Organic bodies versus digital bodies: the differences between hacktivism and cyberterrorism

Claudia Negri Ribalta

A research Paper submitted to the University of Dublin, in partial fulfilment of the requirements for the degree of Master of Science Interactive Digital Media

2018

Declaration

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at: http://www.tcd.ie/calendar

I have also completed the Online Tutorial on avoiding plagiarism 'Ready, Steady, Write', located at http://tcd- ie.libguides.com/plagiarism/ready-steady-write

I declare that the work described in this research Paper is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed: _____

Claudia Sofia Negri Ribalta
11th of May 2018

Permission to lend and/or copy

I agree that Trinity College Library may lend or copy this research Paper upon request.

Signed: _____

Claudia Sofia Negri Ribalta

11th of May 2018

Acknowledgement

I wish to thank my research supervisor, Bertrand Lucat, for his guidance and support for the development of this research paper. I would also like to thank W. for its endless support and advices in this study. Finally, I would like to express my biggest thank to my family, for giving the chance to study this Msc.

Summary

The following research aims at identifying the differences between cyberterrorism and hacktivism. In traditional media, both terms have been used as synonymous. Furthermore, in academia there is still no consensus upon the definition of both of these terms. As a result, there is still an unclear understanding of both phenomenona.

Through concept analysis, the study discusses different definitions and approaches to both ideas. Authors of the conceptualisation range from civil society, academics and formal institutions. After identifying the key components of hacktivism and cyberterrorism, through a qualitative case study, three different net disruption cases are studied. The cases selected are: the digital Zapatistas and FloodNet, Ferizi's hacking trial and Operation Payback and Avenge Assange. All of the cases were selected due to their notoriety, impact and importance in the field.

The findings of this study have concluded that hacktivism and cyberterrorism are different event. However, further research should be done about net disruption, as current theorisation is insufficient to describe and understand current organisations and disruptions, such as Anonymous or Operation Payback.

Thus, this study seeks to contribute to the current literature and discussion about net disruption, through a critical point of view.

Table of Contents

Introduction

Much has been talked about the possible threats of cyberterrorism in the traditional media. The media constantly publishes about the possible use of the internet and the cyber realm by terrorists. Various governments have created different kinds of public policies targeting the topic (e.g. the United States of America or the United Kingdom) and even the North Atlantic Treaty Organisation has recognised cyberterrorism as a possible threat in the future (North Atlantic Treaty, *New threats: the cyber-dimension*, n.d.). Yet the concept remains vague and controversial.

Governments, organisations and academics coin different definitions, depending on their focus. Some definitions focus solely on the digital nature of cyberterrorism The abundance of concepts has made it difficult to compare the conclusions of different streams of research, as there are few common denominators in the various conception of cyberterrorism. Furthermore, due to the large spectrum of definitions available, there is a worrisome stretching of concept that further emphasises this impossibility of contrasting outcomes (Sartori, 1970). Some authors consider cyberterrorism as any activity that can be linked to terrorism ,such as chat rooms for organising terrorist attack or the reproduction of terrorist messages/images. Meanwhile on the other side, cyberterrorism is conceived as an activity that is purely carried out in the cyber realm, with cyber targets, commonly called pure cyberterrorism.

Hacktivism has a more difficult conceptualisation. Although activists of "hacktivism" have been around for decades, most people have a vague sense of what it entails. The organisation Anonymous has been famously linked to this kind of activity. Yet, some consider Anonymous to be a cyberterrorist group, rather than a hacktivist group. This uncertainty further stresses the confusion between concepts, as usually they are used are synonyms, when in fact they are describing different activities (Conway, 2003; Devost et al, 1997; Embar-Seddon, 2002; Vegh, 2002; Debrix, 2001). Furthermore, is hacktivism an adjective to define a whole organisation, or is it a particular tactic, used in specific situations? Can an organisation be political in nature, yet use a variety of tactics like social media protest, hacking and cyberterrorism? And if this is the case, then how does one label the organisation?

In policies, popular culture and common language, cyberterrorism is a synonym of hacktivism, as cyberterrorism is used to describe hacktivist event. How is cyberterrorism different from hacktivism? Cyberterrorism differentiates from hacktivism, in the sense that cyberterrorism's primary objective is inflicting physical, economic or digital harm, to undermine society's support points[1], by instilling fear in a large portion of the population. Whilst hacktivism distort the cyber realm, while assuming the consequences of their actions, in the spirit of civil disobedience

Both concepts might not be completely opposite and could even have some elements in common, such as political motivations, cyber targets or means and illegality in their acts. Nonetheless, they are different, either an activity is hacktivism or a cyberterrorist attack (Devost et al, 1997). Although academically speaking, there can be a conceptualisation that frames both concepts as part of a continuum, as suggested by Goertz (2006). for concept building, in practical terms hacktivism and cyberterrorism must be different. In the creation of public policy and laws, there has to be a clear differentiation of both activities. As Vegh (2002) underlines, the "terminological ambiguities do have serious policy and legislative implications". Taking into account the motives behind online activism or disruption is crucial for understanding the type of activity behind, and it should be analysed if it consists of an illegal act or not (Vegh, 2002; Devost et al, 1997). When convicting a person or organisation for an illegal act, a clear distinction has to be made between concepts; it cannot be a spectrum. Moreover, tackling hacktivism at a governmental level requires different capabilities and poses different threats, compared to cyberterrorism (Devost et al, 1997). "… Political crimes have vastly different implications for national security and defence policy than do other 'common' crimes. Terrorism is a political crime: an attack on the legitimacy of a specific government, ideology or policy" (Devost et al, 1997, pg.76-77). After all, "labelling every malicious use of a computer system as 'terrorism' serves only to exacerbate confusion and even panic among users and the general public…"(Devost et al, 1997, pg. 76).

The requirement of a robust and conscious definition is crucial for research (Goertz and Manzur, 2008; Goertz, 2006). In addition, as Barnards-Wills has stated, "political language is not simply descriptive but also evaluative. To term something a 'war' or not, is not

[1] Society support points can be understood as critical infrastructure, social composition, values, culture, among others.

just to describe, but also to judge" (2011, pg.19), a discussion that can also be extrapolated to the concept of terrorism. There is no agreement about what differentiates hacktivism and cyberterrorism. Moreover, some theorists have suggested the idea that they are the same practice or that they overlap in occasions, trading the intension of the concept for extension (Goertz, 2006). As expressed by Goertz, "good concept-building makes these contrast explicit and systematic" (2006, pg. 24), that directly impact policy making, specially in the grounds of crime, hacktivism and cyberterrorism(Vegh, 2002; Devost et al, 1997).

The aim of this study, is to provide a concise and robust analysis of cyberterrorism and hacktivism, understanding their differences and similarities. This study will be constituted of five parts. After the introduction and methodology, a literary review of both concepts will follow. Optimally, a list of elements for both concepts that distinguishes core attributes of them should be created after an in-depth analysis in the literary review. In section four, through an Qualitative Case Analysis, the proposed definitions are to be analysed with three real life examples, aiming to understand if the concepts studied corresponds to any real events or are yet to be seen. In section five, future research will be identified together with the conclusion.

Methodology

As a key idea of this research is concept analysis, a preliminary introduction of logics and concept analysis notions is fundamental. Firstly, it is necessary to understand the structure of concept analysis. Key ideas such as concept stretching, logic between "and/or", extension and intension will be revised in this section.

After identifying key elements for concept analysis, an in-depth literary review of both hacktivism and cyberterrorism will follow. A brief and simple introduction will open hacktivism and cyberterrorism, addressing the current state of art. After it, certain key definitions of each concepts will be discussed. The article will then review how much each definition is able to travel, alongside its extension and intension, logic behind it, possible misconception and criticism. Other key words from the first section will be used in this section, to provide a better understanding of the different concepts and what consequences they bring. Authors like Lee Jarvis, Dorothy Denning, Pollitt, will be revised from the academic community. Civil society definitions, from authors such as the Critical Art

Ensembles or the Electronic Disturbance Theater will also be covered. There will be a brief mention of definitions from defence institutions, such as the The Department of Defence of the United States or Federal Bureau of Investigation of the United State.

After carefully examining the different definitions, the research will identify the key components of both hacktivism and cyberterrorism. Optimally, those key components will be outlined and listed out, to enable a faster and easier comparison between definitions.

A qualitative case analysis proceeds after the literary review. In this section, key elements of hacktivism and cyberterrorism are contrasted with the case selected. Through this method, the concept building will be applied in real life. The results that this section will help develop further research and questions required regarding the applicability of the cyberterrorism and hacktivism definitions.

Finally, in the conclusion, the results will be summarised and further research identified. The discussion done through the research should be able to conclude if hacktivism and cyberterrorism do effectively exist in real life, if there are (notable) differences between both concepts and possible criticism of the research carried out.

Literary Review

Concept Building and Analysis

One of the first ideas for reviewing a concept, is intension and extension. Any dictionary might tell the reader that " 'intension' indicates the internal content of a term or concept that constitutes its formal definition; and 'extension' indicates its range of applicability by naming the particular objects that it denotes."(The Editors of Encyclopaedia Britannica, *Intension and Extension,* 2018). For a more precise understanding, Drescher (1991) suggests that extension are the cases or "class of things" (Sartori, 1970, pg. 1041) that fall under a concept's scope, meanwhile intension is "the representation of the concept" (pg. 88), i.e. how it is defined, it's properties. In short, intension is the definition of the concept and extension are the cases that fall under that particular concept (Ahram, 2013; Sartori, 1970)

This idea of intension and extension is tightly linked to the "ladder of generality" and "conceptual stretching" of Sartori[2].

On one hand, for broadening/stretching a concept - in other words, making it climb up the ladder of abstraction - Sartori suggests that one has to go about "diminishing its attributes or properties, i.e., by reducing its connotation" (1970, pg. 1041). Using these methods, allows the concept to keep certain precision (its differentiating attributes remain) whilst being more inclusive (Sartori, 1970). However, this still makes the concept more imprecise compared to its original meaning. Vice-versa, to move down the ladder, the intension of the concept should be increased, adding more attributes (Ahram, 2013, pg. 281), "i.e., by augmenting its attributes or properties" (Sartori, 1970, pg. 1041).

The afore mentioned movements of the dimensions (extension and intension) also work as the opposite sides of a ladder (the ladder of generality). As they change, they define the level of abstraction of a concept: high, medium and low level. The higher the level of abstraction, the more general a concept is; if a concept is "high level", it has a "global denotation" (Sartori, 1970, pg. 1041). Medium level concepts, can be designated as general classes in the sense that they are still unique yet they cannot travel as much as high level concepts. Finally, low level concepts are extremely accurate, and thus cannot be applied to a generality.

Under Sartori's impression, it is incorrect to increase the extension of a concept, while trying to keep the same intension. "Sartori used the term **stretching** and **straining** to describe the process by which specific connotation is jettisoned in the course of extending denotation"[3] (Ahram, 2013, pg. 281). Although concepts should travel through time - meaning that they will lose certain intension for it - a concept should not be manipulated to be applied for specific situations. " 'Conceptual stretching' thus means in operation terms, to

[2] Sartori is one of the most well-regarded political scientists. The author made one of the first and most indispensable contributions for concept analysis in social science and political science, discussing about the ladder of generality, concept stretching and straining and intension/extension. With his work *Concept Misinformation in Comparative Politics* (1970), Sartori is still one of the most important authors for concept analysis (Goertz, 2006). For this reason, it seems reasonable to start the literary review about concept analysis with the author.

[3] Emphasis added by the writer

eliminate necessary dimension. This makes the concept more general and simultaneously increases the distances it can travel" (Goertz, 2006, pg. 57).

It is important to highlight certain aspects of the intension/extension tradeoff. Firstly Drescher (1991) points out that concepts with different intension might have the same extension (pg.88-89). Therefore, the problem of *concept stretching* relates to when a concept previously defined is manipulated. Furthermore, Goertz (2006) have identified that the problem of the intension/extension tradeoff could be solved with a conceptualisation by family-resemblance, rather than classical "necessary and sufficient" approach (also in Ahram, 2013, pg. 281). Thus, taking another approach to might prove helpful. Yet, Ahram (2013) has identified that, even in the presence of the different approaches (i.e. family resemblance and necessary and sufficient) "the core of Sartori's contention about concepts remains intact" (pg. 281). Still, there is ongoing investigation and discussion into which kind of concept building methodology is more adequate (A.A. Brenna, 1997; C.Travis, 1997 ; Goertz, 2006; Ahram , 2013; Braumoeller and Goertz, 2000).

As previously said, Goertz (2006) identifies that the trade-off of intension versus extension is a consequence of the classical philosophical approach for concept building, based in *necessary and sufficient conditions*, which stems from Aristotle (Goertz, 2006, pg. 56). As such necessary and sufficient conditions, corresponds to a more classical interpretation of concepts.

Necessary conditions and sufficient conditions *are* different. A necessary condition does not imply that it can be regarded a a sufficient one. "A necessary cause allows an outcome to exist; without the necessary cause, the outcome will not exist. A sufficient cause ensure that the outcomes exists; it produces the outcome" (Dul, 2015 , pg. 11). In other words, X is a necessary condition for Y to occur (Hanks, n.d.), "it is impossible to have Y without X" (Lau and Chan, 2018). As a result, a necessary conditions (X) is an essential condition for Y to occur, and can be more than one condition (Lau and Chan, 2018). In Brennan words (1997) "A necessary condition … is one whose touch is a sine qua non of the truth of the other condition" (pg. 283)

Meanwhile, X is sufficient for Y, as long as the sole presence of X guarantees the Y outcome (Hanks, n.d. ; Lan and Cha, 2018). Contrary to the necessary condition, a sufficient condition is by itself enough to Y to occur. Therefore, a necessary and sufficient condition is one that by it self does guarantee the occurrence of Y and it is essential for it. "It is possible to define various other kinds of necessary and sufficient conditions —including nomic and conceptual ones" (Bennan, 1997, pg. 283), yet this discussion does not fall under the scope of this research paper.

As per definition, necessary conditions do not always have to be of boolean logic (dichotomous necessary conditions), they can be discrete or continuous (Dul, 2015, pg.16). When the necessary conditions are dichotomous, the formulation usually follows up as "X is a necessary condition for Y if X is always present when Y occurs … X is a necessary condition for Y if Y does not occur in the absence of X" (Braumoeller and Goertz, 2000, pg. 846). Meanwhile, a discrete necessary conditions can have different levels of values, such as low, medium or high (Dul, 2015, pg. 19). The question with this kind of conditions, is setting the necessary/minimum level for X and how it will impact . Finally continuous necessary conditions "means that the condition and the outcome can have any value within the limits of the lowest (0%) and highest (100%) values, allowing for even further detail" (Dul, 2015, pg. 20).

For the following research paper, I will use the concept of extension, intension, conceptual stretching, abstraction, generality, necessary and sufficient conditions. The applications of these ideas are going to be used to understand the difference between definitions of cyberterrorism, hacktivism and their criticism. The decision to include this concepts and not other, is based on the idea that they are general ideas to carry out concept analysis. For future research, more terms should be added and discussed in the comparison of definition.

Cyberterrorism

The biggest conflict when studying cyberterrorism is that there is no single definition of terrorism, yet alone cybercrime or cyberterrorism. (Conway,2003; Holt, 2012; Jarvis, Nouri, Whiting, 2014; Embar-Seddon, 2002). Cyberterrorism was coined by Barry Collin in the 80's and since then, it was further studied by Pollitt (an FBI agent) and Denning (Conway, 2003).

Since the attack of 9/11, the term was further discussed by other scholars and authors, and prominently featured in traditional media, as part of the securitisation trend of international relations, policy and defence studies. Nonetheless, there are still multiple definitions of cybercrime and "cyberterror", that makes "it difficult to immediately distinguish these acts…"(Holt, 2012, pg. 338).

Jarvis, Nouri and Whiting (2014 , pg.26) explain that some of the definitions of cyberterrorism are so broad and general, that they suggest that as long as computer technology is involved in the terrorist act (planning, getting information, objective, etc…) the attack can and should be labeled as cyberterrorism (giving as an example, the definitions of Dsouza and Hensgen, 2003). As a result, there has been some stretching of the concept and misinformation surrounding cyberterrorism (Conway, 2003). Definitions such as the one coined by Devost, Sought and Polland (1997, in Conway 2003) that define cyberterrorism as " 'information terrorism' as 'the intentional abuse of a digital information system, network or component toward an end that support or facilitates a terrorist campaign or action' " (pg.3), demonstrates how the concept can be manipulated to adapt certain ideologies. Conway (2003, pg.4) has stated that some definitions try to deliberately pose hacktivism as cyberterrorism, when they are different acts (Holt, 2012; Conway, 2003; Embar-Seddon, 2002; Kenney, 2015). This situation contradicts what Sartori consider to be an appropriate use of concept. Concept should not loose intension to broad the extension; in other words, conceptual stretching should not occur to "adapt" the concept an ideology. Transforming an already low level of abstraction concept into one of medium/high, should be criticised and contested.

Furthermore, much of the discussion involving cyberterrorism, occurs in the media, where cyber vandalism, i.e. hacktivism, is labelled as cyberterrorism, further emphasising the broad confusion between both terms (Holt, 2012; Kenney, 2015; Weiman, 2006; Conway, 2003; , pg.29). The media has exploited "two significant modern fears: the fear of technology and the fear of terrorism" (Embar-Seddon, 2002) when talking about cyberterrorism, exaggerating the real threat of such an attack and, at the same time, misinforming the public.

Given this caveat, as a common ground to start studying the concept, most of the scholars take Denning's (2000) definition as a starting point to their own discussions. The

author´s definition got traction after publicly providing her idea to the US´s House of representatives in 2000. Since then, the definition has been used multiple times, with some modifications. Denning defines cyberterrorism as:

> Cyberterrorism is the **convergence of terrorism and cyberspace**. It is generally understood to mean unlawful attacks and threats of attack **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. Further, to qualify as cyberterrorism, an attack should **result in violence against persons or property, or at least cause enough harm to generate fear.** Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. (2000)[4]

Denning definition has not come without criticism or comments. For example, for Gordon and Ford (2003), Denning's definitions relates more to one of pure terrorism, rather than cyberterrorism: it just adds the word "computers" to redefine it. To put it differently, it is terrorism carried out in another operational theatre, i.e. the information or cyber dimension. Jarvis, Nouri and Whiting, (2014), highlight that Denning's definition identifies that "the target (or consequences) of an attack differentiate this type of politically motivated activity from others"(pg.28). Thus, the definition sets a precedent over how to differentiate cyberterrorism from other unlawful activities: by the target or the consequences

In spite of said criticisms, it is interesting to note certain aspects of Denning definition. For example, the author sets computers or networks as the primary target of the terrorist attack, yet never defines the medium in which they are carried out. Therefore it opens the concept to the following line of questioning: what the target of an attack is a computer and the action is carried out through physical means? Should it still be labelled as cyberterrorism?

[4] Emphasis added by the writer

A necessary condition of cyberterrorism according to Denning, is to generate fear and seek to intimidate/coerce governments. Therefore it remains critical to underline that, under Denning's definition, a cyberterrorist attack is a political attack. It keeps the level of generality in a low/medium level, as it is not all cyber attacks; i.e. an attack seeking profit or stealing money, without a political intent, it not cyberterrorism.

Another definition, that is often quoted is Pollitt's (1998)[5]. Pollitt define cyberterrorism as "the premeditated, **politically motivated attack against information, computer systems, computer programs**, and data which result in **violence against noncombatant** targets by sub national groups or clandestine agents."[6] (1998).

Pollitt and Denning's definitions arise three key aspects/questions to resolve: What is the role of computers in cyberterrorism? What is the motive behind an attack and how important it is? (Is motive enough to define an attack?) What is violence in the cyber realm?

In cyberterrorism, computers can be understood as target, means of action or both. As Gordon and Ford (2003) points out, terrorists can use computers in multiple ways, i.e. as tools to pursuit their objectives. Therefore, saying that using computers in anything related to terrorism is not a sufficient dimension to define something as cyberterrorist; doing so could lead to conceptual stretching which would prompt absurd definitions such as "cell phone terrorism". (Gordon and Ford, 2003, pg.7). Of course, certain organisations that resort to terrorism, will use the internet in the pursuit of their objectives: the internet has been used as a theatre to make their intents and messages known (for propaganda & radicalisation purposes), to gather funding and, recruiting new people (Gordon and Ford, 2003). However, for Conway (2003), only "when computer technology is used as a weapon/target" (pg.5) can it be label an act as cyberterrorism. As such, the sole use of computers for coordinating a terrorist attack, does not imply that such disturbance should be labeled as cyberterrorism. The extension is kept tight, as the concept has high intention. In order to satisfy the conditions of a logical definition of cyberterrorism, information technologies should play a

[5] Mark M Pollitt used to serve in the FBI as a Special Agent and was appointed as director in the FBI's Regional Computer Forensic Laboratory Program. Pollitt worked in the FBI, until his retirement in 2003. While being a special agent, he extensively wrote and studied about computer crimes.

[6] Emphasis added by the writer

major role in the attack, either as the target, the main field of occurrence or the method employed.

The motivation of cyberterrorism, as per its own wording, implies that the motivation should be closely related to classical terrorism. "Cyberspace attack must have a 'terrorist' component in order to be labeled as cyberterrorist" (Conway, 2003, pg.5). In general, it is understood that a terrorist attack has to be politically or ideologically motivated (Holt, 2002, pg.340; Pollitt, 1998; Denning, 2000; Kenney, 2015; Embar-Seddon, 2002). "Terrorism is a political crime: an attack on the legitimacy of a specific government, ideology or policy" (Devost et al, 1997, pg.76-77). By logical extension, a cyber attack that is not politically/ideologically motivated, should not be labelled as cyberterrorism. This assertion does not imply that such an act is not unlawful or unethical, i.e. economic cyber crimes, or that every politically motivated demonstration is cyberterrorist, i.e. a sit in o protest. Thus, being politically motivated is not a sufficient criteria, it is only necessary. In cyberterrorism "the motivation is the normal terrorist motivation of political change" (Embar-Seddon, 2002, pg.1034).

Finally, the answer for what is violent in the cyber realm is not obvious. In the cyber world our lives are not at risk (or at least, not directly). The cyber realm is composed basically of information and destroying information is not what we commonly understand as violence. As Jarvis, Nouri and Whiting, (2014) state, there is no agreement about what violence is. For example Conway (2004) in Jarvis, Nouri, Whiting, (2014) defines that violence is where there is physical harm "against a person or sever economic damage". On the other hand, for Desouza and Hensgen (2003, pg.388) in Jarvis, Nouri, Whiting, (2014) "others believe any terrorist usage of the internet to constitute a sufficient criterion" to define something as violent.

> Holt (2012) provides a useful answer for this dilemma. There are two forms of violence, the first of which includes behaviour that cause emotional harm to individual through online environments… the second form of violence involved the distribution of materials on line that can be used to cause harm in the real or virtual world (pg. 339)

As a possible solution to understand violence in the cyber realm, it should not to thought about it in the traditional way (i.e. physical violence). Instead, violence could present itself in an economical fear or as a disruption on information, infrastructure or networks [7](Holt, 2012). If such approach is to be taken, then another discussion should be addressed: whether our digital bodies are more or equally important, as our organic selves.

If cyberterrorism was to exist, then our digital bodies would have a similar importance in society; that is the core idea behind the criticism to the concept of cyberterrorism. There are only few voices that question the very core idea of the existence of phenomena that one could define as cyberterrorism, often highlighting the ideological implications of the term. Mild critics of cyberterrorism in traditional media are scarce (Vegh, 2002). There are three argumentative lines that question the concept of cyberterrorism.

The first one highlights the idea that many concepts of cyberterrorism allow people, mostly in mass media, to "label every malicious use of computer systems as 'terrorism' " (Devost et al, 1997) denying that the different cyber and electronic disturbances are driven by divergent motivations (Devost et al, 1997; Debrix, 2001; Vegh, 2002). This criticism is based on the extension of the concept used in traditional media to define cyber-terrorism. Terrorism itself, is a concept with medium/low abstraction, that is usually used for very specific cases and does not apply to every disruptive action. Thus, it has a strong level of intention. In reality, according to Vegh (2002) there are different *kinds* of hacking and the intentions behind them are not always malicious, violent nor destructive. Accordingly, cyberterrorism is then one of the many form of hacking, that has a malicious, violent or destructive intent. For this reason, the concept should have a strong level of intention and low abstraction. Furthermore, Debrix (2001) suggested that the media uses the term of cyberterrorism for various types of cyber disturbances, identifying that not all attacks are a threat to national security nor are malicious or professional, . In consequence, taking Vegh's and Devost et al argumentation, labelling cyber-terrorisms as the traditional media does, would be a case of conceptual stretching.

[7] Violence in the cyber realm could be understood not just as physical - although that does not mean it can also be physical - but as a combination of informational, economical and physical.

Debrix (2001) indicates that the media establishes the "genuineness" of a cyberterrorist, based upon the threat to the national security of an attack. "… the 'genuine' cyberterrorist wants to harm, weaken, possible kill" (Debrix, 2001, pg., 159). The criticism both authors (Vegh 2002 and Debrix 2001) realise to this conceptualisation, is that terrorism is a binary term. Something is either terrorist or not, it cannot be "a more or less genuine" act of cyberterrorism (Vegh, 2002; Debrix, 2001). In formal terms, terrorism is not a concept that can be coined under a continuum. There has to be a distinction between "socially justified activism and criminal or even terrorist activities"(Vegh, 2002). A young teenager, cracking a website for humour has not done the same offence as someone disrupting the central grid for electricity with political purposes (assuming that both are possible and attractive to hackers) (Debrix, 2001).

Not having a clear distinction between online-based activism and cyberterrorism, can have effect in policy making (Devost et al, 1997; Vegh, 2002). As Devost et al (1997) point out,

> Terrorism is a political crime: an attack on the legitimacy of a specific government, ideology or policy. Hacking into a system to erase files out of sheer ego, or stealing information with the sole intent to blackmail, is nothing more than simple theft, fraud or extortion, and certainly is not an attack upon the general legitimacy of the government. (pg. 77)

Therefore misinterpreting a criminal act - if we agree with Devost et al that hacking is a crime - with a political act, can have potentially serious legislative and policy conflicts in the future. I'll refer to this in the discussion of hacktivism.

The second argumentative line, indicates that cyberterrorism does not exist and thus is impossible to carry out, because the concept of "terrorism" entails the idea that there is an existential danger to life and puts in evidence the mortality of the individual (Critical Art Ensemble, 2001; Debrix, 2001). To quote the Critical Art Ensemble, "how can terror happen in virtual space, that is, in a space with no people - only information? Have we reached a point in civilisation where we are capable of terrorising digital abstractions?" (pg. 31). Stretching the concept of terrorism to the cyber realm, would be incorrect because in the cyber realm it is impossible to have our lives at risk, as the cyber world only works with our "digital bodies". The Critical Art Ensemble (CAE from now on) was vocal about the idea that

"terrorism on the net" cannot happen and that it is a construct of the government, because "… terrorism requires **organic** bodies to house the terror"[8] (2001, pg. 32).

For the group of artists, the most important aspect of terrorism is that the violence is directed to the citizen, it is random (meaning that the element of surprise is a necessary condition) and creates fear (CAE, 2001). A necessary (yet not sufficient) condition for terrorism to occur, it is randomised and directs citizen.

> … perpetual apprehension of their own mortality, due to what is perceived to be a consistent state of violence. If this panic can be maintained for a long enough period of time, the public will eventually demand negotiations to end this socio psychological state of discomfort. (pg. 31)

Debrix (2001) also reflects upon this condition. The author also highlights the idea of digital and organic bodies.

> By putting our physical bodies inside our extended nervous systems, by means of electric media, we set up a dynamic by which all previous technologies that are mere extension of hands and feet and teeth and bodily heat controls… will be translated into information systems (pg.150 - 151)

Debrix (2001) understands that in our current information age, the organic human body cannot survive without the digital body (pg. 162). In consequence, because of this tight relationship between the organic body and the digital body, cyberterrorism would (if accepted the premise that we are in a post-human condition) target the organic body through the digital body (pg. 162).

Nevertheless, if this is to happen, to be as a reality, the CAE has pointed that is a frightening situation to be in. "What is frightening to CAE about this scenario is that electronic erasure is perceived as equivalent to being killed in a bomb explosion. Now the perception exists that the absence of electronic recognition equal death" (CAE, 2001, pg. 36 - 37)

[8] Emphasis added by the writer

Finally the third line of argumentation, centres on the role of the media in the creation of disproportionate fear of a cyberterrorist attack, suggesting that it is a manipulation from the elite, as a way for silencing dissident voices (CAE, 2001; Debrix, 2001; Vegh, 2002). The media works as an instrument "… for the government to show credible that cyberterrorism does, indeed, exist, or is at least highly probable to occur in the future", to keep exercising "restrictive legislation" (Vegh, 2002). As such this concept of cyberterrorism would be loosely applied to several different phenomena to fulfil its sociological goal of allowing the government to impose tighter controls.

Given all these points, certain elements can be identified as necessary for cyberterrorism to occur, if it is ever possible to happen. These are:

- Must have a clear political motivation, that must have been done public,
- It aims for the destruction of infrastructure, or grave economic harm or irrational widespread of fear in the population,
- Uses digital or cyber means, without having necessarily a digital objective,
- Makes society wonder about their chances of potentially dying (mortality),
- It uses the internet or the media to get as much visibility as possible, in other words, it uses the media a theatre to spread their ideas and be recognised

Some of the element recognised are more obvious than other, all of the are necessary conditions but not sufficient for cyberterrorism to occur. Cyberterrorism is a concept that should have high levels of intension, and low levels of extension and abstraction. Overall, all these elements must be present to cyberterrorism to occur.

Hacktivism

Per wording, the term *hacktivism*, is the conjunction of the words activism and hacking (Vegh, 2002; Scheuerman, 2016; Denning, 2001). As such, the word hacking, under this circumstance, defines the method/tactic activism uses. Moreover, the general understanding of the conjunction of both words, is

> …where 'hacking' is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ('hacking tools'). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyberspace (Denning, 2001,pg. 263),

where the word activism, includes the political motivation behind such actions. Scheuerman (2016), adds that hacktivism is commonly understood as an activity where "…technologically savvy 'hackers' break into computer servers for shaming targeted organisations and their practices; leaking and whistleblowing by groups such as anonymous and Wikileaks or by prominent figures…"(pg. 299).

Although there is no record of the first hacktivism act, the idea of the union of activism and digital disruption started to erupt around the end of the 80's and beginning of the 90's. One of the most noticeable events of hacktivism at the time - an event that Julian Assange in 2006 stated to be one of the first event of hacktivism in history- was the WANK worm attack, that targeted NASA and the US Energy Department (Assange 2006; Denning, 2001; McCormick, 2013). The worm infected the institutional computers of both governmental entities with a clear political motive: civil discontent with the current nuclear project. "That WANK had a bold political intent was immediate. WANK penetrated machines had their login altered"(Assange, 2006) and showed the users / website visitors an image, claiming the machine to have been WANKed.

However, at the time, the event was not catalogued as hacktivism. Such term was not used until (approximately)1998

> …when cDc[9] members Omega, Reid Fleming and Ruffin were chatting online and were, Ruffin said, 'bouncing some wacky ideas around about hacking and political liberation, mostly in the context of working with Chinese hackers post-Tiananmen Square.'
>
> 'The next morning Omega sent an e-mail to the cDc listserv and included for the first time the word hacktivism in the post,' Ruffin said. 'Like most cDc inventions, it was used seriously and ironically at the same time – and when I saw it my head almost exploded.' (Wired Staff, 2004)

Nevertheless, the idea of digital activism and civil disobedience over the net and cyber world, had been previously advanced theoretically by the CAE in 1994 (Wray, 1999 pg.107;

[9] Acronym for Cult of the Dead Cow. The Cult of the Dead Cow, is a hacker organisation, founded in the mid-80's. The organisation defines itself as "The cDc is a leading developer of Internet privacy and security tools, which are all free to the public. In addition, the cDc created the first electronic publication, which is still going strong."(CultoftheDeadCow, *About - Who We Be,* n.d). The group is known for their particular approach to media and *trolling*

Critical Art Ensemble, 1996; Denning, 2001, pg.264). CAE critically engaged with the internet, as a discursive and public sphere and rumbled over the question of the possibility of creating a politicised position over the net (Lane and Dominguez, 2003). In consequence, the group published the (in)famous book of *Electronic Civil Disobedience & Other Unpopular Ideas* (1996), which featured the essay titled *Electronic Civil Disobedience,* previously published in 1994 as a standalone piece. Throughout the essay, the authors emphasised the idea that, due to the nature of the new information society - where information is the new capital and technology is a central actor in society- activism should also be carried out through the internet and other forms of digital/cyber media (CAE, 1996; Wray, 1999 pg.109). Although throughout the essay, CAE does never refer to Electronic Civil Disobedience as hacktivism, readers, academics and the authors have given the essay that interpretation, referring to it as one of the first theorisation about the topic (Mecali, 2017). The new civil disobedience should affect the influx of information, rather the physical world (analogous to the influx of personnel in a company) as information has gained a central status in the modern society (CAE, 1996): "blocking information access is the best means to disrupt any institution, whether it is military, corporate o governmental" (CAE, 1996, pg.13). In short words, the internet should be used as a tool for new activists, as a theatre of action, as a mean to deliver information, creating engagement and empowerment within the society (Wray, 1999, pg. 108; Dean, 2016; Denning, 2001). To further enlighten the scope of this idea, according to the authors, the cyber realm should be used as a " …'recombinant theatre', a practice that works in dynamic relation between the organic and virtual, moving in the various electronic networks where elite power actually resides" (Lane and Dominguez, 2003, pg. 134).

The logic of the argument follows the idea that civil disobedience is a fundamental value in western democracies, that can and should also be applied within the digital world, creating the concept of electronic civil disobedience (CAE, 1994; Dominguez, 2009; Lane and Dominguez, 2003). The CAE takes their inspiration from King's and Rawls' ideas about civil disobedience, where "conscientious acts of political illegality were legitimate only when appealing to some more fundamental ideal of the law" (Scheuerman, 2016, pg. 301). Furthermore, "in Rawls' famous definition, civil disobedience refers to a 'public, non violent, conscientious yet political act contrary to the law usually down with the aim of bringing about a change in the law or policies of the government'" (Rawls, 1971 , pg.364, in Scheuerman, 2016, pg.308), elements that the Critical Art Ensemble considers fundamental

for electronic civil disobedience. Dominguez - one of the founding members of CAE - has expressed in numerous occasions that electronic civil disobedience must follow certain characteristics that differentiate it from other acts of vandalism or protest. These are : "one, it is a public action; two, it is non-violent; three, it willingly accepts the condition of 'deliberate unlawfulness and accepting of responsibility'; four, it is always conscientious concerning it is civil nature"(Dominguez, 2008, pg.664).

> For EDT it has been important that local, national and international courts judge its acts - or those of any group that follow the performance paradigm that we have established - as transparent civil acts of disobedience and not as 'cybercrime' (Dominguez, 2008, pg.1808).

Furthermore to comply with their own rules, Dominguez and his collective, have emphasised the importance of being transparent on their identities and their future plans (Lane and Dominguez, 2003, pg. 138). Being transparent, working in the public sphere, that actions are non-violent, accepting responsibility and that the digital disruption has to be linked to a civil topic, are necessary conditions for electronic civil disobedience (or hacktivism) to occur.

By delimiting the intension of the concept, the Critical Art Ensembles seeks to limit the extension of electronic civil disobedience. Not every digital or cyber disruption is an event of electronic civil disobedience. Digital assassination (deleting all the data of an individual over the net), even though it can be politically motivated, does not constitute civil electronic disobedience, as it violent (it destroyed data) and, in most cases, targeted a private individual, rather than an institution. Or, if there is disruption over the web, such as a digital sit-in, but it is just done *"for the lulz"*, although it might have been non-violent and even public and transparent, if it does not have a clear political motif, it is unjustified and thus does not correspond as electronic civil disobedience. However, the organisation also recognises that there multiple ways to carry our acts of electronic civil disobedience. What they propose are the general alignments and values that such actions should follow as a necessary condition.

On a small remark about hostility and violent actions, the CAE recognises that unauthorised access to information is a hostile and disruptive action. "Whether private information sources are accessed simply to examine the system, or whether the purpose is to

steal or damage the source, the forces always assume that unauthorised access is an act of extreme hostility and should receive maximum punishment" (CAE, 1996, pg.14). The Critical Art Ensemble identifies that there is a difference between a hostile and a violent action; hostility can be present in electronic civil disobedience as a method to engage with the community, yet violence is never accepted. In fact, violence is designated as a sufficient condition for an activity not to be labeled as electronic civil disobedience. Although the organisation is vocal about its disagreement with current punishments for digital trespassing, they accept that certain consequences are acceptable for their actions. After all, a fundamental argument and necessary condition of civil disobedience, is to abide by the rule of law.

In consequence, the CAE considers necessary, most importantly, that any manifestation on the web needs to be transparent, public and non-violent. For Dominguez (2009), the electronic civil disobedience is a response of a new society, where "the activist reply to this change was to teleport the system of trespass and blockage that was historically anchored to civil disobedience to this new phase of economic flows in the age of network" (pg.1806). Therefore for an act to be considered electronic civil disobedience must happen in the public sphere and has to create commitment with society, which I will further discuss in the case analysis section of Digital Zapatistas and the Electronic Disturbance Theatre.

Now, how does a computer criminal differentiate from an activist pursuing electronic civil disobedience or hacktivism? "While the computer criminal seeks profit from actions that damage an individual, the person involved in electronic resistance only attacks institutions" (CAE, 1996, pg. 17). Furthermore, electronic civil disobedience is a non-violent activity, as it is based in civil disobedience (CAE, 1996, pg. 18), like previously stated.

> As in CD [civil disobedience], the primary tactics in ECD [electronic civil disobedience] are trespass and blockage […] blocking information conduits is analogous to blocking physical locations; however, electronic blockage can cause financial stress, that physical blockage cannot and it can be used beyond the local level. ECD is CD reinvigorated. What CD once was, ECD is now (CAE, 1996, pg. 18).

However, the authors are emphatic in stating that, in the same vain as civil disobedience, where activist should not block essential public services (such as hospitals), cyber activists should not block electronic sites that serve to similar purposes (such as, for example, 911). Furthermore, civil electronic disobedience, should not attack individuals (which is referenced as electronic assassination), the data should not be destroyed or damaged nor should civil digital activists attack personal services (such as personal banking or credit records) (CAE, 1996, pg.19). In consequence, electronic civil disobedience should not seek destruction nor violence as it primary objective.

A case could be made, in order to argue that electronic civil disobedience is conceptual stretching from civil disobedience. Yet, both concept follow the same values, seek the same outcome and impose the same limits to their actions. It is true that electronic civil disobedience might look different from a classical approach to civil disobedience. However, the Critical Art Ensemble have justified their case on why electronic civil disobedience is different in act or aesthetics compared to civil disobedience, but it remains faithful to the spirit of civil disobedience, thanks to the limitations that Dominguez and the ensemble have pointed out. As such, the intension of the concept remains the same, it is just and adjective that has been added to civil disobedience to describe the medium of action.

As a final remark, hacktivism or electronic civil disobedience has a semantic component of resistance (Lane and Dominguez, 2008, pg.136).

> Resistance, says Dominguez - following the major theorists of information warfare - can take one of three forms: physical, which would engage and possibly harm the hardware itself; syntactical (a favourite of hackers), which would involve changing the codes by which the machine functions - programming, software, design; and finally, semantic, which involves engaging and undermining the discursive normal and realities of the systems as a whole (Lane and Dominguez, 2008, pg.136).

To sum up, hacktivism or digital civil disobedience must comply with a list of necessary conditions. These are:

- The motivations must be political, seeking to bring change to a law or policy,

- It must be a non-violent nor destructive in its aim; it can be a hostile action or have unwanted violent consequence, but it can never aim for violence nor seek to destroy data,
- It is a transparent action, where the identities of the organisers, the date and the of action are known and publicly available,
- The action occurs in the public sphere and not in a private space, such as disruption of servers,
- The targets are organisations or institutions and not individuals in particular,
- And the organiser assume the political and legal consequences of the actions.

All the characteristics are necessary elements for hacktivism to be labelled as such. Some of the points can be contested and discussed, such as the transparency characteristic in non-democratic regimes, which should be addressed in further research.

Case studies

As already stated in the methodology sections, three cases where selected to study the difference between hacktivism and cyberterrorism. The cases where selected based on how they were - usually - labeled and their notoriety. Therefore, one key case was selected for analysing hacktivism (the digital Zapatistas and FloodNet), one case for analysing cyberterrorism (Ferizi's actions and trial) and one final case, that was in a grey zone (Operation Payback and Operation Avenge Assange, by Anonymous).

Digital Zapatistas and FloodNet

During the decade of the 1990, Mexico had an ongoing struggle with the modern organisation of the Zapatistas, in the state of Chiapas. The Zapatistas opposed the government economic liberalisation and imposition of neoliberalism ideology in the country and state. "The Zapatistas had already been resisting the Mexican government and the larger global forces of neoliberalism for more than a decade" (Dean, 2016). Throughout the years of struggles, other actors got involved, such as the United State of America or the Electronic Disturbance Theater. In particular, Ricardo Dominguez, founding member of the Critical Art Ensemble, had been following the events and struggle of Zapatistas, praising the use of performance as a tool for activism (Lane and Dominguez, 2003). The Zapatistas "…made

tactical use of embodied - and theatrical - presence, the movement took advantage, from the beginning, of the internet as a means to build a global grassroots support network" (Lane and Dominguez, 2003, pg. 135) with websites supporting the resistance, email distribution lists and participation in forums. For Dominguez, the particular tactic of using media and performance as activism and "revolution", was a legacy from the Mayan culture, that sought dialogue and democracy opposed to the InfoWar and Neoliberalism proposed by the Mexican and United State governments (Lane and Dominguez, 2003, pg.135). As such, Dominguez and other fellow members of the Critical Art Ensemble closely followed the situation in Chiapas.

In 1997, one particular event changed the whole course of the resistance for the Zapatistas and, inadvertently also the future digital civil disobedience. In December of 1997, 45 indigenous people from the state of Chiapas were killed, by a paramilitary group (Dean, 2016; Dominguez, 2009, pg., 1807). After the massacre, Ricardo Dominguez brought together fellow artist and researchers (Stefan Wray, Carmin Karasic and Brett Stalbaum) and founded the Electronic Disturbance Theater (EDT from now on). The EDT was founded not only as a "radicalised" answer to the Chiapas massacre, but also "…as an effort to reconcile CAE's theory of electronic civil disobedience…" (Lane and Dominguez, 2008,pg.135). In the words of Wray (1999), "in early 1998, the Electronic Disturbance Theater also began to experiment with ECD [electronic civil disobedience] possibilities, and they created a software product called FloodNet that would flood or blockade websites" (Wray, 1999, pg.110).

Members of the EDT had previously thought of the use of computers and online political activism, how to use digital and organic bodies to manifest civil disobedience. However, the question about how to conduct it was unanswered, until in the

> online forum The Thing […] urged users to manually load and reload the five websites [associated with Mexican Neoliberalism] as many times a possible in the allotted time. With enough support, their presence could have an effect similar to massive street protest or sin-in at a government building, clogging the server infrastructure of their target in the simples way (Dean, 2016).

And thus the idea of the FloodNet occurred to EDT.

FloodNet was basically, a Java applet designed to push an automated reload request to a specific website, in order to "flood" the server of such website, as a way to simulate a physical sit-in in a digital body (Dominguez, 2009; Dean, 2016; Lane and Dominguez, 2016; Wray, 1999; Denning, 2001). Inspired by the post in The Thing forum, *FloodNet* did the same thing without having to reload the website manually and for several hours. It would also

> request nonexistent pages, with such names as "justice" or "human rights" from the Mexican government site, compelling the server to produce a steady, flashing stream of "404 error-reply" message stating: 'justice not found on this site' and 'human rights not found on this site'. In another iteration, FloodNet filled the site's access log with the name of the people killed by Mexican government troops in an effort to create an on-line memorial to the dead (Lane and Dominguez, 2008, pg.139)

The targets: firstly the Mexican and then the United Stated government. The *FloodNet 1.0* script was launched on April the 10th of 1998 and targeted President Zedillo's website (Dominguez, 2009, pg.1807; Lane and Dominguez, 2008). Every seven second, the script would ask for a reload request in the website and it was estimated than more than 10 thousand people participated in the demonstration (Dominguez, 2009, pg.1807; Denning, 2001). As a consequence, several reports indicated that Zedillo's site stopped responding (Dominguez, 2009, pg.1807; Dean, 2019). The second target was Clinton's White House website, where the reload request was sent every three seconds. However, due to the server being bigger and the website having better resources, Clinton's site was not blocked (Dominguez, 2009; Lane and Dominguez, 2008).

Was then *FloodNet* and the EDT demonstration, an act of electronic digital disobedience or cyberterrorism? Does it fulfil the necessary conditions theorised by CAE, previously identified in this article? It is necessary to remember what CAE has said about electronic civil disobedience: "one, it is a public action; two, it is a non-violent; three, it willingly accepts the condition of 'deliberate unlawfulness and accepting of responsibility'; four, it is always conscientious concerning it is civil nature" (Dominguez, 2008, pg.664)

The idea and purpose of the script was explicitly expressed by the organisers of the demonstration. Dominguez (1999, in Denning 2001) directly says, that the purpose was "… to bring the situation in Chiapas to [the] foreground as often as possible. The gesture created

enough ripples with the Pentagon and the Mexican government that they have had to respond using both online and offline tactics" (pg.266). Upon the massacre and abuse of power by the Mexican and United State officials in the conflict of Chiapas, the EDT considered necessary that some sort of electronic civil disobedience was necessary to bring up the attention of the case. The purpose behind was to give visibility to the governmental oppression of the Chiapas' population, whilst also distributing the message and struggle of Zapatistas. In other words, they used the internet as a theatre to spread Zapatistas' message and try to simulate a sit-in.

The *FloodNet* applet was available to download, to anyone who wanted to participate. The "… applet was hosted on a web page on the servers of The Thing, a kind of ISP for artists and activist. It was embedded in a small frame that bore the image of Mexican President Zedillo…" (Dean, 2016). The call for action in the forums was public for anyone to see, as it called for a specific date to swarm Zedillo's and Clinton's sites in order to allow for an effective disturbance in service. Furthermore, the *FloodNet* applet worked in the public space of the internet, it only automated reload requests (compounding the velocity of these asks to the server as more people got involved), without disturbing its networks (Lane and Dominguez, 2003). It never got involved with the back-end of the website, nor did it directly impact on the servers; also the script acted on websites that everyone can access. Furthermore, it not only used a public space for the demonstration, it politicised that presence in said public space.

As mentioned by Dominguez (2008), in order for an activity to be electronic civil disobedience, it has to be public and transparent about their intention, identities and where and when the demonstration will be taken place. The EDT has always been public about the identity of their members. The "… Electronic Disturbance Theater had little interest in playing the role of a shadowy underground resistance" (Dean, 2016). Moreover, everyone could have been potentially aware of when the attack was going to happen, as it was publicly posted over the internet.

> This is important, because ECD [electronic civil disobedience] is about bringing together real bodies and digital bodies in transparent manner that follows the tradition of civil disobedience - that people are willing to break a law (like blocking the street) to uphold a higher law (Dominguez, 2008, pg. 663)

More importantly, *FloodNet* was not a violent applet nor did it destroy any data or infrastructure.

> … No data was destroyed, no web page altered, and most high-capacity servers didn't even crash - but, just like the daily routines and traffic near a large street demonstration, the usual operation of the system was less functional, slowed and possibly overwhelmed by the public action.(Lane and Dominguez, 2008 , pg.139).

Taking into consideration Rawls' (1971, pg.364, in Scheuerman, 2016, pg.308) key point for civil disobedience -"public, nonviolent and conscientious act contrary to the law" - the *FloodNet* incident and the digital Zapatistas fulfil the checklist. The purpose was clear, it was not violent nor did it end with destruction of any type, it was public and carried out in the public sphere, it was transparent, everyone knew the identities of the authors, the authors assumed any consequences of their actions and they targeted public institutions (not individuals), such as governments.

In addition, one critical aspect of the *FloodNet* situation, was the idea that the demonstration created engagement and empowerment of the people of Chiapas and the Zapatistas. It did not only protest against an injustice - in the eyes of authors - but it also intended the creation of a globalised network of support to the people of Chiapas and the Zapatistas (Lane and Dominguez, 2008). By allowing individual users to enter personals messages while asking the server for inexistent sites, it created an engagement between the user and the demonstration. Users could log/deliver their personal beliefs and ideas of the injustice directly into the institutional server. The digital sit-in was no longer just a sit-in, that would lower the site's speed, but it was also a way of the demonstration to inform the institutions directly about their points of view about what had happened.

Finally, FloodNet not only allowed for people to effectively engage in a virtual sit-in but also allowed to send personalised messages to the institution, many of which extended the protest into the realm of critical media and "tactical poetry" (Dean, 2016)

On the other hand, The Digital Zapatistas and FloodNet do not follow the characteristics of cyberterrorism. Firstly, *FloodNet* did not create an irrational or

disproportionate fear within the civilian population. Moreover, it did not jeopardise anyone's mortality; as it was clear that flooding the website of government was not a life threatening situation. Following the civil disobedience key component, it was of public knowledge when the demonstration was going to occur and thus the surprise factor of terrorism was eliminated.

On the violent or destruction characteristics of cyberterrorism, *FloodNet* did not destroy anything. Although the speed of the sites was affected, this situation was soon reverted once the demonstration ended; in other words, it was the simulation of a sit-in in the digital realm. Moreover, the activity occurred in the public sphere of the internet, there was never a trespass of property (although this is an act permitted by the CAE idea of electronic civil disobedience) and anyone who wanted to participate, could do it by downloading the applet from a forum. As expressed before, the applet even featured an engagement tool for the participants to express their feelings towards the cause.

Ardit Ferizi Case

One of the latest cases of "cyberterrorism" in the media, has been the sentence and conviction of Ardit Ferizi. Media outlets have labeled this case as "the first cyberterrorist sentence" in history, and have highlighted the hacking skills of Ferizi (Harte, 2016; Ngui and Hosenball, 2015; Del Quentin, 2016; *The Guardian* ,2016). Yet, Ferizi's case is not as simple as the media outlets have portrayed it.

Ardit Ferizi is a hacker from Kosovo (Ngui and Hosenball, 2015; Weiner, 2016) who hacked into the servers of a retail company and stole the private identifiable data of approximately 1350 military and civil servants from the United States. Ferizi later handed the data to F. Hussain who (Weiner, 2016; U.S Department of Justice, 2016). By the Department of Justice accounts (2016).

> in the name of the Islamic State Hacking Division (ISHD), posted a tweet that contained a document with the PII of approximately 1,300 U.S. military and other personnel that Ferizi had taken from the victim company and provided to Hussain. The document stated, in part, that "we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting

> confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!"

As such, Ferizi was persecuted by the United States government, under the crime of terrorism and hacking (in specific, for breaking 18 U.S. Code § 2339B and 18 U.S. Code § 1030). Assistant Attorney General for National Security, John Carlin, declared that

> Ardit Ferizi is a terrorist hacker who provided material support to ISIL by stealing the personally identifiable information of U.S. service members and federal employees and providing it to ISIL for use against those employees[…]This case is a first of its kind… "(U.S. Department of Justice, 2015).

Furthermore, Carlin has expressed that this is the first time this kind of activity has presented a "real and dangerous national security cyber threat that results from the combination of terrorism and hacking" (John Carlin in Weiner, 2016). The Attorney General has further implied, that terrorism will now start occurring in the cyber and digital realm, due to the new technologies and social medias available, representing the increasing threat that cyberwarfare and cyberterrorism is (Del Quentin, 2016; Weiner, 2016).

While reading the sentence of the Ferizi case (United States v. Ardit Ferizi), under Section II, Part D, point ii and point iii, has repeatedly highlighted the fact the Ardit Ferizi is a hacker, that this sentence will be the first of it's kind and that cyber security is becoming a pressing topic. To quote

> this case represents the first time someone has been arrested for or convicted of providing material support to a terrorist organisation through information that came from computer hacking. While the defendant will be the first terrorist hacker imprisoned for his actions, he is not the first or only terrorist hacker (Section II, part D, point ii, pg. 14 - 15).

To further stress the point, the Sentencing Memo, alerts of the use of the cyber realm and digital spaces as new tools for organising and and committing terrorism (United States v. Ardit Ferizi). "This is Terrorism 2.0 […] using social media, terrorist groups can now achieve their goals from thousands of miles away, by supplying potential operatives with digital information about who to strike, where to strike, and when to strike" (pg. 15 - 16). Finally, the sentence

defines Ferizi's action as a critical for a terrorist operation success, drawing an analogy between an individual providing weapons to a terrorist organisation and hacking a server.

Ardit Ferizi's action, does not correspond to one of hacktivism or electronic civil disobedience. Based upon the conclusion of what characteristics are necessary for an action to be hacktivism, Ferizi's hacking cannot be labeled as hacktivism. Firstly, the action did not take place in the public sphere of the internet, the man in question carried out his activities, while entering the servers of a private company and accessing private identifiable information. Furthermore, it was not transparent, as he never posted nor stated where and when he was going to carry out the action. Ferizi was not clear with his intentions - thus undermining the idea that electronic civil disobedience abides to a higher intention of law or justice - as he later told in court that " 'I feel so bad that what I did made people scared. I'm so sorry'" (Ardit Ferizi in Weiner, 2016).

However, what is most important, is that this case does not correspond to a case of cyberterrorism either: it is a situation where an individual used his digital/cyber abilities, to help a criminal and insurgent organisation, that on a normal basis resorts to terrorism. Moreover, the United States has their own list for organisations labelled as terrorists this is known as the "designated terrorist organisations" (or DTO) which ISIL is a part of. As such, by law, any person that is affiliated or has helped any of the organisations in the DTO list, is immediately considered a terrorist, even if they have never carried out such violent act themselves.

It would be apparent that the hacker had some political intent behind his actions, which was supporting ISIL and going against the United States. Moreover, the actions did have a malicious intent - as Ferizi knew what he was doing and the possible harm that could be done by using the personal data. Taking Holt's (2012) idea of cyber violence, where, one of the forms for digital violence, would be any action that "that cause emotional harm to individual through online environments […] the second form of violence involved the distribution of materials on line that can be used to cause harm in the real or virtual world" (pg. 339), thus Ferizi's actions were violent. During the trial, "Assistant U.S. Attorney Brandon Van Grack said one woman named on the list has begun fearing all Muslims might attack her." (Weiner, 2016), causing emotional distress to the woman. Furthermore, getting

personal data distributed online, corresponds to the second type of violence that Holt identified. Part of the personal information that Ferizi took (and was later distributed by Hussein) were emails, physical addresses and social media passwords. Therefore, it is possible to conclude that Ferizi's hacking was indeed violent and had a political intent.

Nevertheless, having two necessary conditions does not make the Ferizi case one of cyberterrorism. In the first place, Ferizi's hacking did not destroy any infrastructure nor did it cause grave economic harm nor did it cause great amounts of cyber violence/harm as to spread fear. It did cause emotional distress to some of the individuals directly affected by it, yet the extension of such emotional distress was contained to the individuals affected by the hack. In other words, it did not cause wide-spread fear among the population nor did it generate fear among people who were not affected by the case. Identically, and taking the Critical Art Ensemble position, Ferizi's hacking did not undermine the mortality of those affected; their organic bodies did not suffer any consequence. Then again, a case could be made, that contra-factually, in a possible future someone on the kill list could have been assassinated thus, creating a wider spread fear in the population which could possibly be labelled as terrorism. However, in the case of an assassination with information provided via a digital hack, we would still have to consider this to be "normal" terrorism, and not cyberterrorism as the violent action still happened in real life and not in a digital sphere. In addition, that case should be made against Hussein and not Ferizi.

Another key point, area the means and objectives of a terrorist action. As established in previous sections, cyberterrorism should at least have digital means of action, regardless if the objective is digital or not (in contrast to pure cyberterrorism). In reality, Ferizi's case does have a digital means however, the usage of these digital means were not used to *directly* exert violence. Ferizi got the information to support ISIL, he did not orchestrate an act of terrorism himself. The result of his hacking was information, which was then published by ISIL, that could have - eventually - ended in a possible assassination of one of the individual affected. With this in mind, Ferizi actions are still illegal (hacking a company, to then share the illegal personal information he retrieved) and ethically questionable. Despite this, Ferizi's action resemble more of a supporter, than of one a terrorist. In a simple analogy, if someone stole weapons from a shop, to supply them to an organisation that resorts to terrorism, would that make him/her a terrorist or a thief?

Ferizi's case is what Conway (2004) in Jarvis, Nouri, Whiting, (2014) identifies as situation, where the computer or a cyber component, worked as a facilitator for a "possible" terrorist attack. Certainly, posting a kill list online, that includes the personal information of military personnel and civil servants, is worrisome for any government; moreover if such organisation has a reputation for violence, terrorist acts and homicides. In spite of this, Ferizi did not commit a cyberterrorist offence (neither did Hussein), but an e-crime, that of stealing information. If Ferizi actions are to be labeled as cyberterrorist - for handing illegally obtained information to an insurgent organisation - then hosting a website and spreading propaganda of such organisation, should also be considered cyberterrorism. As a result, if this approach is to be taken, the concept of cyberterrorism would be distorted, as it would no longer require the necessary the conditions previously identified: (1) it is a violent action; (2) that aims for the destruction of infrastructure, or grave economic harm or irrational widespread fear between the civilian population; (3) makes society wonder about their chances of potentially dying (mortality); (4) that has a political motivation; (5) seeks to get as much attention for the attack as possible (using the media as a theatre to spread their ideas and be recognised); (6) while using digital or cyber means to carry out such action, with or without a digital objective. Given these points, Ferizi's actions were not an act of cyberterrorism, but rathe those of a cyber crime.

Operation Avenge Assange

Operation Payback (which also included operation Avenge Assange), was a series of DDoS attacks targeted at various organisation, that happened throughout late 2010 and early 2011. Most of the attacks came from the group called Anonymous.

Anonymous is an internet based organisation, that has no physical association nor clear and defined political alignments. It originated in the 4Chan forums around 2003 and 2008 (Klein, 2015; Mansfield-Devine-Devine, 2011). As Wong and Brown (2013) explain

> The name comes from an online meme […] As such, descriptor of Anonymous lack precision. Anonymous can perhaps best be describes as an Internet meme used by a transient and loosely affiliated collection of hackers, activist, trolls, and troublemaker […] Anonymous has no permanent membership, no hierarchy, or leadership and no clear manifesto outlining its purpose or objectives (pg.1019)

Due to the anarchic nature of Anonymous, the groups does not have a clear set of values nor ideas. Schenieder (2013, pg.13) in Klein (2015, pg. 382) explains that Anonymous is activism and prank; it is the combination of both. It is this combination is what is so attractive to others to join. However, Anonymous themselves have claim that they do effectively pursuit certain values and objectives. As the *Credit Cards Hacked* (2013 in Klein, 2015, pg. 308) public release states "We aren't a group. We're an idea. We're an expression of the anger that every person feels when they see injustice".

Finally, Anonymous as an organisation, is new of its kind, as it lacks structure, leadership or representatives; anyone who self claims to represent Anonymous is not a member, as it has been stated by other members of the organisation. In like matter, anyone who wishes to get involve may do so. This anarchic nature is both and advantage and a weakness, as Mansfield-Devine (2011) noted out. Gaining consensus with no hierarchy, defining future targets or organise a DDoS, proves to be an almost impossible task (Mansfield-Devine, 2011). Additionally, the author considers that there is some kind of leadership, in the sense that not everyone can select the topic of conversation of the channels in the IRC (forums where Anonymous discuss) or some members can make press relapses. In words of Mansfield-Devine (2011) "anarchic mobs do not write press releases" (pg.5), yet this is not the theme of the case study.

Operation Payback (from now on Ops Payback) started in September 2011, as retaliation campaign against institutions that had furthered efforts against anti-privacy and copyright protection (Mansfield-Devine, 2011, pg.4 ; Micali, 2017). Ops Payback was one of the most successful and, at the same time, chaotic operations that Anonymous has carried out (Micali, 2017). It first attacked the company Aiplex and then moved to attack other organisations, including the Recording Industry Association of America (RIAA) (Micali, 2017; Mansfield-Devine, 2011).

In the beginning, Anonymous only targeted institutions related to anti-piracy efforts and copyright protection. However, after Wikileaks published thousand of diplomatic cables and became the target of several governmental operations to shut it down, Anonymous became directly involved in global political affairs. Before the occasion, Anonymous was not

known for political debates, such as freedom of speech, information access or transparency (Mansfield-Devine, 2011, pg.4). As a results of the governmental efforts to bring down Wikileaks - with the cooperation of private companies - Anonymous started the Operation Avenge Assange, as part of Ops Payback (Pras et al, 2010; FBI, 2011; Micali, 2017) .

To understand better the situation, lets take the example of PayPal. After the Wikileaks cables were released, PayPal decided to end the services to Wikileaks. Wikileaks used PayPal as a mean to receive donations. "Citing violations of the PayPal terms of service, and in response to WikiLeaks' release of the classified cables, PayPal suspended Wikileaks' accounts so that Wikileaks could no longer receive donations via PayPal" (FBI, 2011). This situation was considered by Anonymous as an act of censorship against freedom of speech and information. Consequently, the group decided that actions should take place, as a form of protest. Thus, through different communication channels - such as Twitter and websites - Anonymous called for protest, in particular, for DDoS attacks (Pras et al, 2010). The main medium for coordination were particular IRCs (Internet Relay Chats), that were used for Ops Payback, in specific the chat named #operationpayback (Micali, 2017, pg. 241). Anyone was invited to manifest their discontent.

Through the IRC chat, Anonymous and those interested, discussed which companies to target, the reason, the date and time of the DDoS attack. The software of preference was LOIC (standing for Low Orbit Ion Canon), which produces a simple DDoS. (Mansfield-Devine, 2011; Micali, 2017). As expressed by Mansfield-Devine (2011),

> LOIC come in two main forms - a Window executable that Anon download and run from their own machines; and a Javascript-based versions (JS-LOIC) designed to be integrated into a web page and there usable by anyone who visits the site… LOIC sent repeated messages containing a string defined by the user to the target machine, opening several connections. With TCP and UDP attacks, the packed sent consist of just the plain text of the message: in HTTP attack, the string is included in a GET request. The Javascript variant only uses HTPP but attempts to make the attack more effective by including random numbers in the URLs it generates, in an effort to prevent caching (pg.5)

It is a simple tool, that anyone can download and use. In the automatic mode, the user enter the IRC server, where the software gets the information of the target (such as the URL and port). On the other side, in the manual mode, the user manually inputs the information, such as the url, IP, attack type, among others. Then, the user then selects *IMMA CHARGIN MAH LAZER* to execute the attack. An example of the user interface can be seen in the image 1.

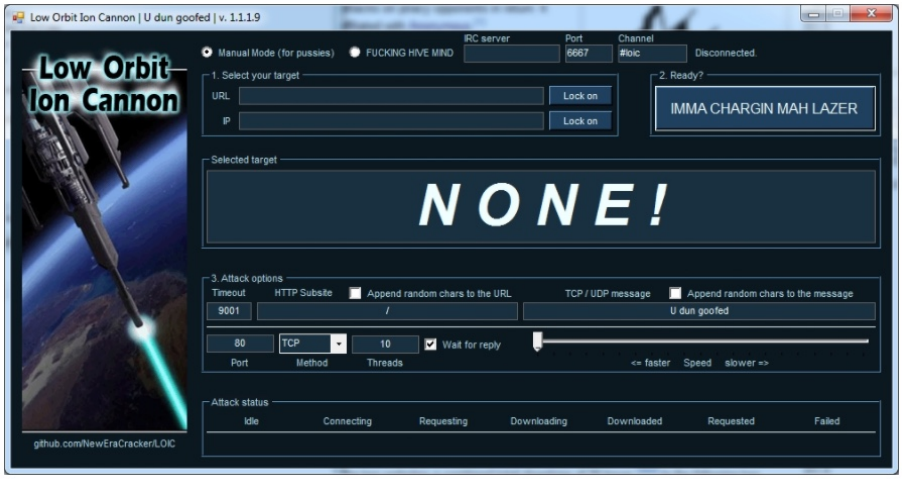

Image 1 - LOIC interface (Panda Security, 2010)

Operation Avenge Assange lasted for almost, 9 days at its peak. Although the operation continued until January of 2011, the highest number of participant was reached between December 4th of 2010 and December 13th of 2010. Based on the report of Panda Security (2010) some of the sites affected with DDoS (and that where effectively disrupted), where PayPal's blog and PayPal's site (which, combined, were down for more than 9 hours), the Swiss bank PostFinance (that was down 33 hours), Senator Liberman Senate website (which was down for a couple of minutes), Aklagare - the Swedish prosecutor's site, that was persecuting Assange - site (that was down for 13 hours), Mastercard's and Visa's sites (both of them where down more than 12 hours), among others. The selection of target was based on

Image 2 - Operation Payback poster(Panda Security, 2010)

what was discussed in the IRC chat (or so is claimed) and how they had impacted Julian Assange and Wikileaks. At the same time, Facebook and Twitter where deleting the official accounts of Anonymous, through which the organisation was announcing their upcoming attacks, as seen in image 2. As a results, other official and unofficial Anonymous accounts appeared.

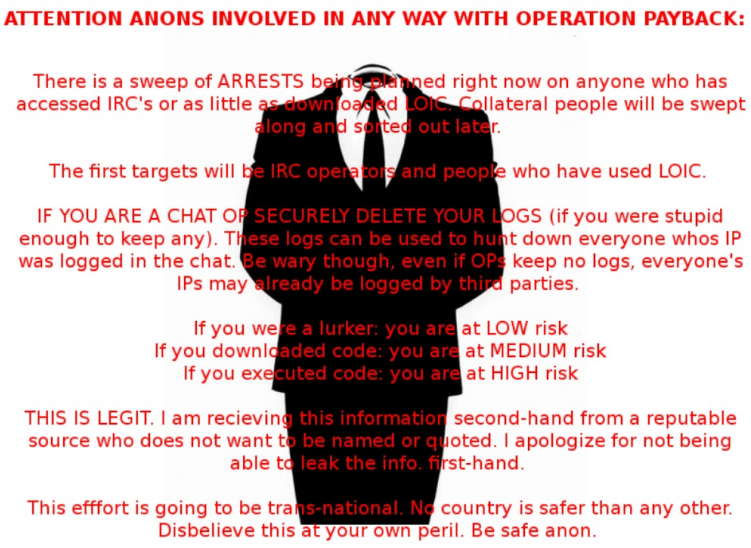

Image 3 - Anonymous press release to stop Ops Payback (Panda Security, 2010)

The series of attacks stopped when some of the users involved got arrested. As reported by Panda Security (2010), it was announced the 13th of December that a second arrest linked to Ops Payback had occurred in the Netherlands. For this reason, an image started circulating around the internet to end all activity related to Ops Payback, as seen in image 3 (Panda Security, 2010).

Where Anonymous action a demonstration of hacktivism? The group intentions where made public through different channels on the internet, as seen in image 4. "Anonymous was motivated by a sense of injustice,156 and these anonymous, disembodied attacks had real-world consequences for those who were hacked." (Wong and Brown, 2013, pg.1023). Furthermore, and as seen in image 4, the organisation explicitly manifested their "core" values: transparency, freedom, democracy and anti-censorship. In that sense, the case fulfils the first condition of hacktivism.

Second, the attack was publicly available through Twitter, Anonymous website and other parts of the internet. After all, it was necessary to have as much people participate in the DDoS as possible, to effectively disrupt the sites. For this reason, it should not be considered a cyberterrorist attack, as the surprise element is not present. Likewise, the objective of the Anonymous is not to terrorise civilians (Wong and Brown, 2013, pg.1016) and the targets are institutions, not individuals. The objective were not civilians.

> ***"While we don't have much of an affiliation with WikiLeaks, we fight for the same: we want transparency (in our case in copyright) and we counter censorship. The attempts to silence WikiLeaks are long strides closer to a world where we can not say what we think and not express how we feel. We can not let this happen, that is why we will find out who is attacking WikiLeaks and with that find out who tries to control our world. What we are going to do when we found them? Except for the usual DDoSing, word will be spread that whoever tries to silence or discourage WikiLeaks, favors world domination rather than freedom and democracy."***

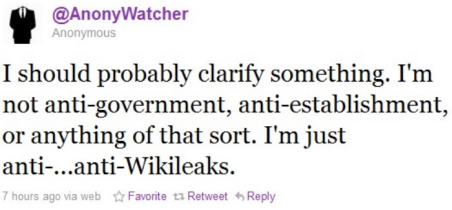

Image 4 - Anonymous support for Wikileaks (Panda Security, 2010)

Another key point, is that in Ops Payback and Operation Avenge Assange, data/information was not deleted. In these particular set of attacks, no data was stolen. However, it was reported that PayPal did suffer an economic loss; PayPal reported that the Anonymous attack cause them approximately 3.5 million pounds in losses (Laville, 2012). Because of this, it seems unreasonable to blatantly say that Ops Payback and Operation Avenge Assange were not violent. If the operation were to be considered violent, then as exposed in the hacktivism section of the thesis, it should not be considered hacktivism. Electronic Civil Disobedience allows certain hostility as a method of protest, yet not violence.

Above all, what is most important about Ops Payback is the transparency of the identities of those involved. All the actions taken were against companies that operate in democracy. Thus concealing the identity was not necessary to carry out electronic civil disobedience. As stated in previous sections, civil disobedience is a fundamental value in western democracies. With this in mind, it should no be a concern for Anonymous to be transparent and open about their identities. Electronic civil disobedience (and hacktivism) implies that activist are breaking the law for a higher value, yet they accept the consequences of their actions. As Dominguez has expressed, "it willingly accepts the condition of 'deliberate unlawfulness and accepting of responsibility' " (Dominguez, 2008, pg.664). However, Anonymous actions and information available show that this is not the case for the organisation.

On of the FAQ of the LOIC program, where was a section concerning the possibility of having the identity leaked through the deployment of the script. For example, Pras et al (2010, pg. 8) share one of the question.

"Q: 'Will I get caught/arrested for using it?'
A: Chances are next to zero. Just blame you have a virus, or simply deny any knowledge of it"

Furthermore, there was a great deal of discussion about how to keep the identity safe while deploying the LOIC script, so users would not get arrested (Mansfield-Devine, 2011; Wong and Brown 2013; Pras et al, 2010). The general consents was that users engaging in the DDoS attack did not want their identities to be revealed.

In reality, the identities of the attackers were known by companies. The LOIC software did not conceal the IP address of the computer launching the software. Thus, when the attack was deployed, the firm's databases will have logged the IP addresses from where the requests were coming (Mansfield-Devine, 2011, pg.6). What is more troublesome, is that probably "the majority of Anonymous have no idea that this is the case" (Mansfield-Devine, 2011, pg.6)

Although, at the end of the attack, the identity of the activists were not conceal, this was an unforeseen consequence. For this reason, it should no be considered as a transparent manifestation; users were worried about getting "caught" for this disobedience, and Anonymous released a mandate to stop actions related to Ops Payback when activist started getting arrested (see image 3).

All things considered, it seems that Anonymous did not wanted to be transparent about their identities and were not willing to accept the responsibility for their efforts. As what was been theorised by CAE about electronic digital disobedience, it is a key and necessary characteristic to be transparent about the identities of the organiser and accept legal responsibilities. It is the case that, from the messages exposed by Anonymous, they were not willing to accept this. Given these points, Operation Payback and Avenge Assange cannot be considered hacktivism.

Then, what is Operation Payback and Avenge Assange? From the research done here, the conclusion is that it is inconclusive, it is neither cyberterrorism nor hacktivism. Further

research should be done on topic of activism and disruption over the net. The particular hierarchy and method of operation of Anonymous does not resemble any other group from the physical world. Hence, new theorisation and research should be carried out in regards on disruption over the net, understanding that it is different from cyberterrorism or any other classical conceptualisation of disruption and activism. New concepts should be produced to describe and understand new phenomena over net.

Conclusions

Hacktivism is a different from cyberterrorism, although they might share common elements. Both are political motivated activities, however they respond to different motivations. Cyberterrorism is a hypothetical situation, that seeks destruction, grave economical harm or irruption of widespread fear in the population. It works through cyber means, although it might not have cyber objectives and uses the element of surprise as a tool to further impact society.

On the other hand, hacktivism is a form of civil disobedience, adapted to the cyber realm. Hacktivism must neither aim for a violent nor destructive outcome (though this can be an unforeseen and unwanted consequence of civil disobedience). In spite of its non-violent characteristics, hacktivism can still be a hostile activity. One of the key features of hacktivism, is that it is an action that occurs in the public sphere, it targets institutions or organisations whilst refraining of targeting individuals. Equally important is the idea that hacktivism is transparent with the identities of the organisers, the date, place and time of the demonstration; and their organisers assume the legal and political consequences of their actions.

Up to date, no cyberterrorist attack - as defined in this research - has occurred. Nevertheless there has been a growing fear between the general population for this kind of situation, due to the increasing interconnectivity of society, in particular since the irruption of the Internet of Things (IoT). As such, a possible research path would be to study the vulnerability and security risks that the Internet of Things poses in regards to potential cyberterrorist attacks.

Through the Operation Payback case analysis, it was concluded that it seems unreasonable to label the discussed set of actions as hacktivism, in spite of their lack of transparency. Moreover, Anonymous cellular-like hierarchy and organisation, makes it troublesome to compare with classical terrorist or civil disobedience organisations. Further research should be done to describe and analyse new organisations on the internet, coining new terms to describe the new phenomena encountered. Conjunction of words, such as hacking and activism, seem to lack the ability to properly describe new phenomena, such as Anonymous. In the long term, better and more robust theorisations regarding the impact of the internet in society is needed.

In conclusion, hacktivism and cyberterrorism, are different activities. They respond to different stimuli and they do not have the same consequences. A better understanding of both terms is needed by further analysing their differences.

Abbreviations

- CAE = Critical Art Ensemble
- EDT = Electronic Disturbance Theater
- ECD = Electronic civil disobedience
- Ops Payback = Operation Payback
- Ops = Operation

Bibliography

1. Ahram, A., (2013) *Concepts and Measurement in Multimethod Research.*: Political Research Quarterly, 66(2), pp. 280-291
2. Assange, J. (2006). *The Curious Origins of Political Hacktivism*. Retrieved March 2018 from https://www.counterpunch.org/2006/11/25/the-curious-origins-of-political-hacktivism/
3. Barnard-Wills, D.(2011). *This is not Cyber war, its a…? Wikileaks, Anonymous and the Politics of Hegemony*. European Conference on Cyber Warfare and Security. 17-23. DOI: 10.4018/ijcwt.2011010102
4. Braumoeller, B. F., & Goertz, G. (2000). *The Methodology of Necessary Conditions*. American Journal of Political Science, 44(4), 844. doi:10.2307/2669285
5. Brennan, A.A. (1997). *Logical Form*. In Lamarque, P. V., & Asher, R. E. (ed). Concise Encyclopaedia of philosophy of language. Exeter: Pergamon, pp. 280 - 281.
6. Brennan, A. (2017), *Necessary and Sufficient Conditions.* In Edward N. Zalta (ed.), The Stanford Encyclopaedia of Philosophy, Retrieved January 18, 2018 https://plato.stanford.edu/archives/sum2017/entries/necessary-sufficient.
7. Collier, D., & Mahon, J. E. (1993). Conceptual "Stretching" Revisited: Adapting Categories in Comparative Analysis. *American Political Science Review, 87*(04), 845-855. doi:10.2307/2938818
8. Conway, M. (2003) *Terrorism and IT: cyberterrorism and terrorist organisations online.* In: Howard, Russell D. and Sawyer, Reid L., (eds.) Terrorism and counterterrorism: understanding the new security environment, readings and interpretations. McGraw-Hill, United States, pp. 271-288. ISBN 9780072873016
9. Critical Art Ensemble (1996). Chapter 1 - Electronic Civil Disobedience. E*lectronic Civil Disobedience & Other Unpopular Ideas*. Autonomedia. pp.7-32
10. Critical Art Ensemble (2001). Chapter 2 - The Mythology of Terrorism on the Net. *Digital Resistance: Exploration in Tactical Media*. Autonomedia . pp29-37
11. CultofTheDeadCow. (no date). *About - Who We Be.* Retrieved February 2018 from http://w3.cultdeadcow.com/cms/about.html
12. Dean, A. (2016) *Tactical Poetics; FloodNet's Virtual Sit-ins*. Retrieved February 2018 from http://rhizome.org/editorial/2016/dec/01/tactical-poetics-floodnets-early-1990s-virtual-sit-ins/
13. Debrix, F. (2001). *Cyberterror and Media-Induced Fears: The Production of Emergency Culture.* Strategies: Journal of Theory, Culture & Politics, 14(1), 149-168. doi:10.1080/10402130120042415
14. Del Quentin, W. (2016). *Hacker from Kosovo who aided Islamic State is sentenced to 20 years in U.S. prison* .Retrieved April 2018 from http://www.latimes.com/nation/la-na-hacker-islamic-state-20160923-snap-story.html
15. Denning, D. (2001). *Activism, Hacktivism and Cyberterrorism: The internet as a tool for influencing foreign policy.* In Networks and Networks - The Future of Terror, Crime and Militancy, Arquilla J, Ronfeldt, D (Ed.) Rand Corporation.

16. Department of Justice - Office of Public Affairs (2016, June 15). *ISIL-Linked Hacker Pleads Guilty to Providing Material Support* [Press Release]. Retrieved April 2018 from https://www.justice.gov/opa/pr/isil-linked-hacker-pleads-guilty-providing-material-support

17. Department of Justice - Office of Public Affairs (2015, October 15). *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges*[Press Release]. Retrieved April 2018 from https://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges

18. Devost, M. G., Houghton, B. K., & Pollard, N. A. (1997). *Information terrorism: Political violence in the information age*. Terrorism and Political Violence, 9(1), 72-83. doi:10.1080/09546559708427387

19. Desouza, KC. Hensgen T (2003). *Semiote emergent framework to address the reality of cyberterrorism.* Technology Forecast Soc Change 70(4):385-396

20. Drescher, G. L. (1991). *Made-up minds: A constructivist approach to artificial intelligence*. Cambridge, Mass: MIT Press, pp. 87-90.

21. Dominguez, R (2008). *Electronic Civil Disobedience Post-9/11*.Third Text 22(5), 661 - 670 doe: 10.1080/09528820802442454

22. Dominguez, R (2009) *Electronic civil Disobedience: Inventing the Future of Online Agitprop Theater* . PMLA 124(5), pp.1806-1812

23. Dul, J. (2015). Necessary Condition Analysis (NCA). *Organisational Research Methods, 19*(1), 10-52. doi: 10.1177/1094428115584005

24. Dul, J. (2015). Necessary Condition Analysis (NCA): Logic and Methodology of Necessary But Not Sufficient Causality. *SSRN Electronic Journal, 19*(1), 10-52. doi:10.2139/ssrn.2588480

25. The Editors of Encyclopaedia Britannica (2018). *Intension and Extension.* Retrieved in January 2018 from Encyclopaedia Britannica from https://www.britannica.com/topic/intension

26. Embar-Seddon, A. (2002). *Cyberterrorism*. American Behavioural Scientist, 45(6), 1033-1043. doi: 10.1177/0002764202045006007

27. Federal Bureau of Investigation - The FBI (2011, July 9). *Sixteen Individual Arrested in the United States for Alleged Roles in Cyber Attacks* [Press Release], retrieved from https://archives.fbi.gov/archives/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks

28. Goertz, G. (2006). *Social science concepts: A users guide*. Princeton, NJ: Princeton University Press.

29. Goertz, G., & Mazur, A. G. (n.d.). Mapping gender and politics concepts: Ten guidelines. *Politics, Gender, and Concepts,* 14-44. doi:10.1017/cbo9780511755910.002

30. Goertz, G., & Starr, H. (2003). Chapter 4 - The Substantive Importance of Necessary Condition. *Necessary conditions: Theory, methodology, and application*s. Lanham: Rowman & Littlefield, pp. 65-75

31. Gordon, S., Ford, R (2003) *Cyberterrorism?*. Symantec Security Response, pp. 1-16

32. Guardian, The (2016). *Hacker who gave Isis 'hitlist' of US targets jailed for 20 years.* Published in The Guardian. Retrieved April 2018 from https://www.theguardian.com/world/2016/sep/24/hacker-who-gave-isis-hitlist-of-us-targets-jailed-for-20-years

33. Harte, J. (2016). *Islamic State-linked hacker makes first U.S. appearance in federal court*. Retrieved April 2018 from https://uk.reuters.com/article/us-usa-justice-hacker/islamic-state-linked-hacker-makes-first-u-s-appearance-in-federal-court-idUKKCN0V602C

34. Holt, T. J. (2012). *Exploring the Intersections of Technology, Crime, and Terror*. Terrorism and Political Violence, 24(2), pp. 337-354. doi:10.1080/09546553.2011.648350

35. Jarvis, L., MacDonald, S. (2014). *What Is Cyberterrorism? Findings From a Survey of Researchers*. Terrorism and Political Violence, 27(4), 657-678. doi:10.1080/09546553.2013.847827

36. Jarvis L., Nouri L., Whiting A. (2014) *Understanding, Locating and Constructing Cyberterrorism.* In: Chen T., Jarvis L., MacDonald S. (Eds) Cyberterrorism. Springer, New York, NY, pp. 25 - 40

37. Lane J., and Dominguez, R. (2003) *Digital Zapatistas.* The Drama Review 47(2), pp.129-144.

38. Lau, J., Chan, J. (2018) *[M06] Necessity and sufficiency*. Retrieved January 18, 2018, from http://philosophy.hku.hk/think/meaning/nsc.php

39. Laville, S (2012). *Anonymous cyber-attacks cost PayPal £3.5m, court told.* Published in The Guardian, retrieved April 2018 from https://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court

40. Mansfield-Devine, S. (2011). *Anonymous: serious threat or mere annoyance?.* Network Security, 1, 4–10. doi: 10.1016/S1353-4858(11)70004-6

41. McCormick, TY. (2013). *Hacktivism: A Short History*. Retrieved March 2018 from http://foreignpolicy.com/2013/04/29/hacktivism-a-short-history/

42. Micali, A (2017). *Towards a nonlinear, material history of digital swarms.* Internet Histories, 1(3), 238-257, doi: 10.1080/24701475.2017.1344051

43. North Atlantic Treaty. (no date). *New threats: the cyber-dimension* . Retrieved March 2018 from https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm

44. Ngui Y. Hosenball, M. (2015). *Malaysia arrests hacker for supplying U.S. targets to Islamic State*. Retrieved from https://www.reuters.com/article/us-malaysia-islamic-state/malaysia-arrests-hacker-for-supplying-u-s-targets-to-islamic-state-idUSKCN0SA05R20151016

45. Panda Security (2010). *'Tis the Season of DDoS - Wikileaks Edition*. Retrieved April 2018 from https://www.pandasecurity.com/mediacenter/news/tis-the-season-of-ddos-wikileaks-editio/

46. Pras, A. Sperotto, A. Giovane, C. Moura, M, Drago, I. Barbosa, R. Sadre, R. Schmidt, R and Hofstede, R(2010). *Attacks by "Anonymous" WikiLeaks Proponent not Anonymous.* Retrieved April 2018 from https://research.utwente.nl/files/5095223/2010-12-CTIT-TR.pdf

47. Pollitt, M. (1998). *Cyberterrorism — fact or fancy?* Computer Fraud & Security, p.8-10.

48. Kenney, M. (2015). *Cyber-Terrorism in a Post-Stuxnet World*. Orbis, 59(1), 111-128. doi:10.1016/j.orbis.2014.11.009

49. Klein, A (2015). *Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press.* Communication Monographs, 82(3), 379-401, doi: 10.1080/03637751.2015.1030682

50. Rawls, J. (1969). The Justification of Civil Disobedience. In Hugo Adam Bedau, ed., *Civil Disobedience: Theory and Practice*, pp. 240–55. New York: Pegasus Books.

51. Sartori, G. (1970). *Concept Misinformation in Comparative Politics*. The American Political Science Review, 64(4), 1033-1053.

52. Scheuerman, W. (2016). *Digital disobedience and the law.* New Political Science 38(3) pp.299-314.

53. Schwartz, S. (2016). *U.S. Sentences Kosovar Albanian ISIS Hacker Ardit Ferizi to 20 Years in Prison.* Retrieve April 2018 from https://www.weeklystandard.com/stephen-schwartz/us-sentences-kosovar-albanian-isis-hacker-ardit-ferizi-to-20-years-in-prison

54. Texas State University. (no date). *Confusion of Necessary with a Sufficient Condition*. Retrieved February 2018 from http://www.txstate.edu/philosophy/resources/fallacy-definitions/Confusion-of-Necessary.html

55. Travis, C. (1997). *Family Resemblance*. In Lamarque, P. V., & Asher, R. E. (1997). Concise encyclopaedia of philosophy of language. Exeter: Pergamon, pp. 113 - 116.

56. United State v. Ardit Ferizi a/k/a "Th3Dir3torY", Sentencing Hearing: Sept. 23, 2016

57. Vegh, S. (2002). *Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking*. First Monday 7(10). [Online]Retrieved January 8, 2018, from http://firstmonday.org/article/view/998/919

58. Weiner, R (2016). *Hacker who sent 'kill list' of U.S. military personnel to ISIS: 'I feel so bad'*. Published in The Washington Post. Retrieved April 2018 from https://www.washingtonpost.com/local/public-safety/hacker-who-sent-kill-list-of-us-military-personnel-to-islamic-state-i-feel-so-bad/2016/09/23/dc0ba0ea-8196-11e6-b002-307601806392_story.html?noredirect=on&utm_term=.11ab72a2ed46

59. Weird Staff. (2004). *Hacktivism and how it got here*. Retrieved March 2018 from https://www.wired.com/2004/07/hacktivism-and-how-it-got-here/

60. Wray, S. (1999). *On Electronic Civil Disobedience*. Peace Review 11(1), pp. 107-111, doi: 10.1080/10402659908426237

61. Wong, W., Brown, a. (2013). *E-bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One*. Perspectives on Politics 11(4), p. 1015 - 1033.

62. 18 U.S. Code § 1030 - Fraud and related activity in connection with computers

63. 18 U.S. Code § 2339B - Providing material support or resources to designated foreign terrorist organisations 62.