVW. Last Accessed 2 March 2020.

Arendt, H. (1972). *Crisis of the Republic*. London: Harcourt Brace Jovanovich.

Armistead, E. (2004). Information Operations: Warfare and the Hard Reality of Soft Power (Issues in Twenty-First Century Warfare). Sterling: Brassey's US

Armstrong, G (2012). Is Hacktivism a Genuine Form of Protest? Available at https://zine.openrightsgroup.org/features/2012/is-hacktivism-a-genuine-form-of-protest. Last Accessed 21 Sep 2020.

Arthur, C. (2015). What will happen to the Lizard Squad hackers? Available at https://www.theguardian.com/technology/2015/feb/20/lizard-squad-hackers-lulzsec-anonymous-what-will-happen. Last Accessed 21 Nov 2020.

Associated Press (2013). Anonymous hacker attack on Israeli websites 'causes little real damage'. Available at https://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites Last Accessed 5 Dec 2020.

Badiou, A. (2005). *Metapolitics*. London: Verso.

Bajak, F. Ukraine digital army brews cyberattacks, intel and infowar. Available at https://abcnews.go.com/Politics/wireStory/ukraine-digital-army-brews-cyberattacks-intel-infowar-83265880. Last Accessed 5 March 2022.

Barberá P, Wang N, Bonneau R, Jost JT, Nagler J, Tucker J, et al. (2015) The Critical Periphery in the Growth of Social Protests. *PLoS ONE.* 10(11): e0143611.

Bartlett, J. (2014). *The Dark Net*. London: Heinemann.

BBC (2012). Anonymous hackers 'cost PayPal £3.5m'. Available at https://www.bbc.co.uk/news/uk-20449474. Last Accessed 06 January 2021.

BBC (2012). Hacker 'steals' Hertfordshire Police officers' data. Available at https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-19432487. Last Accessed 5 Dec 2020.

BBC (2013). Anonymous hacker group: Two jailed for cyber attacks. Available at https://www.bbc.co.uk/news/uk-21187632. Last Accessed 17 January 2021.

BBC (2020). #EndSars protests. Available at https://www.bbc.co.uk/news/topics/cezwd6k5k6vt/endsars-protests. Last Accessed 12 March 2021.

Beaugrande, R. D., & Dressler, W. U. (1981). *Einführung in die textlinguistik*. Tübingen: Niemeyer.

Benkler, Y. (2011). Networks of power, degrees of freedom. International Journal of Communication,5:721–55.

Bennett LW and Segerberg A (2012) The logic of connective action. Information, Communication and Society 15(5): 739–768.

Bennett, W. L., & Segerberg, A. (2013). *The logic of connective action: Digital media and the personalization of contentious politics.* New York: Cambridge University Press.

Beran, D. (2020). The Return of Anonymous: The Infamous Hacker Group Reemerges From The Shadows. Available at https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/. Last Accessed 21 Nov 2020.

Bergadano, F., Carretto F., Cogno, F. and Ragno, D. (2019) Defacement Detection with Passive Adversaries. *Algorithms*. 12(150).

Bernard, R. (2018). Anonymous And The New Face Of Hacktivism: What To Look Out For In 2018. Available at https://www.digitalshadows.com/blog-and-research/anonymous-and-the-new-face-of-hacktivism-what-to-look-out-for-in-2018/. Last Accessed 10 Dec 2020.

Beyer, J. (2011). *Youth and the generation of political consciousness online.* (Doctoral dissertation). Available from ProQuest Dissertations & Theses database.

Beyer, J. (2013). The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. *Journal of Computer-Mediated Communication*. 19 (2), 141-154.

Bimber, B. (2000). The study of information technology and civic engagement. *Political Communication*, 17 (4): 329-333

Bimber, B., Flanagin, A. J. & Stohl, C. (2005). Reconceptualizing collective action in the contemporary media environment. Communication Theory, 15:389-413.

Black, J (2002) '(2002) Critical reflections on regulation. CARR Discussion Papers (DP 4). Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, London, UK.

Booth, R. (2011). US security firm Stratfor attacked by 'Robin Hood' hackers. Available at https://www.theguardian.com/technology/2011/dec/27/security-stratfor-hackers-credit-cards. Last Accessed 13 April 2013

Breindl, Y., (2009). Internet-based Protest in European Policy- Making: the Case of Digital Activism, International Journal of E-politics, 1(1):57-72

Breindl, Y (2010). Critique of the Democratic Potentialities of the Internet: A Review of Current Theory and Practice. *tripleC* 8(1): 43-59

Brenner, S and Clarke, L. (2005). Distributed Security: Preventing Cybercrime. *The John Marshall Journal of Information Technology and Privacy Law*. 23(4), 659-710.

Brewer, J., & Hunter, A. (1989). *Sage library of social research, Vol. 175. Multimethod research: A synthesis of styles*. California: Sage.

Brownlee, K. (2012). Conscientious Objection and Civil Disobedience. Legal Studies Research Paper No. 2012-15. Available at https://poseidon01.ssrn.com/delivery.php?ID=0850251171170950061091050210050860250520870720450170350730860311000211200671081090990540341000451120220040721050180860900661271120130120440190701181101111200940830060950330620010650841241000750

87087117087064108124104102097103098004030104080106028064106&EXT=pdf&INDEX=TRUE. Last Accessed 12 June 2020

Bruns A (2008) Blogs, Wikipedia, Second Life, and Beyond. From Production to Produsage. New York: Peter Lang.

Brunner, E. (2017). Wild public networks and affective movements in China: Environmental activism, social media, and protest in Maoming. *Journal of Communication* 67: 665-677.

Bryman, A. (2008) *Social research methods*, 4th edition, Oxford, Oxford University Press

Buchwald, C. C. (2000). A case study of Canada's Coalition for Public Information in the information highway policy-making process. *Library & Information Science Research*. 22: 123–144.

Buechler, S. (1995). New Social Movement Theories. *The Sociological Quarterly*. 36(3): 441-464.

Burke, K. (1950). *A Rhetoric of Motives*. New York: Prentice-Hall.

Burton, J. (2015) NATO's cyber defence: strategic challenges and institutional adaptation. *Defence Studies.* 15(4):297-319.

Business Insider (2016). The Anonymous attack on Donald Trump is setting off a hacker civil war. Available at https://www.businessinsider.com/anonymous-hackers-trump-war-2016-3?r=US&IR=T. Last accessed 11 Nov 2020.

Bussolati, N. (2015). "The Rise of Non-State Actors in Cyberwarfare". In: Ohlin, J., Govern, K., and Finkelstein, C. Cyber War: Law and Ethics for Virtual Conflicts.

Cabinet Office (2015). National Risk Register of Civil Emergencies. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf. Last Accessed 13 April 2021.

Cabinet Office (2022). National Cyber Strategy 2022. Available at https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022. Last Accessed 20 Feb 2022.

Calderaro, A. (2018). Social media and politics. In: Outhwaite, William and Turner, Stephen eds. *The SAGE Handbook of Political Sociology*. London: Sage 781-796

Calderaro, A. (2020). Overcoming Fragmentation in Cyber Diplomacy: The Promise of Cyber Capacity Building. Available at https://www.ispionline.it/it/pubblicazione/overcoming-fragmentation-cyber-diplomacy-promise-cyber-capacity-building-25418. Last Accessed 8 Dec 2020.

Calderaro, A & Craig, A (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building, *Third World Quarterly*, 41(6):917-938.

Calderaro, A.. 2021. “Diplomacy and Responsibilities in the Transnational Governance of the Cyber Domain.” In The Routledge Handbook of Responsibility in World Politics, eds. Hannes Hansen-Magnusson and Antje Vetterlein. London; New York: Routledge.

Calderaro, A and Marzouki, M (2022). Global Internet governance: an unchartered diplomacy terrain. In: Calderaro, Andrea and Marzouki, Meryem eds. *Internet Diplomacy: Shaping the Global Politics of Cyberspace*. Rowman & Littlefield.

Cammaerts, B. (2007). Media and communication strategies of glocalized activists: Beyond media-centric thinking. In: Cammaerts, Bart and Carpentier, Nico, (eds.) *Reclaiming the Media: Communication Rights and Democratic Media Roles.* European Communication Research and Education Association series (3). Intellect: Bristol, UK. 265-288.

Cammaerts, B (2013). Networked Resistance: The Case of WikiLeaks. Journal of Computer-Mediated Communication. 18(4):420-436.

Captain, S. (2011). The Real Role Of Anonymous In Occupy Wall Street. Available at https://www.fastcompany.com/1788397/real-role-anonymous-occupy-wall-street. Last Accessed 1 March 2021.

Caren, N., Andrews, K. & Lu, T (2020). Contemporary Social Movements in a Hybrid Media Environment. *Annual Review of Sociology*. 46(1):443-465.

Castells, M. (1997). *The Power of Identity*. Cambridge: Blackwells.

Castells, M. (1999). ‘An introduction to the information age’. In H. Mackay & T. O’Sullivan (Eds.), *The media reader: Continuity and transformation*. London: Sage. 398–410.

Castells, M. (2007). Communication, Power and Counter-power in the Network Society, International Journal of Communication (1):238-266

Castells, M. (2009). *Communication Power*. New York: Oxford University Press.

Castells, M (2012). *Networks of outrage and hope – social movements in the Internet age*. Chichester: Wiley.

Cavelty, M. D. (2010). Cyber-Security. In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies*: 154-162. London: Routledge.

Centre for International Governance Innovation & IPSOS (2016). 2016 CIGI-Ipsos Global Survey on Internet Security and Trust. Available at https://www.cigionline.org/internet-survey-2016. Last Accessed 20 Dec 2020.

Chadwick, A. (2006). Internet Politics: States, citizens, and new communication technologies. New York, NY: Oxford University Press.

Chaos Computer Club (2021). *Hacker Ethics*. Available at https://www.ccc.de/en/hackerethics. Last Accessed 21 Jan 2021.

Charlet, K. and King, H. (2020). The Future of Cybersecurity Policy. Copublished by the IEEE Computer and Reliability Societies. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8965260 Last Accessed 3 Dec 2021.

Chenoweth, E. & Stephan, M. (2011). *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict*. New York: Columbia University Press

Choucri, N., Madnick, J., & Ferwerda, J. (2014) Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*. 20(2), 96-121.

Christou G., Raska M. (2021) Cybersecurity. In: Christiansen T., Kirchner E., Tan S.S. (eds) *The European Union's Security Relations with Asian Partners*. The European Union in International Affairs. Cham: Palgrave Macmillan

Cimpanu, C (2015). Anonymous Hacks Thai Telecom Firm to Protest Internet Censorship Plans. Available at https://news.softpedia.com/news/anonymous-hacks-thai-telecom-firm-to-protest-internet-censorship-plans-495289.shtml. Last Accessed 10 Dec 2020

Clark, D, Berson, T and Lin, H.S (2014) *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.* National Research Council. Washington, DC: The National Academies Press.

Clarke, R and Knake. R (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins

Cloudflare (2020). What is a DDoS Attack? Available at https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/. Last Accessed 2 Dec 2020.

Cohen, C. (1966). Civil Disobedience and the Law. *Rutgers Law Review*. 21(1), 1-42.

Cohen, J.L (1985). Strategy or Identity: New Theoretical Paradigms and Contemporary Social Movements. *Social Research: An International Quaterly*. 53(1): 663-716.

Coleman, G. (2011). Anonymous: From the Lulz to Collective Action. Available at: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action. Last Accessed 7 Sep 2019.

Coleman, G. (2013). Our Weirdness is Free. Available at https://www.canopycanopycanopy.com/issues/15/contents/our_weirdness_is_free. Last Accessed 3 March 2021.

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

Collister, S. (2014). Abstract hacktivism as a model for postanarchist organizing. Ephemera: Theory and Politics in Organization. 14(4): 765-779.

Constantinides, P., Henfridsson, O. and Parker, G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*. 29(2): 381-400

Cooper, A. & Coetzee, S. (2020). On the Ethics of Using Publicly-Available Data. Conference on e-Business, e-Services and e-Society: I3E 2020: Responsible Design, Implementation and Use of Information and Communication Technology pp 159-171. Available at https://link.springer.com/chapter/10.1007/978-3-030-45002-1_14. Last Accessed 5 Feb 2021.

Corbett, E (1974). The rhetoric of protest. Available at https://www.tandfonline.com/doi/abs/10.1080/02773947409390388. Last Accessed 3 Feb 2021.

Corbineau, B., Barchechath, E. (2003). The Discourse on eDemocracy: Where are We Heading? In Building the Knowledge Economy: Issues, Applications; Case Studies, IOS Press, Oxford, UK.

Correia, J.V.(2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom. *SN COMPUT. SCI*. 3(84): 1-31.

Cotton, B. (2018). How Many Cyber Attacks are Attempted on UK Businesses Per Day? Available at https://www.businessleader.co.uk/how-many-cyber-attacks-are-attempted-on-uk-businesses-per-day/54688/. Last Accessed 2 Jan 2021.

Council of Europe (2017) International Cooperation against Cybercrime. Available at https://www.coe.int/en/web/cybercrime/international-cooperation. Last Accessed 4 Sep 2019.

Council of Europe (2017) Chart of signatures and ratifications of Treaty 185. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Last Accessed 4 Sep 2019.

Cox, R. & Foust, C. (2009). Social movement rhetoric. In Lunsford, A., Wilson, H. & Eberly, R. (Eds) *The SAGE handbook of rhetorical studies*. p 605-627. Thousand Oaks, CA: SAGE Publications, Inc.

CPNI (2021). Threat Landscape. Available at https://www.cpni.gov.uk/threat-landscape. Last Accessed 13 April 2021.

CPS (2019). Cybercrime - prosecution guidance. Available at https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. Last Accessed 12 April 2021.

CPS (2021). Terrorism. Available at https://www.cps.gov.uk/crime-info/terrorism. Last Accessed 14 Feb 2022.

Craigen, D., Diakun-Thibault, N. and Purse, R (2014). Defining Cybersecurity. *Technology Innovation Management Review.* 4(10): 13-21.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed method approaches*. London: Sage Publications, Inc.

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

Cross, F. (2003). Decision-making in the US Circuit Courts of Appeals. *California Law Review*. 91(6), 1457-1516.

Dagdelen, D (2012). Anonymous, Wikileaks and Operation Payback: A Path to Political Action through IRC and Twitter. Available at http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/Dagdelen2.pdf. Last Accessed 5 May 2020.

Dahlberg L (2007) Rethinking the fragmentation of the cyberpublic: from consensus to contestation. New Media and Society 9(5): 827–847.

Dalton, R., Kuechler, M., and Burklin, W. (1990). The Challenge of the New Movements. In Dalton, R and Kuechler, M: *Challenging the Political Order*. Oxford: Oxford University Press.

Darmois, E and Schmeder, G (2016). Cybersecurity: as case for a European approach. Paper commissioned by the Human Security Study Group. Available at https://www.fes-europe.eu/fileadmin/public/editorfiles/events/Feb2016/FES_LSE_Cybersecurity_Schmeder_Darmois_2016_02_23.pdf. Last accessed 3 May 2020.

Davis (J). Hacktivist vs. cyberterrorist: Understanding the 5 enemies of healthcare IT security. Healthy IT News Available at https://www.healthcareitnews.com/news/hacktivist-vs-cyberterrorist-understanding-5-enemies-healthcare-it-security. Last Accessed 15 Dec 2021.

DCMS (2019). Cyber Security Breaches 2019. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf. Last Accessed 21 Nov 2020.

DCMS (2019). Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views. Available at https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views. Last Accessed 13 April 2021.

DCMS (2020). Online Harms White Paper: Full government response to the consultation. Available at https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response. Last Accessed 12 April 2021

DCMS (2021). Draft Online Safety Bill. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf. Last Accessed 14 Feb 2022.

DCMS (2022). New laws proposed to strengthen the UK's resilience from cyber attack. Available at https://www.gov.uk/government/news/new-laws-proposed-to-strengthen-the-uks-resilience-from-cyber-attack. Last Accessed 2 Feb 2022.

DEFRA. (2006) The Code of Practice on Litter and Refuse. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/218806/cop-litter.pdf. Last Accessed 12 April 2021.

Della Porta, D and Diani, M (1999). *Social Movements: An Introduction*. Oxford: Blackwell.

Delmas, C (2018). Is Hacktivism the New Civil Disobedience? *Raisons politiques*. 69(1): 63-81.

Denning, D.E. (2000). "Cyberterrorism", Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.

Denning, D. E. (2001). “Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy”. In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Edited by: Arquilla, J. and Ronfeldt, D. California: RAND Corporation. 239–288. Available at http://www.iwar.org.uk/cyberterror/resources/denning.htm. Last Accessed 27 August 2020.

Democracy Now (2013). Steubenville Rape Trial: Blogger Who Exposed Case Speaks Out After Ohio Teens Found Guilty. Available at: https://www.democracynow.org/2013/3/18/steubenville_rape_trial_blogger_who_exposed. Last Accessed 5 Sep 2019.

Diani, M (1992). The Concept of Social Movement. *The Sociological Review*. 40 (1): 1-25

Diani, M and McAdam, D. (2003). *Social Movements and Networks: Relational Approaches to Collective Action: Relational Approaches to Collective Action*. Oxford: Oxford University Press.

Dictionary.com (2021). Tango down. Available at https://www.dictionary.com/e/slang/tango-down/. Last Accessed 3 March 2021.

Doherty, B., Plows, A., Wall, D., (2003). The Preferred Way of Doing Things: The British Direct Action Movement. *Parliamentary Affairs* 56: 669–686.

Donalds, C and Osei-Bryson, K.M, "A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction" (2014). *CONF-IRM 2014 Proceedings.* 5.

Donath, J. (1996) Identity and Deception in the Virtual Community. *Communities in Cyberspace*. In: Kollock, P. and Smith M (eds) Communities in Cyberspace.

Downing, J.D.H., 2001. *Radical Media: Rebellious communication and social movements.* Sage, Thousands Oaks, CA.f

Dunn, K. & Neumann, I. (2016). *Undertaking Discourse Analysis for Social Research*. Ann Arbor: University of Michigan Press.

Dupont, B (2004) Security in the age of networks. *Policing & Society.* 14(1): 76–91.

E-Estonia (2022). E Governance. Available at https://e-estonia.com/solutions/e-governance/e-democracy/. Last Accessed 10 March 2022.

Earl, J., Schussman, A. (2003). The new site of activism: Online organizations, movement entrepreneurs, and the changing location of social movement decision-making. Consensus Decision Making: Northern Ireland and Indigenous Movements, (24):155-187.

Earl J, Kimport K. (2011). *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: MIT Press.

EasyJet (2020). Notice of cyber security incident. Available at http://otp.investis.com/clients/uk/easyjet1/rns/regulatory-story.aspx?cid=2&newsid=1391756. Last Accessed 10 April 2020.

Edri (2017). The privacy movement and dissent: Protest. Available at https://edri.org/our-work/privacy-movement-dissent-protest/. Last Accessed 13 August 2020.

Ely, A. (2004). Prosecutorial Discretion as an Ethical Necessity: The Ashcroft Memorandum's Curtailment of the Prosecutor's Duty to Seek Justice. *Cornell Law Review.* 90(1), 237-278.

Else, H. (2018). Radical open-access plan could spell end to journal subscriptions. Available at https://www.nature.com/articles/d41586-018-06178-7. Last Accessed 12 Jan 2021.

Equality, and Human Rights Commission (2020). Article 10: Freedom of expression. Available at https://www.equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression. Last Accessed 9 April 2021.

ENISA (2021) Sectoral/ thematic threat analysis: ENISA Threat Landscape. Available at https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis/@@download/fullReport. Last Accessed 14 Feb 2022.

Erlingsson, G and Persson, M. (2011). The Swedish Pirate Party and the 2009 European Parliament Election: Protest or Issue Voting? *Politics*. 31(3) 121-128.

Etzioni, A. & Etzioni, O. (1999). Face-to-Face and Computer-Mediated Communities, A Comparative Analysis. The Information Society, (15): 241-248.

European External Action Service (EEAS). (2019a, August 1). ASEAN-EU Statement on Cybersecurity Cooperation. Joint Press Release. Available at https://eeas.europa.eu/headquarters/headquarters-Homepage_sv/66196/ASEAN-EU%20Statement%20on%20Cybersecurity%20Cooperation Last Accessed 1 Feb 2022

European Parliament (2021). The NIS2 Directive: A high common level of cybersecurity in the EU. Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Last Accessed 14 Feb 2021

Evans, M. and Scott, P. (2017). "Fraud and cyber crime are now the country's most common offences". Available at https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/. Last Accessed 16 Nov 2019.

Farmer, F. (2014). Hacktivism: A Social Movement? A functional approach to the rhetoric used by Anonymous. MA Dissertation.

Fearon, J. D. (1998). Deliberation as Discussion. In J. Elster (Ed.). *Deliberative Democracy* Cambridge: Cambridge University Press. 44–68.

Feinberg, A. (2014). The Birth off the Internet Troll. Available at https://gizmodo.com/the-first-internet-troll-1652485292. Last Accessed 1 March 2021.

Fine, G. A. (1995). Public Narration and Group Culture: Discerning Discourse in Social Movements. *Social Movements and Culture.* H. Johnston and B. Klandermans. Minneapolis, University of Minnesota Press: pp. 127-143.

Finnemore, M. and Hollis, D.B. (2016) Constructing Norms for Global Cybersecurity. *The American Journal of International Law*. 110(3) 425-479.

Fitzpatrick, A. (2012). Wikileaks Wins Battle Against Visa, Mastercard. Available at: https://mashable.com/2012/07/12/wikileaks-wins-battle-against-visa-mastercard/?europe=true#Tpv7WhWhzaqG. Last Accessed: 2 Sep 2019.

Fleming, P. & Stohl, M. (2000) 'Myth and Realities of Cyberterrorism', paper presented at the *International Conference on Countering Terrorism Through Enhanced International Cooperation*, 22-24 September, 2000, Courmayeur, Italy.

Foot,K.A. & Schneider, S.M. (2002) Online action in campaign 2000: An exploratory analysis of the US political web sphere. *Journal of Broadcasting & Electronic Media*, 46 (2): 222-244

Friedberg, B. and Donovan, J. (2019). On the Internet, Nobody Knows You're a Bot: Pseudoanonymous Influence Operations and Networked Social Movements. *Journal of Design and Science*. 6. Available at https://jods.mitpress.mit.edu/pub/2gnso48a/release/8. Last Accessed 12 March 2021.

Fuchs, C. (2012). Some Reflections on Manuel Castells' Book Networks of Outrage and Hope. Social Movements in the Internet Age. *tripleC*. 10(2): 775-797

Fuchs, C. (2013). The Anonymous movement in the context of liberalism and socialism. *Interface: a journal for and about social movements*. 5(2): 345-376.

Furedi, F. (2007). The only thing we have to fear is the 'culture of fear' itself. *American Journal of Sociology.* 32: 231-234

Gamson, W., Fireman,B., and Steven R. (1982). *Encounters with Unjust Authority*. Homewood: Dorsey.

Gamson, W. (1992a). "The social psychology of collective action." In A. D. Morris & C. McClurgMueller (Eds.), *Frontiers in social movement theory* (pp. 53–76). New Haven, CT: Yale University Press.

Gamson, W. A. (1992b). *Talking politics*. New York: Cambridge University Press

Ganesh, S., & Stohl, C. (2013). From Wall Street to Wellington: Protests in an era of digital ubiquity. *Communication Monographs*, 80(4): 425–451.

Gaokar, D. (2002) Publics and counterpublics. *Quarterly Journal of Speech*. 88(4): 410-412

Garrett, R. K. (2006). Protest in an information society: A review of literature on social movements and new ICTs. Information, *Communication & Society*, 9(2): 202-224.

George, J. and Leidner, D (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*. 29(3):100249.

Gerring, J. (2012). Mere Description. *British Journal of Political Science*. 42(4): 721 - 746,

Gibbs, A (2015). The man behind the Anonymous mask. Available at https://www.cnbc.com/2015/12/29/the-man-behind-the-anonymous-mask-v-for-vendettas-david-lloyd.html. Last Accessed 12 March 2020

Gil-Garcia, J. & Pardo, T (2006). Multi-method Approaches to Understanding the Complexity of E-Government. *International Journal of Computers, Systems and Signals*. 7(2):3-17.

Gill, R. (2000). Discourse Analysis. In Bauer, M and Gaskell, G. (eds.): Qualitative Researching with Text, Image and Sound London: SAGE. 172-190

Gillen, M. (2012). ‘Human versus Inalienable Rights: Is there still a future for online protest in the Anonymous world?’ *European Journal for Law and Technology*. 3(1).

Giugni, M. (1998). “Was it Worth the Effort? The Outcomes and Consequences of Social Movements.” *Annual Review of Sociology* 98: 371-93.

Goffman, E. (1974). *Frame Analysis*. Cambridge: Harvard University Press

Goldsmith, K (2010) “Can we stop the global cyber arms race?” Washington Post.

Gonzalez-Bailon, S and Wang, N (2016). Networked Discontent: The Anatomy of Protest Campaigns in Social Media. *Social Networks*. 44 (1): 95-104.

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. *Popular Communication*. 13(1) 74-86.

Goodwin, J and Jasper, J. (2014). Editors’ Introduction. In: Goodwin, J and Jasper, J. *The Social Movements Reader: Cases and Concepts*. New York: Wiley-Blackwell. 1-9.

Gordon, S & Ford, R (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13-20.

Gregg, R. (1971). The Ego-Function of the Rhetoric of Protest Author(s). Philosophy & Rhetoric. 4(2) (Spring): 71-91

Gregory, A (2020). Million Mask March: More than 100 anti-lockdown protesters arrested in London on first night of shutdown. Available at https://www.independent.co.uk/news/uk/home-news/million-mask-march-lockdown-arrests-london-police-b1626808.html. Last Accessed 7 Dec 2020.

Greenawalt, K. (1989). *Conflicts of Law and Morality*. New York: Oxford University Press.

Greensalde, R. (2011). When is a Twitter storm a real Twitter storm? Available at https://www.theguardian.com/media/greenslade/2011/dec/09/twitter-social-media. Last Accessed 14 April 2021

Greijdanus, H., de Matos Fernandes, C., Turner-Zwinkels, F., Honari, A., Roos, C., Rosenbusch,H and Postmes, T. (2020). The psychology of online activism and social movements: relations between online and offline collective action. *Current Opinion in Psychology*. 35: 49-54.

Griffin, A. (2020). ‘Anonymous’ Online Activists See Huge, Unexplained Surge in Support Amid Black Lives Matter Protests. Available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-activists-online-george-floyd-protests-black-lives-matter-a9544261.html. Last Accessed 5 March 2021.

Griffin, M. (1952). The Rhetoric of Historical Movements. *Quarterly Journal of Speech*. 38: 184-88

Gronbeck, B.E. (1973). The rhetoric of social-institutional change: Black action at Michigan. In G.P. Mohrmann, C. Stewart, and D.J. Ochs (Eds) E*xplorations in rhetorical criticism* (p. 96-113). University Park, PA: Pennsylvania State University.

Gronbeck, B. E. (1975). Rhetorical history and rhetorical criticism: A distinction. *The Speech Teacher*. 24, 309-320.

Gross, G. (2012). Swedish Websites Down after Anonymous Threats. Available at: https://www.computerworld.com/article/2492053/security0/swedish-websites-down-after-anonymous-threats.html. Last Accessed 6 Sep 2019.

Grossman, W. (2013). Digital Activist's Suicide Casts Spotlight on Growth of Open-Access Movement. . Available at:

https://www.scientificamerican.com/article/digital-activists-suicide-casts-spotlight-on-growth-of-open-access-movement/. Last Accessed 3 Jan 2021

Gusfield, J. (1994). The Reflexivity of Social Movements: Collective Behaviour and Mass Society Theory Revisited. In: Larana, Johnston and Gusfield: New Social Movements. Philadelphia: Temple University Press

Habermas, Jürgen. (1962/1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, translated by Thomas Burger with the assistance of Frederick Lawrence. Cambridge: Polity Press.

Habermas, J. (1984-1987). *The Theory of Communicative Action.* (2 Volumes). Boston: Beacon Press.

Habermas, J and Calhoun, M. (1985). Right and Violence: A German Trauma. Cultural Critique. 1(1)125-139.

HackRead (2012). Australian Attorney General Websites Taken Down for #OpFreeAssange. Available at https://www.hackread.com/australian-attorney-general-websites-taken-down-for-opfreeassange/ Last Accessed 5 Dec 2020.

HackRead (2015). Anonymous Targets Thai Govt, Leaks Data from State-owned Telecom Firm. Available at https://www.hackread.com/anonymous-targets-thai-govt-telecom-firm/. Last Accessed 10 Dec 2020.

Halliday, J. and Arthur, C. (2010). Wikileaks: Who are the hackers behind Operation Payback. Available at https://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal. Last Accessed 11 May 2020.

Halliday, J. (2013). Anonymous hackers jailed for cyber attacks. Available at https://www.theguardian.com/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks. Last Accessed 10 April 2021.

Hampson, N. (2012). Hacktivism: A New Breed of Protest in a Networked World. *Boston College International and Comparative Law Review*. 35:2, 511-542

Hannigan, J. (1985). "Alain Touraine, Manuel Castells and social movement theory: a critical appraisal." *Sociological Quarterly* 26:435-54.

Hay Newman (2019). Hacktivists Are on the Rise - but Less Effective Than Ever. Available at: https://www.wired.com/story/hacktivism-sudan-ddos-protest/. Last Accessed 13 Dec 2020.

Haywood, D (2018). *The Ethic of the Code: Values, Networks and Narrative Among the Civic Hacking Community.* Doctoral thesis, Goldsmiths, University of London [Thesis]

Häyhtiö, T., Rinne, J. (2008). Introduction: Seeking the citizenry on the internet - Emerging virtual creativity, In Häyhtiö, T., Rinne, J. (eds.), Net Working/ Networking: Citizen Initiated internet Politics, Tampere: Tampere University Press

Henley, J and Harding, H. (2016). *Iceland election could propel radical Pirate party into power.* Available: https://www.theguardian.com/world/2016/oct/26/iceland-election-could-propel-radical-pirate-party-into-power. Last accessed 6 Sep 2019.

Hess, D and Martin, B. (2006). Repression, Backfire, and the Theory of Transformative Events. *Mobilization: An International Quarterly.* 11(2), 249-267.

Hess, D. J., Breyman, S., Campbell, N., Martin, B., (2008), Science, Technology, and Social Movements, In Hackett, E.J., Amsterdamska, O., Lynch, M., Wajcman, J. (eds.), The Handbook of Science and Technology Studies, (pp. 473-498), 3rd edition, Cambridge: MIT Press.

Hill, J. and Marion, N. (2016). Presidential Rhetoric and Cybercrime: Tangible and Symbolic Policy Statements. *Criminology, Criminal Justice, Law & Society*. 17(2) 1-17.

Himanen, P. (2001). *The Hacker Ethic*. New York: Random House Trade Paperbacks.

Himma, K. (2005). Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified? Forthcoming in Kenneth Einar Himma (ed.), *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues*, Jones & Bartlett.

Himma, K. (2006) “Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?” In: Himma, K (ed.) *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues*. Boston: Jones & Bartlett.

Himma, K. (2007). *Internet Security: Hacking, Counterhacking, and Society*. London: Jones and Bartlett.

Hintz, A., 2010. *Civil Society Media and Global Governance. Intervening into the World Summit on the Information Society*. LIT Verlag, Berlin.

Home Office (2021). Police, Crime, Sentencing and Courts Bill 2021: protest powers factsheet. Available at https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-protest-powers-factsheet. Last Accessed 12 April 2021.

Home Office (2021) Computer Misuse Act 1990: call for information. https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information. Last Accessed 10 March 2022.

HM Government (2016). National Cyber Security Strategy 2016-2021. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Last Accessed 4 Dec 2020.

Hoffer, E (1951). *The True Believer.* New York: Harper and Row
Hopkins, C (2020). Anonymous claims it wasn't behind Operation Last Resort. Available at https://www.dailydot.com/unclick/anonymous-operation-last-resort-hoax/. Last Accessed 9 Dec 2020.

House of Commons (2013). E-crime - Fifth Report of Session 2013–14. Available at https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf. Last Accessed 4 Dec 2021.

Howard, P and Hussain, M. (2013). *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. New York, NY: Oxford University Press.

Hunt, S., Benford, R., and Snow, D. (1994). Identity Fields: Framing Processes and the Social Construction of Movement Identities. In Larana, Johnston and Gusfield: *New Social Movements*. Philadelphia: Temple University Press .185-208

Huschle, B. (2002). "Cyber Disobedience: When Is Hacktivism Civil Disobedience?" *The International Journal of Applied Philosophy* 16 (1): 69–83.

Hussain, M., & Howard, P. (2013). What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring. *International Studies Review*, 15(1), 48-66.

Hussain, A., Shaikh, S.A., Dawda, S., and Carr, M. (2018). An evidence quality assessment model for cybersecurity policymaking. In: *Proceedings of the Twelfth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection*. Arlington: Springer.

IBM (2020). Cost of Data Breach report 2020. Available at https://www.ibm.com/security/data-breach. Last Accessed 1 Nov 2020.

IBM (2020) IBM X-Force Threat Intelligence Index 2015-2020. Available at https://www.ibm.com/security/data-breach/threat-intelligence. Last Accessed 11 Nov 2020.

Interpol. (2018). Cybercrime. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Last accessed 5 Dec 2019.

Inglehart , R. (1990). Values, Ideology, and Cognitive Mobilization in New Social Movements. In Dalton, R and Kuechler, M: *Challenging the Political Order*. Oxford: Oxford University Press. 43-66

ISOC (2011). Of Cybercrime and Cybersecurity. Available at https://www.internetsociety.org/blog/2011/09/of-cybercrime-and-cybersecurity/. Last Accessed 23 May 2020.

ISP Review (2018). High Court Rules Part of UK ISP Internet Snooping Law is Unlawful. Available at https://www.ispreview.co.uk/index.php/2018/04/high-court-rules-uk-isp-internet-snooping-law-is-unlawful.html. Last Accessed 24 May 2020.

ITPro (2020). What is the Computer Misuse Act? Available at https://www.itpro.co.uk/it-legislation/28174/what-is-the-computer-misuse-act. Last Accessed 20 May 2020.

Jasper, J. (2011). Emotions and Social Movements: Twenty Years of Theory and Research. *The Annual Review of Sociology*. 37: 285-303. Available at https://canvas.harvard.edu/files/3747722/download?download_frd=1. Last accessed 14 April 2021

Jahankhani, H., A. and Al-Nemrat, Hosseinian-Far, A (2014). Cybercrime classification and characteristics. In: Bosco,F., Staniforth, A, and AkhgarB. Cyber Crime and Cyber Terrorism Investigator's Handbook. Elsevier. 149-164f

Jackson, S. J. (2018). "Progressive Social Movements and the Internet." In Cloud, D. (ed), Oxford Encyclopedia of Communication and Critical Studies. Oxford University Press.

Jakobi, A. (2013). *Common Goods and Evils? The Formation of Global Crime Governance*. Oxford: Oxford University Press.

Jenkins, C. (1983). "Resource Mobilization Theory and the Study of Social Movements". *Annual Review of Sociology*. 9: 527-553.

Jenkins, C. and Form, W. (2006). "Social Movements and Social Change." Pp. 331-49 in *The Handbook of Political Sociology: States, Civil Societies, and Globalization*, edited by Thomas Janoski, Robert Alford, Alexander Hicks, and Mildred A. Schwartz. Cambridge: Cambridge University Press.

Jensen, J. L., (2006). The Minnesota E-Democracy Project; Mobilizing the Mobilized? In Internet and Politics, (pp. 39-58) Routledge, Oxon, UK.

Jensen, R. (2006). Analyzing Social Movement Rhetoric. *Rhetoric Review*. 25(4): 372-375.

Joint Committee on Human Rights (2009). Demonstrating respect for rights? A human rights approach to policing protest. Available at https://publications.parliament.uk/pa/jt200809/jtselect/jtrights/47/47i.pdf. Last Accessed 10 March 2022.

Jordan, T. (2002). *Activism!: direct action, hacktivism and the future of society*. London:Reaktion books

Jordan, T. (2002). *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge.

Jordan, T and Taylor, P (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Karagiannopoulos, V. (2018). *Living with Hacktivism: From Conflict to Symbiosis*. Basingstoke: Palgrave Macmillan.

Karagiannopoulos, V. (2020). A short history of hacktivism: its past and present and what can we learn from it. In: Owen, T and Marshall, J (Eds) *Rethinking Cybercrime: Critical Debates.* 63-86.

Karagiannopoulos, V (2021). A decade since 'the year of the hacktivist', online protests look set to return. Available at https://theconversation.com/a-decade-since-the-year-of-the-hacktivist-online-protests-look-set-to-return-163329. Last Accessed 2 Feb 2022

Karatzogianni, A (2015). *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*. New York: Palgrave Macmillan.

Karpf. D. (2010). Online political mobilization from the advocacy group's perspective: Looking beyond clicktivism. *Policy & Internet*, 2 (4):7-41

Katagiri, N (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity.* 00(0):1–9

Kavada, A. (2009). Collective Action and the 'Participatory Web': A Comparative Analysis of Avaaz.org and Openesf.net, Paper presented at the Conference "Shaping Europe in a Globalized World? Protest Movement and the Rise of a Transnational Civil Society", Zurich, June 23-26, 2009.

Kellermann, T. (2010). Building a Foundation for Global Cybercrime law Enforcement. Computer Fraud and Security. May, (5), 5-8.

Kelly, B. (2012). Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' Can and Should Influence Cybersecurity Reform. *Boston University Law Review*. 92(5), 1663-1711.

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. 59(1): 111-128.

Kyan, O. (2021). Establishing Cybersecurity Norms in the United Nations: The Role of U.S.-Russia Divergence. Available at https://hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/. Last Accessed 10 March 2022.

Kizza, J.M. (2010). *Ethical and Social Issues in the Information Age*. London: Singer-Verlag.

Klandermans, B. (1988) The formation and mobilization of consensus. In: Klandermans B, Kriesi H and Tarrow S (eds) *From Structure to Action: Comparing Social Movement Research across Cultures.* Greenwich, CT: JAI Press, pp. 173–196

Klandermans, B. (1992). "The Social Construction of Protest and Multiorganisational Fields". In Morris and Mueller: *Frontiers of Social Movement Theory*. New Haven: Yale University Press

Klandermans, B. (1994). Transient Identities? Membership Patterns in the Dutch Peace Movements. In Larana, Johnston, and Gusfield: *New Social Movements*. Philadelphia: Temple University Press.

Klang, M. (2004). Civil Disobedience Online. Journal of Information, Communication and Ethics in Society. 2(2), 75-83.

Klein, AG. (2015). Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. *Communication Monographs*. 82(3): 379-401

Kneip, V. & Niesyto, J. (2007) Interconnectivity in the 'public of publics' - the example of Anti-Corporate Campaigns. Paper presented at Changing politics through digital networks: The role of ICTs in the formation of new social and political actors and actions, University of Florence.

Kobayashi, T., Ikeda, K. i., & Miyata, K. (2006). Social capital online: Collective use of the internet and reciprocity as lubricants of democracy. Information, Communication & Society, (9):582-611.

Kovacs, E. (2013). Website of AngloAmerican Mining Company Hacked by Anonymous for OpGreenRights. Available at https://news.softpedia.com/news/Website-of-AngloAmerican-Mining-Company-Hacked-By-Anonymous-for-OpGreenRights-335092.shtml. Last Accessed 5 Dec 2020.

Krapp, P. (2003). Terror and Play, or What Was Hacktivism? *Grey Room* 21(8):70-93

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In: Cyberpower and National Security. (Eds) Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. National Defense University Press, Washington, D.C. Available at https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210. Last Accessed 3 Dec 2021.

Langman, L. (2005). "From Virtual Public Spheres to Global Justice: A Critical Theory of Internetworked Social Movements". *Sociological Theory*. 23(1):42-47.

Langman, L. (2015). "An Overview: Hegemony, Ideology and the Reproduction of Domination". *Critical Sociology*. 41(3):425-432.

Larson, M. (2006). Descriptive Statistics and Graphical Displays. *Circulation*.114:76–81. Available at https://www.ahajournals.org/doi/full/10.1161/CIRCULATIONAHA.105.584474. Last Accessed 10 April 2021.

Lastdrager, E.E (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Sci.* 3(9):1-10.

Leach, J. (2000). Rhetorical Analysis. In: Bauer, M. & Gaskell, G. (Eds) *Qualitative Researching with Text, Image and Sound: A Practical Handbook for Social Research*. Caifornia: SAGE. 207-226.

Lee, R.M, and Rid,T. (2014) OMG Cyber! *The RUSI Journal*. 159(5), 4–12.

Lehrer, A. (1988). A Note on the Semantics of -Ist and -Ism. American Speech. 63(2), 181-185

Lehtonen, P. (2008). Civic expression on the Net: Different faces of public engagement?, In Häyhtiö, T., Rinne, J. (eds.), Net Working/ Networking: Citizen Initiated internet Politics, (pp. 163-188), Tampere : Tampere University Press.

Leppanen, A., Kiravuo, T., Kajantie, S. (2016). Policing the cyber-physical space. *Police Journal: Theory, Practice and Principles.* 89(4), 290-310

Lessig, L. (2006). *Code and Other Laws of Cyberspace*, Version 2.0. New York: Basic Books.

Levy, P (2002). *Cyberdémocratie: essai de philosophie politique*, Paris: Odile Jacob.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York: Anchor Press/Doubleday.

Levi, M., Doid, A., Gundur, R., Wall, D., and Williams, M. (2015) "The Implications of Economic Cybercrime for Policing." *City of London Research Report*, October. Available at http://orca-mwe.cf.ac.uk/88156/1/Economic-Cybercrime-FullReport.pdf. Last Accessed Dec 20 2019.

Leyden, J. (2012). UK cops: How we sniffed out convicted AnonOps admin ‘Nerdo’. Available at https://www.theregister.com/2012/12/14/uk_anon_investigation/. Last Accessed 13 May 2020.

Leyden, J. (2015). How a hack on Prince Phillip’s Prestel account led to UK computer law. Available at: https://www.theregister.com/2015/03/26/prestel_hack_anniversary_prince_philip_computer_misuse/. Last Accessed May 25 2020.

Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law and Technology*. 27(1): 302–330.

Lievrouw L (2011) Alternative and Activist New Media. Cambridge: Polity.

Libcom.org (2011). Anonymous Anarchist Action hacktivist group founded. Available at https://libcom.org/news/anonymous-anarchist-action-hacktivist-group-founded-10032011. Last Accessed 6 Dec 2020.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage.

Lin H. (2010). Offensive cyber operations and the use of force. *J Natl Security Law Policy*. 4(63): 63-86

Lo, C. Y. H. (1992). Communities of Challengers in Social Movement Theory. *Frontiers in social movement theory*. A. D. Morris and C. McClurg Mueller. New Haven, Yale University Press: 224-247.

Lohrmann, D. (2017). “The dramatic rise in hacktivism”. Available at https://techcrunch.com/2017/02/22/the-dramatic-rise-in-hacktivism/ Last accessed 15 Nov 2019.

Ludlow, P. (2013). What is a “hacktivist?” The New York Times. Available at http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/ Last Accessed 12 Jan 2021.

MacEwan, N. (2008). The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future. *Criminal Law Review.* 12, 955-967.

Manion, M & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *Computers and Society*. June 2000. Available at http://www.csis.pace.edu/cis101/CIS_101_Fall_2007_Spring_2008/LearningPodTopics/SocialResponsibility/Terrorism-or-Civil-Disobedience.pdf. Last Accessed 23 June 2020.

Marchand, H (1969). *The Categories and Types of Present Day English Word Formation.* Munich: Beck.

Margolis, M., & Resnick, D. (2000). *Politics as Usual: The Cyberspace 'Revolution'*. Thousand Oak, CA: Sage.

Marion, N. (2010). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. *International Journal of Cyber Criminology*. 4(1&2), 699-712.

Marsh, M,. & White, E. (2006). Content Analysis: A Flexible Methodology. *Library Trends.* 55(1): 22-45.

Martin, R (2013). Anonymous Starting OpUSA, Want To Send A Message To President Obama. Available at https://www.eteknix.com/anonymous-starting-opusa-want-to-send-a-message-to-president-obama/. Last Accessed 5 Dec 2020.

Maurushat, A. (2012). *Ethical hacking: A report for the national cyber security division of public safety Canada*. Report obtained with permission of the author. Report available as a FOI request.

Mautner, G. (2005). Time to get wired: Using web-based corpora in critical discourse analysis *Discourse & Society.* 1 6(6): 809 - 828

McAdam, D, McCarthy J. D. and Zald, M. (Eds.). (1996). *Comparative Perspectives on Social Movements: Political Opportunity, Mobilizing Structures and Cultural Framings*. New York: Cambridge University Press.

McCarthy, J and Zald, M. (1977). "Resource Mobilization and Social Movements: A Partial Theory." *American Journal of Sociology*. 82(6):1212-1241.

McCarthy, J and Zald, M. (1987). The trend of social movements in America: Professionalization and resource mobilization. *Social movements in an organizational society: Collected essays.* New York: Routledge.

McCarthy, J. (1997). "The Globalization of Social Movement Theory." 243-259. In: Smith, J., Chatfield., and Pagnucco, R. *Transnational Social Movements and Global Politics: Solidarity Beyond the State*. New York: Syracuse University Press.

McCarthy, J and McPhail, C. (1997). "The Institutionalization of Protest in the United States." 83-110. In: Meyer, D. and Tarrow, S. *Social Movement Society*. Oxford: Rowman & Littlefield Publishers.

McLaurin, J. (2011). Making cyberspace safe for democracy: the challenge posed by denial-of-service attacks. *Yale Law and Policy Review*, 30(1), 211-254

McGuire, M. (2007). *Hypercrime: The New Geometry of Harm*. Oxford:Routledge-Cavendish.

McKinney, C. (2018). Printing the network: AIDS activism and online access in the 1980s. *Continuum: Journal of Media & Cultural Studies*. 32(1): 7–17.

Melucci, A. (1989). *Nomads of the Present: Social Movements and Individual Needs in Contemporary Italian Society*. Philadelphia: Temple University Press

Melucci, A. (1996*). Challenging Codes: Collective Action in the Information Age*. Cambridge: Cambridge University Press.

Mercea D. (2012) Digital prefigurative participation: the entwinement of online communication and offline participation in protest events. New Media & Society 14(1): 153–169.

Merriam-Webster Dictionary (2021). Troll. Available at https://www.merriam-webster.com/dictionary/troll. Last Accessed 2 Dec 2021.

Milan, S. (2015). Hacktivism as a radical media practice. In: Atton, C (Eds) *Routledge Companion to Alternative and Community Media*. Routledge. 550-560

Milbrath, L. (1965). *Political participation: How and why do people get involved in politics?* (1st ed.). Chicago: Rand McNally.

Milliken, (1999). The Study of Discourse in International Relations. A Critique of Research and Methods. *European Journal of International Relations*. 5 (2): 225–54.

Mingers, J. (2001). Combining is research methods: Towards a pluralist methodology. *Information Systems Research*. 12(3), 240-259.

Montgomery, L. (2021). 2020 locked in shift to open access publishing, but Australia is lagging. Available at https://theconversation.com/2020-locked-in-shift-to-open-access-publishing-but-australia-is-lagging-150284. Last Accessed 22 April 2021.

Morozov, E. (2009) Iran elections: a twitter revolution? The Washington Post. Available at: http://www. washingtonpost.com Last accessed 12 July 2019.

Morozov. (2009). *Foreign Policy: Brave New World Of Slacktivism.*Available: https://www.npr.org/templates/story/story.php?storyId=104302141&t=1535021176206&t=1548502621325. Last accessed 10 Sep 2019.

Mueller, C. (1994). Conflict Networks and The Origins of Women's Liberations. In Larana, Johnston and Gusfield: New Social Movements. Philadelphia: Temple University Press

Murphy, L. (2020). #OpSafeWinter: Anonymous fights homelessness worldwide. Available at https://www.dailydot.com/unclick/op-safe-winter-anonymous/. Last accessed 1 March 2021.

Murphy, H. (2022). Ukraine war sparks revival of hacktivism. Available at https://www.ft.com/content/9ea0dccf-8983-4740-8e8d-82c0213512d4. Last Accessed 4 March 2022.

Nam. T (2010). Internet effects on political participation: an empirical study on the reinforcement vs. mobilization effect. In Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance (ICEGOV '10). *Association for Computing Machinery,* New York, NY, USA, 307–316.

The NATO Cooperative Cyber Defence Centre of Excellence (2017). The Tallinn Manual. Available at https://ccdcoe.org/research/tallinn-manual/. Last Accessed 14 Feb 2022.

Naughton, J. (2015). Aaron Swartz stood up for freedom and fairness – and was hounded to his death. Available at https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy. Last Accessed 10 May 2020.

NCA(2018). “Cyber Crime ” Available at: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime Accessed 11 November 2019.

NCA (1990). “A Guide to the Computer Misuse Act 1990 (CMA)”. Available at http://www.nationalcrimeagency.gov.uk/publications/760-a-guide-to-the-computer-misuse-act/file . Last Accessed 18 Dec 2019.

NCA (National Crime Agency Strategic Cyber Industry Group). 2016a. “Cyber Crime Assessment 2016 – Need for a Stronger Law Enforcement and Business Partnership to Fight Cyber Crime.” NCA. Accessed 5 Sep 2019. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

NCSC (2016) Common Cyber Attacks: Reducing the Impact. Available at https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact#downloads. Last Accessed 22 Nov 2020.

NCSC (2016). A new approach for cyber security in the UK. Available at https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk. Last Accessed 13 April 2021.

NCSC (2015). Denial of Service (DoS) guidance. Available a https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection. Last Accessed 14 April 2021.

NCSC (2018). Annual Review 2018. Available at: https://www.ncsc.gov.uk/content/files/ncsc_2018-annual-review.pdf. Last Accessed 17 Dec 2019.

NCSC (2018). Advice to thwart 'devastating' cyber attacks on small charities. Available at https://www.ncsc.gov.uk/news/advice-thwart-devastating-cyber-attacks-small-charities. Last Accessed 13 April 2021.

NCSC (2020). Denial of Service (DoS) guidance. Available at https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection. Last Accessed 2 Dec 2020.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., Gagnon, F. (1999), Cyber terror prospects and implications, *Centre for the Study of Terrorism and Irregular Warfare*, Monterey, CA.

Netsparker (2021). What is the SQL Injection Vulnerability & How to Prevent it?. Available at https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/#WhatIsAnSQLInjectionVulnerability. Last Accessed 2 Dec 2020.

Neumayer, C. and Svensson, J. (2016). "Activism and radical politics in the digital age: Towards a typology." *Convergence: The International Journal of Research into New Media Technologies.* 22(2):131-146.

Newman, I., & Benz, C. R. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum.* Carbondale: University of Illinois Press.

New Statesman (2019). Why is the number of active hacktivist groups plummeting?. Available at https://tech.newstatesman.com/security/hacktivist-groups. Last Accessed 12 Nov 2020.

Ngak, C (2013). 13 members of hacking group Anonymous indicted over "Operation Payback". Available at https://www.cbsnews.com/news/13-members-of-hacking-group-anonymous-indicted-over-operation-payback/. Last Accessed 11 May 2020.

Nhan, J, Huey, L (2008) Policing through nodes, clusters and bandwidth: The role of network relations in the prevention of and response to cyber-crimes. In: Leman-Langlois, S (ed.) *Technocrime: Technology, Crime and Social Control*. Portland, 66-87.

Niesyto, J. (2007). Comparative Study of Transnational Anti-Corporate Campaigns - Research Design and Preliminary Results. In LMU Munich, Germany.

NIST. (2022). Virus. Available at https://csrc.nist.gov/glossary/term/virus. Last Accessed 10 March 2022.

Nunziato, D. (2005). The Death of the Public Forum in Cyberspace. *Berkeley Technology Law Journal*. 20(2), 1115-1171.

Nutley, S., Davies, H., and Walter, I. (2002) Evidence based policy and practice: cross sector lessons from the UK. *Working Paper 9, Social Policy Research and Evaluation*, Wellington, New Zealand.

Nye, SJ. (2010). Cyber Power. Belfer Center for Science and International Affairs. Available at https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. Last Accessed 2 Dec 2021

Nye, SJ. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5(4): 18-38.

Olsen, M. (1968). Perceived Legitimacy of Social Protest Actions. *Social Problems*. 15(3) Winter: 297–310,

Olson, M. (1965/1971). *The Logic of Collective Action. Public Goods and the Theory of Groups.* Cambridge, MA: Harvard University Press.

Olson, P. (2013). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous and the global cyber insurgency.* London: Heinemann.

O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime? *Trinity College Law Review.* 16, 137.

ONS (Office for National Statistics). 2015. "Improving Crime Statistics in England and Wales." Accessed Sep 2018.

Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (2021). *Resolution 73/27 Final Report*. Available at https://www.un.org/disarmament/open-ended-working-group/. Last Accessed 2 Feb 2022.

Open Society Foundations (2019). Understanding Ukraine's Euromaidan Protests. Available at https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests. Last Accessed 13 March 2021.

Operation Green Rights (2013). Anglo American hacked : "We curse you!". Available at http://operationgreenrights.blogspot.com/2013/03/anglo-american-we-shame-you.html. Last Accessed 5 Dec 2020.

Opp, KD. (2009). *Theories of Political Protest and Social Movements: A Multidisciplinary Introduction, Critique, and Synthesis*. Oxon: Routledge.

Palfrey, G (2010) Four Phases of Internet Regulation. *Social Research*, 77(3) Fall 2010 Berkman Center Research Publication No. 2010-9,

Panda Security (2020). What is Hacktivism? Campaigns That Shaped the Movement. Available at https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism/. Last Accessed 8 Dec 2020.

Paltridge, P. (2012). *Discourse analysis: an introduction*. London : Blomsbury Academic

Pasquale, F. (2010). 'Trusting (and Verifying) Online Intermediaries' Policing' In: Szoka, B and Marcus, A (eds) *The Next Digital Decade: Essays on the Future of the Internet*. Washington DC: Techfreedom.

Perez, T. (2020). Does National Security Outweigh the Right to Privacy? Available at https://www.theperspective.com/debates/living/national-security-outweigh-right-privacy/. Last Accessed 13 March 2021.

Petee, T., Corzine, J., Huff-Corzine, L., Clifford, J. and Weaver, G. (2010). Defining "Cyber-crime": Issues in Determining the Nature and Scope of Computer Related Offences. In: Finnie, T., Peter, T. and Jarvis, J (eds) *Future Challenges of Cybercrime. Volume 5: Proceedings of the Futures Working Group.* Available at http://www.foresightfordevelopment.org/sobipro/55/1162-future-challenges-of-cybercrime-volume-5-proceedings-of-the-futures-working-group Last Accessed 5 Sep 2019

Pidd, H. & Robinson, G. (2020). Ransomware attack leaves council facing huge bill to restore services. Available at https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack. Last Accessed 3 Jan 2021.

Pont, J., Abu Oun, O., Brierley, C., Arief, B. and Hernandez-Castro, J.C. (2019) A Roadmap for Improving the Impact of Anti-Ransomware Research. In: *NordSec 2019: The 24th Nordic Conference on Secure IT Systems*, November 18-20, 2019, Aalborg, Denmark. Available at https://kar.kent.ac.uk/76942/1/Paper24.pdf. Last Accessed 10 March 2022.

Ponta, A. (2021). Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes. *Insights*. 25(14) Online. Available at https://www.asil.org/sites/default/files/ASIL_Insights_2021_V25_I14_0.pdf. Last Accessed 2 Feb 2022

Potter, J. (1996) Discourse analysis and constructivist approaches: theoretical background. In Richardson, J. (ed): *Handbook of Qualitative Research Methods for Psychology and the Social* Sciences. Leicester: British Psychological Society.

Powell, A., (2008). Co-productions of Technology, Culture and Policy in the North American Community Wireless Networking Movement. PhD Thesis, Concordia University, Montréal.

Retrieved March, 30, 2009, from: http://www.alisonpowell.ca/?page_id=71 Last Accessd 10 Sep 2019

Price, V., & Cappella, J. N. (2002). Online Deliberation and Its Influence: The Electronic Dialogue Project in Campaign 2000. *IT & Society* 1(1): 303–329.

Putnam, R. D. (1993). Making democracy work. Civic traditions in Modern Italy, Princeton: Princeton University Press.

Putnam, R. D. (2000) Bowling Alone: The Collapse and Revival of American Community, New York: Simon and Schuster.

QASSAMCYBERFIGHTERS (2012).Bank of America and New York Stock Exchange under attack unt. Available at https://pastebin.com/mCHia4W5. Last Accessed 6 Dec 2020.

QASSAMCYBERFIGHTERS (2013). Phase 4, Operation Ababil. Available at https://pastebin.com/22WJ6m9U. Last Accessed 9 Dec 2020.

RadioFreeEurope Radio Liberty (2011). Old-School Hacker Oxblood Ruffin Discusses Anonymous And The Future Of Hacktivism. Available at https://www.rferl.org/a/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html. Last Accessed 22 Nov 2020.

RadioFreeEurope Radio Liberty (2012). Parmy Olson on Anonymous: ‘A Growing Phenomenon That We Don’t Yet Understand’. Available at https://www.rferl.org/a/parmy-olson-on-anonymous-a-growing-phenomenon-that-we-dont-yet-understand/24607895.html. Last Accessed 22 Nov 2020.

Rainie, L., Smith, A., Lehman Schlozman, K., Brady, H. and Verba, S. (2012). Social Media and Political Engagement. Pew Research Center’s Internet & American Life Project. Available at https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2012/PIP_SocialMediaAndPoliticalEngagement_PDF.pdf. Last Accessed 25 March 2021.

Ranalli, R (2019). Erica Chenoweth illuminates the value of nonviolent resistance in societal conflicts. Available at https://www.hks.harvard.edu/faculty-research/policy-topics/advocacy-social-movements/paths-resistance-erica-chenoweths-research. Last Accessed 9 Dec 2020.

Ranario, M. (2008). *Identifying the Ideology of “Hacktivism”.* Available at http://www.slashdocs.com/nitwwk/hacktivism-as-non-violence.html. Last Accessed 29/04/2014.

Rasmussen, M. (2012). Accountability and Consistency in Policy Development. Available at: https://www.complianceweek.com/news/news-article/accountability-and-consistency-in-policy-development#.XE3h5M_7RAY. Last Accessed 2 Jan 2019.

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

Real, D., and Irwin, J. (2010). Unconscious Influences on Judicial Decision-Making: The Illusion of Objectivity. *McGeorge Law Review*. 42(1) 1-18.

Reuters (2015). Thailand scraps unpopular Internet 'Great Firewall' plan. Available at https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015. Last Accessed 11 Dec 2020.

Reynolds, G. (2013). Ham Sandwich Nation: Due Process When Everything is a Crime. Legal Studies Research Paper No 206, University of Tennessee.

Roberts, P (2020). Are K-Pop Fans the New Anonymous? Don't Count On It. Available at https://www.forbes.com/sites/paulfroberts/2020/06/24/are-k-pop-fans-the-new-anonymous-dont-count-on-it/?sh=5aac69e342f2. Last Accessed 21 Nov 2020.

Robson, D (2019). The '3.5% rule': How a small minority can change the world. Available at https://www.bbc.com/future/article/20190513-it-only-takes-35-of-people-to-change-the-world. Last Accessed 13 Dec 2020.

Rochon, T. (1998). *Culture Moves: Ideas, Activism, and Changing Values.* New Jersey: Princeton University Press.

Romagna, M. (2019). Hacktivism: Conceptualization, Techniques, and Historical View. In: T. J. Holt, A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* 743-769.

Rosenbaum, J & Bouvier (2020). Twitter, social movements and the logic of connective action: Activism in the 21st century – an introduction. *Participations: Journal of Audience & Reception Studies.* 17(1):120-125.

Rosenblatt, S. (2020). What's Anonymous Up to Now. Available at https://www.darkreading.com/theedge/whats-anonymous-up-to-now/b/d-id/1338112. Last Accessed 21 Nov 2020.

Rouse, M (2020). Hacktivism. Available at https://searchsecurity.techtarget.com/definition/hacktivism. Last Accessed 23 May 2020.

RPC (2018). Hacking prosecutions fall for a further year despite the threat of cyber crime. Available at https://www.rpc.co.uk/press-and-media/hacking-prosecutions-fall-for-a-further-year-despite-the-threat-of-cyber-crime/. Last Accessed 18 May 2020.

Rucht, D. (1988). Themes, Logics and Arenas of Social Movements: A Structural Approach. In: Klandermans, Kriesi and Tarrow: *International Social Movement Research, Vol I, From Structure to Action.* Greenwich: JAI Press.

Rucht, D. (1994). Modernisierung und neue soziale Bewegungen. Deutschland, Frankreich und USA im Vergleich, Frankfurt/New York: Campus.

Ruhl, C. Hollis, D. Hoffman, W. and Maurer, T (2020). Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads Working Paper. *Carnegie Endowment for International Peace.* Available at https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf. Last Accessed 14 Feb 2022.

Samuel, A (2001). Digital Disobedience: Hacktivism in Political Context. Prepared for delivery on the panel, The Internet as Agent of Change: Bridging Barriers to Cultural, Political and Activist Discourse, at the Annual Meeting of the American Political Science Association, San Francisco, CA, August 29 – September 2, 2001. Available at https://www.arifyildirim.com/ilt510/alexandra.samuel.pdf. Last Accessed 2 Dec 2021.

Samuel, A (2004). *Hacktivism and the Future of Political Participation*. DPhil Thesis, Harvard University.

Saul, B and Heath, K. (2021). Cyber terrorism. In: Tsagourias, N and Buchan, R. *Research Handbook on International Law and Cyberspace.* 147–167

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6 ed.) London: Pearson.

Saunders, J (2017). Tackling Cybercrime - the UK response. *Journal of Cyber Policy*. 2(1) 4-15.

Sauter, M (2014). *The Coming Swarm*. London: Bloomsbury. 1-2.

Savage, C (2020). Chelsea Manning Is Ordered Released From Jail. Available at https://www.nytimes.com/2020/03/12/us/politics/chelsea-manning-released-jail.html. Last Accessed 12 Dec 2020.

Schmitt, M. N. and Watts, S. (2016). Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. *Journal of Conflict and Security Law.* 21(3):1-17

Schradie J. (2011). The digital production gap: The digital divide and Web 2.0 collide. *Poetics*. 39 (2):145-168,

Schradie J. (2018). The digital activism gap: How class and costs shape online collective action. *Social Problems*. 65 (1): 51-74, Schradie J. (2019). *The Revolution That Wasn't: How Digital Activism Favors Conservatives.* Boston: Harvard University Press.

Schultz, J (2013). The Effects of #OpUSA. Available at https://blogs.cisco.com/security/the-effects-of-opusa. Last Accessed 5 Dec 2020.

Scott, A. and Street, J. (2000). From media politics to e-protest, Information, Communication and Society, 3 (2): 215-40

Scottish Qualifications Authority (2008). "What is Computer Misuse?" Available at https://www.sqa.org.uk/e-learning/ITLaw01CD/page_03.htm. Last Accessed 18 Dec 2018.

Security Boulevard (2020). Analysis of the Top10 Hacktivist Operations. Available at https://securityboulevard.com/2020/06/analysis-of-the-top10-hacktivist-operations/. Last Accessed 3 Feb 2021.

Security Intelligence (2019). The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015. Available at https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/. Last Accessed 11 Nov 2020.

Selander L, & Jarvenpaa, SL (2016). Digital action repertoires and transforming a social movement organization. *MIS Quarterly*. 40 (2) (2016), pp. 331-352

Sexton, M. (2016). *UK Cyber Security Strategy and Active Cyber Defence - issues and risks.* Journal of Cyber Policy. 1(2), 222- 242.

Shaw, G. (2012). Hacker Group Releases Online Record of Second Alleged Amanda Todd Stalker. Available at: https://vancouversun.com/news/staff-blogs/man-loses-job-over-amanda-todd-slur-hacker-group-releases-online-record-of-second-alleged-stalker. Last Accessed 5 Sep 2019.

Shenkein, J. (1978). Explanation of transcription notation. In J. Shenkein (Ed.), *Studies in the organization of conversational interaction*. New York: Academic Press.

Shirky C. (2008). *Here Comes Everybody: The Power of Organizing Without Organizations.* New York: Penguin.

Simon, J. (2007). *Governing through Crime*. Oxford: Oxford University Press.

Simons, H. (1970). Requirements, problems, and strategies: A theory of persuasion for social movements. *Quarterly Journal of Speech*. 56(1): 1-11.

Slaton, C. D. (1992). *Televote: Expanding Citizen Participation in the Quantum Ag*e. New York, NY: Praeger Publishers.

Slavina, A & Brym, R. (2020) Demonstrating in the internet age: a test of Castells' theory. *Social Movement Studies*. 19(2): 201-221

Snow, D, and Oliver, P. (1995). "Social Movements and Collective Behavior: Social Psychological Dimensions and Considerations." Pp. 57l -599 in *Sociological Perspectives on Social Psvchology*, edited by Karen S. Cook, Gary Alan Fine, and James S. House. Boston: Allyn and Bacon

Snow, D., Rochford, E., Worden, S. and Benford. (1986). "Frame Alignment Processes, Micromobilization, and Movement Participation." *American Sociological Review.* 51(4):464-481.

Snow, D., Soule, S. and Kriesi, H. (2004). Mapping the terrain. In Wiley, J (Ed) The Blackwell companion to social movements. Oxford: Blackwell.

Solomon, R (2017). Electronic protests: Hacktivism as a form of protest in Uganda. *Computer Law & Security Review.* 33(5): 718-728,

Sorell, T. (2015) Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. *Journal of Human Rights Practice*. 7(13), 391-410.

Spiegelhalter, D. (2019). The Art of Statistics: Learning from Data. London: Pelican Books.

Statista Research Department (2013). Share of people who went on a demonstration in Great Britain 1983-2011. Available at https://www.statista.com/statistics/285863/protesting-political-engagement-in-great-britain-gb/. Last Accessed 13 Dec 2020.

Stewart, C. (1980). A Functional Approach to the Rhetoric of Movements. Central Speech Journal. 31: Available at: https://www.tandfonline.com/doi/pdf/10.1080/10510978009368070. Last Accessed 12 Dec 2020.

Stewart, E. (2019). We are (Still) the 99 Percent. Available at https://www.occupy.com/article/we-are-still-99-percent. Last Accessed 12 March 2021.

Stoecker, R. (1995). Community, Movement, Organization: The Problem of Identity Convergence in Collective Action. *The Sociological Quarterly*. 36: 111-130.

Storing, H. (2002). 'The Case Against Civil Disobedience'. In Bedau, H.A (Ed) *Civil Disobedience in Focus*. London: Routledge.

Strauss, S. & Feiz, P. (2014). *Discourse analysis :putting our worlds into words*. New York : Routledge /Taylor & Francis Group

Sunstein, C. (2005). *Laws of Fear: Beyond the Precautionary Principle*. Cambridge: Cambridge University Press.

SWGfL. (2021). Reputation Alerts: Frequently Asked Questions (FAQs). Available at : https://swgfl.org.uk/products/reputation-alerts/faqs/#understand. Last Accessed 3 Feb 2021.

Taho NYMOUS (2014). Anonymous Live on CNN 2013 broke into cnn. Available at https://www.youtube.com/watch?v=4EVMRH8S7OA. Last Accessed 12 March 2021.

Tarrow, S. (1998). *Power in Movement. Social Movements, Collective Action and Politics* (2nd edition). Cambridge: Cambridge University Press.

Tashakkori, A., & Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. Thousand Oaks, CA: Sage.

Tashakkori, A. & Creswell, J. (2007). Editorial: Exploring the Nature of Research Questions in Mixed Methods Research. *Journal of Mixed Methods Research*. 1(3): 207-211.

Taylor, P. (2005). From hackers to hacktivists: speed bumps on the global superhighway*?. New Media Society.* 7(5):625–646.

Techopedia (2021). Account Hijacking. Available at https://www.techopedia.com/definition/24632/account-hijacking. Last Accessed 1 Dec 2020.

Techopedia (2012). Twitterstorm. Available at https://www.techopedia.com/definition/29624/twitterstorm. Last Accessed 12 April 2021

The CyberSecurity Expert.com (2013). Available at https://www.thecybersecurityexpert.com/anonymous-opusa-goes-without-a-bang/. Last Accessed 5 Dec 2020.

Thomas, S. (2012). Cyber Protests and Electronic Disobedience': Examining Non-Violence in Times of Cyber Politics. *Quarterly Journal of the Gandhi Peace Foundation.* 34(3&4), 293-306.

Thomas, T. (2016). *Policing Sexual Offences and Sexual Offenders*. London: Palgrave MacMillan.

Thompson, G. (2020). Members of Anonymous Hack UN Website to Support Taiwan. Available at https://www.binarydefense.com/threat_watch/members-of-anonymous-hack-un-website-to-support-taiwan/. Last Accessed 5 Jan 2021.

through h4x0r3d's eyes (2010). Message from #Anonymous: Operation Manning (by anonyops). Available at https://h4x0r3d.tumblr.com/post/7579913669/message-from-anonymous-operation-manning-by/amp. Last Accessed 11 Dec 2020.

Tidy, J. (2020). Redcar cyber-attack: Council using pen and paper. Available at https://www.bbc.co.uk/news/technology-51504482. Last Accessed 3 Jan 2021.

Tilly, C., (1978). *From mobilization to revolution*. New York: Random House.

Tilly, C (2006). WUNC. In: Thompson Schnapp, J and Tiews, M (Eds) *Crowds*. Stanford: Stanford University Press.

Tilly, C. and Wood L. (2015). *Social movements 1768–2012*.New York: Routledge

Tomblin, J & Jenion G (2016) Sentencing 'Anonymous': exacerbating the civil divide between online citizens and government. *Police Practice and Research*. 17 (6), 507-519.

Toch, H. (1965). *The Social Psychology of Social Movements.* Indianapolis: Bobbs-Merrill.

TrendMicro (2018). A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks. Available at https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf. Last Accessed 3 Dec 2020.

TrendMicro (2018). Digital Vandals: Exploring the Methods and Motivations behind Web Defacement and Hacktivism. Available at https://www.trendmicro.com/vinfo/gb/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists. Last Accessed 26 June 2020.

Trevisan, F. (2016). *Disability rights advocacy online: Voice, empowerment and global connectivity.* Oxfordshire, UK: Taylor & Francis.

Uba, K. & Bosi. (2009). Introduction: The Outcomes of Social Movements. *Mobilization: An International Journal* 14(4): 409-415

UKEssays. (November 2018). *Types of research strategies*. Retrieved from https://www.ukessays.com/essays/estate-management/research-strategies.php?vref=1 Last Accessed 12 Feb 2021

UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (2021). *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.* Available at https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf. Last Accessed 2 Feb 2022.

Vaast, E., Safadi, H., Lapointe, L., Negoita, B. (2017). Social media affordances for connective action - an examination of microblogging use during the Gulf of Mexico oil spill. *MIS Quarterly*. 41 (4):1179-1205. Available at https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2003.tb00216.x. Last Accessed 13 April 2021.

Van De Donk, W., Loader, B.D., Nixon, P.G & Rucht, D. (eds.) (2004) *Cyberprotest: New Media, Citizens, and Social Movements*, London: Routledge.

van Haaster, J., Gevers, R. and Sprengers, M. (2016). *Cyber Guerilla.* Cambridge: Elsevier

Veerasamy, N, (2020), Cyberterrorism–the spectre that is the convergence of the physical and virtual worlds. In: Benson and Mcalaney (Eds.) *In Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press.

Vegh, S. (2003). ‘Classifying forms of online activism: The case of cyberprotests against the world bank’. In M. McCaughey & M. D. Ayers (Eds.), *Cyberactivism: Online activism in theory and practice.* New York: Routledge. 71 – 96.

Vitak, J., Zube, P., Smock, A.,Carr, C., Ellison, N. and Lampe. C. (2011). It's Complicated: Facebook Users' Political Participation in the 2008 Election. *Cyberpsychology, Behavior, and Social Networking*. 14(3), 107-114

Vromen, A. (2008). Political change and the internet in Australia: introducing GetUp, In Häyhtiö, T., Rinne, J. (eds.), Net Working/ Networking: Citizen Initiated internet Politics, (pp. 103-126), Tampere: Tampere University Press.

Walker-Osborn, C., & McLeod, B. (2015). Getting tough on cyber crime. *ITNOW*, 57(2), 32-33.

Wall, D. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace. *Police Practice and Research*. 8(2), 183-205.

Wakefield, J. (2020). EasyJet admits data of nine million hacked. Available at https://www.bbc.co.uk/news/technology-52722626?utm_source=dlvr.it&. Last Accessed 1 Nov 2020.

War on Want (2017). Israeli apartheid factsheet. Available at https://waronwant.org/news-analysis/israeli-apartheid-factsheet. Last Accessed 12 March 2021.

Warren, L. and Keneally, M. (2012). The Internet Vigilantes: Anonymous Hackers' group outs man, 32, 'who drove girl, 15, to Suicide by Spreading Topless Photos of Her. Available at: https://www.dailymail.co.uk/news/article-2218532/Amanda-Todd-Anonymous-names-man-drove-teen-kill-spreading-nude-pictures.html. Last Accessed 6 Sep 2019.

Wall, D.S. (2005a) 'The Internet as a Conduit for Criminals', In: Pattavina, A., Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage. 77-98

Wall, D.S. (2005b) "The Email of the Species is More Deadlier than the Mail: Digital Realism and the Governance of Spam as Cybercrime', European Journal on Criminal Policy and Research.

Weatherhead, C (2014). Tweet available at https://twitter.com/cjfweatherhead/status/431059633071878144. Last Accessed 18 February 2021.

Weber, A. (2003). The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal, 18(1). 425-446.

Weber, R (1990). *Basic Content Analysis*. California: Sage.

Wedawatta, G., Ingirige, B. & Amaratunga, D. (2011). Case study as a research strategy: Investigating extreme weather resilience of construction SMEs in the UK. Available at https://usir.salford.ac.uk/id/eprint/18250/1/6. Last Accessed 03 Feb 2021.

Weimann, G. (2004) Cyberterrorism How Real Is the Threat? United States Institute of Peace _ Special Report. Available at https://www.usip.org/sites/default/files/sr119.pdf. Last Accessed 3 Jan 2022.

Wellman, B., Quan-Haase, A., Boase, J., Chen, W, Hampton, K., Isla de Diaz, I. and Miyata, K. (2003) The Social Affordances of the Internet for Networked Individualism. *Journal of Computer-Mediated Communication.* 8(3).

White, C. S. (1997). Citizen Participation and the Internet: Prospects for Civic Deliberation in the Information Age. *Social Studies*. 88(1): 23–28.

Willems E. (2019) From Cyberwar to Hacktivism. In: *Cyberdanger.* Springer, Cham.

Willihnganz, J (2008) The Rhetorical Analysis. Available at: https://web.stanford.edu/~jonahw/PWR1/RhetoricalAnalysis.html Last Accessed 3 Feb 2021.

Wilson, C (2009). Cyber Crime. In Kramer, Starr, and Wentz. Cyberpower and National Security. Available at https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-18.pdf?ver=2017-06-16-115054-803 Last Accessed 2 Jan 2022.

Wong, W.H and Brown, P.A. (2013). E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One. *Perspectives on Politics*. 11(4):1015-1033.

Wray, S. (1998). Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics. *Switch New Media Journal*, 4(2).

Wray, S. (1999) "On Electrical Civil Disobedience." *Peace Review* 11(1): 107-11.

Wright, S. (2004). Informing, Communicating and ICTs in Contemporary Anti-Capitalism Movements. In W. van de Donk, B. D. Loader, P. G. Nixon, & D. Rucht (Eds.), *Cyberprotest: New Media, Citizens and Social Movements* (1st ed.). London: Routledge. 77–93

Yar, M. (2005), Computer Hacking: Just Another Case of Juvenile Delinquency*?. The Howard Journal of Criminal Justice*, 44: 387–399.

Yar, M. (2006) Cybercrime and Society. London: SAGE Publications

Yin, R. K. (2003) *Case study research: Design and methods*, 3rd edition, London, SAGE Publications.

Young, AG.(2018). Using ICT for social good: Cultural identity restoration through emancipatory pedagogy. *Info Systems J*. 28: 340– 358

Yzer, M. C. & Southwell, B.G., (2008). New Communication Technologies, Old Questions. *American Behavioral Scientist*. (52):8-20

Zald, M and Ash, R. (1966). Social Movement Organizations: Growth, Decay and Change. *Social Forces.* 44(3): 327-341.

Zedner, L. (2007). Pre-Crime and Post-Criminology. *Theoretical Criminology*. 11(2), 261- 281.

Zeviar-Geese, G (1997–1998). The state of the law on cyberjurisdiction and cybercrime on the internet.In: California Pacific School of Law, *Gonzaga Journal of International Law*, vol. 1

Zuckerman, E. (2014). Foreword. In: Sauter, M *The Coming Swarm*. London: Bloomsbury. Xii-xv.

Legislation and Case Law

Oya Ataman v Turkey. App no 74552/01

Bills.parliament.uk (2021). Police, Crime, Sentencing and Courts Bill. Available at https://bills.parliament.uk/bills/2839. Last Accessed 16 April 2021

Council of Europe (2001). Convention on Cybercrime. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. Last accessed 5 Dec 2019.

DPP v Jones (1997) 2 Cr. App. R. 155, HL

DPP v McKeown (1997) 2 Cr. App. R. 155, HL

EUR-LEX (2005). Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005F0214. Last Accessed 18 Dec 2020.

EUR-LEX (2012). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market /* COM/2012/0238 final - 2012/0146 (COD) */. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012PC0238. Last Accessed 18 Dec 2020.

EUR-LEX (2013). Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040. Last Accessed 18 Dec 2020.

EUR-LEX (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC. Last Accessed 18 Dec 2020.

Legislation.gov.uk (1949). “Registered Designs Act”. Available at http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/88/contents. Last Accessed Last Accessed 18 Dec 2020.

.

Legislation.gov.uk (1959). “Obscene Publications Act”. Available at http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents.Last Accessed 18 Dec 2020.
.

Legislation.gov.uk (1960). “Indecency with Children Act” Available at http://www.legislation.gov.uk/ukpga/Eliz2/8-9/33/enacted. Last Accessed 25 May 2019.

Legislation.gov.uk (1968). “Firearms Act” Available at http://www.legislation.gov.uk/ukpga/1968/27/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1968). “Theft Act”. Available at http://www.legislation.gov.uk/ukpga/1968/60. Last Accessed 25 May 2019.

Legislation.gov.uk (1971). “Misuse of Drugs Act” Available at http://www.legislation.gov.uk/ukpga/1971/38/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1971). “Criminal Damage Act“ Available at https://www.legislation.gov.uk/ukpga/1971/48/contents. Last Accessed 10 March 2022.

Legislation.gov.uk (1977). “Criminal Law Act” Available at http://www.legislation.gov.uk/ukpga/1977/45/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1978). ”Theft Act” Available at http://www.legislation.gov.uk/ukpga/1978/31. Last Accessed 25 May 2019.

Legislation.gov.uk (1978). “Protection of Children Act” Available at http://www.legislation.gov.uk/ukpga/1978/37. Last Accessed 25 May 2019.

Legislation.gov.uk (1981).”Forgery and Counterfeiting Act”. Available athttp://www.legislation.gov.uk/ukpga/1981/45. Last Accessed 25 May 2019.

Legislation.gov.uk (1988). “Copyright, Designs and Patents Act” Available at http://www.legislation.gov.uk/ukpga/1988/48/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1988). “Malicious Communications Act”. Available at http://www.legislation.gov.uk/ukpga/1988/27/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1994). ”Trade Marks Act” Available athttp://www.legislation.gov.uk/ukpga/1994/26/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (1990). “Computer Misuse Act”. Available at https://www.legislation.gov.uk/ukpga/1990/18/contents. Last Accessed 18 Dec 2020.

Legislation.gov.uk (1998). “Human Rights Act”. Available at https://www.legislation.gov.uk/ukpga/1998/42/contents. Last Accessed 2 Jan 2019.

Legislation.gov.uk (2000). “The Terrorism Act”. Available at https://www.legislation.gov.uk/ukpga/2000/11/contents. Last Accessed 20 Feb 2022
Legislation.gov.uk (2002). “The Electronic Commerce (EC Directive) Regulations” Available at http://www.legislation.gov.uk/uksi/2002/2013/contents/made Last Accessed 25 May 2019.

Legislation.gov.uk (2002). ”Proceeds of Crime Act”. Available athttp://www.legislation.gov.uk/ukpga/2002/29/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (2003). “Sexual Offences Act”. Available at http://www.legislation.gov.uk/ukpga/2003/42/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (2003). “Communications Act”. Available at http://www.legislation.gov.uk/ukpga/2003/21/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (2003). “Anti-social Behaviour Act”. Available at https://www.legislation.gov.uk/ukpga/2003/38/contents. Last Accessed 20 Feb 2022.

Legislation.gov.uk (2006). “Fraud Act” Available at http://www.legislation.gov.uk/ukpga/2006/35/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (2006). “The Terrorism Act”. Available at https://www.legislation.gov.uk/ukpga/2006/11/contents . Last Accessed 20 Feb 2022

Legislation.gov.uk (2008). “The Counter Terrorism Act”. Available at https://www.legislation.gov.uk/ukpga/2008/28/contents. Last Accessed 20 Feb 2022

Legislation.gov.uk (2010). ”Video Recordings Act” Available at http://www.legislation.gov.uk/ukpga/2010/1/contents. Last Accessed 25 May 2019.

Legislation.gov.uk (2015). “Criminal Justice and Courts Act” Available at http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted. Last Accessed 25 May 2019.

Legislation.gov.uk (2015). “Serious Crime Act 2015”. Available at http://www.legislation.gov.uk/ukpga/2015/9/contents/enacted. Last Accessed 25 May 2019.

Legislation.gov.uk (2016). “Investigatory Powers Act 2016”. Available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted. Last Accessed 25 May 2019.

Legislation.gov.uk (2018). “Data Protection Act”. Available at http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. Last Accessed 25 May 2019.

Legislation.gov.uk (2008). “The Counter Terrorism and Border Security Act”. Available at https://www.legislation.gov.uk/ukpga/2019/3/contents/enacted. Last Accessed 20 Feb 2022

R v Gold and Schifreen (1984) 1 AC 1063 (HL).

R v Sheppard and Whittle (2010). EWCA Crim 65.

R v Smith (2004). QB 1418.

Shuttlesworth v. City of Birmingham, 394 U.S. 147, 161 (1969)

UN (1973). *International Convention on the Suppression and Punishment of the Crime of Apartheid*. G.A. res. 3068 (XXVIII)), 28 U.N. GAOR Supp. (No. 30) at 75, U.N. Doc. A/9030 (1974), 1015 U.N.T.S. 243, entered into force July 18, 1976. Available at un.org/en/genocideprevention/documents/atrocity-crimes/Doc.10_International%20Convention%20on%20the%20Suppression%20and%20Punishment%20of%20the%20Crime%20of%20Apartheid.pdf. Last Accessed 12 March 2020.

Datasets used

AZSecure-data.org. Anonops IRC channel Sep 2016-May 2018. Created by the University of Arizona (NSF #ACI-1443019), Drexel University, University of Virginia, University of Texas at Dallas, and University of Utah. Available to download from https://www.azsecure-data.org/internet-relay-chat.html. Downloaded on 6 August 2020. Last Accessed 13 April 2021.

Cambridge Computer Crime Database. Compiled by Professor Alice Hutchings. Available at https://www.cl.cam.ac.uk/~ah793/cccd.html. Last Accessed 27 Jan 2022.

Cyber attack timelines 2012-2019. Compiled by Paolo Passeri. Available on request at https://www.hackmageddon.com/. Downloaded on 6 August 2020. Last Accessed on 13 April 2021

DCMS Cyber Security Breaches Survey 2017. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017. Last Accessed 27 Jan 2022.

DCMS Cyber Security Breaches Survey 2018. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018. Last Accessed 27 Jan 2022.

DCMS Cyber Security Breaches Survey 2019. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019. Last Accessed 27 Jan 2022.

DCMS Cyber Security Breaches Survey 2020. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020. Last Accessed 27 Jan 2022.

DCMS Cyber Security Breaches Survey 2021. Available at https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021. Last Accessed 27 Jan 2022.

SWGfL Reputation Alerts Sentiment Analysis. Available when subscribed and logged in: https://swgfl.org.uk/login/

Zone H cybercrime archive. Available http://www.zone-h.org/archive/special=1. Downloaded on 29 Jan 2022.

Primary Sources

@anonops. Available at https://twitter.com/anonops?lang=en. Downloaded 12 November 2020

@BelarussianCyberPartisans. Available at https://twitter.com/cpartisans?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor. Downloaded 24 January 2022.

@chaosupdates. Available at https://twitter.com/chaosupdates?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor. Downloaded 24 January 2022.

@GhostSquadHacks. Available at https://en.wikipedia.org/wiki/Ghost_Squad_Hackers. Downloaded 24 January 2022.

@MMM_London. Available at https://twitter.com/mmm_london?lang=en. Downloaded 12 November 2020.

@Op_Russia. Available at https://twitter.com/op_russia?lang=en. Downloaded 12 November 2020.

@OpFreePalestine. Available at https://twitter.com/opfreepalestin3. Downloaded 12 November 2020.

@OpGreenRights. Available at https://twitter.com/opgreenrights?lang=en. Last Accessed 12 Novemnber 2020.

@OpIsrael. Available at https://twitter.com/op_israel?lang=en. Downloaded 12 November 2020.

@OpKillingBay. Available at https://twitter.com/OpKillingBay. Downloaded 12 November 2020.

@OpLastResort. Available at https://twitter.com/oplastresort?lang=en. Downloaded 12 November 2020.

@OpLiberation. Available at https://twitter.com/opliberation?lang=en. Downloaded 12 November 2020.

@OpSyria. Available at https://twitter.com/opsyria. Downloaded 12 November 2020.

@TheAnonMovement. Available at: https://twitter.com/theanonmovement?lang=en. Downloaded 11 November 2020.

@todayininfosec. Available at https://twitter.com/todayininfosec/status/1317085055160885250. Last Accessed 15 March 2021.

@YourAnonCentral. Available at https://twitter.com/YourAnonCentral. Downloaded 11 November 2020.

@YourAnonNews. Available at: https://twitter.com/YourAnonNews. Downloaded 11 November 2020.

@YourAnonOne. Available at https://twitter.com/youranonone?lang=en. Downloaded 11 November 2020.