THE "ANONYMOUS" MOVEMENT: HACKTIVISM AS AN EMERGING FORM OF

POLITICAL PARTICIPATION

by

Galina Mikhaylova, M.S.

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Arts
with a Major in Sociology
December 2014

Committee Members:

    Nathan Pino, Chair

    Patti Giuffre

    Mina S. Guirguis

**FAIR USE AND AUTHOR'S PERMISSION STATEMENT**

**Fair Use**

This work is protected by the Copyright Laws of the United States (Public Law 94-553, section 107). Consistent with fair use as defined in the Copyright Laws, brief quotations from this material are allowed with proper acknowledgement. Use of this material for financial gain without the author's express written permission is not allowed.

**Duplication Permission**

## ACKNOWLEDGEMENTS

**TABLE OF CONTENTS**

**Page**

CHAPTER

# LIST OF TABLES

# LIST OF FIGURES

## ABSTRACT

This thesis focuses on the phenomenon of hacktivism, and specifically the hacktivist collective known as *Anonymous*. Hacktivists can be defined as politically motivated hackers. Hacktivists are different from other types of hackers because their motivations are driven by the pursuit of social change, as opposed to seeking profit or intellectual pursuit. Hacktivism is a new controversial form of civic participation, which will most likely continue to have an impact on the Internet and the world. A lack of detailed sociological research on hacktivists serves as the rationale for this study.

This study specifically focused on the experiences of the hacktivist community in the United States, known under the name of *Anonymous*. This thesis focused on, but is not limited to: a) examining how members of *Anonymous* define themselves, as well as how security professionals (a.k.a. ethical hackers) define or view hacktivists; b) how hacktivists operate and/or organize; and c) examining hacktivist culture and ethical stances (including whether hacktivism can be considered permissible or ethical). My research employed two primary strategies: content analysis of the *Anonymous* message boards and in-depth interviews with security professionals. The two approaches were meant to be complimentary: while the content analysis draws a picture of how members of *Anonymous* see themselves and their goals; the interviews were meant to draw the picture of how others view or understand hacktivists.

# I. INTRODUCTION

Hacktivists, or politically motivated hackers, are different from other types of hackers because their motivations are driven by the pursuit of social change, versus seeking profit or intellectual pursuit). Hacktivism is a relatively new, but already well-established, controversial form of civic participation, which will most likely continue to have an impact on the Internet and the world. Wray (1998) suggests that hacktivism is "likely to continue to gain attention" and "will evolve in response to changing global economic and political conditions" (Wray 1998:12).

Although, a number of scholars have written about hacktivism in the past decade, a scientific explanation for the behavior is almost non-existent. A thorough sociological study of these individuals is needed in order to explain such an important social phenomenon, and a lack of detailed research serves as the rationale for this study. In order to grasp the hacktivist community and culture fully, it is important to study the community in two broad ways: on the one hand, it is important to examine hacktivists' self-conceptualization (i.e., how the community views itself, as well as their goals and roles in society); on the other hand, it is important to study hacktivists from the standpoint of others (i.e., the media, government, other scholars, etc.). This study implements both approaches. In Part 1 (content analysis), I describe the results of a content analysis of hacktivist message boards. Such analysis provides insight into how the hacktivists collective *Anonymous* sees their roles and goals, as well as the culture, values and beliefs with which members of the group identify. The second part of my research deals with the 'insight of others,' namely the insights of security professionals from a major security firm, into the hacktivist collective. The interviews' analysis is

aimed at uncovering how security professionals conceptualize and define hacktivists. The

combination of these two research approaches, the content analysis and interviews, is

helpful at drawing a more detailed and diverse picture of the hacktivist community.

## Research Questions

I formulated my research questions in the following way: a) How do *Anonymous'*

members identify/view themselves? What are their incentives for joining the group? 2)

How does *Anonymous* function as a group? What are their major goals and aims? 3)

What is the structure of the group (i.e. hierarchy, chain of command, etc.)? What are the

ways of recruiting members, if such exist? 4) How do group's members (if they do) deal

with the risks associated with *Anonymous'* activities? How often does hacktivism take

place, are many members of *Anonymous* involved in hacktivism or hacktivism-related

activities?

## II. LITERATURE REVIEW

## Hacktivism: The Background

### The Evolution of the Hacker Community: From Hacking to Hacktivism

Hacktivism, put simply, stands for "politically motivated hacking" (Jordan 2002). The term represents a blend of two terms: "hacking" and "activism." According to Taylor (2001) and Conway (2003), hacktivists represent a newer generation of hackers, which emerged in the mid-1990s. Before hacktivists, there were: a) "true" hackers, or the computer pioneers of the 1950s and 1960s, who 'toyed' with the capabilities of computers at MIT and other American universities; b) 'hardware hackers,' or the computer innovators of the 1970s; c) a generation of 'crackers' of the 1980s, also known as hackers who exploited systems for malicious purposes; d) 'microserfs,' also known as programmers of the 1990s who exhibited different "aspects of the hacker subculture" (p.2), while simultaneously subscribing to the corporate culture of companies like Microsoft. Hacktivism was shaped in an intellectual climate surrounded by the impacts of globalization (Taylor 2001). While previous generations of hackers were manifestations of a celebration of technology, hacktivists are different from previous generations of hackers in that hacktivism is primarily celebrating human agency (Taylor 2005). The significance of hacktivism is seen in its unique methods, which "seek to imaginatively ally technology-based techniques with traditional and indigenous cultural resources" (Taylor 2005:644).

### Hacktivist Ethics & the 'Villainification' of Hacktivists

Hacktivist ethics are closely intertwined with the original hacker ethics. The term 'hacker ethics' was first coined by the journalist Steve Levy in his 1984 book "Hackers: Heroes

of the Computer Revolution". Levy described hacker ethics as consisting of the following basic principles: 1) everyone should have unlimited and unrestricted access to computers; 2) information wants to be free and, therefore, must be free; 3) one should mistrust any type of authority, and promote decentralization; 4) hackers are to be judged by their technical abilities, instead of "bogus criteria, such as degrees, age, race, or position" (Fitri 2011:6); 5) hackers' activities on computers should be considered acts of art and beauty; and 6) computers are thought of as positive phenomenon, which can change one's life for the better (Manion and Goodrum 2000; Fitri 2011). The hacker community has always opposed private ownership and/or censorship of information, as evident from the aforementioned hacker ethic. They viewed every technology as having two conflicting possibilities: technology can be either dominated or emancipated. Hackers saw themselves as emancipators of technology. Full democratization of technology, in other words, was the major ideology of the hacker community.

Hacktivists share many, if not all, of the principles of the original hacker ethic. Both hacker and hacktivist ethics are libertarian and anarchist in nature: their ethics puts them "on a collision course with the commercial-industrial complex who wish to own and control the Internet" (Manion and Goodrum 2000:18). Hacktivists can thus be conceptualized as opponents of the power elite, which, in turn, seeks to use technology to promote its own agendas. It is no surprise, then, that hacktivists have been portrayed by the state and the media as villains and threats to society. Since most hacktivists' acts are committed against government and corporate powers, hacktivism has quickly become equated with cyber terrorism. However, hacktivists themselves openly condemn cyber terrorism. Some scholars (Manion and Goodrum 2000) state that hacktivists are indeed

4

different from cyber terrorists: while cyber terrorists use technology (including the Internet) to commit terrorists acts, hacktivists act more in agreement with civil disobedience than with terrorism.

An act of civil disobedience is based on the following principles: a) one should not commit damage to people or property; b) one's actions should be non-violent; c) one should not seek personal profit; d) one should have a strong ethical motivation for committing an act of civil disobedience; and e) one should be willing to take personal responsibility for his/her actions (Manion and Goodrum 2000). Hacktivism is somewhat, although not fully, consistent with the philosophy of civil disobedience, especially in its stances on ethics and violence. It is important, then, to distinguish hacktivism from cyber terrorism (which uses violent methods) or cyber criminals (who seek profit or personal gain). Even though all three use technology as a tool to achieve their goals, their motivations are quite different. Fitri (2011) suggests another comparison that illustrates these differences very clearly: while cyber terrorism aims at destruction, hacktivism is aimed at disruption.

### *The Culture of Hacktivism*

Peer-reviewed literature identifies the following basic components of hacktivist culture: conspiracy theorizing, obsession with privacy and secrecy, membership fluidity, anarchic heritage and anti-capitalist sentiment, and the culture of humor and creativity.

Krapp (2005) points out that conspiracy theorizing represents a part of Internet culture, and, therefore, also a part of hacktivist culture, since hacktivism is closely tied to communication online. The author suggests that conspiracy theorizing represents "the native mode of thinking online," (Krapp 2005:76), or a mode of theorizing about politics and history. Conspiracy thinking allows Internet users, and hacktivists, to take "refuge in

the comforting thought that something important always remains hidden" (Krapp 2005:77). Conspiracy theories provide Internet users with alternative ways to visualize politics or history, especially in cases when official versions appear incomplete or biased.

Secrecy and anonymity represent another important part of online interaction, which is also evident in hacktivist culture. Gillen (2012) states that the culture of the Internet is historically rooted in relative anonymity for users; it is not surprising, then, that privacy and anonymity represents an important issue for both hackers and hacktivists. Wray (1998) concurs by stating that politicized hackers have a very distinct style of organization; politicized hacks are characterized by being "secret, private, low key, and anonymous" (p. 7) in nature. Jordan and Taylor (1998), in his sociological study of hackers, also points out that anonymity (i.e., the secrecy of a hacker's identity offline) represents an integral component of the hacker community. The numerous online identities and pseudonyms hackers (and hacktivists) may use online are used with the purpose of masking the 'true' identity of a hacker in real life. Secrecy of a hacker's true identity has always been crucial for hacker and hacktivist communities, as hacking represents an illegal activity that is heavily scrutinized by the state.

Another crucial component of the hacker community, which is tightly related to the hacktivist community, is the culture of membership fluidity. The fluidity of the hacker community is characterized by the fast rate at which membership changes and evolves (Jordan and Taylor 1998). Many social movements share characteristics of being informal networks rather than formal organizations. Both the hacker and hacktivist communities have highly permeable boundaries: their communities have no formal ceremonies or rituals, or ruling bodies. It comes as no surprise, then, that "the informal

and networked nature of the hacking community, combined with its illicit and sometimes obsessional nature means that a high turnover of hackers occurs" (p. 766). Even though both hacker and hacktivist communities may express a desire to organize formally, high pressures from law enforcement typically prevents such formal organization. The hacker community, for example, may fear that a formal organization of hackers might eventually attract too much attention and lead to the capture of members (Jordan and Taylor 1998). Thus, hacker and hacktivist communities often have an overall loose structure and represent an informal community. Jordan (2002) claims that hacktivist communities may lack the solidarity that is typically present among demonstrators in mass street protests. In other words, it may be much harder for hacktivists to build solidarity due to the fact that they do not see one another and have limited personal contact:

> "There are no passers-by in cyber space. Whereas a street demonstration will reach whoever happens to be in the vicinity – protesters and passers-by – and whoever watches media reporting, no such chance encounters will occur in cyberspace. No might solidarity be built, as each protester will not know how many others are participating at the same time" (p. 125).

Another aspect that characterizes hacktivist culture is the anarchic heritage of hacktivists. Hackers were the founding fathers of the internet; they laid down the foundations of political protest in cyber space, based on their ethical commitment to anti-censorship and freedom of information, as well as based on their technological capabilities. This left hacktivists with "something of an anarchic heritage and an anarchistic approach to activism" (Gillen 2012). Hacktivist movements are also characterized by anti-corporate or anti-capitalist sentiment. The idea that the capitalism has lost its legitimacy, as well the idea that capitalism is unable to communicate with its citizens, is strongly resonated in the hacktivist community (Gillen 2012). In other words,

hacktivists have always strongly aligned "with the ideas of justice, freedom, solidarity and liberty" (p. 22).

The hacker community has contributed to a series of computer-related innovations in the past, which was done "in the spirit of playful exploration" that has always characterized this community (Krapp 2005). Hacktivist culture borrows this aspect of hacker culture; and is oftentimes characterized by its use of humor and creativity in combination with hacking. Hacktivists often employ rude, absurd, creative, and playful methods of communicating their message, as well as sarcasm and black humor (Fuchs 2014). The famous hacktivist collective *Anonymous*, for instance, is known for making videos in very artistic and creative ways. Members of the group often show an "extraordinary, unhindered creativity" (p. 89) when they launch an operation or simply want to communicate an idea to the public and to the media.

### *Is Hacktivism Ethical?*

A number of peer-reviewed studies are dedicated to the ethical considerations of hacktivism. It is worth mentioning that while early literature on hacktivism (in the 1990s and early 2000s) portrayed it in a more critical light, more recent academic work takes a more positive and/or defensive position toward hacktivism. For example, while Milone (2003) stresses that hacktivists need to be better educated about the importance of national infrastructure (i.e., the critical systems that promote core functions in modern societies, like telecommunications, power, or transportation) and the need for responsible hacktivism, newer research stresses the importance of hacktivism as a phenomenon in general. Hampton (2012), for example, emphasizes that it is crucial to differentiate between expressive hacktivism (i.e., hacktivism that does not involve compromising computers and networks) and hacktivism that is actually aimed at creating serious

disruptions. Further, Hampton suggests that forms of hacktivism "that are primarily expressive…and do not involve obtaining or exploiting illegal access to computers and networks for commercial advantage or financial gain…should receive at least some protection as a legitimate form of protest" (p. 531). In other words, some hacktivism is morally permissible, such as expressible hacktivism that merely conveys a message, and should be legally protected, while other forms of hacktivism that cause direct harm (e.g., DDoS attacks or hacktivism that results in information theft and hijacking of private property) should be rightfully punished.

Some authors (Manion and Goodrum 2000; Himma 2005) point out that hacktivism closely resembles civil disobedience. Similar to civil disobedience, which can be viewed as "morally justifiable as a protest against injustice" (Himma 2005:1), hacktivism can also be conceptualized as a justifiable form of political activism, since hacktivism targets governments and corporations for, at least in some cases, very valid reasons (Manion and Goodrum 2000). Similar to Hampton (2012), Himma concludes that some expressive forms of hacktivism are permissible, and should not be punished as harshly as hacktivism that causes significant damage (e.g., financial losses to a company, etc). In sum, even though hacktivism may resemble civil disobedience in the sense that hacktivists claim they use no violence and/or cause no physical damage, their actions can still cause harm; thus, hacktivism can be considered a legitimate form of civil participation, but each instance of hacktivism should be considered on a case-to-case basis (Himma 2005).

**What Triggers Hacktivism?**

In order to understand how the phenomenon of hacktivism came to be in the first place, it is important to examine the factors that contributed to its emergence. Some peer-reviewed literature provides insight into these factors and help provide context. Researchers name the following primary 'triggers' that facilitated the rise of hacktivism. These factors are also responsible, in part, for the fact that activism began a shift to the digital realm: 1) the expansion of information technology in the modern world; 2) the context of global crisis and growing political awareness within hacker communities; 3) state suppression and/or limitation of traditional protest; and 4) state and corporate control of intellectual property (i.e., copyright) and the Internet.

*The Role of Technology*

Numerous authors attribute the upsurge in hacktivism, as well as digital activism, to the growing importance of technology in the modern world. "The expansion of information and telecommunication technologies has resulted in the emergence of new urban virtual cultures" (p. 317), according to Papadimitriou (2006). The evolution from a traditional society to a communication society, in other words, has led to the emergence of virtual cultures and sub-cultures. Those virtual cultures, in turn, have formed a variety of social and political movements online, that operate on both local and global levels. Papadimitriou (2006) refers to the online realm, or the Internet, as 'Notopia': in which 'no' stands for absence, while '-topia' (or 'topos') stands for place(s). In other world, the Internet can be conceptualized as a number of places that have no name, fixed location, or identity. Hacktivists, according to Papadimitriou, emerged from 'Notopia' and use the Internet as a 'battlefield' to promote their political ideologies.

'Notopia', or an unmappable space of the Internet, provided an ideal place for cyber groups and cyber cultures to form, thrive, and organize. Van Laer and Van Aelst (2010) suggest that activism also moved to the online realm because the Internet allows protestors to promote political ideologies on a more global level and across physical distances, something crucial for activists in today's context of globalization: "…as economical and political power has gradually moved to the international level, the internet has enabled social movements to follow that transition and operate more globally" (p. 1146)

Taylor (2001) concurs with this idea by stating that today's political and corporate leaders are some of the most wired in the world. It is thus very unwise for activists to ignore the role of computers and the Internet in the modern world. Technology is successfully implemented and used by state and corporate powers as a tool for promoting their interests. Citizens, and among them, hackers, followed in these steps and shifted activism to cyberspace, as well. Jensen, Danziger and Venkatesh (2007) suggest that "among Americans online, more than 80% say the Internet plays a vital role in their daily routines" (p. 39). The Internet, according to Jensen, Danziger and Venkatesh, constitutes a new channel that fosters the formation of new communities. These online communities are, in many ways, superior to traditional offline communities.

One of the significant advantages of online communities is that the Internet as a medium "can mobilize additional segments of the political community who do not participate offline" (Jensen, Danziger and Venkatesh 2010). The Internet, according to the authors, represents a powerful tool to raise youth political consciousness. In other words, cyberspace has the capability to facilitate political discussions that tend to attract

"a wider variety of demographic groups" (p. 41), who would otherwise not participate politically. Another important quality of the Internet is that it helps to mitigate socio-economic status (SES).

Similarly to Papadimitriou (2006), who claims that the Internet (or 'Notopia') creates communities that are characterized by anonymity, diversity and togetherness, Jensen, Danziger and Venkatesh (2010) conclude that the Internet promotes "a greater democratization of the political process" (p. 47), because the SES variable becomes irrelevant online. It was long established that a healthy democracy cannot be achieved without a healthy civil society. The Internet, or the 'virtual community' (Jensen, Danziger and Venkatesh, 2010), represents a new arena that provides individuals with new dynamics and opportunities for creating such healthy civil society. The authors conclude that democratic processes are indeed occurring online, and that cyberspace represents a "distinct, socially embedded, medium in which political behavior takes places" (p. 47), rather than a mere extension of offline political engagement.

Beyer (2014) echoes a similar idea. The author analyzed "freedom of information" movements (such as *Anonymous*, *WikiLeaks*, and the *International Pirate Party*), and concluded that the Internet represents a powerful tool to shape people's political beliefs and actions. The Internet is especially effective at mobilizing younger generations: "young people online are willing to mobilize on behalf of abstract right claims, and that willingness spreads quickly across the social spaces online" (p. 150). Thus, the Internet has a strong potential not only for creating social and political movements, but also changing society. Hearn, Mahncke, and Williams (2009) agree by stating that "the development of the Internet and globalization in many ways are

12

increasingly challenging internationals relations" (p. 4) by providing people with new ways to participate in local and international politics.

Lastly, Fitri (2011) suggests that the Internet, besides being a powerful tool for generating support for non-violent political causes, also "changes the nature of collective action" (p. 5). More specifically, cyberspace empowers participants in a way that physical spaces simply cannot empower individuals: "the Internet permits an unprecedented empowerment of the individual" (p. 5). The Internet as a tool for democracy discourse is both empowering and attractive for activists and hacktivists, because it provides people with new, more effective methods of political participation. For example, the Internet allows for the fast and inexpensive collection and publishing of information, as well as communicating with others and coordinating action on a global scale more effectively.

Activists around the world will likely continue to become more technologically knowledgeable and equipped; activists' fascination with technology has already played a direct role in formation of hacktivist movements (Taylor 2001). The Internet has empowered activists and led to the formation of a new movement, known as hacktivism; technology, according to scholars, is to remain a crucial tool for shaping political discourse today and in the future.

### *Global Crisis and the Growing Political Awareness of Hackers*

Two other aspects that greatly contributed to the emergence of hacktivism are global crisis, manifested through governments' impingement on people's rights, and growing political awareness within the hacker community. Taylor (2001) suggests that over time, hackers have become more politically aware, which directly contributed to the birth of hacktivism. Taylor (2005) states that it is quite logical and natural that hacking, over

time, evolved into hacktivism. Hacking originally celebrated "human ingenuity over technological systems" (p. 626); later on, however, hacking has become a celebration of technology in itself. In other words, Taylor (2005) argues that human agency was lost in the hacker community, and hacking began to be associated with human subordinance to technology and powerlessness: hacking has become "an uncritical celebration of those systems for their own sake" (p. 626). The dichotomy of human agency and technological structures are quite important in understanding why hacktivism transitioned into hacktivism.

Hackers becoming politically aware and involved in activism has completely changed how hacking is perceived and conceptualized: from being subordinated to technology and simply pursuing technological means as an end result, hackers started to see themselves as social and political "warriors." According to Taylor (2005), hackers have undergone a transition from "politically unenlightened" individuals with "pathological conformity to the mores of industrial society" and "parasites" (p. 630), to politically informed and proactive individuals. The hacker community needed this 'refocusing' in order to resolve "the human-technology power imbalance" (p. 627). Another study (Taylor 2001) also suggests that hackers evolved into hacktivists in order to be "accepted as a legitimate part of society" (p. 1). In other words, this transition from hackers to hacktivists was a response to their increasingly growing marginal status.

Yet another significant factor that contributed to the upsurge in hacktivism is the 'global crisis': the political and economic context of the modern world. The global crisis can be exemplified in globalizations' negative impacts (such as inequality, unfair labor laws, etc.), for instance, or the growth of corporate and state power across the globe.

"Political and social concerns surrounding global capitalism" (Taylor 2001) captured the attention of hackers. Hacktivism has emerged as a critique of the "abuse and corruption of corporations, banks and governments" (Fuchs 2013). In other words, both an economic crisis of capitalism and a crisis of the state, across the world, created the context in which resistance is shaped, in this case in the form of hacktivism.

### *Suppression of Traditional Protests*

Some scholars suggest that hacktivism can be conceptualized as a response to the state's suppression of traditional methods of protest (i.e., street protests). Although hacktivism is not directly caused by the state's suppression of street protests, the upsurge in hacktivism is related to governments' attempts to control, minimize, or ban traditional protest.

Yip and Webber (2011) suggest that the "inability to physically or verbally express the feeling" (p. 2) results in people's feeling *ressentiment*. In their study, the authors use the concept of ressentiment, which states that actors engage in social movements, or protests, when they feel deprived of certain rights they feel entitled to, to explain why an upsurge in hacktivism happened in modern China. Throughout history, the Chinese government often shut down "the traditional physical ways in which Chinese citizens could voice their anger over political matters" (p. 3). It is the "lack of freedom for physical protests" (p. 3) that led Chinese citizens to use an alternative arena for protest: the Internet. According to Yip and Webber, hacktivism represents a creative way to resist the government's control of physical spaces, as well as an opportunity for citizens to express their emotions and feelings of ressentiment. The authors also hypothesize that in times of important political events, hacktivism membership (the number of people participating in hacktivist activities) would rise. Yip and Webber's

study (2011) confirmed the hypothesis: hacktivism in China (e.g., the hacktivist forum's membership) rose during times when the Chinese people were or felt threatened by their government.

Similar to Yip and Webber, Fuchs (2013) states that hacktivists often become involved in situations where traditional protests are under attack. More specifically, Fuchs provides the example of *Anonymous,* and their involvement in the Occupy Wall Street Movement (OWS). The hacktivist collective *Anonymous* took interest in the OWS movement when peaceful street protestors were threatened by the police. In other words, hacktivists became involved as a result of police brutality and aggression toward street activists.

### *Control of Intellectual Property & the Internet*

A series of studies suggest that hacktivism has emerged as a response to state and corporate control of intellectual property. Bakioglu (2013) suggests hacktivism has emerged as a network-based initiative in response to "privacy violations that occurred at the behest of copyright," as well as "tensions between intellectual property and privacy" (p. 1). Bakioglu uses the concept of *global network capitalism* (GNC) in his analysis of the digital rights movements and hacktivism. GNC is defined in the following way by Fuchs (2007):

> "Global network capitalism is based on a transnational organisational model, organisations cross national boundaries, the novel aspect is that organisations and social networks are increasingly globally distributed, that actors and substructures are located globally and change dynamically (new nodes can be continuously added and removed), and that the flows of capital, power, money, commodities, people and information are processed globally at high-speed. Cyberspace allows the global flexibilisation and global extension of social systems in space, and the overcoming of temporal limits, it supports the transnationalisation of capitalism. Global network capitalism is based on structural inequalities; it is made up of segmented (economic, political, cultural) spaces in which

central hubs (transnational corporations, certain political actors, regions, and countries, western lifestyles and worldviews) centralise the production, control and flows of economic, political and cultural capital (property, power, skills). Global network capitalism is an antagonistic system; transnational networks are both spaces of domination and spaces of potential liberation from domination" (p. 49).

Both Fuchs (2007) and Bakioglu (2013) note that GNC represents an antagonistic place, in which both control of information and the resistance to such control co-exist. In other words, while the state or corporations may attempt to control intellectual property (such as through copyright), there is also an opposition to such control (e.g., hacktivist movements). A specific case of such resistance can be seen in the example of the Operation Payback, launched by the famous hacktivist and activist group *Anonymous*, which emerged as a response to attacks on digital piracy.

Government attempts to exert influence over communication technologies, and the Internet in particular, also triggered hacktivism, according to Hearn, Mahncke, and Williams (2009). Hacktivism represents "distributed citizen-based warfare" (p. 1) against global political and corporate superpowers. Hearn, Mahncke, and Williams (2009) use the medium theory to explain why hacktivism came into existence. Medium theory "assumes that tools such as the Internet are not neutral and are subject to human agency" (p. 1). More specifically, medium theory proposes the following idea: when a new form of communication is introduced into a society (for example, the Internet), the society will be affected culturally, socially, politically and economically as a result of the introduction of this medium (Hearn, Mahncke, and Williams 2009). The Internet is obviously "changing the landscape of political discourse and advocacy" (Fitri 2011). The birth of the Internet has also resulted in the emergence of power relations between authorities that

17

actively try to create a 'monopoly of knowledge' and the society in which they exist. Hacktivism emerges as a response to such digital hegemony of state and corporation.

Hacktivism can be seen as a response to the threats to modern communication technologies, posed by the elite. Hacktivism came to be partially because there was a need to defend cyber space from the hegemony of political and economic elites. In this respect, hacktivism can be conceptualized as 'culture jamming,' according to Hearn, Mahncke, and Williams (2009). The authors define culture jamming as "manipulation of the mass media by artists and activists" with the purpose of creating "alternative meanings or [countering] hegemony" (p. 2). A classic example of culture jamming can be seen in graffiti: while graffiti can appear to be "billboard banditry" at first look, it has an underlying purpose that goes beyond vandalism: undermining the intentions of those who created the billboard or advertisement. Similarly, hacktivism emerged not with the purpose of vandalism, but rather with the purpose of challenging corporate and state power over technology, as well as raising awareness about the dangers of such control to society.

## The Hacktivist Collective "Anonymous"

### *Background*

The collective, known under the name *Anonymous*, can be defined as a networked movement, which is often referred to as a hacktivist community by scholars (Fuchs 2014). Fuchs (2014) describes *Anonymous* as "unpredictable, anarchistic, disturbing, ambiguous, confusing, exaggeratory collective of the nameless, a loose network without members  that has loose goals in which  everyone can participate" (p. 91).

Even though scholars often refer to *Anonymous* as "the Anonymous hacker group" (Hai-Jew 2013), or a hacktivist group, the true membership of the collective is not

very well-known. It is known, however, that *Anonymous* represents an all-inclusive

collective that may consist of both hacker and hacktivist, as well as individuals with less

technological knowledge. Fuchs (2014), for instance, claims that *Anonymous* is

compromised of hackers, geeks, technologists, human rights advocates, and activists.

 *Anonymous* originated on the message board 4chan.org, which is dedicated to

Japanese mangas (Ifrah 2008; Mansfield-Devine 2011). The message board does not

require users to register an account or reveal their identity, and the majority of users go

by the name "anonymous," which was later adopted by the group *Anonymous*.  One of

the first collective actions by *Anonymous* can be tracked to 2006, when members on the

4chan boards organized and carried out "the blockage and disturbance of the teenage

online community Habbo Hotel" (Fuchs 2014). The same year *Anonymous* launched a

campaign against Hal Turner, a talk radio host known for white supremacy and fascist

viewpoints.

 While some earlier campaigns by the collective were motivated by a desire to

'troll' (i.e. frustrate) individuals they did not approve of, or simply to get a laugh,

*Anonymous* became more political in 2008, when it launched 'Project Chanology' against

the Church of Scientology (Fuchs 2014; Serracino-Inglott 2013).  In other words,

Anonymous began as a collective with primarily prankster intentions, but later evolved

into an organization that "adopted a more politically-oriented ethos" (Wong and Brown

2013).

 By 2010, *Anonymous* had become an internationally recognized, scandalous

group. The group launched DDoS attacks as part of Operation Payback against Amazon,

PayPal, MasterCard, Visa, and PostFinance, in 2010 in response to these companies'

attempts to block donations to WikiLeaks, an international non-profit journalist

organization that leaks and publishes confidential information provided by anonymous

sources. *Anonymous* was very supportive towards WikiLeaks throughout the incident and

currently. It is logical to presume that the ideologies of both *Anonymous* and WikiLeaks

overlap (Serracino-Inglott 2013): both promote extreme transparency for institutions in

combination with strong privacy rights for individuals.

***"Anonymous" as 'Cyber Vigilantes'***

Serracino-Inglott (2013) proposes that *Anonymous* can be better understood through the

concept of 'cyber vigilantes.' The author starts by saying that vigilantism, as a

phenomenon, should not necessarily be interpreted as unjustified, wrong, or immoral.

The phenomenon of vigilantism is typically used to describe fictional characters (e.g.,

Batman or Superman), who stand up for the weak in times when the law fails to defend

them. Vigilantism can be defined as "the organized use of violence, or threat of violence,

by an agent or agents who are not willingly accountable to the state, for the purpose of

controlling (preventing and/or punishing) criminal and non-criminal, but still deviant

actions" (p. 221). Vigilantes are driven or inspired by concerns for justice and the well-

being of their community.

To be qualified as a 'vigilante,' one should meet all of the following criteria

(Serracino-Inglott 2013): 1) the action of vigilantism is to be carried out by a person who

is not willingly accountable to the authorities; 2) an act of vigilantism should be a

premeditated action; 3) an act of vigilantism must be in agreement with the vigilante's

"system of minimally defensible values" (p. 221); 4) an act of vigilantism must be

motivated by a concern for justice or the well-being of the community; and 5) an act of

vigilantism is to contain violence or threat of violence toward the perceived 'opponents.'

According to Serracino-Inglott (2013), *Anonymous* fulfills all of the aforementioned criteria, except for the threat of violence. However, Serracino-Inglott states that in the modern, technological world it is important to redefine the concept of violence. Although violence is traditionally seen as a physical act, in the virtual world it can be re-conceptualized as "the expression of punitive intent," and "no less powerful than a threat of violence for satisfying the vigilante's concern for justice" (p. 230). If we conceptualize violence as punishment, rather than physical violence, hacktivism can fulfill the fifth criterion for vigilantism, as well. According to Serracino-Inglott (2013), *Anonymous* can indeed be considered vigilante because of their use of punishment and threats of punishment.

Vigilantism can be conceptualized as "purposeful directed action" (p. 232). Its primary purpose is to defend the well-being of the community and to make sure that cherished norms and values are being defended and maintained. Thus, even though vigilantes use violence (or punishment), the latter is somewhat meaningful and necessary for society in some cases. Use of violence/punishment represents a necessary component of vigilantism. *Anonymous* can be seen as 'positive deviants,' according to Serracino-Inglott. In addition, *Anonymous* also represent 'deviant innovators':

> "Rather than rejecting the means to achieve social goals, they over-conform to them, taking the ideas that digital technology permits perfect replication to its extreme normative conclusion (expressed as antagonism to Intellectual Property, demands for increased transparency from institutions and substantial protection of individuals' privacy rights " (p. 237).

### *"Anonymous" as 'E-Bandits' & the 'Politics of No One'*

Wong and Brown (2013) use the concept of 'e-banditry' for their analysis of *Anonymous*. The concept of e-bandits represents an extension or continuation of the concept of "social

bandit," which was introduced by a British Marxist historian, Eric Hobsbawm. Social bandits represent noble robbers (or 'Robin Hoods'), who fight injustice primarily by taking from the rich and giving to the poor. Social bandits see themselves as righteous because they see themselves, as well as people they strive to defend, as victims of injustice. E-bandits, in turn, represent modern day Robin Hoods, believing that freedom of the Internet is being threatened by the major powers within society (the state and corporations). Just like social bandits, e-bandits (i.e., *Anonymous*) see their actions as justified and/or morally permissible. In other words, activism-gone-electronic can be conceptualized as "e-banditry," or hacktivism.

Unlike previous generations of hackers, who attempted to hide their activities, most hacktivists want their actions to be noticed or discovered. E-bandits are different from other hacktivists is that they are willing to "engage in illegal, extra-illegal and legal activities that result in negative or at least costly outcomes for their targets, thus distinguishing them from some hacktivists who simply want to post videos on behalf of a cause" (p. 1022). In other words, *Anonymous,* as e-bandits, represent a separate subgroup among political hackers. *Anonymous* pursues activism through the anonymizing technologies of cyberspace. The use of such technologies makes it hard, if not impossible, for others to discover their identities. Even other members of *Anonymous* often struggle to identify one another.

E-banditry is accomplished through the use of anonymizing technologies and represents an important social phenomenon, as well as an anarchist movement. E-banditry, according to Wong and Brown (2013) inspires "new ways of thinking about democracy and citizen activism" (p. 1022). The Internet has a strong mobilizing

potential, and the modern Internet's (Web 2.0) anonymizing capability creates a condition for 'the politics of no one.' Wong and Brown (2013) define the 'politics of no one' as politics of actors without identities (the identities of e-bandits always remain hidden or concealed). Anonymity in this case is used as a tool for political action rather than as a tool for building networks and communities. E-banditry is liberating and inspiring, in that it allows everyone to join the movement, including 'atypical' activists. E-banditry, in other words, is "all about getting people involved without giving them faces, names or even necessarily a position to defend" (p. 1020). The significance of the politics of no one and e-banditry should not be overlooked, especially in the face of state and corporate attempts to control the Internet.

*Political Worldviews & Core Values of "Anonymous"*

Fuchs (2013) describes *Anonymous* as a collective with fluid and heterogeneous political worldviews. The collective's political beliefs represent a fusion of "anarchism, liberalism, communism, and libertarianism" (p. 345). *Anonymous* is a pluralistic movement, in which different views and ideologies co-exist and complement each other. Coleman (2013) concurs by saying that the diversity and vibrancy of the group's political ideology is an essential component of *Anonymous* culture. This vibrancy of political worldviews has directly contributed to the, so far, success and effectiveness of the collective. Some scholars (Wong and Brown 2013) propose that *Anonymous'* political goals revolve around the following major issues: 1) anti-censorship and freedom of speech; 2) privacy; and 3) Internet security.

Fuchs (2013) mentions the following basic political values of *Anonymous* (borrowed from the 'Anonymous Manifesto'): a fight for a transparent, fair, and

accountable community, in which information is free (i.e., uncensored or uncontrolled), and protection of citizens' liberties and rights. *Anonymous* as a collective is especially antagonistic towards states' surveillance and/or impingement on the privacy of its citizens. *Anonymous* stated (Fuchs 2013) that it bases its political values on the following core principles: "1) the media should not be attacked; 2) critical infrastructure should not be attacked, and 3) one should work for justice and freedom" (p. 347).

"The focus on the libertarian values of freedom of speech, expression, assembly, information, and press dominates Anonymous' political communication" (Fuchs 2013). Even though *Anonymous* shares libertarian values, the group does not embrace corporate or state power. To date, the main targets of *Anonymous* have been government and corporate. *Anonymous* particularly sees a threat in the latter. Freedom of the Internet (which represents a central issue for Anons) and of the people are both threatened by corporate and state powers, according to *Anonymous*. The collective demands that the Internet be controlled by civil society, instead. *Anonymous* is also known as a strong opponent of class inequality, and is preoccupied with socio-economic justice worldwide (Fuchs 2013). As a result of his empirical analysis of *Anonymous*' public communication, Fuchs (2013) concluded that: 55% of Anons aligned with pure liberal values; 8% with pure socialist values, and "22% blended liberalism and socialism" (p. 371).

### Organizational Channels of "Anonymous"

Anonymous often states that they represent an idea (Fuchs 2013), it is common to see members posting or espousing the following motto in online videos, chat rooms, and on message boards: "Anonymous is everyone. Anonymous is no one. Anonymous exists as an idea" (p. 348). The survey of peer-reviewed literature on the group's organizational channels makes it clear that *Anonymous* does not have a clearly defined membership:

anyone can join or leave the group at any time. *Anonymous*, as some scholars also note, claims that it does not have any leadership and/or hierarchy. Some authors (Shalin Hai-Jew 2013) acknowledge that the loose or fragmented character of *Anonymous* may contribute greatly to the group's adaptability and resilience. A lack of hierarchy may also be viewed as a strategy of the group. However, it is worth mentioning that the collective does not represent a purely leaderless group (Fuchs 2013). Some scholars emphasize that there are core activists within *Anonymous* "with specific technical skills, media skills, and organizational skills who carry out the core of hacking activities" (p. 349). So, while a clear-cut hierarchy may indeed not exist within the collective, a certain division of labor is evident.

*Anonymous* can be characterized as a hacktivist collective that uses a critical mass to achieve its goals, the group is reliant on a large number of the members participating in an attack or 'operation' (Mansfield-Devine 2011). Scientists (Conway 2003; Jordan 2002) divide hacktivists into two basic categories: mass virtual direct action (MVDA) and individual virtual direct action (IVDA). Hacktivists who fall under the MVDA category are those who rely on reaching a critical mass, while hacktivists who fall under IVDA act alone.

Although *Anonymous* is known for providing members with both options for virtual direct action, overall, the group, overall, is reliant upon 'critical mass' (i.e., mutual efforts). This is especially evident in *Anonymous'* launches of distributed denial-of service (DDoS) attacks, which are carried out with the help of automated applications, such as LOIC and HOIC, that members of *Anonymous* use to overload/crash websites with traffic. Serracino-Inglott (2013) concurs by stating that Anons show strong

preference for Internet Relay Chats (IRCs), message boards, as well as file-sharing services: all of which is indicative that the collective attaches special value to "diffusing control of strategic assets throughout the community" (p. 227). Anons, in other words, show appreciation for the community; the community or communitarian spirit of *Anonymous* can be evident though the fact that the group frequently uses mutual support efforts as a strategy for achieving goals.

*Anonymous* represents a participatory collective (Coleman 2013). Non-tech savvy individuals are welcome to participate in *Anonymous'* activities: one may, for instance, choose to help others write press releases and reports, or to give media interviews; people who have designing skills can use their abilities for designing propaganda posters or editing videos, and so on. To join the group, one simply has to identify with *Anonymous* and its core values. *Anonymous* neither expects particular abilities, nor requires them from those individuals willing to join. While 'true' hackers' opinions and skills may be respected and/or appreciated within *Anonymous*, they "don't erect entrance barriers nor control the evolution of Anonymous" (p. 12). In other world, *Anonymous* is an all-inclusive group that welcomes help from all fronts. Mansfield-Divine (2011) and Shalin Hai- Jew (2013) also note that many *Anonymous* members lack sophisticated computer or hacking skills. DDoS attacks, which *Anonymous* members often employ to crash opponents' sites, are not technically complicated in nature. Thus, it is logical to conclude that *Anonymous* does not represent a pure hacktivist community, since many participants are not technically-savvy.

Coleman (2013) also provides interesting insights into how *Anonymou*s' members choose targets. The author proposes that the operations of the collective are primarily

reactive, and that various local and international events or incidents can serve as triggers for action by *Anonymous*. *Anonymous* represents a collective of individuals who react to events rather than choose them randomly or chaotically. Lastly, Coleman (2013) suggests that *Anonymous* should be conceptualized as a reaction to certain trends in society (e.g., governments worldwide attempting to control the Internet). *Anonymous* can thus be seen as a positive social phenomenon because the collective, along with other hacktivist groups, provide citizens with new creative "avenues for personal and collective participation" (p. 17). It is worth mentioning that even though *Anonymous* is often portrayed as a group of violent hackers by the media, most Anons never break the law (Coleman 2013).

Mansfield-Devine (2011) suggests another positive effect of *Anonymous* and similar groups. The collective helps to raise security awareness and remind us that modern technology is incredibly vulnerable. Security is lacking in modern computer system and software: "systems aren't patched up to date like they should be" (p. 7), and hacktivists constantly remind society of these facts.

***The Importance of Anonymity and the Guy Fawkes Masks***

Fuchs (2013) states that "the employment of symbolic means of expression is particularly important for Anonymous" (p.3 49). The masks worn by members serve as an expressive means to grab media attention, and therefore represent a media strategy, according to Fuchs (2013). Coleman (2013) suggests another theory to explain the group's use of Guy Fawkes masks. According to Coleman, the masks have a symbolic purpose: "Guy Fawkes masks and headless suited men…symbolically and spectacularly [assert] the idea of anonymity, which they embody in deed and words" (p. 15). In other words, Coleman proposes that masks convey the message that anonymity is something of utmost

importance to *Anonymous*. The masks are also part of the group's culture of "unpredictability and mystery" (p. 15) as the masks raise a variety of questions about who *Anonymous* is and what will they do next.

Serracino-Inglott (2013) also suggests that anonymity and pseudonymity represent an integral part of the *Anonymous* movement, rather than the mere means of protection that members use to avoid being identified or arrested. The culture of anonymity that clearly exists within the collective "is built upon the importance attached to the ability to express oneself freely" (p. 219). Fuchs (2013) suggests that members of *Anonymous* use the masks, as well as computerized voices, in their videos in order to protect their identities, which allows the participant to express his or her thoughts more freely.

### *Importance of Humor and Creativity*

Fuchs (2014) claims that the culture of *Anonymous* is generally built around doing unusual things (p. 94). Fuchs states that humor represents an important element of *Anonymous*' culture and is used by the collective as a political weapon: "Anonymous makes fun of its political opponents and uses clownery (in the form of Guy Fawkes Masks armies) as a symbolic strategy to attain the media's and public's attention" (p. 104).

Unlike other hacktivist and activist collectives, *Anonymous* is known for using creativity as a tool to promote its goals. The group's videos are technologically complex, professionalized, according to Fuchs (2013), and can be conceptualized as "small artworks, highly creative and artistic" (p. 350). The highly artistic style of *Anonymous* is manifested through their "digital craftwork": a combination of digital "arts and crafts" such as videos, press releases, posters, and so on.

## III. METHODOLOGY

### About the Forums

The forums of Anonnews.org represent a place where anyone can post messages anonymously. In other words, the forums do not require users to register or provide any type of personal information. In fact, in order to post on the forums, one only needs to confirm that he/she is human by simply typing a given random combination of symbols and numbers (known as a CAPTCHA, this is a typical to confirm a user is human) in the window below your post. Users remain practically unidentified on the forum. The majority of people posting messages do so under the same generic nickname 'Anonymous,' while only a small fraction of users choose to use other, slightly more unique, nicknames. I only noticed a few users, throughout the time I spent on the forums, who used nicknames resembling real peoples' names. Clearly, anonymity on the forums is one of the guiding principles which are agreed upon by its users.

A glance over the forum's content is enough to realize that this message boards are far from what people typically think of or associate with a traditional forum. While traditional forums and message boards tend to have administrators (generally known as 'admins' or 'moderators'), who 'watch over' their members, regulate, or in some other way control the content of the board, the Anonnews.org forum has no moderators, or, at least, their presence is not felt. The absence of moderators is shown through the free flow of information, which includes large amounts of spam (advertisements and random posts by strangers is just one example). In fact, going through the content of the forum was more like going through an unknown forest: stepping over branches and leaves, and only occasionally finding tips that gave me some sense of direction as I was going towards. It is quite rare for a forum to be completely unregulated since a lack of regulation typically

makes it much harder to navigate through posts. The forums on Anonnews.org are indeed hard to navigate.

The developers of the forums, however, make an attempt to organize the forum by dividing the posts into broad categories. The broad categories or sections of the forum currently include (from top to bottom) 'AnonNews.org Notices & Feedback,' 'Anonymity, Cryptography, Decentralization, and Security,' 'Anonymous,' 'I'm looking for…,' 'Internet & Media.' 'Non-English,' and 'Politics and Government.' Despite the fact that the developers grouped posts into different sections, some of the content still barely makes sense: every section of the forum is infiltrated with spam. Not surprisingly, I had to take every word with a grain of salt.
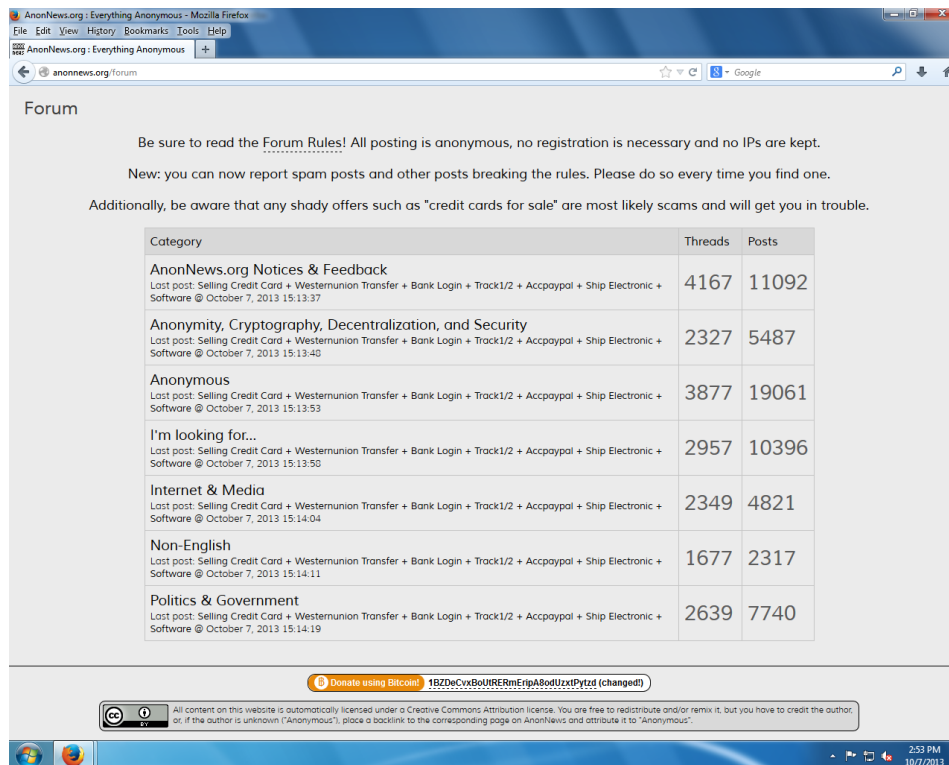


**Figure 1. The main page of the forum: www.anonnews.org**

Even in the 'Forum Rules' section of the website, the forums are described as "a mess of spam and scams" (Anonnews.org 2013). Despite this, it appears as if there are

still some attempts made to eliminate the issue: "[The forums] will change. A new spam removal tool has already been made, and you may have noticed already that spam is removed faster now…" (Anonnews.org 2013). After spending a decent amount of time on the forum, however, I have trained my eye to distinguish between 'real posts' and spam. As time passed, some themes finally started to emerge.

I grouped the themes into three broad categories, based on their content, for a more organized analysis. The first group, which is dedicated to answering the question of who *Anonymous* are, as well as showing how group members view themselves or/and identify, revealed the following patterns/themes: a) *Anonymous* represent an idea rather than a group; b) *Anonymous* is not likely a hacktivist group, although hacktivists definitely exist within the group; and c) *Anonymous* rejects leadership/hierarchy which leads to the possibility that leadership may indeed not exist within the group.

The second group of themes is the patterns that describe how *Anonymous* functions as a group. These themes include: a) members discussing the ways current and/or future members of *Anonymous* join or leave the group; b) members of the group discussing how *Anonymous* organizes/reaches common ground, especially in times when group members decide to take action (hack, have a street protest, etc.); c) the ways that group members see their goal within *Anonymous*; and d) the public image of the group, which was often debated on the forums.

Finally, the third group of themes revolve around the values and beliefs of the group members. The themes in this group include: a) the way group members view and understand hacking and security; b) the symbolism of Guy Fawkes masks, which members of *Anonymous* frequently wear during street protests, as well as online; c) the

theme of group members' identifying as either peace makers or revolutionaries; and d)

the theme of anarchism, which was oftentimes brought about and/or discussed by

members of *Anonymous*.

## Content Analysis Specifics

Since very little research has been done on hacktivism and/or hacktivists, and *Anonymous*

in particular, my research purpose was mainly to conduct manifest content analysis

(content analysis which describes and analyzes the information readily available on the

message boards) versus latent content analysis, or the analysis of hidden messages.

When I started analyzing the forum's content, I realized it would be a time-

consuming task since it is infiltrated by spammers. A large portion of the content on the

forums was taken by messages that either did not make any sense, or were simply

irrelevant to my study. Therefore, I had to come up with specific measures of how the

data was to be sorted through and analyzed. Each section of the forum included multiple

threads. Here is an example of the way in which content appears when visiting each of

the forum's major sections:
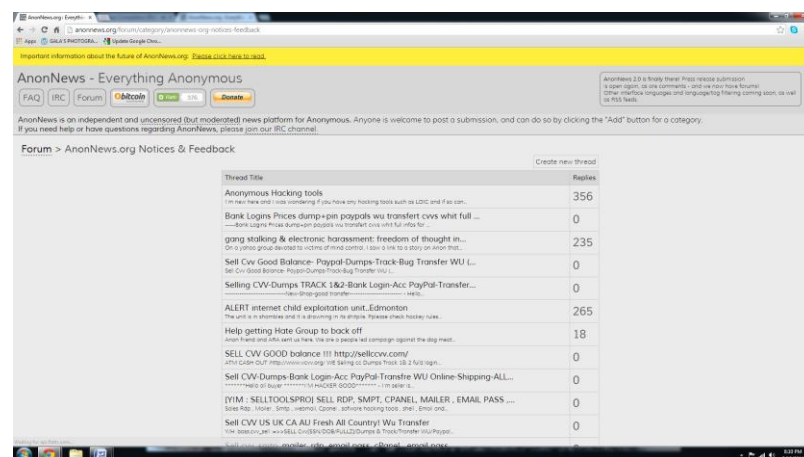


**Figure 2. Forum's threads: the conversations in each of the forum's sections are presented in a list format; each thread displays the number of user responses (or 'replies').**

The first step in my content analysis was to go through each thread/topic separately and briefly overview its content to get a feel for how people post and reply. After going through approximately 20-30 of such threads, I got a general idea of what the content was and whether it was worthy of closer examination. The number of replies and the name of each thread itself also often pointed toward what content could be expected in each of the discussions. For example, when a discussion had 0 or very few responses and/or had a title like "Selling CVV-Dumps TRACK 1&2-Bank Login," this indicated that the discussion was most likely spammed (i.e., someone trying to sell questionable services/products, etc.) and/or had non-pertinent content. The low response rate also indicted that users of the forums most likely had no interest in a specific thread/topic.



**Figure 3. Sorting the threads/topics based on the number of replies (or the interest of the responding group members) and the name of the thread**

After I went through each of the threads/topics, I decided which to eliminate. Those that were eliminated mostly consisted of topics with zero replies. The entire list of topics was printed and the selected topics marked off for further analysis. The listed of eliminated topics looked like the following:

| Thread Title | Replies |
|---|---|
| **Bank Logins Prices dump+pin paypals wu transfert cvvs whit full ...** <br> -----Bank Logins Prices dump+pin paypals wu transfert cvvs whit full infos for... | 0 |
| **gang stalking & electronic harassment: freedom of thought in...** <br> On a yahoo group devoted to victims of mind control, I saw a link to a story on Anon that... | 235 |
| **Sell Cvv Good Balance- Paypal-Dumps-Track-Bug Transfer WU (...** <br> Sell Cvv Good Balance- Paypal-Dumps-Track-Bug Transfer WU (... | 0 |
| **Selling CVV-Dumps TRACK 1&2-Bank Login-Acc PayPal-Transfer...** <br> -------------------------New-Shop-good transfer------------------------- - Hello... | 0 |
| **ALERT internet child exploitation unit..Edmonton** <br> The unit is in shambles and it is drowning in its shitpile. Pplease check hockey rules... | 265 |
| **Help getting Hate Group to back off** <br> Anon friend and ARA sent us here. We are a people led campaign against the dog meat... | 18 |
| **SELL CVV GOOD balance !!! http://sellccvv.com/** <br> ATM CASH OUT :http://www.vcvv.org/ WE Selling cc Dumps Track 1& 2 fullz login... | 0 |
| **Sell CVV-Dumps-Bank Login-Acc PayPal-Transfre WU Online-Shipping-ALL...** <br> *******Hello all buyer *******I'M HACKER GOOD******* - I'm seller is... | 0 |
| **[Y!M : SELLTOOLSPRO] SELL RDP, SMPT, CPANEL, MAILER , EMAIL PASS ,...** <br> Sales Rdp , Mailer , Smtp , webmail, Cpanel , sofware hacking tools , shell , Email and... | 0 |

**Figure 4. Further analysis of the forum's topics:** list of forum topics was copied and pasted in Microsoft Word; the grayed out topics indicate the topics that will not be analyzed further

Once all of the topics in each section of the forum had been reviewed and eliminated of 'bad' topics, I had significantly less to read through. My next step was reading through each of the topics carefully instead of just eyeballing the content. As I was reading through each of the discussions, I placed some comments on the sides that helped me to sum up what direction the discussion was going in and what members simply discussed. As I marked the topics, certain themes started to appear. For example, I noticed that security and different computer tools/programs were discussed more frequently than, let's say, topics on how to hack people's Facebook accounts, which were more rare and unwelcomed by the majority of group members.
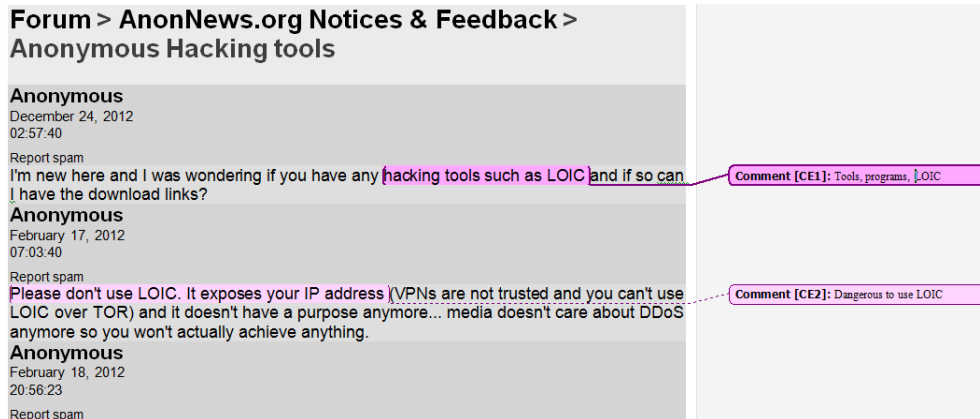
**Figure 5. Identifying wide subjects within each forum's thread**

As I read through the conversations, I began to notice that some of the subjects (for example, discussions of tools and programs for hacking or securing one's computer) were more favored than other subjects by the forum members. As I read the discussions, I would note, in a separate document, the list of most frequently repeating subjects. At this point, I also began separating the subjects into groups. For example, topics dedicated to programs like LOIC, or discussions about how to hack, were brought together into one category named "Technical conversations," while discussions specifically about Anonymous as a group (what the group is about, etc.) were brought together under "Anonymous Basics." The list of subjects that I identified was originally created in handwritten form, but for the purpose of example, I created a digital list that resembles my original.

Forum's Topics
Technical conversations:
  LOIC
  TOR
  How to secure IP address
  Learn how to hack
  DDoS
  Doxing
  How to stay Anonymous
Anonymous basics:
  Anonymous is idea
  Anonymous as a loose collective
  Anonymous is non-traditional group
  No leadership/hierarchy
  Public influence of Anonymous
  Diversity within Anonymous
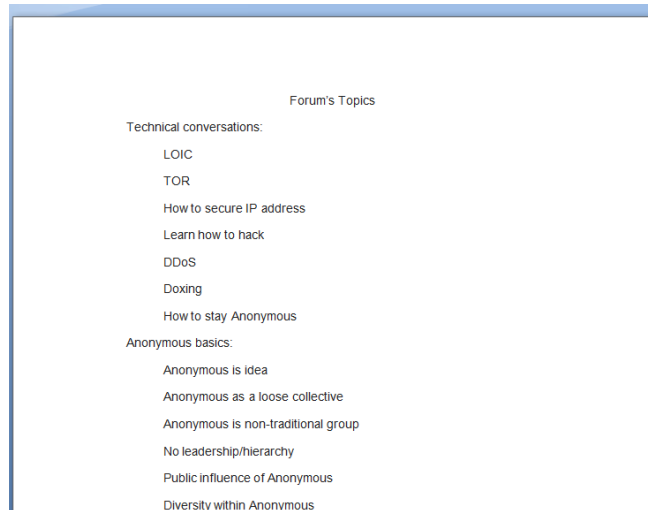
**Figure 6. The list of most frequently repeating subjects/topics**

My next step was to organize the subjects in a better way, so they could make more sense. For example, the discussions of programs such as LOIC (Low Orbit Ion Cannon) or HOIC (High Orbit Ion Cannon) were related to a discussion on how to secure your IP address, in the sense that both were discussed in relation to a wider interest of users – maintaining security while online/hacking. While some of the conversations represented a part of a bigger theme, other subjects/topics were less so, even though they were mentioned from time to time. For example, different 'techniques,' such as using LOIC for DDoSing a site or Doxing for stealing sensitive/valuable information, were mentioned in the discussions; however, they were not mentioned nearly enough to become a separate theme as they were mentioned casually but never discussed in detail or represented the center of the discussion.
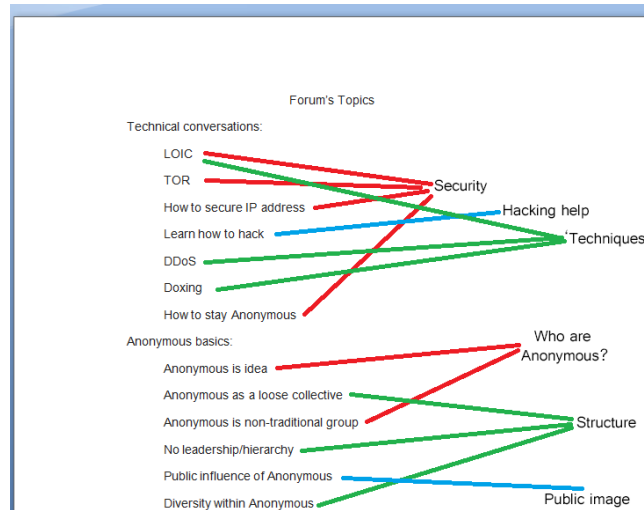
**Figure 7. Re-grouped subjects/topics**

In other words, because some of the subjects were related or were essentially the same, I regrouped/merged multiple subjects to make up larger, more encompassing themes. After I decided on a complete list of themes, I re-read the content of the forum once again with the purpose of selecting quotes that reflected the ideas best. I copy and pasted each quote in a separate document while also including the link to the thread from which the quote was taken, in case I needed to further review the thread. The list of quotes looked the following way:
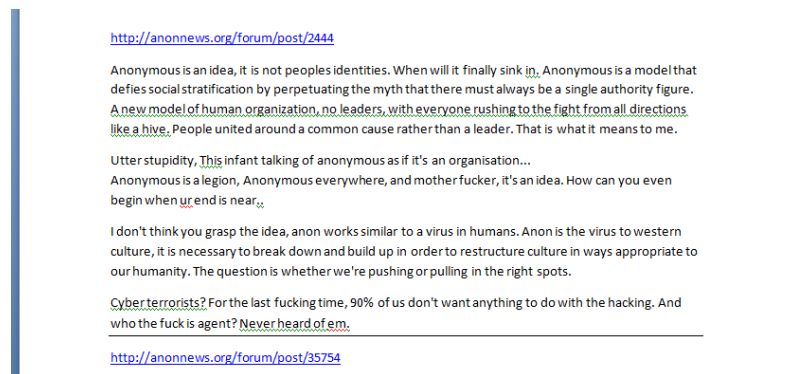


**Figure 8. Selected quotations for content analysis in Microsoft Word document**

After the large themes were identified, along with quotes that represented/backed up the themes, I could start writing up my report. Not all of the quotations were used; while some of them were used repeatedly throughout the report.

**Interviews Specifics**

The goal of interviewing security professionals was to discover their understanding and perspective on hacktivism, as well as groups like *Anonymous*. The company my respondents are employed with represents one of the largest security companies in the United States, and operate worldwide. For the purpose of protecting my respondents, I am not disclosing the name of their firm. The company offers security technology, security management services, and operates a consulting firm that specializes in incident response (forensics), security research, as well as network and application penetration testing.

My respondents held positions of Security Analyst or Security Consultant, and were responsible for performing network and application penetration tests; most had been with the company for an extended period of time (at least a few years). Below is the breakdown of the job titles for my interviewees:

Security Professionals' Official Positions within *Security Company X*

Respondent #1 – Security Consultant
Respondent #2 – Senior Security Consultant

Respondent #3 – Security Analyst
Respondent #4 – Security Analyst
Respondent #5 – Security Analyst
Respondent #6 – Security Analyst

Each interview contained eight questions, which eventually formed the themes I am analyzing below. Question one asked the respondents about their familiarity with

hacktivism and/or groups like *Anonymous* ("What do you know about hacktivism and/or the group *Anonymous*?"; when the respondents provides answer that was too short, I often asked a follow-up question, "What specifically do you know/have heard of hacktivism or *Anonymous*?").

Question two concerned the effects of hacktivism on the security industry: in this question I asked the respondents whether they believed hacktivism had changed the security industry in any way, or whether, they felt the effects of hacktivism personally? ("What effects have hacktivists and the groups like *Anonymous* had on the security industry?", and "Have you personally felt any effects of hacktivism on your work?").

Questions three to eight were more focused on the specifics of hacktivism. My goal was to see how the respondents conceptualized hacktivism and groups like *Anonymous*, and what were their personal feelings were about them. My third question examined the respondents' ethical perspectives in relation to hacktivism ("Is hacktivism ethical, in your opinion?"). Even though hacktivism is illegal, my goal was to understand how the respondents viewed hacktivism from legal, moral, and ethical standpoints.

Question four examined the issue of anonymity: I asked my respondents about possible reasons why anonymity is so important for hacktivists, as well as traditional activists ("In your opinion, what are some of the main reasons hacktivists choose to stay anonymous?").

Question five dealt with alternatives to hacktivism: I asked my respondents about the effectiveness of hacktivism, and if they thought there are better ways of promoting social change, in place of hacking ("In your mind, what are viable alternatives to hacktivism, if there are any?").

Question six asked my respondents whether they, as security professionals, viewed hacktivists as dangerous individuals ("Are individuals who are involved in hacktivism dangerous?").

Question seven asked my respondents about the possible causes of hacktivism, as well as the reasons that hacktivism has become a wide-spread phenomenon ("What do you attribute the current increase in hacktivism to? Does or can society benefit from hacktivism in any way, in your opinion?").

Lastly, question eight dealt with the question of the security of the Internet and modern computer systems: "What can be done to make the Internet safer (including protection from individuals such as hacktivists)?"

An analysis of the responses the security professionals provided me has resulted in nine themes, which are discussed below in detail. The themes are the following: 1) security professionals' familiarity with hacktivism; 2) security professionals' personal outlook on hacktivism; 3) *Anonymous* and their hacking skills; 4) the ethics behind hacktivism; 5) hacktivism and its effects on the security industry; 6) *Anonymous* and the importance of Guy Fawkes Masks; 7) security professionals' explanation of hacktivism's popularity; and 8) alternatives to hacktivism.

## IV. ANALYSIS OF ONLINE FORUM

### Who are Anonymous?

#### *Anonymous: An Idea or Group?*

When I started browsing the forum, my very first question about *Anonymous* as a group was: what or who are *Anonymous*? More specifically, I wanted to know how group members define themselves personally and to each other as opposed to how the media or general public understands or defines them. The forum's posts shed some light in regards to this question. To my surprise, *Anonymous*' members most commonly define themselves as just an idea. *Anonymous* as simply representing an idea was the most common theme I discovered while reading the forum's content. The majority of Anons (short for *Anonymous*' members) stated that *Anonymous* is rather an idea than a group or organization:

> "…Anonymous is just an idea, an idea that is within all of us, an idea that we are more than they tell us we are at the pupil or on the news."

> "[Anonymous] is an idea, an umbrella which covers a huge variety of small groups or individuals with ideas and goals of their own."

> "…there is no group, no organization, just an idea."

> "…Yes, Anonymous is a "group", but more-so than that, Anonymous is an idea. An idea that people have rights, an idea that corruption should be revealed and cut out. An idea that we all deserve freedom and liberty, and that it is worth fighting for. As cliché as it sounds, more-so than being 'part of' Anonymous, you ARE Anonymous."

> "…This is not what this movement is about. The reason there is no leadership is because there is no actual GROUP. When you stand up for what is right, you are Anonymous. When you fight back against oppression and unfair laws, you are Anonymous. When you stand up and say NO to unrighteous attacks on civil liberty and freedom, YOU ARE ANONYMOUS. Anonymous isn't a group. It is an idea. IT IS FREEDOM personified." (Anonnews.org 2013)

It seems like a notion of that *Anonymous* is just an idea rather than a group, has become widespread among many *Anons*. Despite such widespread agreement, members' opinions on what constitutes *Anonymous* were not completely unanimous: while some members stated that *Anonymous* is not a group at all or that it does not even really exist, others claimed that it is indeed a 'group,' just not a traditional one. Schaefer's sociological glossary defines a group as "any number of people with similar norms, values, and expectations who interact with one another on a regular basis" (McGraw-Hill Online Learning Center 2013). If one relies on this definition of groups, then *Anonymous* is indeed not quite a traditional group. Firstly, *Anonymous*' members, based on my observations, tend to have very diverse opinions and values. While a large portion of the 'group' finds agreement on core issues (typically pro-social issues), there are multiple subsets of *Anonymous* whose members may reject some or all of these generally agreed-upon beliefs. Some Anons go as far as saying that the 'group' has no values whatsoever: "…Anonymous is a name anyone can use, it does not stand for any ideas, processes, groups, or anything else. Anonymous has no meaning other than as a banner to use for literary anything" (Anonnews.org 2013).

However, many members, as I mentioned previously, do agree that core values are shared among most Anons:

> "…Anonymous is not a group of operatives. It is a "legion" of
> GATHERERS (notice I emphasized on the word Gatherers, because as
> "being" anonymous means that we are just a group of people. We are
> hackers, students, and more, irrespective of what position we hold. Truly
> being an "anonymous" is to uphold the pro-social values and NOT too
> abuse them" (Anongnews.org 2013).

So, as to similarity of the views, one may argue that the views among a large portion of Anons are indeed similar/shared. While some members may adopt different

views, general views on what constitutes 'good' and 'bad' among *Anonymous'* members are indeed similar and/or are shared.

Secondly, based on my observations, *Anonymous'* members do not have tight, regular-basis communication with each other; the forums' communication flows freely allowing new members and/or random people at any time – the communication between members seems rather random and spontaneous. While Anonnews.org provides members with chat rooms, forums, and other ways of exchanging information, regular-basis or tight communication among members is not visible, nor can it be visible. All of the members use the same nickname ('Anonymous'), so it makes it practically impossible to say whether people who post are the same people or completely new members. Additionally, it is hard to say whether members communicate with each other regularly because there is an overwhelming amount of spammers and 'trollers' – individuals who purposefully start an argument attacking other members without attempting to listen to others' arguments – on the forum. Some members may communicate with each other regularly through e-mail or private messaging, however, the forums do not reflect how often or regularly communication takes places between members. It is even hard to say whether long-term members even exist on the forums – the communication on the message boards is rather fluid and unregulated. My conclusion in regard to the regularity of communication between members is that the communication/exchange of information does take place but it is hard to say whether it is regular or just random (e.g., when an opportunity for communication/exchange of information presents itself).

Perhaps, a concept of groups that *Anonymous* can fit in best is the concept of secondary groups – the concept that evolved from the concept of primary groups,

developed by Charles Cooley. Even though Cooley never directly mentioned secondary

groups in his writings, many authors share an opinion that he was also responsible for the

creation of the concept of secondary groups (Faris 1932). Secondary groups can be

described as somewhat opposites of their primary groups: unlike in primary groups,

individuals in secondary groups tend to communicate with each other on a less personal

level or be less personally engaged in group matters. Relationships in secondary groups

tend to be more informal (e.g., online communication versus face-to face

communication), as well as not as long-lasting. Secondary groups mostly reach cohesion

by maintaining the same goals. Lastly, in secondary groups individuals have a 'choice' of

joining or exiting the group, while in many primary groups (e.g., families) individuals

may not have such a choice; individuals' roles and positions in secondary groups are also

more interchangeable, and individuals in secondary groups tend to be more replaceable in

general than individuals in primary groups (Faris 1932). *Anonymous* can be thought of as

a secondary group: its members share similar goals and beliefs; however, their

relationships have a temporary character – members can come and go at any time they

please. New members are welcome from all 'fronts,' and all members are considered

equally valuable, but nonetheless replaceable. Additionally, *Anonymous* has no strict

rules or codes by which members must abide. Shortly, *Anonymous* can be considered a

contemporary secondary group that attracts its members worldwide for the cause of

fighting for freedoms and liberties of all individuals.

Faris (1932) interestingly points out that in some cases, secondary groups may

take on some qualities or characteristics of primary groups. Just like in primary groups,

individuals in secondary groups may occasionally get personally involved in the goals of

44

the group or feel strongly identified with a group: "Even in large and scattered groups – particularly those we call "social movements" – the struggle for liberty, freedom, justice, or any great cause may call into existence the very experiences and relations which we are able to find in the primary group." While most members of *Anonymous* may not want to be personally engaged in the group's activities, other members on occasion do become deeply involved while fighting for 'the cause.' Individuals like Jeremy Hammond, Hector Xavier Monsegur, Mercedes Renee Haefer, Christopher Doyan, and many others *Anons* arrested by the U.S. authorities (Smith 2013) serve as an example that even the most loose, informal groups may be highly significant to some members.

So, does *Anonymous* represent an actual group? The answer to this question is both a yes and no. As a collective, regardless of how loose or fragmented it is, *Anonymous* does seem to have shared beliefs and goals, and would therefore qualify as an actual group. Another reason *Anonymous* may be considered a group is because its influence can be hardly ignored by the media and the public (Arthur 2011; Zetter 2011; Pauli 2012; Sieczkowski 2012; Boone 2013; Gibbs 2013); widespread influence of the group and its recognition as a group by the public serves as further proof that it exists. It not only exists, but also functions successfully: its members seem quite capable of achieving their goals (e.g., hacking government websites and corporate servers). Some members of *Anonymous* may even get defensive when someone is attacking the group and state the group's influence in response:

> "…Anonymous has a lot of public influence and it can make a real change
> if that influence is applied in the right direction, you just need to decide
> what that direction is going to be…"

"Anonymous is not dead. Anonymous is growing, expanding daily. The effects are reaching new audiences, and even the recent arrests only bring more publicity."

"…Anonymous has thousands of members. Don't underestimate anonymous" (Anonnews.org 2013).

But despite being a non-traditional group, *Anonymous* members still spread the notion that the group is just an idea. Why? After reading numerous responses by Anons, I started to believe that such a concept may be used by the members purposefully. It seems like presenting the group as an idea is beneficial to its members for a variety of reasons, as well as symbolic to the group's beliefs and goals. Some of those reasons and symbolism can be seen in the quotes below:

Truth will never die (*Anonymous* believes that truth is unstoppable):

> "Nothing lasts forever, some day Anon may be gone too. The idea however remains. The truth, as inconvenient as it is to some, will find a way…"

Every member is valuable and capable, no hierarchy is needed:

> "… we cannot forget that the greatest strength of Anonymous is the fact that there is no leadership, no matter who gets arrested or … (do I really need to spell it out?) Anonymous as a whole cannot be damaged or compromised, or stopped. Every single one of us is ready, willing and capable (there goes the optimism again) to step up and lead those who will follow. We need that invulnerability to succeed."

If *Anonymous* is just an idea, it cannot be destroyed:

> "The idea behind anonymous was exactly that "we are anonymous" "we are an idea" Ideas can't be destroyed, they can't be manipulated but they can spread."

> "Anonymous is an idea. Ideas don't die."

> "An idea can change the world. Ideas are powerful. You cannot kiss an idea, cannot touch it, or hold it. Ideas do not bleed, they do not feel pain, they do not love, and most importantly – ideas do not die. Anonymous is a

necessary evil, a philosophical anarchy against oppressors and deceivers of this planet."

*Anonymous* does not need promotion; they can be useful to anyone:

"…Anonymous has no main aim, it needs no self-promotion, and is nothing more than a banner, a name to use. It makes no sense to try and promote Anonymous…"

""The anon name" does not need developing. It is a name that is whatever it happens to be. There is no intended goal for it, nor can there ever be. Leave it be, use it where applicable, do not try to promote Anonymous- it's a waste of time, time that is much better spent by actively trying to change what is wrong in the world and not just talking about it."

"Anonymous is not a group or organization. It is an idea. Ideas do not have "leaders", or "voices", or a "spokesperson"…"

*Anonymous* is open to everyone:

"…Anonymous is an idea. Anyone even a pimply faced sore loser can be Anonymous… Deal with it."

*Anonymous* echoes society's needs; as people's needs change, *Anonymous* changes as well:

"Anonymous isn't a movement. Anonymous is involved in activism because there is a need for activism not because activism is the nature of Anonymous."

Members of *Anonymous* as free individuals:

"…Anonymous does not have a clear definition or a goal. And it shouldn't have one. The whole point of Anonymous is that it's whatever people make of it, trying to define it defeats the whole point. Each structure has its advantaged and disadvantages, and while the disadvantage of Anonymous is that it's hard to understand for people, the advantage is that it allows total freedom to those involved in it."

Everyone has the right to maintain their individuality:

"To be truly Anonymous… is to be yourself."

*Anonymous* as a non-traditional group:

"…The notion that 'a group of people needs a goal' is one that applies to traditional groups and is commonly accepted as 'true' – but there is, in

47

fact, nothing that logically requires this to be true the case for a name to be commonly used" (Anonnews.org 2013).

In short, *Anonymous* is using the metaphor of an idea to empower its members. *Anonymous* has emerged as a loose collective fighting against corrupt governments and corporations. Most people would likely agree that these can be quite powerful enemies. Many people associated with the group have been, and currently are, under surveillance, or even worse – arrested and prosecuted. As a group, fighting for a noble, yet difficult cause, *Anonymous* must send a powerful message to its members. One of the ways of doing so is to present the group as an idea – ideas, after all, cannot be hurt or killed, they can only be spread. Ideas are also fluid: members of the group are granted complete freedom to do as they please, and open discussions are always welcomed on the forums.

*Anonymous* as an idea also echoes Anons' views on typical organizational bureaucracy. In most formal groups or organizations, people are expected to comply by rules and respect hierarchy; people in bureaucratic organizations can also often lose sight of what is important. It is also common that people have to follow the 'politics' of the group/organization they belong to, which may eventually lead to people losing their individuality or shifting their views in a direction they did not predict in the first place. It appears as if *Anonymous* want to reject the notion of a group (or organization) altogether, because they associate  the word 'group' with bureaucracies, or, more specifically, corrupt governments and organizations: the very things they are fighting against. Groups and organizations can fall into crisis or lose core members essential to their well-being. If *Anonymous* is just an idea, it cannot be affected by hierarchies or the loss of its members. Clearly, *Anonymous* opposes hierarchies and the notion that some people may carry more importance than others. Many Anons wrote on the forum about their hatred of hierarchies

– hierarchies, in the view of many *Anons*, create inequality, another thing they are fighting against. If the group has no hierarchy and no one holds ultimate power, then the group cannot suffer from corruption or cannot destroy itself from within. Presenting the group as an idea symbolizes equality and the absence of hierarchy.

*Anonymous* is a fluid organization: just like an idea, *Anonymous* can shift or change; members are granted complete freedom and/or creativity. Unlike groups, whose members often have to come through a series of steps to join or leave, members of Anonymous are free of such rules. It seems like presenting *Anonymous* as an idea, which has no leadership or rules, makes it more attractive for new people to join. People can not only join and leave as they please, but also have the power of interpreting existing idea in their own way. Such freedom and openness of the group allows for a lower barrier to entry for new members. Anonymous makes the process of recruitment less complicated.

Lastly, *Anonymous* as just an idea means that it does not exist or has ever existed as a tangible group, which is a belief that many Anons are happy to have others hold. Many people on the forum stated that they were not sure whether *Anonymous* still exited. Other claimed that *Anonymous* has changed and/or split into different subgroups, and it is not the same group anymore. One may argue that Anons use this notion to confuse the public. Indeed, as one person on the forum stated, it is hard to understand *Anonymous*. If people cannot gain an understanding of how *Anonymous* operates specifically, then there is less chance that any members can be caught.

In sum, *Anonymous* does represent a group in the sense that they share similar views and beliefs, for the most part, and occasionally gather for the purpose of a protest, hack, etc. On the other hand, *Anonymous* members do not view themselves as a group.

Since *Anonymous*' members strongly oppose many qualities inherent in traditional groups and organizations, they choose to view themselves as an idea that has no identity, hierarchy, leadership, or rules. Anyone can be *Anonymous* and no one is *Anonymous* at the same time.

### Anonymous as a Force for Good

Another repeating theme I have discovered on the forum was that members repeatedly claimed they believed *Anonymous*, as a collective, carries an important weight in people's lives both in the United States and across the world because it represents 'a force for good.' This is a major function of *Anonymous*, according to many people posting on the forums. Besides being a force for good, *Anonymous* symbolizes humanity and people themselves:

> "Anonymous is an embodiment of humanity, with no remorse, or emotion…"

> "…Anonymous is for better world, the betterment of all human beings."

> "If you are wondering whether you should be afraid of Anonymous, ask yourself: should I be afraid of humanity?"

> "Anonymous is about preserving the liberties and freedoms of humanity, regardless of race, color, religion, political views. It is about bettering society, and ousting corruption from seats of power…"

> "…I believe that we are force for good, and most definitely one to be reckoned with. We live in a time where the future of mankind can literally be changed by turning a key and pushing a button, the stakes have never been greater" (Anonnews.org 2013).

Anons claimed repeatedly that they are representing people in what they are doing, and that their primary duty is to make the world a better place. One member of the forum expanded a little bit more on his/her experience of being a part of *Anonymous*:

"Being a part of anonymous is a wonderful experience that takes a lot of dedication, care, and love of the freedom we have a right to have. It has risks and it is worth it watching

the world change one person or server at a time" (Anonnews.org 2013).  While some

members claimed that the risks of being a member of *Anonymous* are worth it, others

stated that *Anonymous*, as a collective, has no choice but to protect people's liberties,

regardless of the risks:

> "Anonymous exists because the world is in trouble. The United States,
> supposedly the "land of the free" is more accurately described as a
> surveillance state. Some would say a police state. The freedoms the people
> once had are gone, the government runs the world, and the corporations
> run the government. Corruption is rampant, and people are doing nothing.
> Hence, those that see the problem and want to do something, those who
> feel that freedom is worth fighting for, became known as Anonymous…"
> (Anonnews.org 2013).

> Protecting freedoms and liberties is one of the most frequently mentioned issues

on the message boards, when people discussed why the group had to continue to exist.

Many people on the forums claimed that defending the freedom of people and/or freedom

of information represents one of the most essential goals of *Anonymous*, on which most

Anons agree upon:

> "…the core values and principles of what we stand for: Life. Liberty. And
> the Pursuit of Happiness. No matter how many quotes I hear, that one is
> the one that still rings true to me as being the ultimate goal for a group of
> people… You may interpret it a little differently, but the meaning remains
> the same. People as well as information, need to be free."

> "…we can at least agree on a few simple broad goals, for example:
> Freedom of speech and information, supporting human rights for EVERY
> living being on the planet, etc. that will give us enough structure to band
> together without giving up that which makes us strong" (Anonnews.org
> 2013).

> Some group members also stated that *Anonymous* has the responsibility to protect

the freedoms all of individuals both online and in real life. Many people on the forums, in

fact, stated that Anons' activities are not, nor should they be, limited to the Internet only,

but should rather expand beyond World Wide Web to traditional street activism:

"[Our rights and responsibilities are] to defend our, and everyone's basic need and rights. To defend freedom, both in the online realm and outside of the internet. To take matters into our own hands when the system fails to serve proper justice."

"Our responsibilities are to remain an active part of said government. We need to have our voices heard in the decisions being made. We also need to keep those in power from taking our rights, which we have failed time and again to do."

"…Working to preserve out liberties… that is the essence of Anonymous today."

"…We are here to be the protection of freedom that everyone needs. Not to go far with this understand, but we could be considered everyday heroes of the homefront."

*Anonymous* has been long known for their participation in the Occupy Wall Street protests (Knafo 2011; Kazmi 2011); so their existence is not tied to purely digital activism and hacktivism. Members of the group often defined *Anonymous* as an opportunity, which can be used by anyone who wants to be creative and/or want to help in the fight for the 'good cause.' Some Anons seemed to be comfortable with just writing on message boards or participating in other online activities, while others felt much stronger about going to the street and joining traditional protesters. In short, members of *Anonymous* seemed to be approving of both online and real life involvement, whichever each member felt most comfortable with. Anons simple presented the group as an opportunity:

"…Anonymous is opportunity to do something if you are willing to roll up your sleeves."

"…Want to attend a protest? Why not organize one? This site is the perfect place to organize protests. I urge anybody incapable of being a hacktivist to either organize or sign onto protests on this site and be a good old fashioned street activist."

"…Anonymous provides a community and a way to become involved in societal change without the need to put yourself in danger of being targeted personally" (Anonnews.org 2013).

In sum, many Anons on the forum viewed/presented *Anonymous* as an open community, which is oriented towards positive change in societies around the world; *Anonymous* is open for all people, members claimed, as long as one is willing to take a stand or make a difference. In which way is completely up to the individual. *Anonymous*, in many members' views, is an opportunity to do something good in the world. *Anonymous* as a community exists in both the real world and online, and therefore provides numerous opportunities to become involved for each individual. If someone wants to help on behalf of *Anonymous*, they have a choice of how they want to help. Clearly, *Anonymous* represents a group with diverse membership and diverse ways of accomplishing their high priority goals. Most Anons see the major goals of the group to be fighting for justice and freedom; but each individual is free to interpret this in their own way.

### Anonymous as a Hacktivist Group

One of the themes I discovered on the forums in regard to the hacking activities of the group is that *Anonymous,* as a loose collective, does not consist of mostly hacktivists or hackers. Many people on the message board, in fact, claimed that the majority of *Anonymous'* members are just 'regular folks' who are not technologically savvy. Many members claimed that despite the common view of *Anonymous* as 'evil hackers,' many people who actually associate themselves with the group prefer to help in other ways, separate from hacking or becoming involved in any other illegal activities. Some members even became upset over others calling *Anonymous* a hacktivist group. Many of them felt that labeling *Anonymous* as simply a hacktivist group is non-inclusive of other members. Many on the forums stated that the group represents much more than just a group of hackers; in fact, advanced hackers, hacktivists, or just technologically capable

53

people, represent just a small portion of *Anonymous*. Many on the forum felt that it was

simply not right to call *Anonymous* a group of hacktivists, since such a definition would

unavoidably exclude the contributions made by the members who are not tech-capable.

This is what some people said in regards to hacktivism within *Anonymous*:

"You do not have to be a hacker to help Anonymous…"

"The point of Anon is to gather minds of such capabilities that can help in
each of their own ways…"

"…I am no hacker and my efforts are rarely online. I must do most of
what I do in the real world…"

"Anonymous isn't all about hacking into computer databases… For the
most part, anonymous as a whole lot of people who just talk casually
about how bad things are, give links to proof, and tell others."

"It's disappointing when someone believes "Anonymous" are hackers.
We're a group of [activists], freedom fighters, Not hackers…"

"Anonymous… covers a huge variety of small groups or individuals with ideas
and goals of their own. The vast majority of anons are not hackers, we are
ordinary people with a hunger to do something good, something meaningful."

"…The media paints Anonymous as a group of "elite hackers" that are out
to cause chaos. That could not be further from the truth. Yes, there are
some people in Anonymous that "hack", but that is actually a relatively
small group… Walk down the street, take not of every fifth person. That's
what Anonymous looks like."

"…Anonymous  is not a hacking elite, it's a movement, a belief, a vision a
way as a collective to say no to those who abuse our trust and those who
abuse others. Anonymous just is" (Anonnews.org 2013).

Some members on the forums argued that *Anonymous* is split into two major

groups: original members, or the hacktivists, and current (and more recent) members,

also known as supporters. While such a grasp of the group may be partially correct, in the

sense that *Anonymous'* members can be identified as either hackers and/or tech-savvy

members, or as people who contribute to the group's activities through other (non-

computer related) means, such a definition also implies that some members (specifically, the hackers) are superior to the members who lack such skills. Many people on the message boards became upset over such a definition. They claimed that, within the group, each member is equal and that there are no 'original' or 'current' members – all Anons are absolutely equal in all respects. In sum, many people, while agreeing that *Anonymous* can generally be divided into hackers and non-hackers, have rejected the definition of members who do not possess any hacking skills as 'supporters.' The word 'supporters', in their view, implies that they merely provide support to the members who hack. Most people on the forums have agreed that Anons who have helped the group through traditional activism or other, non-illegal means are just as valuable as those who operate (legally or illegally) online. One member on the forums expanded on why some people tend to categorize *Anonymous* into hackers and non-hackers, as well as on some of the origins of the group:

> "…Anonymous doesn't have a "original hacktivist group" and a "support group', it's all one group. Anonymous originated as a group that caused trouble and generally trolled people and raised hell. Then they started getting into political issues, and became an activist organization. At that point, there were a small amount of people who decided to do simple "hacktivist" activities such as DDoSing the Church of Scientology's website and other shit like that. The real "hacking" started with LulSec which was a group of six Anonymous members who went and generally raised hell for the establishment through hacking all their computers. That was when the media started really covering Anonymous, hence why everyone thinks it's a "hacking group"… If you fight for justice and do what you can to stop and protest unfair laws etc… you are Anonymous. That's what Anonymous is. The "hacktivist" is just a small percentage, but they are no different from you and I" (Anonnews.org 2013).

Clearly, the majority of people who responded on the forums supported the notion of equality for all members, regardless of their technical skills. Along with equality, another common theme on the forum was that many claimed they were 'common' people

anyone can meet in real life, or that they are not different from any 'regular' person: "…You are a person like everyone else here we are equal" (Anonnews.org 2013).

Members of *Anonymous* on the forum clearly showed that they stand for equal status and opportunities for everyone who wants to associate himself/herself with the name of group. Along with this, forum members showed openness and respect to the fact that different members of *Anonymous* may hold various views and beliefs. Many stated that one's opinions and beliefs do not have to be the same as other people's; as long as they can agree on broad goals (i.e., fighting for the freedom of people and/or information) and contributes in any way he/she can, it is okay to believe in anything one wants to believe. As an Anon stated: "…We have everyone from anarcho-communists to the ultra-conservative gun nuts here. People can espouse their beliefs if they want… We all have our own beliefs but at the end of the day we all agree on one thing; we are being lied to" (Anonnews.org 2013). Another member stated being all-inclusive represents an essence of the group because *Anonymous* cannot risk losing voices; any voice is essential to fighting for the cause the group's members have identified among themselves: being supportive of every members' beliefs and views "…has allowed us to grow in numbers and be all-inclusive, every voice counts, every ideal which is a worthy goal fits within our umbrella" (Anonnews.org 2013). This leads to the following theme: *Anonymous* representing a leaderless or structureless organization.

**Group's Structure and Functioning**

*Anonymous as a Leaderless Group*

Members on the forum almost unanimously claimed that *Anonymous* as a group does not have any leaders or hierarchy. I did not find any opinions among the people on the forums that would oppose this view of the group. In this respect, it is possible to say

that representation of *Anonymous* as a leaderless group has a high approval among

members or that members want others to see the group as such. Many people on the

message board stated that *Anonymous* does not represent a group at all, or at least does

not represent a traditional group for this specific reason – traditional groups and

organizations typically have hierarchies and leaders. An overwhelming amount of people

on the message board have supported the notion that *Anonymous* being a leaderless group

represents one of their largest strengths: all members are viewed as equally important,

which both appeals to and inspires already existing and future members of *Anonymous*.

Many people who claimed to be associated with *Anonymous* stated they strongly believed

in the freedoms and liberties of all human beings; for that reason, they also believed that

*Anonymous* should never have leaders or value some members above others:

> "Anonymous is a decentralized group no one tells people of anonymous to do anything. We have free will and diced on an individual basis what we should or should not do."

> "We don't have a leader. A movement against authority without authority drives authority insane; they can't break down a movement by corrupting the leader…"

> "Anonymous has no leaders; we will still be stronger than ever."

> "…Anonymous is a hydra, cut off the head and we will grow two back."

> "…Anonymous does not consist of any leaders, or dictators present among any specific group. No one can harm us because we're invisible. Join us."

> "…We have no leaders, no hierarchy. We are just ordinary people trying to make the world a better place in whatever way we can…"

> "[Anonymous are] an accidental collectivism made up of detached individuals, resembling a highly organized conspiracy and lacking a deliberate origin."

> "Anonymous DOES NOT HAVE LEADERS. That defeats the purpose… Anonymous has and never will have a leader… When you power in to one person hand or a few, this is [where we get a problem]."

"…Imagine for a moment that we have a leader, or group of leaders and then those people are hunted down and taken from us. What happens to Anonymous then? We would be lost, fragmented, and other individuals with agendas of their own (which may be different from ours) would begin campaigning to replace those leaders. We will have reinvented politics and will end up with the same self serving mess that we have in government already."

"…the greatest strength of Anonymous is the fact there is no leadership, no matter who gets arrested… Anonymous as a whole cannot be damaged or compromised, or stopped… We need that invulnerability to succeed."
 (Anonnews.org 2013).

Many people on the forum associated hierarchies with restraints and the censoring of individuals. Others viewed hierarchies as a danger to human individuality (since hierarchies typically value some members more than others, depending on a person's location within the hierarchy). Moreover, many on the forum tended to associate hierarchies with government and bureaucracies. Governments and bureaucracies (as well as the corruption that oftentimes stems from them) are things that many members stated they view as 'evil' or 'wrong', since they impose danger on humans' individuality and freedoms:

"No government has the right to impose censorship on any human being, we are all equal and should be treated as such…"

"Governments believe that it has the right to tell you what you are allowed to see, hear or create. We find this insulting to our individuality as human being. We fully support freedom of expression for all whether we agree with them or not."

"As a member of Anonymous, I am thoroughly disgusted. What you are doing is the classic example of tyranny, the very concept we fight against. You claiming to be the leader of anonymous is not only insulting to the current members, but you also spit on the graves of the members who died in prison because of their dedication. If this is simple trolling, I implore you to cease and desist immediately, before it's too late" (Anonnews.org 2013).

In sum, *Anonymous* being a leaderless group serves a few purposes: a) being leaderless provides members of the group with better protection from the authorities by simply confusing them (it is practically impossible to identify who is/was in charge of a protest, attack, etc.); b) a leaderless *Anonymous* means there is an endless supply of members and contributors who are considered equal among each other – regardless of who leaves the group or is arrested, there will be other members who can replace those ones that have left; c) lack of hierarchy empowers members by sending a message that everyone is unique and valuable, and that all contributions, regardless of how big or small, are equally important; d) being leaderless makes *Anonymous* a collective that is (theoretically) balanced and uncorrupted from within – nothing, as one member said, can corrupt *Anonymous* from within since there are no leaders who could take advantage of their power; e) the absence of leaders grants complete freedom and creativity to members of the group, meaning no one can control what members think or believe in; and, lastly, f) being leaderless symbolizes the group's rejection/opposition of corrupted authority, government, or bureaucracy, all of which tend to have rigid rules and/or hierarchies and which attempt, in any way, to censor or limit individuals.

### *How to Join Anonymous?*

The opinions of members in regard to the membership of the group, or how to join or quit *Anonymous*, correspond with a video *Anonymous* published on YouTube (Figure 9). The video provides a valuable insight into membership, as well as how the group functions in general: for example, how members can identify each other and what measures should be taken to ensure each other's online safety. The video content is similar, almost down to the point, with what people on the forums have stated when they talked about *Anonymous'* structure and functioning.
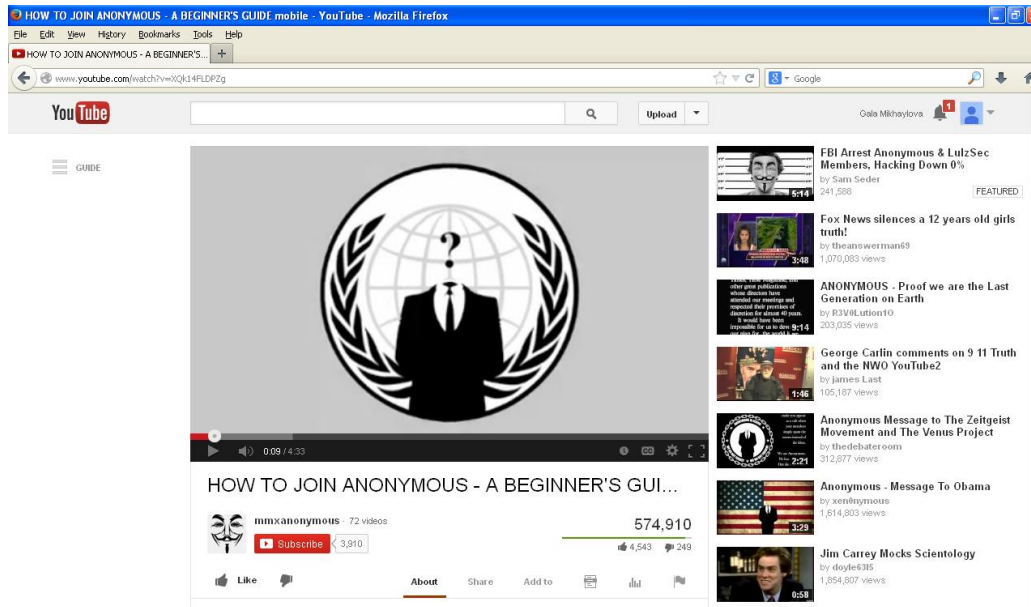
**Figure 9.** *Anonymous'* **video on how to join the group, published on YouTube.com**
**(http://www.youtube.com/watch?v=XQk14FLDPZg).**

The anonymous voice in the video states:

"You can not join Anonymous. Nobody can join Anonymous.
Anonymous is not an organization. It is not a club, a party or even a
movement. There is no charter, no manifest, no membership fees.
Anonymous has no leaders, no gurus, no ideologists. In fact, it does not
even have a fixed ideology" (Anonymous 2010).

People on the forum seemed to generally support this notion of membership. Just

like many *Anonymous* members rejected the idea of a hierarchy or leadership, they also

showed their dislike for the idea of rules for entering or leaving the group. Most people

on the message boards claimed that in order to join *Anonymous*, one simply needs to

accept loose 'goals' the members have generally agreed upon. Many noted that

*Anonymous* as a loose collective does not deny membership to anyone. Anyone who

wishes to be a part of the group can do so:

"…there is no structure to [Anonymous] at all and by extension no real
requirements to "being a member" of the group. Anyone really could say
they're part of it really."

"…joining anonymous is as easy as simply wishing to join. Want to join? Congratulations. You are now a member. That's it. you don't need to be a superhacker, you just need to help... those of you who deny the right of other joining anonymous have absolutely no right, nor authority to do so. Anyone claiming any sort of position in power in anonymous is lying. There is no ranking system. There are no leaders."

"You obviously haven't read up enough on Anonymous, to join is to simply decide if you believe in the idea and the movement, you are already a part of it" (Anonnews.org 2013).

Most people on the message board seemed to agree that *Anonymous* does not have, nor should have, rules or guidelines at all. Any rules or guidelines, in the opinions of the forum members, are restricting and/or unnecessary. People often commented: "…you don't need how-to guides. Just be active in the Anonymous community. Express your opinions on different suggested operations, and… join some protests" (Anonnews.org 2013). It appeared as if people on the forum believed that the process of joining is not needed because it would just take up the time people could otherwise spend contributing to the groups' goals and activities. Other stated that lack of rules and norms within *Anonymous* is essential to group's functioning and survival. Some people stated, for instance, that free exchange of information/collaboration among members would not be possible if any sort of rules were in place:

"…[Anonymous] is not an organisation, it does not ask you for proof of identity. It` is just a label given to a network of people who have started talking secretly with each other out of earshot of the oppressors. People who want justice served and life to be worth living again. a label that allows us to find each other and know that we are on a similar page and believe in similar ideal. It gives us the ability to exchange knowledge freely and without worry that our identities will be compromised, brining the wrath of the big brother upon us. We should not be afraid of our leaders, but we are, and with good cause. If we expect to fight them, we need to come together. that is what anonymous is, simply a name to type into a search box, that allows us to find each other" (Anonnews.org 2013).

So, similarly to the idea of a leaderless organization, the idea of having no rules or proof of identity provides members with better online 'security' (i.e., it is harder to track or identify members because everyone acts 'freely' in regard to joining or leaving the group), as well as an opportunity to communicate openly. Removing rigid rules and codes makes *Anonymous* more attractive to potential future members. The absence of rules or codes also symbolizes the group's values: values such as a belief that human beings' individuality and creativity should be embraced and that organizations/groups should not mark people as insiders or outsiders, since everyone is created equal.

### *How Members of Anonymous Organize?*

The literature that exists on *Anonymous* does not provide a clear answer in regards to how the group's members organize/connect with each other. The message board, on which communication between many *Anonymous* members takes place, did not provide an explicit answer to this question, either. However, after reading numerous posts, I began to believe a few methods exist which members can use in order to connect with each other.

A number of people on the forum stated that it may be at times quite hard for the members to organize. Some of these difficulties occur due to the fact *Anonymous* as a group does not seem to have any official rules/codes/guidelines – in fact, many members expressed frustration when others asked what rules they should follow. A lack of rules or codes, indeed, may be confusing to many. Many people on the forum stated that different members found different ways of getting in touch with each other, depending on which ones they found most convenient and practical. While some stated that they preferred private communication, or communication 'behind the scene' (private emailing or messaging members they wished to communicate with), others stated that the safest and most common way for members to connect with each other is to post their opinions

and/or comments under the forum section for each operation. The website
(www.Anonnews.org) has a section where future 'operations' (i.e. actions the group is
planning to undertake) are posted and discussed. Most operation names start with
"#Op[Name of Operation]."
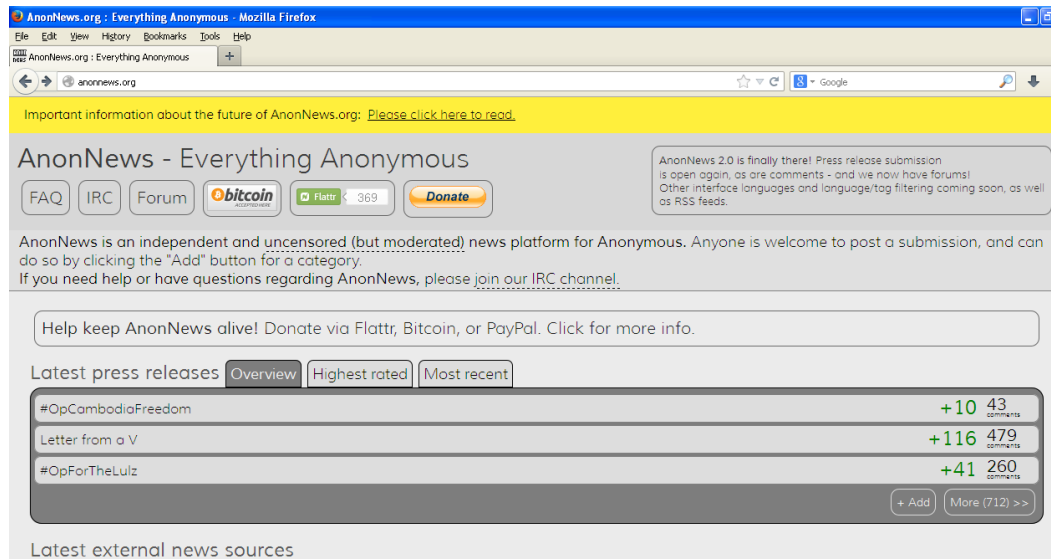


**Figure 10. The section of Anonnews.org, where future 'operations' are posted and
discussed. This section of the website is also known as 'Latest Press Releases.'**

Some members stated that agreement among members is often achieved when
people start posting responses under each of the operations in the 'Latest Press Releases'
section of the website. When people responding to each thread find agreement, then
*Anonymous* as a group can be considered to reach a final decision on an issue or topic.
One person on the message board stated: "…Anonymous is kind of water. You mix
something in it, water now holds that thing in itself… when many anons agree for
something, [it] becomes agreed by anonymous" (Anonnews.org 2013). Others stated
similar opinion: the consensus and decision making within *Anonymous* is often reached
similarly to the ways it is done in modern democracies – through a majority vote, or
when a majority of members share similar views on an issue. When a large portion of

people associating themselves with the group widely agree on something, it becomes possible to say that *Anonymous* as a group has reached a decision or agreement. Each operation in the 'Latest Press Releases' section typically opens by stating what the issue/problem is; then a tentative course of action is proposed. Members typically respond under each 'operation' post stating what they like or dislike. It may be argued that if the majority of people responding under each 'operation' find agreement, the group as a whole may be considered organized for action or is ready to take steps beyond discussing the topic.

Even though many people on the forums claim that complete consensus is practically impossible to achieve within *Anonymous*, because it is so fragmented and lacks a governing body, sometimes a democratic process may occur. One member said:

> "…Anonymous is not a democracy and asking for Anons to gather consensus very clearly shows a lack of understanding as to how Anonymous works. If anything, Anonymous can be considered anarchist (according to the real definition, not the burn-everything-to-shit definition that media tends to use), as there is no governing body and Anonymous-wide decisions cannot be made, not even through consensus. It is only within individual operations, networks, and cells, that a democratic body often exists…" (Anonnews.org 2013).

It appears that *Anonymous* may be too diverse and large for the group to reach unanimous agreement. As I stated before, *Anonymous* most certainly represents a fragmented group, which makes organizing difficult for it members at times. However, as the member above stated, organization among members can be achieved through personal initiative – i.e., when someone posts/proposes an 'operation' on the website. If an operation, originally initiated by one individual or a small group of members, becomes accepted by many other members, then those people may organize and indeed act together in order to solve a problem. Some members on the forum stated that despite a

64

lack of a governing body within *Anonymous* and the difficulties that stem from it,

members are nevertheless capable of agreeing with each other and act together to achieve

common goals:

> "…[the current Anonymous are] a loose collection of individuals, who are able to decide on a goal, gather people who agree with us and act on that goal without having to wade through some bureaucratic leadership structure to accomplish anything is a stroke of genius. I say we must remain true to that vision which has allowed us to grow in numbers and be all-inclusive, every voice counts, every ideal which is a worthy goal fits within our umbrella" (Anonnews.org 2013).

The video on how to join *Anonymous*, which the group has published on

YouTube, also sheds light on how members of the group may communicate and/or

connect with each other. The video states:

> "How to get in contact with others?
>
> Anonymous has no centralized infrastructure. We use existing facilities of the Internet, especially social networks, and we are ready to hop on to the next one if this one seems compromised, is under attack, or starts to bore us.
>
> At the time of this writing, Facebook, Twitter and the IRC appear to host the most active congregations. But this may change at any time. Still, these are probably the best places to get started. Look for terms like "anonymous", "anonops" and other keywords that might be connected to our activities.
>
> … Many of us like to wear Guy Fawkes masks on demonstrations. Some of us even show them in their profile pictures in social networks. That helps to recognize each other." (Anonymous 2010).

It appears as if the group's members currently prefer social networks like

Facebook and Twitter to communicate with each other. It comes as no surprise, since

social networking sites are widely popular, and nearly everyone already has an account

registered on some of them. The video clearly recommends that current and the future

members search the web by entering the group name, or words and slogans associated

with the group, into search engines. It seems that there are no clear-cut ways of engaging

in conversation with *Anonymous* members, but there are rather vague guidelines, like

searching the web or trying to explore social networks. Members can recognize each

other by profile pictures: an overwhelming amount of the group's members use a picture

portraying a person wearing a Guy Fawkes mask, similar to the one below (Figure 11).



**Figure 11. Guy Fawkes mask**

In sum, *Anonymous'* members have a variety of ways to get in touch with each

other and/or organize – social networks, numerous *Anonymous* websites, IRC chat rooms,

forums, and so on. As with the other aspects of the groups' public life, there are no

clearly defined rules which tell members how to find each other and interact. Social

networks, websites, IRC chat rooms, and discussion boards seem to be viewed as the

most efficient and quick methods at the moment, but this may change in the future as the

group finds other, more appropriate or convenient methods. The group's communication

is fluid and creative: members are given total freedom and creativity when it comes to

how they want to get connected with other members. And *Anonymous* as a whole seems

to be satisfied with such an arrangement.

*Anonymous: What are Their Goals?*

As previously stated, *Anonymous* does not have any rules set in stone. The same can be applied to the goals of *Anonymous*: as the group evolves and changes, its goals are shifting and changing, as well. However, some of the group's broad goals, which a vast majority of members seem to currently agree upon, can be identified. By examining members' communication on the forum, in terms of their perception of the group's major goals, and some repeating themes become apparent.

I have separated the group's goals into four major groups: general goals; civil and political matters; education and awareness; and information and privacy (Table 1). I grouped the goals in a left to right order: from more general goals (left) to more specific goals (middle and right). The goals are not grouped based on their importance, *Anonymous* members seem to disagree on which goals are more or less important; each member of the group typically has his or her own opinion on which goals have more importance. Regardless of this, most on the forums seem to agree that each goal outlined below represents goal of the *Anonymous*.

**Table 1. The goals of *Anonymous* based on forum responses**

| GENERAL GOALS | CIVIL & POLITICAL GOALS | EDUCATION & AWARENESS GOALS | INOFRMATION & PRIVACY GOALS |
|---|---|---|---|
| -Making a positive change in the world<br><br>-Standing up to what is wrong/being force for good<br><br>-Being | -Standing up to oppressors/fighting against authorities<br><br>-Fighting against corruption<br><br>-Protecting and preserving all people's liberties and | -Bringing clarity to world's issues and problems<br><br>-Educating yourself and others<br><br>-Spreading knowledge and information/spreading | - Protecting freedom of information<br><br>-Standing up for Internet rights/being the 'unofficial watchmen of the Internet' |

| active/activism | freedoms (the Bill of Rights)<br><br>-Fighting injustices/fighting for justice for all people<br><br>-Instilling sense of collectivism and interdependence<br><br>-Being politically active | awareness about the world's issues and problems<br><br>-Discussing world's issues and problems | -Protecting privacy of all individuals<br><br>-Fighting against censorship |
| --- | --- | --- | --- |

The most general goal of *Anonymous*, as many forum members stated, is just being a force for good in the world. Many Anons stated that they believe every member should make an attempt to contribute to a positive change in the world, regardless of how small or large this contribution may be:

> "…Anonymous is for a better world, the betterment of all human beings."

> "…Anonymous provides a community and a way to become involved in societal change without the need to put yourself in danger of being targeted personally."

> "To be truly Anonymous… is to be yourself. To be a role-model. To be a [revolutionary] [meaning: a person who upholds, changes, makes a revolution regardless of how big or small. It could be even a change of character!...and to uphold the values of harmony, independency and responsibility of your decisions and actions… Take up any role, be it the lowest or the highest, take pleasure in what you do, because it is the worst not to try, and not to care, and not to understand."

Many members saw *Anonymous* as an opportunity to do something good, and what constitutes 'good' is for every individual to decide. Many Anons stated that being active is core to the group, regardless of one's technical abilities. Everyone, according to *Anonymous* members on the message boards, can contribute. Many also stated that even the smallest contribution toward positive change in the world is better than inaction.

While many Anons said the group's main goal is to bring positive change in the world, many others stated more specific goals. Political and civil matters seemed to preoccupy a large portion of the forum members. Many identified major goals as standing up to oppressors; or more specifically, governments and corporations. *Anonymous* members seem to share a belief that these two constitute major oppressors in the U.S. and worldwide. Some of the members stated the following:

> "…Anonymous is not about sabotaging things… For me, it is about standing up to our true oppressors and securing our own freedoms against those who would limit them for the own reasons…"

> "Our responsibilities are to remain an active part of said government. We need to have our voices heard in the decisions being made. We also need to keep those in power from taking our rights, which we have failed time and again to do. In the Constitution it expressly states that if the government oversteps their bounds, it is illegitimate and it is the right and DUTY of the people to abolish it and re-instate it. We are currently past that point, and something needs to be fixed."

> "[Anonymous takes interest in] basically everything the government has done in the past 100 years. There have been so many breaches of our rights as people that I couldn't possibly outline them here, but it's most definitely accelerated since… 9/11... now we have the PATRIOT Act, warrant-less wiretaps, DHS, TSA, Obamacare, the NDAA, indefinite detention, secret arrests, torture, execution of sovereign citizens on American soil, drones, domestic drone use, domestic drone hits, etc… The list goes on. These are all infractions of our rights, and under constitutional law, as a citizen I/you/we all have the DUTY to stop it. Any one of those things on the list is grounds for impeachment and some for life-long imprisonment for high treason… We need to stand up."

> "[Anonymous] is about bettering society, and ousting corruption from seats of power" (Anonnews.org 2013).

Many members of *Anonymous* emphasized the importance of being politically engaged and active. Most political conversation on the forums, however, were dedicated to issues and problems within the United States, which led me to believe that *Anonymous* has a very strong member base in America.

Many individuals on the forum stated that defending freedoms and liberties of all

human beings represents a major goal for *Anonymous*; many individuals cited the

Constitution and the Bill of Rights when talking about defining the goal(s) of the

group. While some Anons disagreed about what constitutes the main goal of the

group, a vast majority of members agreed that fighting for the liberties and

freedoms of all people indeed represents one of the most important goals of

*Anonymous*. An overwhelming amount of members shared the belief that

governments and corporations represent the biggest threat to human liberties

around the globe. Many Anons clearly stated that they saw governments and

corporations as major opponents and/or oppressors of people's rights in the world.

While some members of the forums focused on political problems and

issues at large, some other members pointed out that *Anonynous* as a group should

rather focus on uniting people. One member stated:

> "[Our moral goal] is undoing moral individualism and instilling a sense of collectivism. Objectives = solidarity amongst all people and undoing the theft of surplus labour value that is capitalism…"

> "We must not fight amongst ourselves, we must maintain the freedom of the individual. The only things worth fighting against are oppression, hatred, fear, violence, slavery in any form, and anything which divides us or makes some more important or valuable than others. Let our goal be to care as much for the most impoverished child in Ethiopia as we do for our immediate family, because he/she IS our family. We are one, we are all equal, and everyone counts…" (Anonnews.org 2013).

People on the forums who stated that the group's goal should be promoting

solidarity and the idea of people working together as one made up a minority on the

message board. Most members of *Anonymous* preferred to focus on large-scale politics,

discussing current politics or government-related problems and issues. Conversations

about authorities' violating human rights and freedoms, based on my observations, had a rather general character – people mostly discussed how bad government/corporations are without providing specific examples. In some cases, members of the forums made references to laws such as the Patriot Act and NDAA Indefinite Detention bill, and more rarely to international or other countries' laws, which also led me to believe that *Anonymous* as a group may be especially focused on political issues in the United States. Some members discussed how governments and corporations should be regulated and what governments should improve on. Some members made remarks like the following: "…Every man, woman and child should [be able to afford] the most basic of needs. This includes medical, housing, food and education. Investing in the youth of the world is the single most important task of any intellectual society" (Anonnews.org 2013).

Some other politically-related discussions on the forum were dedicated to activism and the importance of just 'being involved.' Many *Anonymous* members, instead of discussing government-related issues and problems, rather emphasized the importance of being civilly and politically active. Some Anons stated that people should take a strong interest, as well as act, in regard to political and state matters, which is what constitutes a citizen:

> "What role does anybody plays in society? We are a group of people working from every country, in every locale, in every language, religion, color, ethnic background for a common purpose. We live to better the world in the end, and act through whatever means that individuals deems appropriate…"

> "… being a patriot is a loose definition of what Anonymous is all about. Not necessarily an American Patriot, but a global patriot, one who believes in those unalienable rights of humanity that we so desperately need to protect…"

71

"A citizen is one who lives under the constitution… and follows what it states. A citizen is one who is active in the government, when something like NDAA or expansion of the PATRIOT act come up, they speak up about it. They will contact their senators and representatives to make sure the voice of the people is heard. A citizen is someone who will actively fight to protect and preserve our freedoms and liberties against all enemies, foreign and domestic" (Anonnews.org 2013).

Some members of the forum stated that they believed members of *Anonymous* are nothing but responsible citizens who try to actively protect people's rights and freedoms. Putting it differently, they simply claimed to be activists, either traditional or digital. Many emphasized that their main goal within *Anonymous* was just being active when it comes to government matters.

A large portion of people on the forums talked specifically about educating the masses as a way to stay active. They stated that they are staying active by educating others or by spreading important information through any means they have. Many members emphasized the importance of bringing about public awareness when it came to political matters; I have therefore concluded that education and awareness represent an important goal for a significant number of *Anonymous* members. Many individuals claimed that, contradictory to many people's opinion that *Anonymous* is about hacking or hacktivism, they saw their major goal as educating others, clearing up myths and misconceptions, as well as bringing about awareness of political problems and issues. Here is what some of the members on the message boards stated:

"…I am no hacker and my efforts are rarely online… And what do I do? I spread information, share questions. It really takes little more than that. It did not take long to see the people and world around me begin to seek out answers and then start sharing information and spreading their own questions."

"…I think anonymous' primary purpose thusfar has been to spread knowledge and awareness of a burning society… Those with a higher

purpose than spreading knowledge (like myself) began only after being exposed to so many strange truths we were never shown."

"My view of Anonymous is to draw attention to injustices so that the masses can see them for what they truly are."

"…The point is to get information out to the masses. Information that is really harmful to the ruling elite… Information [is] the cause of the last 40 years of US involvement in wars… The reason why more Americans aren't as pissed as they should be is because they are simply unaware."

"…I know nothing about hacking and can't do it, although I'd love to. Maybe some information given to a lot of people and not just through youtube postings can cause enough anger to get the proverbial ball rolling."

"It is important to educate the younger generation, as they have been raised to accept the controls applied to them; they have no knowledge or experience of what freedom is supposed to be like, as the older ones experienced. Educate them and help them to spread the word…"

"All of us can do something, if you are not a hacker (as many of us are not) you can still… spread the information as far and wide as possible. Share links to the projects, videos, and information as widely as you can, on every social network you are on. Email links to your friends, go to protests, counter-protests and demonstrations, make your voice heard… The most talented and knowledgeable hacker can do little without our support our voices raised, our standing together passionately supporting the cause of justice for all humanity" (Anonnews.org 2013).

Many members of *Anonymous* stated that they viewed spreading information just as important as the ability to hack. While hacking skills are highly valued within the *Anonymous* community and many people on the forum expressed an interest in learning how to hack, educating the public got just as much respect and attention from members of the group. Many people on the message board also conceptualized information as the most powerful weapon; many, for example, stated that misinformation or any type of misuse of information by the government led to problems. On the same note, many also viewed information as a solution or a 'weapon' that could be used by people in order to

solve problems within society. Many people on the forum said that they believed that spreading awareness about societal problems and issues can lead to peaceful revolution and/or change within a society. Overall, many people on the message board stated that they believed information is powerful and that people involved in bringing about awareness should be given equal respect as people who have hacking skills.

Other members also stated that being a part of *Anonymous* is just discussing problems and issues in real life and online. Many Anons stated that being a member of *Anonymous* simply means talking about problems and issues, no matter what one's beliefs are. One member stated: "For the most part, Anonymous is a whole lot of people who just talk casually about how bad things are [and] give links to proof…" (Anonnews.org 2013).

Lastly, a significant amount of members on the forum stated that they saw their major goal as protecting the freedom of information, and freedom of the Internet in particular. Among other goals, members also named protection of privacy and fighting against censorship in both real life and online realms. Some members stated the following:

> "…I believe our main goal is to free information and bring an end to censorship."

> "Of course the main underlying theme of Anon is freedom and privacy, more so freedom of the Internet and information. That in turn leads to helping those who are oppressed and keeping one's self from becoming in that position…"

> "…We are a collective of people who join the fight against internet censorship and privacy…" (Anonnews.org 2013).

Similar to some previously mentioned members who believed that information represents a powerful 'tool' or a 'weapon' that can be used in resolving societal problems

74

and issues, these members believed that because information is so powerful, it must be

protected. Many Anons stated they believed that oppression starts with censorship and

the regulation of sources of information. Sources such as news and the Internet should be

free of regulation and censorship, many stated. In sum, these members conceptualized

free information as a source of education, upon which liberation and freedoms depends.

### *Anonymous: Public Image & Perception*

Some discussions on the message boards build around *Anonymous'* public image or

reputation. While some members clearly stated that *Anonymous* should not be concerned

with its public image and that it does not need to be promoted in any way, other members

have also noted that the group's reputation has been damaged due to the fact that some

sub-groups within *Anonymous* have been involved in questionable activities, like

attempting to hack Facebook accounts. Some members of the group stated that because of

how *Anonymous* operates (the group does not have clear-cut rules or does not identify its

members) the group will be blamed for the actions of a few individuals committing 'bad

things' on behalf of the group. Because everyone can claim to be a part of *Anonymous*,

the group often has to take responsibility for actions it may not have been involved with.

One of the individuals on the forum has stated:

> "… It is always possible that some asshole will do something evil while
> using the name Anonymous, but there is really nothing we can do to
> prevent that unless we have the prior knowledge. Every living person has
> the right to use the name [of Anonymous]."

> "Anonymous' stereotypes and misconceptions are basically the same
> thing. The media paints Anonymous as a group of "elite hackers" that are
> out to cause chaos. That could not be further from the truth. Yes, there are
> some people in Anonymous that "hack", but that is actually a relatively
> small group. I believe that LulSec has a lot to do with that, as they
> were/are Anonymous members, but they were out hacking all the time,
> [just for the fun of it]. Then the media can spin what they were doing onto
> the whole group."

"…unfortunately, there will always be those who want to use [the name of Anonymous] to justify their own agendas. Selfish people who cause harm and hack computer systems for no purpose [than] to massage their own egos. These people are not anonymous…" (Anonnews.org 2013).

Many members stated that many people may take advantage of *Anonymous* or commit malicious actions on its behalf, but the group, or the majority of its members, cannot do anything to stop those individuals. Most members on the forums have agreed that this is a downside of being a part of *Anonymous*: while its members are granted a lot of freedom, they also are occasionally blamed by the media or random individuals for acts they did not commit. The majority of forum participants claimed that Anonymous only hacks when it is absolutely necessary or when there is a good cause that the majority of members have come to agree upon. Hacking, or any other malicious acts, are never justified without a good cause, many members of the forum have stated. Unfortunately, they stated, there will be always individuals with their own aims whose actions will be damaging to *Anonymous*' public image and/or reputation.

## Group's Values and Beliefs

### On Hacking and Security

As I read the forum content, I realized there is a pattern in terms of how forum members view hacking skills or hacking in general. The majority of responses about hacking were normally triggered by somebody posting a thread in which the thread initiator asked for help learning about hacking. The majority of responses to such threads were quite negative: many forum members responded by saying that hacking skills are very complicated and that someone, regardless of his/her abilities to learn, cannot learn hacking quickly; on the upside, hacking is a complicated, time-consuming process that can take years to comprehend. Learning hacking skills, forum members stated, requires a

lot of time, personal discipline, and independence – one must be able to learn to be self-reliant and do his/her own personal research, instead of asking others to teach him/her how to hack. Many people who responded to threads about hacking also emphasized that hacking is a powerful skill that only a few people have. They also often added that only a few deserve hacking skills, since it is a dangerous and powerful 'tool,' and that one has to be a very responsible individual to be trusted to hack, he/she should use hacking skills in only ethical, responsible ways. Here is what some of the individuals stated in regards to hacking:

> "…Hacking is not a game, it is not a lifestyle, it is a job… a dedication to something that one believes in. Hacking is serious stuff, so if you ask Anon how to hack so that [you can] go into [your] ex's [Facebook] account, then get the hell out. You don't belong."

> "There is no tool you can use, there is no one lesson to teach you how to hack. Hacking is something extremely complicated, it's not kid game. You must know HTML, Javascript, PHP and many other web languages to get feeling how website functions. Then, you have to learn a lot about computers [themselves] like signals, or cryptography. It's a way of living, not a one month tutorial lesson"
> (Anonnews.org 2013).

Many members of the forums made it very clear that hacking people's Facebook/Twitter profiles is completely against what the groups stands for.  Members of *Anonymous* stated that hacking should rather be used in rare cases, where traditional or digital activism fails, and a goal can only be achieved by more serious methods. Hacking, they stated, should be used for a good cause/reason, and never for malicious purposes, such as stealing money. Interestingly enough, some members stated that even though *Anonymous* as a whole opposes malicious hacking, some subgroups or individuals associating themselves with the group have committed malicious hacking in the past on behalf of the group. *Anonymous*, according to many, has taken hits to its reputation in the

past because of the few who chose to use their hacking skills irresponsibly or selfishly.

Many, however agreed that the majority of members of *Anonymous* believe in ethical

hacking. Many *Anonymous'* members went as far as defining hacking in their own way,

the way most group members understand it:

> "[Hacking] is the definition of acquiring information to help the masses
> and to keep dishonest people, companies and Government on their toes,
> [Anonymous] don't do it for malicious intent (although some have), but to
> help. [Hacking] takes years upon years of skill and hard work to
> understand code and the path it takes to lead you there. PLEASE stop with
> the stupid requests to be a hacker. PLEASE!"

> "… read [the rules] of this forum, clearly states 'Please don't post 'how to
> hack' topics anywhere, for those kinds of things there are sites like
> HackForums. there's a link for fools like you…" (Anonnews.org 2013).

Despite the fact that rules about requests to be taught hacking skills are posted on

the message boards (although some members may have not found or read them), an

overwhelming amount of messages were posted asking forum members to share their

hacking knowledge/skills. Most of the time, such requests were treated negatively; the

rules of the message boards indeed clearly prohibit such requests.

*Anonymous* members also clearly chose to re-define hacking. Traditionally, a

hacker has been defined as "a person who secretly gets access to a computer system in

order to get information [and] cause damage" (Merriam-Webster 2013). However,

*Anonymous* members chose to give hackers and hacking a rather positive connotation by

defining hacking as a set of computer skills used to break into computer systems. While

such access is clearly unauthorized, and hence illegal, it is only to be used for a good

cause, like exposing the truth(s) about a corporation/government/an individual that

*Anonymous* finds responsible for 'wrongdoings.' The majority of forum members stated

that hacking skills should be chosen to be used for a collective purpose, with which many

members agree; hacking should be never used for individual or private purposes. Hacking

for private purposes is what forums members saw/defined as malicious hacking:

> "Anonymous doesn't hack for personal reasons so please stop asking for information on how to hack accounts and so on, if you know anything about anonymous then you know we hack for a cause."

> "…Anonymous is not a school. That's not what WE stand for. WE are anonymous not a personal army for some idiot who thinks he can use us."

> "I am anonymous. To the people writing us wanting to be taught "how to hack:" There are a lot of un-gracious people on here who lack the articulation and finesse to explain the wise response, or perhaps they simply don't care to spell it out for you. Do allow me: on the way to acquiring knowledge of any thing, you learn things which change your original reasons for wanting the knowledge. The new reasons will in turn alter your perspective on why the knowledge is good to have. This is a safety valve built into all learning, whereby those who acquire knowledge cannot help but make other discoveries which prevent malicious or petty use of the knowledge… [Hacking] is knowledge which prevents its' own misuse, by being hard to obtain. So please, all you folks who want to know how to CRACK, as cracking and hacking are two entirely different things, sit down and examine why it is you want to know. Will your reason be the same in ten years? Twenty? If you know the answer is no, then save yourself some time and learn how to play a nice game of chess" (Anonnews.org 2013).

One of the members of the forums, when asked when it is okay to hack, said the

following:

> "Is it okay, or is it right? If your school has a strict no-violence policy, is it "okay" to punch a bully in self-defense? Is it "okay" to punch that same bully when they are doing nothing to you? Is it "okay" to kill someone when they break into your home and have your family hostage? Is it "okay" to kill that same burglar on the street when the are doing no harm? There is a difference between "hacking for the shits and giggles" and so-called "hacktivism". There is also a difference between what is "okay" and what is "right". Is it right/okay to hack into someone's computer to get their bank account information? In my opinion, no. It is not. Now, is it okay to hack into that same computer and gain access to a remote server that is used by the NSA to illegally spy on people? Perhaps. It depends on many things, a blanket question such as "is it okay to hack" is much to vague to give a proper answer. There is a time and a place for everything, violence, speeding, running a red light, murder, hacking. It is all very

circumstantial. So, I believe that your question refers to what Anonymous does in regards to hacking. And I will say right now that I do not do anything illegal. But, in many ways I do believe that what Anonymous does is "okay", but it is "okay" because it is the right thing to do. The founding fathers of this country were killing people over less than what we put up with today" (Anonnews.org 2013).

Many members stated that they think hacking skills represent a powerful 'tool' that can be used for both good and bad causes. They stated that because so many people want to use hacking irresponsibly, knowledge about hacking and/or cracking should be protected. Hackers, who mastered their computer skills to a higher degree should not reveal their knowledge easily, but should rather protect that knowledge as much as they can. Many stated that they believed hacking is equal to magic implying that hackers, just like magicians, often seem to do impossible things: "…keep in mind a hacker is just a magician. They never reveal their ways or tools. You are a fool if you do. [Training or teaching someone] can backfire. Learn yourself. [Do] research" (Anonnews.org 2013).

While some people responded negatively towards requests of being taught hacking skills, other individuals on the forums tried to be rather helpful and provide advice on how one can learn more about computers and hacking. As indicated earlier, some members of the forums directed individual who wanted to learn computers skills to websites like HackForums.com or even Google. Other forums' members, meanwhile, provided advice on computer security in general. A big emphasis/accent was made on securing your computer/system. Many people on the forums pointed out that because of *Anonymous'* somewhat negative reputation, members of the group have to stay cautious and secure at all times. An overwhelming amount of people on message boards advocated for awareness and being careful when it came to using computers; many mentioned that the (United States) government is continually spying on the members, so they have take

all measures possible to stay invisible and/or unidentified online. Whether hacking, or

just having conversations on message boards, members stated they need to maintain

security. Some of the members, who seemed to have better knowledge about computer

security, often provided helpful advice to others, while also promoting self-reliance and

computer security:

> "…Don't download HOIC or LOIC. It will certainly get an untrained,
> uninformed, and unprepared user in [trouble]. If you want to learn how to
> hack, learn from the best… There used to be numerous sites indexes by
> google when i was in college. HackerIndustries, the BlackHat group.
> There's even tutorials on how to build viruses – which will get you in no
> deeper trouble than hacking anyway… I suggest if you want to learn
> hacking, you learn hacking techniques. Do not rely on some
> preprogrammed toolkit to do it for you, because from what I've seen they
> are not good enough to keep you safe…"

> "Please don't use LOIC. It exposes your IP address (VPNs are not trusted
> and you can't use LOIC over TOR) and it doesn't have a purpose
> anymore…"

> "No. DO NOT USE LOIC. It is VERY easy to trace it. Perhaps back when
> it was first introduced it was usable, but by today's standards LOIC is a
> fantastic way to get arrested. There are other manners to DDoS a website,
> and other manners of taking one down. Do your research, if it's well
> known, it's probably no good. That's not always the case, but it's a good
> rule of thumb."

> "As far as forums like this, be careful. Do not give out identifying
> personal info to anyone. Because this is open to anyone, there are any
> numbers of idiots, trolls, feds, you name it here. I hate to say this, but for
> your own safety, trust no one here or on any Anonymous forum (there are
> many)… I'm not trying to scare you, or hinder your activism in any way,
> just offering info to help you protect yourself."

> "If you want to use an ordinary mail client…
>   1. Download  and configure Tor (everyone should have done this
>      already)
>   2. Go to a mail client that has loose verification like gmx.con
>   3. Make an e-mail with false information
>   4. As long as you use tor and/or multiple proxies while visiting that e-
>      mail you are anonymous

There are also temporary emails that last for a day or an hour. You can use tor to remain anonymous while using them…" (Anonnews.org 2013).

Suggestions or advice on the forums ranged from how to secure your computer or network to how to stay secure while using e-mail or a social network. Almost every thread where one asked a question about security received some serious responses in the sense that forum members genuinely tried to answer questions to their best ability. While reading those responses, I had a feeling that security and/or staying unidentified represents something truly important to most members of *Anonymous*. Some members mentioned that the government is likely to be watching members of the group, and that members of *Anonymous* should be aware of this. Some of the members stated that while participation in the group's activities is important and appreciated, every single member should first take steps to secure himself/herself, whether he acts online or in real life. Other members stated that only online participation can be completely secure, or as secure as it can get. In other words, some members of *Anonymous* showed some skepticism towards real life protests, while still often recognizing their importance. One member, for example, claimed that street protests are no longer secure because of how state officials/policemen treat protestors:

"Protests are brilliant way to get yourself on the NSA terror watch list. The police use facial recognition cameras to identify the protestors and enroll them in their "potential terror" list. I'm not saying don't go, absolutely protests are important, just be aware. Don't be stupid" (Anonnews.org 2013).

Overall, members of the forums showed a lot of interest in how to stay anonymous/unidentified. Part of this interest in anonymity and security has been triggered by mistrust in authorities, such as governments. The forum's discussions had an atmosphere of overall distrust in anyone/anything with a great deal of power. Anonymity

and security was often referred on the forums as the 'keys to success' of the group or something that group members saw as part of *Anonymous*' identity. Many members, participating in real life protests, made an point to wear Guy Fawkes masks, which they viewed as a way of protecting their identities on the streets.

*On Symbols: Guy Fawkes Masks*

Many members of the group have mentioned on the forum that *Anonymous* often becomes inspired by famous books and/or movies. Among the most frequently mentioned movies was the film *V for Vendetta* by James McTeigue; among the most mentioned books were *V for Vendetta* by Alan Moore, *Animal Farm* and *1984* by George Orwell. One common theme that united the aforementioned films and novels was the opposition to tyrannical/totalitarian leaders by rebels. Members of *Anonymous* often compared themselves to major characters in the aforementioned books and film. When someone on the forum asked about what *Anonymous* is and what they stand for, many members often reply in the following manner: "…watch V for Vendetta, research some more and then watch it again, each time you will take more from the movie. It's very metaphorical but does contain a great deal of truth" (Anonnews.org 2013).

Many people on the forum also mentioned that the idea of wearing Guy Fawkes masks was drawn from the novel *V for Vendetta*. The original members, according to the forums' participants, chose the graphical novel as a reference or guidance for their activism and many activism-related ideas. Meanwhile, other people on the forums claimed that many earlier members of *Anonymous* drew inspiration from the actual historical figure, Guy, also known as Guido, Fawkes. Guy Fawkes was a rebel who was in charge of the Gunpowder Plot, a failed assassination attempt on life of King James I, who later served as inspiration for a holiday in Great Britain, known as Guy Fawkes Night,

November 5th.  Many members claimed that they did not just wear Guy Fawkes masks,

which became widely popularized after the movie *V for Vendetta* was released, but were

also inspired by the actual ideas of Guy Fawkes. Here is what one of the forums' members

has said in this respect:

> "…I [also consider myself] a member of the original group, which is
> stated to have been organized in the late 1800's in the UK and Italy. If
> you've ever heard of Guido Fawkes you know what I'm talking about, not
> just the man we all copy our masks from, but the actual ideals that Guido
> "Guy" Fawkes stood for… I'm a part of [today's Anonymous], but also
> consider myself an original member, I go to protests and take peaceful
> action against oppressors such as the United States current government…
> This was represented in the movie V for Vendetta. V, the main character,
> took physical action against the totalitarian and fascist governments of the
> UK in the future, and currently, the governments of the UK are
> steamrolling towards this future, V took action against the governments
> and in the end won, he was also martyred for the Anonymous cause. This
> is exactly what Guido Fawkes attempted to do in the 1600's, he attempted
> to blow up the UK parliament buildings and was captured and executed
> for treason, Guido was martyred that day and 200 years later, Anonymous
> formed" (Anonnews.org 2013).

When talking about an "original group", this member refers to earlier members of

*Anonymous*, who were not hacktivists, but were rather traditional/street activists who

took peaceful actions. The earlier members of *Anonymous*, in this member's words, were

also an extension of the activists of the 1806, who protested against the UK government.

By "modern Anonymous", this member of the forum means the hacktivist subgroup of

the *Anonymous*. Similarly to this participant, many other members also stated that earlier

members of the group were just activists and that hacking and digital activism came on

later on.

While some members claimed that Guy Fawkes masks are being used by

*Anonymous* members rather symbolically to convey Guy Fawkes ideas, other members

also claimed that the masks are being used for practical purposes, as well. Many

individuals on the forums claimed they feared to join real life protests and expose their

faces, because of police brutality and facial recognition technology the government uses

against protestors:

> "The police use facial recognition cameras to identify the protestors and enroll them in their "potential terror" list. I'm not saying don't go, absolutely protests are important, just be aware…"; "…[Protecting our identities is the reason] why we wear Guy Fawkes masks."

> "…I see so much going on and nothing is being done… police tazing pregnant women, police brutality left and right, and in the current job I report on what goes on, but being "friends" and what not with the police and government officials, I am forced to put on a smile and buy them drinks…" (Anonnews.org 2013).

The name of the group first came around to protect the names of the members,

according to many individuals on the forums. Some people on the message board claimed

that this is how *Anonymous* as a group came to be: people needed a group that provided

an opportunity to participate in societal change without taking risks. One member stated:

"…Anonymous provides a community and a way to get involved without the need to put

yourself in danger of being targeted personally" (Anonnes.org 2013). Others meanwhile

raised some concerns about members being arrested: "[Some Anonymous members do

not take steps to protect their identities], hence why a lot of "Anon" is have FBI agents

bust in their doors and arrested. I'm hearing more and more of "Anons" being

arrested…" (Anonnews.org 2013).

Overall, individuals on the *Anonymous* forum made it clear that the Guy Fawkes

mask, which members often wear during peaceful street protests, as well as display

online, are used for a few primary purposes. The first reason is symbolic one: by wearing

the Guy Fawkes masks, which are widely recognized and known in the UK and now

around the globe, members convey the ideas of freedom fighting and standing up to

oppressors. The masks also became a sort of trademark of *Anonymous*, which I believe

was not planned in the sense that members were not/are not making any serious attempt

to intentionally promote the group. Many people on the forum, in fact, stated that

*Anonymous* does not need any promotion like other, more traditional groups do.

Eventually, though, this trademark helped to promote *Anonymous* as a collective. The

collective known as *Anonymous* gained significant fame over time both due to their

actions and the way the group managed the security of its members.

The second reason for using masks is rather functional: the group members

simply want to protect their identities and/or avoid being arrested and even prosecuted,

even though they may not be doing anything illegal. Having an opportunity to participate

in civil disobedience and/or digital activism, or even hacktivism, without exposing

personal information and/or identity makes protests more attractive to potential members,

both those who want to protest on the street and those who prefer to protest on the

Internet.

### *Anonymous: Peace Makers vs. Revolutionaries*

A great amount of individuals on the forum have stated that they, as well as *Anonymous*

as a whole, oppose violence or/and violent actions. Many stated that violence is only

justified in extreme situations, but for the most part is unnecessary. Forum participants

often referred to *Anonymous* as a peaceful entity, as well as called themselves

'peacemakers.' At the same time, many members of the forum stated that they did not

consider hacking or breaking into computer systems violent. Here is what some of the

people have stated in regards to violence and peace:

> "Revolution is necessary, hacking systems to expose corruption is
> NESSESARY. Violent means ARE NEVER necessary. The minute

Anonymous becomes violent is the minute Anonymous has lost its purpose…"

"…There are a select few who may give a bad name [to Anonymous] such as the person you are quoting about "destroying governments", but they are in a very, very small minority. Anonymous as a whole is a peaceful organization. We don't want to start a civil war, we are fighting to wake people up to the corruption that is prevalent in the governments of the world today. Within any group, there will always be a "bad apple" or an outcast that doesn't represent the whole… If things got bad would Anonymous join in the fight? Probably some of them I'm sure, others I'm sure wouldn't. But nobody is pushing for a war. Nobody is pushing to "destroy the government"… Get your facts straight…"

"War is a crime against humanity and should be dealt as such..."

"We are not fighting a war with violence, we are trying to avoid violence BUT our oppressors ARE using violence and we are defending ourselves and warning them that they are going too far and if they don't stop we will take action, that's it."

"…The elites are trying to provoke a war. They are doing this because people are walking up way [too] fast and their plan could easily come apart. We don't have to have a war to win, and they know it" (Anonnews.org 2013).

Numerous members of *Anonymous* stated that they associate violence and brutality with government officials - individuals *Anonymous* as a group consider opponents; they said it was ridiculous to associate violence with the group since most Anons chose to embrace peaceful activism. Many individuals stated that they felt offended when they heard someone accusing *Anonymous* of violent actions: according to many forum participants, the majority of members are trying to promote peaceful actions when it comes to both street and online activism, rather than violence.

At the same time, many people on the forums viewed hacking positively, especially when it was viewed in the context of fighting for a good cause. Many forum participants claimed they believed there is a strict line between hacking for fun, or for no

specific purpose, and hacktivism, which they viewed as appropriate and sometimes

necessary for reaching the goal of promoting social change. That is what one member

said in the response to the question "Is it okay to hack?":

> "… There is a difference between "hacking for the shits and giggles" and so-called "hacktivism". There is also a difference between what is "okay" and what is "right". Is it right/okay to hack into someone's computer to get their bank account information? In my opinion, no. It is not. Now, is it okay to hack into that same computer and gain access to a remote server that is used by the NSA to illegally spy on people? Perhaps. It depends on many things, a blanket question such as "is it okay to hack" is much too vague to give a proper answer. There is a time and a place for everything, violence, speeding, running a red light, murder, hacking. It is all very circumstantial. So, I believe that your question refers to what Anonymous does in regards to hacking. And I will say right now that I do not do anything illegal. But, in many ways I do believe that what Anonymous does is "okay", but it is "okay" because it is the right thing to do. The founding fathers of this country were killing people over less than what we put up with today... They've taken almost everything we have, and you may not realize it yet, but the US is following the same course that Nazi Germany and Soviet Russia took prior to their mass killings. Time is short, and if hacking can prevent something like that, I personally believe that it is not only "okay", but it is the duty of the people" (Anonnews.org 2013).

So, just as with violence, some members believed that hacking should be used in

rare cases, when other measures prove ineffective. Hacking, according to the above

mentioned member as well as some other individuals on the forum, can be the

right/appropriate course of action in situations where regular protests fail to achieve the

desired result(s). However, many also stated that such an extreme measure as hacking

should always be considered carefully and applied with all appropriate ethical

considerations in mind.

While many members referred to *Anonymous* as a peaceful organization, an

overwhelming amount of members also referred to themselves as revolutionaries. This

paradoxical self-definition re-occurred throughout the message boards over and over

again. On one side, members of *Anonymous* stated that they supported peace; on the other side, they also claimed that one of the main purposes of the group is to bring about a revolution that will be able to solve some of the political and social problems they have identified in the U.S. and around the globe. Many members have insisted that the "revolution" should be brought about peacefully, while others stated that if bringing about change requires more radical actions, *Anonymous* members should be ready to partake such actions: "…I don't advocate violence; but on the other hand – if speaking out and standing together cannot accomplish the goal – then, sadly, what must be done must be done" (Anonnews.org 2013).

Some forum participants expressed sadness when discussing earlier members of *Anonymous* and comparing them with a new generation of *Anonymous*' members. One of the participants said that earlier members were revolutionaries, but most of today's members just prefer to have discussions online, partly out of the fear of getting in trouble for their activism: "I am sad. I feel like the revolutionary group that Anonymous once was has just faded away, leaving only a few that actually still care about our country…" (Anonnews.org 2013). Another person stated: "…There are still huge numbers of people who are "revolutionaries", such as myself, but being that people are being arrested and killed for speaking their beliefs many have decided to become quieter" (Anonnews.org 2013).

Many people on the forum defined "revolutionaries" as street protestors opposed to actual individuals starting a revolution (the traditional definition of a revolutionary), which in most cases implies violence/radical measures. The majority of members, in other words, conceptualized a "revolutionary" as a peaceful and often a traditional, street

activist. Many members claimed to be participating in Occupy Wall Street protests, as well as in the protests that were triggered or inspired by Occupy Wall Street. Many of the forum members also used the word "social worriers" when describing themselves, which was used synonymously to "revolutionaries", although it did not have a negative connotation (i.e., the word "revolutionary" is often given a negative connotation since it is often associated with overthrowing the government or people with legitimate power). Regardless of which words members chose to use when describing themselves, they tried to convey an idea that they as *Anonymous* members want to fix societal problems, even if this requires courage and risk taking (e.g., going to the streets and facing police or participating in DDoS attack online).

When topics like civil war or overthrowing existing government(s) was brought up on the message board, Anons had various views on such issue. Some stated that *Anonymous* would not start such a war or conflict. One member noted: "If a civil war starts it will not be Anonymous that starts it. It will be the elitists..." (Anonnews.org 2013). Some members argued that *Anonymous* is simply too fragmented and decentralized to start such a war/revolution; besides, the group does not formally have any leaders or "principal players" who would lead the crowd if such a thing was to be proposed. Other members agreed that a civil war might be necessary and that they would support it if it came about, but *Anonymous* as a group would not be likely to initiate it. Some members stated that they strongly opposed the idea of anarchy or the idea of overthrowing the existing government and that the group should rather achieve its goals by peaceful means.

*Anonymous: On Anarchy*

Anarchism has been discussed on the forums fairly consistently. One of the ways it has

been discussed is in relation to *Anonymous*' reputation/public image – i.e., the media

labeling the group as anarchic. There was no unanimous agreement on the forums on this

issue, however. While some members claimed to be anarchists and/or support the notion

of anarchism, other members rejected it wholeheartedly. As one member said (in

response to the question 'Does *Anonymous* stand for anarchy?'), "No, Anonymous

doesn't stand for anything. It doesn't have universal ideologies, values, or goals. Only

individual anons can really stand for something" (Anonnews.org 2014). Similarly to this

member's opinion, many others said that the group is too fragmented and/or split on how

they view anarchism, as well as other topics, meaning the group cannot really be called

anarchic as a whole, since only certain subgroup(s) or members of *Anonymous* consider

themselves anarchists. However, as I was reading through the content of the forums, I

noticed that generally the members tend to split into three broad categories: those that

view anarchism positively (i.e., accept all of the tenants of anarchy), those who view it

negatively (i.e., view anarchy as harmful and/or dangerous), and those that approve of

certain features of anarchy, while also approving of representative democracy and

capitalism.  The third group's views on anarchy were somewhat 'in the middle' between

members who claimed to be anarchists and members who claimed to despise anarchy.

The *Anonymous* members who claimed to favor anarchy/anarchism have

defined and understood it in a certain way, which they often clarified for those claiming

that anarchism is harmful. The majority of Anons supporting anarchism favored a

specific type of anarchism – social anarchism, also known as socialist or libertarian

anarchism. Social anarchism can be defined as a "body of anti-authoritarian ideas," that

emphasizes "a collectivist commitment to social freedom" (Bookchin 2005). In other words, social anarchists consider mutual efforts as essential to achieving social freedom and equality, as well as emphasize community and its needs over individuals' needs. This branch of anarchism is commonly associated with the works of Pierre-Joseph *Proudhon,* Mikhail Bakunin *and* Peter *Kropotkin* (Purkis and Bowen 2004), whose names were frequently mentioned and/or referred to by some of the members on the forums.

Social anarchists can be defined as individuals standing against capitalism, globalization, powerful (e.g., transnational) corporations, inequality, and hierarchy. Social anarchists believe that power relationships exist everywhere in society, whether it is in political sphere or any other, non-political, sphere – e.g., cultural, economical, social, etc. Social anarchists are anti-capitalists, who consider all forms of power equally threatening to a community, and therefore try to resist all types of hierarchies and oppression. The state, however, is viewed as the main source of power by social anarchists; thus, the state or the government should be resisted most of all out of all other sources of power (Purkis and Bowen 2004). Another key idea to this branch of anarchism is the belief in the "feasibility of life without a state after the downfall of Capitalism," "the capacity of individuals to do things on their own" (self-organization), and "spontaneous direct action…without bureaucratised revolutionary leadership" (Purkis and Bowen 2004:26). Some of these ideas were definitely echoed on the *Anonymous* forums.

Additionally, social anarchism draws on Marx's critique of capitalism and concept of alienation. Social anarchists see capitalism as an exploitative, dehumanizing system. However, unlike Marx, social anarchists do not favor the idea of a 'dictatorship

of the proletariat.' Social anarchists simply reject any type of ruling elite. The establishment of a dictatorship of the working class (which was proposed by Marx) is viewed as just as dangerous as the establishment of capitalist leaders in the eyes of social anarchists, since any leaders (due to human nature, which can be easily corrupted by power) would eventually create hierarchies and oppression in society (Purkis and Bowen 2004). Overall, social anarchists view any type of authority as threatening to people's creativity and freedoms. Social anarchists believe that no group or individual should have control over source(s) of power, as power has corrupting consequences on individuals. Social anarchists reject the idea of representational politics, "creation of centralized, hierarchal political party," or "establishing themselves as prophetic revolutionary leaders" (p. 25). Unlike Marx, social anarchists also reject the idea of revolutionary potential existing only in the industrialized working class. Unlike Marx, social anarchists have a more inclusive view of revolutionary agencies. Anyone and everyone in society, in their view, should participate in resistance towards sources of power.

Members of the forums, who have claimed to be anarchists and/or support the notion of anarchy, have discussed some of the tenants of social anarchy I have presented above. The topics that were brought up and discussed in the forums in relation to (social) anarchy included six major topics: 1) defining anarchy (i.e., members discussing how they define anarchy); 2) resisting major sources of power (i.e., government and corporations) as one of the major goals of (social) anarchists; 3) self-representation versus representative democracy; 4) the issue of freedom, creativity and self-expression; 5) social justice and emphasis on community as essential issues of (social) anarchy and/or anarchists; and 6) (social) anarchy as inevitable and/or natural for *Anonymous* as a group.

One of the most commonly brought up issues by self-pronounced anarchists was the ways they define, view, or understand anarchy. As I mentioned previously, most of the Anons seem to favor social/collective anarchy over other forms of anarchy. Although the group may (and probably does) contain members who choose to support other types of anarchy, as well (among other forms of anarchy the members also mentioned anarcho-communism and anarcho-syndicalism). Many of the members emphasized that the ideas of a leaderless community, individual freedom and collectivist commitment to social freedom were those that they liked the most:

> "Any idea that is leaderless, decentralized and emphasizes individual freedom while working within the framework of collective is anarchist. If you are interested in anarchism you should…follow a few links. Reading Noam Chomsky, Bakunin, [Kropotkin] should help your understanding…" (Anonnews.org 2014).

Other members claimed that they preferred social anarchy because it puts emphasis on community and mutualism, unlike anarcho-individualists (the supporters of individualist anarchism), who despite having the same goal of removing government, place emphasis on individuals' needs:

> "I would also like to add that personally, I have a problem with anarcho-capitalist/anarcho-individualist views, only in so far that they can fuel greed, over accumulation, forms of hierarchy, and an arms race for self defense…" (Anonnews.org 2014).

Oftentimes, the members supporting the notion of anarchy, used the term "direct democracy" synonymously to the term "social anarchy." Many preferred calling it that way because of the stigma/negative associations attached to the word "anarchy." Some members claimed that direct democracy (or collective anarchy) is a way forward for the United States or any other modern country that wants to be a state free of corrupt leaders/politicians. Some of the Anons often posted links to Wikipedia pages, talking

about collectivist anarchism and direct democracy in order to educate other members of

the forums:

> "…A collective anarchy has proven to work really well in the past,
> without depression/recession cycles like is seen in democracies. What we
> have today is a pseudo-democracy – where you have a democracy but it's
> really only run by elites. I challenge you to read and understand the
> following information…especially the Collectivist anarchism link… I
> would challenge you to look at each economical system and ONLY
> AFTER THAT come back to me and tell me with today's technology I am
> wrong with collective anarchism/direct democracy as being the way
> forward…as opposed to your continuance of representation…"

> "You (like many other people) have misunderstood the meaning of the
> word Anarchy. Today it is synonymous with chaos and destruction (which
> is what the governments…want you to think it means) but all it really
> means is no rulers. It doesn't imply no law, it doesn't even have to mean
> no government. It just means that instead of somebody making decisions
> for the people the people make the decisions for themselves (aka direct
> democracy)" (Anonnews.org 2014).

Others defined being pro-anarchy or anarchic as simply being a revolutionary

fighting against oppression and/or for the rights of the oppressed:

> "Jesus was a revolutionary. Think about it. There are paintings of Jesus in
> Latin America depicting Jesus with a rifle slung over his shoulder which
> makes sense. Jesus sided with the interests of the poor and the poor who
> are forced to arms to survive look to their spiritual leader for inspiration
> and strength to continue a difficult yet morally righteous struggle. The
> rifle emphasizes the righteousness of the struggle against [oppression]
> especially when it is as it is in many cases the struggle to survive with
> freedom and dignity as somehow distant dreams."

> "…Anyone who lives differently within an oppressive structure is radical
> and revolutionary. What I plan to do in life and with whatever resources I
> arbitrarily gain, is to implement more bridges (metaphorical) between
> communities (or classes) and try to level out the playing
> field…"(Anonnews.org 2014).

Lastly, some Anons simply viewed 'being anarchic' as the ability to question

authority and/or feeling little need for government, but not necessarily complete removal

of it. It was unusual to find members who, despite claiming to be anarchists, did not

wholeheartedly reject the notion of government. Even though most self-claimed anarchists on the forums claimed to be against the *current* government, some of them were in favor of the idea of removing government on general. One Anon, for instance, said: "Though I'm an Anarchist I need a government, however not as it is currently practiced… We need taxes, for schools, bridges, etc… If there was no government whatsoever how would one suggest funding infrastructure and positive freedoms (healthcare/education/workers/workers comp/subsidized housing, accessibility, etc.)?" (Anonnews.org 2014).

Some Anons complained that many members and people in general imply violence or civil war when they talk about anarchy, when, if fact, a large portion of Anons define anarchy as less reliance and dependence on government (sometimes members also used the term "extreme libertarianism" synonymously to the term "collective anarchism"):

> "I have always thought people imply too much with anarchism. To me at least, it simply means there is not another person who has the ability to decide things that affect my life without having anything to do with, or even speaking to me. In other words, I always thought of it as the lack of a NEED for government…" (Anonnews.org 2014).

Some of the members, however, seemed to believe that any power structure or government would eventually become corrupt. Therefore, they stated, their goal should be achieving the specific goal of removing the power structure, regardless of what it may be. One of the members noted that *Anonymous* has been split for a while into members who "demand return to purely limited, Republican government" (Anonnews.org 2014), also known as 'Constitutionalists,' and members who are in favor of a complete removal of government, or the self-

proclaimed 'Anonymouses.' However, that same member noted, even if the

Constitutionalists reach their goal of reforming the state, they would eventually

face the same problem – corrupt elites:

> "[Once] the Constitutionalists begin to reform the Government…that's
> about the point where Anonymous will begin to defeat the new power
> structure because it would appear to be creating another Capitalist society,
> something which [most of Anonymous] does not want" (Anonnews.org
> 2014).

Another aspect of anarchy that was frequently discussed by the forum members

was resisting the primary sources of power and fighting power structures: namely, the

government and corporations. Anti-government and anti-corporation sentiments were

extremely popular on the forums, in general, enough to make them a separate theme, but

anti-government and ant-corporation themes were also often brought up specifically in

relation to discussions of anarchy. As I stated previously, anarchy generally implies

resistance towards social control and power. Many members of the forums claimed that

they saw government and corporations as their major opponents, or the targets they were

fighting against:

> "[This movement is] dedicated to taking down high-ranking politicians,
> including the president himself."

> "I believe that we do need to stand up together, to not take the constant
> attacks on our freedom and rights anymore. Unfortunately the only way I
> see this rebellion working is for blood to be shed, though many different
> variations of rebellion may happen. The more logical path [would be] for
> the people to rise up against their government…" (Anonnews.org 2014).

Even though there were some members on the forums who stated that civil war

(involving violence) is inevitable, there were many self-proclaimed anarchists who

believed that taking down the government would not result in any violence. Most, if not

all, members of *Anonymous* who were supportive of the notion of anarchy, thought of

violence very negatively, but they admitted that in some cases violence is necessary. Some members, including the ones who were pro-anarchy, claimed that peaceful action was always their first choice but recently peaceful efforts had not been working so well for activists and /or hacktivists. One Anon said: "I would love a peaceful resistance and to gain peace through this, but is not working. People protest all the time, even in mass, yet the government still pushes them down. They still make laws to prevent the protests…They still treat people as the enemy. We need to start treating them as the enemy. We must fight back…" (Anonnews.org 2014).

The anarchy-related conversations often revolved around discussion about the issue of representation: representation by government (as in representative democracy) versus direct voting (as in direct democracy). As I previously mentioned, the term "direct democracy" was often used synonymously to the term "social anarchy" or "collective anarchy." The self-claimed collective anarchists on the forums did not favor representational politics, but rather advocated for putting self-government in place or so-called community-based laws and rules. Many members of *Anonymous*, who seemed to embrace the notion of anarchy, stated that self-governance, in their view, represents the best option compared to elected officials who are acting on behalf of the people. Direct voting, in these members' view, represented a more fair and effective ways to organize communities. Moreover, direct democracy would not as likely to lead to corruption as the current system does, many members stated:

> "The problem here is not the law. The problem is the lawmakers. There should, in my opinion, be no law such that absolutely nowhere can one go to escape it without being incredibly wealthy. People are not all the same, and absolutely NOBODY should be subject to any law they did not personally agree to be bound by. In no other way can true law exist. Now should one have to choose between life in a lawless anarchy (my personal

favorite) or servitude in a perpetual prison of debt…All forms of government at all levels should be tried in a long-term and competitive way and if a governance (or lack there-of) catches on, it will automatically spread."

"Today's anarchy is: instead of minimal government, how about no government? Human nature shows that people suck. Power corrupts, and absolute power corrupts absolutely. We this happening currently with the Obama administration…Anarchy may not solve the problem of human nature, but it solves the problem of having potential for another Hitler…"

"Representation is the most elemental form of alienation…"

"Our Founding Fathers were unaware of how corruptive Representative Voting was…" (Anonnews.org 2014).

Another reason that people on the forums stated for being in favor of direct democracy/collective anarchy is that it allows for more creativity, self-expression and freedom overall among individuals. Some of the Anons stated that they chose to be anarchists because that is what any person who wishes to preserve his or her freedom of expression, would do:

"Thinking feeling people who wish no limits on association, creativity, expression, exploration of heart and intellect without limits choose Anarchism… read some Chomsky, Bakunin, Kropotkin… Socialists and Anarchists will encourage you to read and make up your own mind…" (Anonnews.org 2014).

While some people named self-expression and creativity as a positive side of having social/collective anarchy, other members preferred rather to focus on the issues of social justice and community. Many self-claimed anarchists on the forums stated that social/collective anarchism is the best method because it places emphasis on community (rather than on individuals) and is aimed at achieving equality within a community.

"I'm an anarcho-syndicalist/activist, but my view is not necessarily shared… The principles of insulting/hierarchy/male dominance/and wasting time not fighting injustice are none to which I subscribe."

"[In collective anarchy], everyone has equal rights, and equal say. This basically destroys the possibility of manipulation, and brings up true equality, freedom. A classless, moneyless society, of no higher or lower power." (Anonnews.org 2014).

Lastly, some *Anonymous* members stated that the presence of anarchists within Anonynous is understandable, if not logical, since *Anonymous* itself represents a somewhat anarchic collective, in the sense that the group is taking on some of the ideas of social anarchy, such as the hatred of hierarchies and leadership and support for direct collective action to achieve goals. Other members explained that anarchists' presence within *Anonymous* is due to the history of the group: *Anonymous*, they claimed, had originated as a group consisting of mostly hackers and Internet anarchists, but as time went by, the presence of anarchists/individuals supporting the notion of anarchy has significantly dropped. Despite that, the group as a whole still seemed to favor some of the ideas of collective anarchy, as well as contain some members who refer to themselves as anarchists:

> "Anonymous functions as a voluntary association quasi-democratic collective (if you have no idea what that means, then you have no business asking for an educated discussion) in which individual agendas can be propagated to become part of the collective's overall agenda. Specifically, the current overall agenda of Anonymous at the moment is a broad platform of anti-oppression, anti-censorship, anti-tyranny, propagating free speech, social justice, political & moral equality, multiculturalism (to a certain degree), soft anarchism, hacktivism, and so forth, as dictated by the current composition of [its] membership and perception by the media."

> "Anonymous (used as a mass noun) is a loosely associated hacktivist group. It originated in 2003 on the imageboard 4chan, representing the concept of many online and offline community users simultaneously existing as an anarchic, digitized global brain…" (Anonnews.org 2014).

In other words, some members, especially those who seemed to be pro-anarchy, claimed that *Anonymous* already represents a collective anarchic entity in a metaphorical

sense : a) it lacks leadership/hierarchy; b) it represents a voluntary association, meaning that members can enter and leave whenever they want; c) *Anonymous'* success depends upon mutual/collective actions of many members; and d) the group's major opponents are the government and corporations, the sources of power and social control, that members of *Anonymous* are actively trying to resist.

Overall, the members of *Anonymous* represent a diverse community that is inclusive of people with different views on anarchy. Based on my observations of the forums' discussions, I have concluded that the majority of people on the forums are supportive of the specific type of anarchy known as social anarchy.  Most members picked these forms of anarchy because they put an emphasis on community and togetherness, rather than on individualism. While some of members went as far as saying they wanted no government and/or a lawless society, others claimed that they just wanted less government, or a different government. However, the notion of social justice and equality for everyone was shared by all of the members supporting the notion of anarchy. The members shared an agreement, that despite what specific version of anarchy they preferred, they all believed that their goal should be fighting to eliminate corruption and social injustice, as well as liberty over government.

Despite these facts, many members on the *Anonymous* forums spoke fondly of anarchy and even proposed it as an alternative to the current U.S. government, an overwhelming amount of people held opposing, and quite negative, views regarding anarchy. The members who spoke negatively of anarchy also stated that even though they did not support the current government, they also believe that government is necessary and generally good. Many stated that *Anonymous* as a whole is not radical enough to

support the notion of no government whatsoever; moreover, anarchy would lead to even

worst situations than the current corrupted government:

> "Anarchy is not the answer nor the basis of Anonymous. The basis of
> Anonymous, when it comes to politics and government involvement is to
> ensure the freedoms of citizens, and prevent tyranny... anarchy will also
> only introduce more laws against freedom."

> "…you must be stupid to think Anonymous is against the government.
> Many people probably do think it is but what is the alternative? Complete
> anarchy, where everyone gets robbed or shot and in the end we end up
> either as hunters living off the land back where we started or EXTINCT...
> [What Anonymous is] actually against is corruption and misuse of power
> inside the government. "

> "[Anonymous is supportive of] not anarchy, but removing ridiculous laws
> like the national defense…which allows the government to use the United
> States as a battlefield and indefinitely arrest anyone without suspicion or
> even trial…"

> "A nation of rule-less anarchy as just as bad if not worse than what is
> going on right now" (Anonnews.org 2014).

The members who rejected anarchy typically associated it with chaos, violence

and criminals, and/or terrorists. Moreover, they claimed that because *Anonymous* as a

whole does not support violence – and that is what anarchy would eventually lead to –,

anarchy is against *Anonymous'* core goal of embracing peace. Revolution, they claimed,

must be achieved peacefully and without violence. Some people stated they believe that

anarchy is criminal-based organization: "Every attempt at true anarchy has failed…

[because it breaks] down to the base concept of mob rule" (Anonnews.org 2014).

Many of those members, even though admitting that the current government is

flawed and needs to be reformed, also stated that the complete removal of government is

not possible – the absence of government and laws, they stated, would lead to crime and

lack of order within society. Moreover, most people (e.g., Americans) would not support

the notion of no government. *Anonymous*, they claimed, would not be supported by the general population (since humans are naturally inclined toward fearing chaos and violence) and would simply fail at its efforts to establish anarchy:

> "Do not test the government too much, and do not let the government take us down. Do not let us become the terrorists. Do not let us become anarchists. Do not let us become social murderers. PLEASE practice restraint, and please don't waste the protestors effort just because you want to prove your point with violence. The government does not feel sympathy for social murderers or outlaws, and I want to prevent…class welfare."

> "You are stupid to go after the government…because the general population will not support you."

> "…The government is the expression of the people and no matter how flawed it is people have a very natural fear of anarchy" (Anonnews.org 2014).

On the top of that, the anti-anarchy members stated, human nature is all about organizing things and creating order and stability – humans are 'wired' to preserve themselves, and maintaining order is an essential part of human survival. Some people even admitted that they wish *Anonymous* itself would be more organized. Overall, the majority of people on the forums that were against anarchy said that even if anarchy was possible to achieve, it is just a bad system and would never work in practice:

> "…Anonymous does need some organization. [I also believe that] total anarchy will never work out."

> "The human mind will always organize things. Anarchy is impossible."

> "I'm no Anarchist. Rules are good when enforced fairly and when they don't infringe on liberty" (Anonnews.org 2014).

Overall, the members who held negative opinion about anarchy only agreed with 'anarchists' on one issue - that the government is corrupted and that *Anonymous* should work together toward stopping it from making and/or implementing unfair laws and

attacking citizens and their freedoms. When it came to other issues, however, members rejecting anarchy believed quite opposite things, which were specifically: a) anarchy was viewed for the most part synonymously to violence and chaos; b) violence was viewed as unnecessary and undesirable (violence was also rejected as a means for *Anonymous* to achieve its goals); c) *Anonymous*, the anti-anarchy members claimed, is against violence, and, therefore, it stands against anarchy; d) human nature naturally organizes things and desires order for survival; e) anarchy is impossible in practice because people desire government and would support it if anarchists were to overthrow it; f) anarchy was viewed as criminal-based while the government/representative democracy, regardless of its corrupted officials, was mostly viewed as the most legitimate, commonsense system; and, finally, g) overthrowing government was viewed as impossible in practice since the government has more resources (better weapons, defense systems, etc.) to protect itself from anarchists.

Lastly, some people on the forum held somewhat neutral views on anarchy/anarchism, meaning that they wanted some changes to be introduced to the current government/system but did not desire to get rid of government completely. In other words, those members who were 'in between' on their view of anarchy wanted to keep the current system of governance (i.e., representative democracy), but simultaneously wanted to 'tweak' certain laws and/or rules. One Anon suggested a system which he/she named "A Moralist Willful free society" (purposefully trying to avoid the word "anarchy," since the term has a rather negative connotation), and proposed the following changes/'tweaks' to the existing government:

> "The current system can work with a few base changes. [Firstly, we
> need to] remove the central bank that actually rules the country, and make

it unconstitutional to have a central banking system. [Secondly, we need to] adopt the constitutional amendment that takes away the ability of a corporation to use money as its "freedom of speech'… [Thirdly, we need to] remove the electoral college. Use actual popular vote to determine elections, and use only methods with public over site to verify vote counts… [Fourthly, we need to] break up the 2 party system by insuring that parties are grated and limited to the same amount of money they can receive to run for public office, and impose a term limit on all political offices. [P]ass law that no entity may donate more than $200 to any one running for public office, and all donations are subject to public scrutiny… [Fifthly, we need to] any law agency not run by a publicly elected official… [Sixthly, we need to] remove all redundant federal policing agencies. We do not need 20+ federal police agencies all doing the same thing on each other toes. We only really need the FBI… [We also need to] remove FEMA and instead place a responsibility in the hands of the individual states. [Lastly, we need to] remove the "16$^{th}$" amendment as it was never ratified by the states and has already been ruled on by the supreme court to grant no new tax authority to the government… I don't want to call [the proposed] system anarchy…because it's not exactly the same systems…This has to end at the own will of the presidential leaders everywhere. They have to resign. No one mafia group is going to hold power over the rest any longer… I'd call this system a Moralist Willful free society based on the common interest" (Anonnews.org 2014).

Similar to this member, other Anons also made proposals on what needed to be changed. Many people have shared an agreement that the Federal Reserve should be dismantled, since it represents "a private bank [that] has been secretly stealing trillions" (Anonnews.org 2014). Similar to the members who claimed themselves as anarchists, members who shared a neutral perspective on anarchy generally placed an emphasis on communal needs, mutualism, and the interests of society overall. They also agreed with self-proclaimed anarchists that society should be governed by the people and that everyone should have equal rights and equal say in political and social matters.

To simplify the differences between the split members, on their view of anarchy, I created the table that outlines those differences through comparison (Table 2). Overall, it can be said that all members of the *Anonymous* forums have the same goal – achieving

equality and social justice through collective action – but the members differed on the

means by which they wanted to reach those goals.

**Table 2. The differences in views between the members who support anarchy, the ones who reject anarchy and the ones who view it neutrally**

| | **Members supporting the notion of anarchy** | **Members rejecting the notion of anarchy** | **Members holding neutral views on anarchy** |
|---|---|---|---|
| 1. *Anarchy is defined as:* | Individual freedom achieved through collective effort; absence of leaders/hierarchy; revolution against oppressive structure | Violence; chaos; lack of order and laws; system that is run by criminals (or mobs); radical system | System that aims at creating state with little to no government, which is often archived through violent means |
| 2. *Views of government* | Government is viewed negatively; it should be either removed completely or be extremely limited; the emphasis is placed on self-organization | Government is criticized but overall viewed positively; government is viewed as essential for preserving and maintaining society | Government has potential for existing if it is being reformed properly and extensively |
| 3. *Views on violence* | Violence is viewed negatively but it is sometimes viewed as a "necessary evil" – i.e., it cannot be avoided in some situations. Revolution/civil war is sometimes viewed positively and/or suggested as a way for solving the problems | Violence is viewed extremely negatively; viewed as the opposite of what the group stands for | Violence is viewed negatively; members propose methods to reform the government that do not involve/imply violence or civil war |
| 4. Emphasis is placed on: | The needs of community, mutualism, achieving freedom and equality | The needs of community, mutualism, achieving freedom and equality | The needs of community, mutualism, achieving freedom and equality |

| | | | |
|---|---|---|---|
| 5. The primary goal of *Anonymous* should be: | Removing the government or limiting its power in serious ways; achieving classless, money-less society; having a system in which every person can vote directly (i.e., direct democracy) | Leaving the government/political system (i.e., representative democracy) as it is; removing harmful laws (e.g., SOPA, etc.) and introduce new 'good' laws | Making substantial changes to the government (to the point of 'tweaking' Constitution) but, at the same time, not changing the whole political system (like anarchists propose) |

## Content Analysis: Results

My content analysis of the *Anonymous* message boards yielded the following major

discoveries:

1)      The members of *Anonymous* claim that the collective represents an idea, rather

than an actual group. Such a definition of the collective by its members is likely used

because members of *Anonymous* are highly opposed to the idea of traditional groups or

organizations (the latter because it implies hierarchy, rules, and inequality among

members). Although *Anonymous* is ambiguous, fluid, and difficult to grasp, my research

established that it does represent a group. *Anonymous* represents a 'group' because

members share basic, core values by which they can organize effectively. Moreover,

*Anonymous* has some influence in the United States and across the globe. The fact that

others recognize *Anonymous* as a distinct 'group,' points to the conclusion that, in fact,

*Anonymous* is a group. However, *Anonymous* lacks many important characteristics of a

traditional group, and would be better conceptualized as a secondary, non-traditional

group.  This conclusion is supported by academic literature. Fuchs (2013), for example,

states that even though *Anonymous* represent a fluid and heterogeneous collective,

members want it to be seen as an idea, rather than a group, "we can see it as a collective"

(p. 345). Fuchs adds that *Anonymous* represents an unconventional, non-traditional

movement that has emerged as a result of the liquefaction of society – i.e., the social

processes becoming more fluid, liquid, and temporary. According to Fuchs (2013), and

confirmed by the results of this content analysis, *Anonymous* represents a liquid social

movement:

> "[Anonymous] expresses the liquefaction of society at the level of social
> movements. It more than other movements permanently transgresses the
> boundaries between individual and collective action, online and offline,
> movement and non-movement, networking and autonomy, spatial distance
> and presence, anonymity and knowledge, play and protest work,
> entertainment/fun and politics, presence and absence, appearance and
> disappearance, the mundane and the uncommon, normality and absurdity,
> the real and the symbolic, online and offline action, conventional and
> unconventional behaviour" (p. 351).

2)       Members of *Anonymous* see themselves as a force for good, and justify their

methods. More specifically, the group sees itself as a group of 'social warriors,' whose

primary goal is to produce positive social change in the world. Many members state that

*Anonymous* symbolizes humanity and the people as a whole; members often state on the

forum that they see their core goals as defending and preserving the freedoms and

liberties of the people and the oppressed. Members also state that *Anonymous* is forced to

exist because 'humanity is in trouble.' This vision of themselves corresponds with the

concept of 'cyber-vigilantes' or 'positive deviants,' by Serracino-Inglott (2013).  Even

though 'cyber vigilantes' may use punishment or the threat of punishment as a means to

achieve their goals, they see such threats as justified and instrumental for creating a

positive social change. The notion of 'necessary violence' or 'necessary punishment' is

examined in more detail in the analysis of the values and beliefs of *Anonymous*. Analysis

of the message board revealed that members of *Anonymous* share two contradictory

values: on the one hand, members seem to value the idea of peace and generally seem to be opposed to violence; on the other hand, members see revolution or the use of violence as necessary in some instances, when other measures fail. This shows further support for Serracino-Inglott's (2013) concept of cyber-vigilantes.

3)      Another finding about *Anonymous* concerns their use of hacking. More specifically, I was interested to discover how often hacking methods were employed by the group, and the overall technical knowledge within the group. As a result of my analysis, I found that even though *Anonymous* is often labeled as a 'hacktivist' or 'hacker' group by the media, and even some scholars, *Anonymous* does not represent a purely hacktivist group. In fact, only a small number of members have hacking or in-depth technical knowledge.  This corresponds with the findings of other researchers (Coleman 2013; Mansfield-Divine 2011; Shalin Hai- Jew 2013), who found that many individuals within *Anonymous* have no hacking skills. My findings show that a lack of technical skills is characteristically true of not just many members, but rather the majority of members. Members of *Anonymous* are equally open to accepting the technical and non-technical individuals as members.

4)      As to the organizational channels (the structure and functioning) of *Anonymous*, I have discovered that members strongly oppose leadership and/or hierarchy: Anons claim that they do not have any leadership. Anons often state on the forum that they believe *Anonymous* represents a purely decentralized group. Members of *Anonymous* emphasize that a lack of leadership does not only reflect the members' opposition to hierarchy, but also makes the group more resilient:  if there are no leaders, many Anons state, arrests and/or loss of members cannot affect the group. Anons often use the metaphor of the

Hydra (an ancient, reptilian monster with multiple heads) to convey the message that members can be easily replaced. Anons also emphasized that anyone can join the group by simply agreeing with the core beliefs of *Anonymous*, and that the group does not have any formal rules for joining or leaving, making it easier for members to enter and/or exit the collective. The fluidity of membership within *Anonymous*, as well the high turnover of members, is consistent with Jordan and Taylor's (1998) sociological analysis of hackers. The authors stated that hacker communities are impersonal in nature and tend to lack formal organization. Hacktivist culture, and the culture of *Anonymous* in particular, is extremely similar to hacker culture in this respect.

I have also established that *Anonymous* represents a community-oriented group: a group that heavily relies on the number of members participating. This is evident, for example, in how the group chooses targets. Because *Anonymous* does not have official leadership or rules for selecting whom to attack, Anons typically use technology (in the form of IRCs, forums, social media sites, etc.) for gathering and discussing important issues. The decision to target an organization is typically achieved by a collective 'vote,' the more people to voice their agreement to participate in an 'Operation,' or raid, or the more people that discuss the proposed plan of action, the greater the likelihood that the 'Operation' will be later carried out. This reliance on community corresponds with the findings of Serracino-Inglott (2013), who suggested that *Anonymous* is heavily dependent on reaching a critical mass, and generally exhibits a communitarian spirit; this leaning towards community represents an integral component of *Anonymous*' culture.

The group's reliance on technology as a tool for connecting with others is also noted by other scholars. Wong and Brown (2013), for example, conceptualized

*Anonymous* as 'e-bandits' or modern day 'Robin Hoods.' E-bandits, according to the authors, represent a distinct type of hacktivist/activist because, unlike other type of hacktivists, e-bandits use anonymizing technology (technology that completely conceals the actors' identities) as a tool for both organizing and accomplishing their goals. My analysis of the forum shows that *Anonymous* not only extensively uses technology for organizing, but also places high importance on remaining unidentified. I concur with Wong and Brown that *Anonymous* indeed represents a distinct type of hacktivist group.

As a result of my content analysis, I have also created a typology of *Anonymous'* goals. These goals consist of: 1) general or non-specified goals (e.g., fighting against injustice, etc.); 2) civil and political goals (typically revolving around issues concerning civil liberties, political issues, and standing up to the government); 3) education and awareness goals (revolving around educating others and spreading awareness about issues); and 4) information and privacy goals (revolving around issues like privacy, anti-censorship, and freedom of information). The diverse spectrum of *Anonymous'* goals points, once again, to the group's fluidity and all-inclusiveness of ideologies and worldviews. Members, in other words, are free to define and/or choose their own goals within *Anonymous*. This finding is consistent with the writings of some scholars. Fuchs (2013), for instance, describes *Anonymous* as a politically heterogeneous group, which welcomes political and social ideologies from all fronts, as long as they are in agreement with the core beliefs of the group (such as standing up to oppressors, etc).

5)      When I examined *Anonymous'* values and beliefs, I dedicated a significant portion of my analysis to discussing the importance of Guy Fawkes and the masks' utility to the group. My analysis reveals that the group uses masks for the following primary reasons:

a) masks serve as a symbolic means for expressing the group's opposition to authorities and/or the government; b) the masks serve a practical purpose of concealing the actors' identities, so that they can avoid being identified and/or arrested; and c) the masks are used as a sort of trademark for promoting the group (caused unintentionally by media focus on the mask). These findings are consistent with some peer-reviewed research. Coleman (2013), for example, mentions in her research that *Anonymous* most likely uses the masks for symbolical purposes. Unlike my findings, however, Coleman suggests that the Guy Fawkes masks are used by Anons to express the importance of privacy and anonymity: something the group values very highly. Coleman also suggests that the group enjoys the element of mystery that surrounds wearing the masks. This element of unpredictability and/or mystery often helps grab media and public attention, so it is also possible that *Anonymous* uses the Guy Fawkes mask as a way to attract attention.

The last section of my content analysis deals with the anarchic heritage, or anarchic leanings, of *Anonymous*. My analysis shows that members of the group hold very diverse views on anarchy: while some members identify as anarchists or generally support the notion, others think of it negative or neutrally. What is certain is that anarchism does represent a portion of *Anonymous* culture and, therefore, should not be ignored. Academic literature does not explore this element of the group's culture extensively; however, some authors did note that both hacker and hacktivist cultures are marked by an anarchic spirit (Gillen 2013).

## V. INTERVIEWS WITH SECURITY PROFESSIONALS

### Theme One: Familiarity with Hacktivism

The first interview question asked if the respondent had heard of *Anonymous* and/or hacktivism, and if so, the extent of their knowledge. Not surprisingly, all were familiar with the topics – both *Anonymous* and hacktivism in general. The interviewees fell into two major categories: those who were somewhat familiar with *Anonymous* and hacktivism (e.g., they were reading about the topic in the news, frequented message boards dedicated to hacktivism, and/or followed the topic in some other fashion). The second category of security professionals had more of a personal familiarity with *Anonymous* and/or hacktivism, meaning they took an interest in the activities of the group, beyond simply reading about them (e.g., they were involved in some sort of activism in the past, mostly before *Anonymous* became famous for its political hacking). No respondents from either of the two groups confirmed any current involvement with *Anonymous* or any other hacktivist group.

Specifically, concerning familiarity with *Anonymous* and hacktivism, four interviewees out of six were somewhat familiar with the group and the topic of hacktivism (through news, television and other sources); while two interviewees out of six either strongly alluded to, or outright stated that they used to have a more direct involvement with *Anonymous* and/or hacktivism (it was, however, stated that none of their activities included any illegal acts on their part). One of the interviewees, for example, said: "I've actually done some work with *Anonymous*, um… so, like you said, hacktivism is hacking for political purposes, much of what *Anonymous* did when I did some stuff with *Anonymous* was not hacktivism because it wasn't, it didn't have a political purpose" (Respondent #2, 2014).

All of the security professionals had an in-depth knowledge about *Anonymous*, stating facts reaching from the background and origin of the group to how *Anonymous* function and/or operates. Many security professionals, for example, mentioned that *Anonymous* is an off-shoot of *LulzSec*, another famous hacker group that pre-dates *Anonymous* and is famous for its members having profound hacking skills. *LulzSec*'s members, according to my interviewees, generally had better hacking skills than *Anonymous*, and are generally considered to be more capable when it comes to hacking expertise. *LulzSec*'s members are generally more respected in hacker circles than members of *Anonymous*.

Another important fact that many interviewees mentioned was that *Anonymous* did not emerge as a hacktivist group originally, but rather started with something referred to as "Operation Chanology," a protest movement against the church of Scientology, whose practices were strongly opposed by early members of *Anonymous*. Operation Chanology was mostly about "getting a laugh" or passing the time. However, eventually *Anonymous* became more involved with political hacking and soon became focused on matters of politics and activism rather than hacking for fun or out of boredom, and became known as a hacktivist group. The security professionals' opinions corresponded with what was discovered earlier on the forums. On the message boards, many members of *Anonymous* stated that the group originally began as a community that "caused trouble and generally trolled people and raised hell" (Anonnews.org 2013). Other *anons* stated that the group began with traditional activism and only later used hacking as a method of protest. What all *anons* agreed on, however, was that hacktivism was never the main focus of *Anonymous* when it first began. Similar to my interviewees, on the forums, many

members of *Anonymous* also mentioned the Church of Scientology as a turning point for the group - getting back at Scientology (*Anonymous* DDoS'd their website) changed the focus of the group from having no political focus to becoming seriously involved with activism. Members of the group realized that they could use their hacking abilities to do good, rather than to simply play pranks.

The name for the group itself, "Anonymous", came from the message boards 4Chan, a famous forum on the Internet where members are allowed to post anonymously without registering or leaving any trace of their identity. As 4Chan did not have any nicknames or any identifying information, members referred to themselves as to just *Anonymous*; or as *anons,* individually. The name "Anonymous" is also believed to have a symbolic meaning – the group's members often state that their goal is to fight for Internet privacy and freedom of information. The name itself, thus, symbolizes the group's position on such issues; being anonymous is highly important to most members. Many hacktivists believe that anonymity and security are highly treasured and should be protected by all means, and advise others on ways to protect their anonymity.

The most agreed upon topics, which all of the security professionals discussed in their interviews, were the following. In response to my first question – "What is your general knowledge of *Anonymous* and/or hacktivism?":

1) On *Anonymous* being a large, loose and all-inclusive group:

> "…It's a loose conglomerate, no one is in charge, [it is a] group where you can kind of take on a mantle yourself, do something, declare war on *Monsanto* or whoever… and then do… make your scary videos and all that" (Participant #2, 2014).

> "That's the problem you run into with any group that's very loose and all inclusive like that. Um, and actually I hate to use the…I hate to use this, um, this comparison, haha… but it's very similar to Al-Qaeda, where you

don't actually have to like get a certificate of anything to be part of Al-Qaeda and there're all these branches here and there that say they're part of Al-Qaeda, and other parts of Al-Qaeda say "No, no, what are you doing? No…", and so it's…it's, um, whenever you have a group that has very loose membership policies where you say: "You can use our name, that's fine, go ahead, you know, you are completely anonymous," or this or that… anyone can use it, anyone can do anything, and so you're doing it in the name of the group, and then everyone else says "No, no, no, we don't…we don't condone this", but you can't say that because you are including everybody, you know….by including everyone, you are condoning anybody doing anything in your name. Yeah, so, I mean if I go, you know, take a tire iron and bash someone's car and break all of their windows and say "Anonymous did this", technically Anonymous did it" (Participant #6, 2014).

"They seem a little… disorganized… I think it's hard to say that you're behind a group like that one way or the other, just because it's kind of flavor of the week. They're gonna go do what they're gonna do" (Participant #1, 2014).

"…With *Anonymous*, you are supposed to be… you don't know who anyone is, they wanna be just that, *Anonymous*. But, yeah, um, everyone has their own belief system within there" (Participant #4, 2014).

"[The group's members have diverse views and] … when you get a group that large, it's going to happen" (Participant #4, 2014).

2) On participating in *Anonymous*:

"…There's no leadership that's gonna tell them, right, and so it's really hard to classify them as anything, right, because all that is… is somebody's saying like…um, like, it's almost like a…like pure democracy, right, where there's nobody sending orders or trying to organize things; someone says "hey, we should do this," and if they can convince enough people to do it, it sort of reaches a critical mass and they go do it" (Participant #1, 2014).

"…the thing that helps them and hurts them most that there's absolutely no real leadership, and while that creates like a purely crowd sourced democratic sort of way of activism because if someone comes up with an idea and posts it and says "These guys are doing bad things", you know, "we should do something about it to help, you know, puppies or something", and if everyone thinks it's a good idea they'll join in. But if someone says "My science teacher is a jerk, we need to find out, you know, where he stores his money and take it", uh "No". And the biggest thing that you see on 4Chan is "We are not your personal army"…is

the…like the resounding sort of thing when someone says, you know, "This is my ex girlfriend's boyfriend, find out about him", you know, "We are not your personal army, we are not"…and that's the thing, you have to have an actual goal that everybody can get behind" (Participant #6, 2014).

"Yeah, [*Anonymous* is] almost like crowd sourced activism" (Participant #6, 2014).

"[*Anonymous* is] like Republicans, you know. If you say you're Republican, you're Republican. If you do something in the name of, you know, Republicans, technically you are doing it in the name of Republicans, it's just that you are possibly a very small minority within the Republicans, right? And… so, similarly, you can say that you a part of *Anonymous* and you are, and that you are doing something in the name of *Anonymous*, which you are…" (Participant #2, 2014).

My respondents' answers corresponded with the results of my content analysis of the forums. Members of *Anonymous* stated repeatedly that they represent: a) a decentralized group; b) a group that has no real leadership and opposes hierarchy in general; and c) a group that anyone can join or leave easily at any point. Some of my respondents compared *Anonymous* with Republicans and even Al-Qaeda. The comparisons were made to accentuate the fact that anyone can claim their affiliation with *Anonymous* simply because they share the beliefs of the group. Just like one can claim to be a Republican by claiming that he/she shares the Republican values, one can be considered to be a member of *Anonymous* simply because that individual claims to be a member of the group. Many members of *Anonymous* stated on the forums that there are no requirements for joining or leaving the group, one has simply to "believe in the idea and the movement" (Anonnews.org 2013).

Overall, all of the security professionals seemed to be well-informed about hacktivism and *Anonymous* in particular; the participants also generally agreed upon/had the same opinion on subjects like the background and origin of *Anonymous*, lack of

hierarchy and leadership within the group, and participation and membership 'rules' (or lack of thereof) within *Anonymous*.

**Theme Two: Security Professionals' Personal View on Hacktivism**

One of my early questions in the interviews dealt with how respondents felt about hacktivism in general and whether they thought of it as ethical. I was interested in discovering how the security professionals, or the legal hackers, felt about hacktivism personally. All of the six interviewees stated that they viewed hacktivism positively; although, some of them also added that hacktivism can have either very positive or negative consequences, depending on a situation or circumstances. I discuss the negative effects of hacktivism in more detail later, when examining the ethics behind hacking for political purposes. This theme, however, concerns my respondents' personal feelings on hacktivism and *Anonymous*. Since all of my respondents felt very positively about hacktivism, overall (while having a reasonable amount of caution about the phenomenon, simultaneously), I will cover the positive views of hacktivism that my respondents discussed with me.

Many of the respondents stated that they believe that hacking for political and social causes is a good thing overall. Hacktivism, when done for the right causes and by the right people, can bring about many positive changes to a society. One of the examples of such positive changes, for example, is that *Anonymous* is actively fighting for transparency and freedom of information. Similarly to Snowden and the NSA scandal, many leaks by *Anonymous* have helped to shed a light on certain problems within governments across the globe (*Anonymous* is known for leaking documents on governments all over the world). Many of my interviewees agreed that anything that moves a society towards transparency is generally a good thing:

"My personal belief is that anything that moves us towards transparency is
always a positive effect. The Snowden's leak was a positive effect, um,
you know, the Pentagon papers, Watergate, all of that… if it is increasing
transparency, it's a positive effect. Information wants to be free"
(Respondent #5, 2014).

"You know, WikiLeaks and the hackers that have worked to support
WikiLeaks, um, have done a great job with increasing transparency"
(Respondent #2, 2014).

Many of the security professionals also expressed the opinion that hacktivism

represents a direct response to socio-political problems within a society. Hacktivism is

typically triggered by a government or corporation being unresponsive to people's needs

and wants. One of my respondents stated that the direction in which hacktivism will

develop in the future directly depends on whether anything changes in the political arena.

If corruption persists, hacktivism is likely to remain; if certain political issues get better,

hacktivism may see a phase of decrease in popularity:

"A lot of that depends on the direction that the things that are causing
hacktivism go. If our government sees that the people are craving
transparency and honesty and an open government, then hacktivism will
no longer have the same purpose that it does today. It won't be as
prevalent if we don't need it as much. An alternative is… the government
does more to subjugate its citizens, you know, they do more surveillance
programs, they do…you know, they start deporting hacktivists to Gitmo,
or whatever. And then hacktivism is just gonna get worse, I mean… so I
guess, it really depends on all of the things that are driving it 'cause it's,
you know, it's a symptom of a larger disease" (Respondent #5, 2014).

The idea that hacktivism represents a response to political and social troubles

corresponds with the opinion of some members of *Anonymous,* who stated on the forums

that the primary reason the group gained political focus was because "the world is in

trouble" (Anonnews.org 2013). Many members of the group stated that the group

continues to exist because someone needs to protect people's interests from governments

and corporations.

The idea that political events affect the way hacktivism develops was mirrored in

a study by Yip and Webber (2011), who in their article "Hacktivism: A Theoretical and

Empirical Exploration of China's Cyber Warriors" explore the ways in which hacktivism

is triggered by political events. More specifically, the authors decided to test their

hypothesis that membership in hacktivists' groups will rise at times of important political

events (e.g., when the government denies freedom to its people). Yip and Webber proved

that there is a "correlation between membership growth patterns of the hacktivist online

forums and the timing of the political events" (2011:2). The authors based their

hypothesis on the concept of relative deprivation, which was first formulated by Walter

Runciman (i.e., people participating in social movements as a way of acquiring

something to which they feel deprived). In the Yip and Webber study, specifically, the

authors argued that when Chinese people feel the most threatened and/or suppressed by

their government, the amount of hacktivists would go up accordingly. Similar to the Yip

and Webber study, some of my respondents stated that they feel hacktivism will become

an even bigger phenomenon, if social and political problems in the U.S. continue to be

unresolved, or get worse.

Overall, all of the security professionals in one way or another expressed

sympathy towards hacktivism and/or *Anonymous*:

> "So, I think some of the stuff they do, I think it's… I think it's, you know,
> good to protest some of the things [hacktivists] protest, that kind of thing.
> So, I mean, I'd say that some of their causes I could get behind"
> (Respondent #1, 2014).

> "But there are some things [hacktivists] do that I can get behind for sure:
> exposing corruption, definitely for me… I can get behind that"
> (Respondent #4, 2014).

"I think *Anonymous* may have existed as a non-political movement in the past but it got swept up in a larger, growing attitude… and... so, I'm not necessarily for it but I understand why it exists. And I have sympathies towards it." (Respondent #3, 2014).

"If you are fighting injustice and the only real weapon that you have available to you is hacking, um, I think that maybe crosses the boundary from activism into something else, but I still see that as justified" (Respondent #2, 2014).

"[Hacktivism] definitely kind of fits into [the] vigilante sort of idea, and you can argue that it worked for the greater good even if it was fake, even if it was just a bomb threat… even if they might have been fake bombs, they still saved a lot of people a lot of trouble, so…and, at the very worse, [hacktivists] saved some trouble, and, at the very best, they saved lives" (Respondent #6, 2014).

"[*Anonymous*] always seems to be doing it for a good cause in general, I mean, sometimes they just go off and do crappy things, but in general they always rally behind these good causes like supporting WikiLeaks, supporting truth and freedom and stuff like that" (Respondent #5, 2014).

## Theme Three: "Anonymous" and Their Hacking Skills

*Anonymous* and their members' ability to hack, as well as the subject of hacktivism, has become a separate theme throughout the interviews. I discussed these issues with my interview participants very extensively. All of the interviewees have agreed that: a) hacktivism pre-dated *Anonymous*; b) *Anonymous* was not always a hacktivist group (i.e., *Anonymous* used to be a group that hacked for fun rather than a political cause, and only over time the group has become known as 'hacktivist'); and c) even though *Anonymous* is known as 'that hacktivist group,' most members of *Anonymous* don't have any real hacking skills; in fact, most of them are not very tech-savvy. Most members of *Anonymous* consist of people with average/basic computer skills.

The topic of *Anonymous'* members not being real hackers was the focus of discussion for these research participants. All of the security professionals agreed that most of what *Anonymous* does as a group cannot be called hacking or true hacktivism.

121

Some of the security professionals mentioned that the fact people refer to *Anonymous* as 'a hacktivist group' is somewhat misleading since hacking assumes one understands programming, security, and complex methods of gaining access to a resource on the Internet. My respondents' view corresponds with what many *Anonymous* members have said, in this regard, on the forums: many claimed that the majority of members are not tech-savvy individuals. Many members of the group, in fact, openly state that only a small portion of the group represents hackers and hacktivists; the rest represent either traditional activists (people who participate in regular street rallies) or digital activists (people who engage in legal activism online, such as electronic advocacy or e-campaigning).

Some of the security professionals said that hacktivism is a badly phrased concept, since it assumes that some sort of hacking is used to achieve a political goal. In reality, most self-proclaimed hacktivists within *Anonymous* don't possess any real hacking skills, although they do use technology and the Internet for achieving a political goal. However, hacking, in all of the security professionals' view, involves in-depth computer skills, not just using technology, which almost anyone can do. One of my respondents said the following

> "Hacktivism is an unfortunate term… a lot of [hacktivism] really is just online activism. And in the case of like those websites, things I was talking about, there's no hacking involved, there's a bunch of people who download a piece of software… and it's just denial-of-service seen on the websites. So, in my mind, that's not hacking but it's called hacktivism" (Participant #3, 2014).

Academic literature (Conway 2003; Jordan 2002) defines hacking as illicit computer intrusion by criminals and explorers with the intention to cause damage or steal information. While some members of *Anonymous* most certainly have done this in the

122

past, most members of the group are not hackers in accordance with this specific

definition. In other words, members of *Anonymous* do not have the ability to gain such

unauthorized access, and therefore cannot be called hackers, according to security

professionals.

My interview participants stated that most *Anonymous'* members use the tools

known as Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC). Those

tools can be defined as applications one may use to flood a website with traffic to the

point that the website crashes. This again corresponds with what I have discovered by

analyzing the *Anonymous* forums. LOIC and HOIC were mentioned repeatedly by *anons*

on the forums – people on the message board discussed things such as how to use the

programs properly and which of the two represents a superior program.

Anyone can use the LOIC and HOIC applications: they are created in a way that

any user, even the most inexperienced with computers and technology, can easily learn to

use them. This indeed seems to be the truth: many members of *Anonymous* on the forums

state that the programs are easy to use. Users simply needed to look up step by step

instructions on how to use them, and these instructions were often posted on the forum

for new users.

The technical effect that LOIC and HOIC produce is called a DDoS, a

"Distributed Denial-of Service" attack. To crash a website or to flood it with a great

amount of traffic, all the participants have to do is download either of the applications.

Then, the users would typically launch the application at a predetermined time, sending

internet traffic to the target website. Such a targeted effort is effective at overloading a

website and temporarily disabling it; however, such a method cannot be qualified as

hacking since hacking typically uses more complex forms of gaining control over a site

or a network. LOIC and HOIC applications are most effective when a large amount of

users are using the application at the same time. In other words, if one wants to hack a

site, LOIC and HOIC are pretty ineffective tools.  If, however, one would like to

temporarily disable a website, it can be effective with a large group of like-minded users

participating.



**Figure 12: LOIC/HOIC application – how it works?**

A user who wants to crash a website would typically enter the URL or IP address

of the site he or she wants to flood with traffic (the image above), and then press a button

to send repeated requests to that website. When a large group of people send requests like

this simultaneously, this can cause it to crash. Similar effects often happen in day-to-day

life to sites that aren't being attacked, when too many customers, for instance, are using

the website and it goes offline as a result. One security professional explained how

LOIC/HOIC applications work in the following way:

> "So, the majority of hacktivists in *Anonymous* run a tool called the *Low-
> Orbit Ion Cannon*. I think they have a *High Orbit* one now, too… Pretty
> much what it is, is you give it an address online to target, and it throws out
> a denial of service attack.  So it's just gonna throw requests out to this IP
> address or domain name or whatever until it gets flooded or whatever and
> crashes. That's sort of similar to pressing the "hack" button on a black box,
> right? Most of them don't know how it works, and I don't think the
> majority of them could pull off an attack more complex than typing in an
> address and pressing the attack button. That being said, I know there were
> a few of them, particularly when they had, um, *Lulzsec*, which was sort of

124

a part of *Anonymous*, and it seemed like they had some guys there with some real, uh, hacking chops" (Participant #1, 2014)

In sum, using applications like LOIC and HOIC does not qualify one as a hacker, anyone can use or be taught to use those applications:

"So, *Anonymous* is, from what I know… um, a large majority of them are not very computer-savvy. It's a lot of people who just wanna make a difference, so they kind of come in and just, like, do what they are told, they download tools that they know that the people who are more technical know of, and they DDoS a site, um, versus just a regular DoS because it's a group of them, so, yeah, like I said, a large majority of them are not, um, too technical, especially when you look at *Anonymous* – generally, what they are doing is DDoS-ing and not doing a very technical attack but then you get… like I was talking before, the offshoot of *Anonymous*, *Lulzsec* was a group of very technical hackers, who… they were doing more, I believe it was SQL injections and [the like]" (Participant #4, 2014).

"One of their main tool is called Low Orbit Ion Cannon, right, where the… the idea is if you want to take down a website, in the past you had to organize you and a bunch of people to actually know how to DoS it, know how to, you know, install a script or, um, write a script to keep making these requests to take it down, to overload the server. With Low Orbit Ion Cannon, you download an application and that's it, it does it all for you, you decide…you get to determine who you want to connect with… you just install a client on your computer and it will talk to whoever you wanna talk to, right, and that person will direct every computer that's connected to them against this one. So, you know, it's literally…someone says "I'm gonna take down American Express. Anyone who wants to do that, download Low Orbit Ion Cannon, and connect with me." Here we go, that's it, like four clicks, and now I'm part of Anonymous DDoS-ing American Express" (Participant #6, 2014).

"A lot of [*Anonymous* does] doesn't involve hacking, just annoying the crap out of people" (Participant #2, 2014).

Another point that was made by the respondents was that *Anonymous* has to have an easy way of attacking a website or a network. The simplicity and ease of use of applications like LOIC and HOIC brings members of the group together and makes each feel like he/she can contribute, despite not being a tech-savvy person:

125

"*Anonymous* for a long time was using the tool called Low Orbit Ion Cannon, which was a traffic flooding tool. And it basically just, you know, um, when a whole bunch of people used it on the same target at once, it would often bring that system down because it couldn't handle the amount of traffic being sent to it. Um, they've since retired that tool because it doesn't do anything to protect, you know, like your IP address. It doesn't do anything to anonymize you, so it's very obvious who's attacking when people are using Low Orbit Ion Cannon. Um, the replacement, High Orbit Ion Cannon, has been, um, I haven't actually taken a look at that particular tool at all but my understanding is that it does, at least, something to provide some anonymity. Um, yeah, but I mean that's the sort of thing, where you just, you know… they had to, because there were so many non-technical *Anonymous* members… um, in order to organize a raid, where they do something like a distributed denial of service attack, um, they needed something that was simple enough for anybody to use. So, you just, you know, distributed the tool somehow and say, you know, put in this value and this value and this value, and then hit "Go" and you're helping" (Participant #2, 2014).

In other words, in order to be effective or be able to organize, *Anonymous* needs to have a simple means of carrying out an attack, so that all members can participate. If anyone can use a tool, that means an unlimited number of people can participate in the group's activities. The fact that anyone can use simple applications like LOIC and HOIC also gives non tech-savvy members of *Anonymous* a sense of importance: they may feel they are just as important as the members who have an in-depth knowledge of internet security, since all can contribute equally to the cause of the group. So, if applications like LOIC and HOIC did not exist or weren't available, *Anonymous*' composition may be different today – possibly a smaller group consisting of skilled hackers. But *Anonymous* as we know it today is a rather large, diverse group that attracts people with different computer skills. My forum research aligns with the latter statement – members of *Anonymous* often took offense when they were referred to as a 'hacktivist group.' Many *anons* on the forum claimed that it would not be fair to characterize the group as such, since the majority of its members do not represents hacktivists. They may be called cyber

126

criminals, but there is a clear distinction between computer criminals and hackers: the

former uses technology to commit an illegal act, but does not possess in-depth technology

knowledge; the latter is both computer knowledgeable and committing a crime with

technology.

Some security professionals also noted that the media has had some role in how

*Anonymous* became known as a 'hacktivist group': some in the media have contributed to

the myth of *Anonymous'* hacking skills, which are mostly non-existent, according to the

respondents. Because most people do not understand what hacking really means or what

skills it requires, many individuals tend to overestimate what *Anonymous* has done and/or

are doing:

> "…The media and hackers have always had an, uh, convoluted
> relationship. I think technology beyond sort of the basics, like Facebook
> and stuff like that. The stuff that everyone knows how to do.  I don't think
> the media is very good at trying to understand technology and technology
> related news. And I think when you talk about these, like, superhackers,
> right, um, it sensationalizes things, and that's good for the news program.
> That makes people interested and they wanna watch it" (Participant #1,
> 2014).

> "We do all kinds of interviews with [journalists], there's all kinds of press
> releases … it's common if they're doing some kind of interview with a
> hacker, and they don't understand what he's talking about, right, they'll try
> to explain what he's talking about as best they can, right. Normally that
> involves… just like when you're talking to somebody, you'll tell them
> something very complex and then simplify it for them if they're not really
> knowledgeable within that field. And so they take the simplified bits and
> put those in there, right, but there's always that sorta spin to it, of like,
> superhacker who's crouched in the dark in his basement, typing away on
> his computer for 24 hours a day. Um, and so that's sorta the common… I
> guess that's the best way to say it, is that's the common stereotype for
> hackers, right? And I don't think the media is knowledgeable enough
> about technology and security to sorta sift through all that and differentiate
> between, like, yeah this guy really is a superhacker, he's pulled off all
> these complex attacks, and here's a group of kids that download a tool that
> let's them do a denial of service attack.  And so they're just always sort of
> apply that blanket stereotype whenever hackers come into a story"
> (Participant #1, 2014).

Similar to my interview respondents, *Anonymous'* members also pointed out that the media has had a tremendous influence on the group's reputation, by labeling them as 'hacktivists' or 'hackers.' One *anon*, for example, stated: "The media paints *Anonymous* as a group of "elite hackers"…That could not be further from the truth" (Anonnews.org 2013).

In sum, even though *Anonymous* consists of mostly non-hackers, according to my interview respondents, the media often contributes to the spread of the stereotype of *Anonymous* being a 'hacker group.' Even though *Anonymous* may have some hackers among its membership, the group primarily consists of non tech-savvy people. The respondents' opinions corresponds with the results of my content analysis: throughout my research of the online message boards where *Anonymous'* members communicate, I have found that the majority of the members neither identified themselves as hackers, nor seemed to have any in-depth hacking abilities.

**Theme Four: Ethics behind Hacktivism**

When it came to the discussion of ethics in relation to hacking for a political cause, all security professionals had the same opinion: hacktivism can be both ethical and unethical, and it is a matter of who is behind hacktivism and what is the cause. In other words, hacktivism can be both beneficial and harmful depending on the circumstances:

> "Hacktivism is really just hacking with the intention of causing some sort of social change. It could be a negative change, like you could have, for instance, maybe some fundamentalist Christian groups hack into, like, abortion clinics to see who's having an abortion and harass them – that would still be hacktivism but that would be negative. So I think hacktivism is in and of itself, neither negative or positive" (Participant #5, 2014).

One of the interviewees, for example, said that when it come to *Anonymous*, it is important to differentiate between illegal and wrong. While something may be illegal, it

128

may not necessarily wrong, as well. According to the respondent, there is nothing

inherently wrong with activism or hacktivism, as long as it is done for a good cause and

by well-intentioned people:

> "Ethics are, you know, obviously very tricky, there are lots of different ethical models, um, from an ethical model of "do no harm," hacktivism is not ethical because they're doing harm. But, you know, I think there's definitely a difference between illegal and wrong. And it's very important to keep that in mind when you think about questions of ethics. Um, I think… I think there's nothing inherently wrong with activism, and hacking to achieve that goal… there's nothing necessarily wrong with that" (Participant #2, 2014).

One member, on the message board, states a similar idea. That there is a

difference between what is okay to do and what is right to do: "There is… a difference

between what is "okay" and what is "right". Is it okay/right to hack into someone's

computer to get their bank account information? In my opinion, no… Now, it is okay to

hack into the same computer and gain access to a remote server that is used by the NSA

to illegally spy on people? Perhaps" (Anonnews.org 2013).

Overall, the idea that hacktivism is permissible, as long as it is ethical,

corresponds with the opinions of *Anonymous*' members on the message boards. Many

*anons* claimed that they strongly believe in ethical hacking, which they defined as

hacking to achieve a positive social change. Hacking, according to many *anons*,

represents a powerful tool; thus, hacking should be used only for good, and only be used

in circumstances where it is absolutely necessary. In sum, both my interview respondents

and *Anonymous* members expressed a similar idea – hacktivism or hacking can be

considered ethical, as long as it is used for positive social change rather than for a

malicious purpose. In other words, both security professionals and *Anonymous*' members

defined ethical hacktivism very similarly – as hacktivism that is aimed at positive change.

A few participants mentioned the idea of vigilante justice: when a certain amount of harm is done in order to prevent a greater harm. One respondent referred to Batman movies, when a superhero takes justice into his own hands, but does so to protect the people of his city. Another security professional made a reference to the protagonist of the famous American TV show *Dexter*, in which the main character kills murderers and other criminals in order to prevent those individuals from committing another crime. This is what some respondents said in regards to vigilante justice:

> "I think killing somebody is wrong but if you know that that person is going… is… if somebody is about to kill six people and you kill them, you save lives. You saved five lives…you are up by five, right? Um, and actually the show *Dexter* explores that particular ethical question pretty well" (Participant #2, 2014).

> "I think, you know, doing something harmful to prevent greater harm, um, from a utilitarian standpoint, you know most good for the most number of people, can be definitely seem ethical... um, especially, with an organization like Scientology, um, which has been in the past very abusive towards its members, you know… harming Scientology to prevent harm to the people Scientology is harming, that I see as ethical. Um, other things not as much, you know" (Participant #2, 2014).

> "I think sometimes, it's like a Batman movie… you have to take matters into your own hands, and when police aren't on your side… but you're good, even though you are criminal" (Participant #3, 2014).

Some agreed that vigilante justice is not always a good thing. Sometimes it can do a lot of harm. However, oftentimes vigilante justice comes to exist as a result of a lack of attention to peoples' interests – e.g., when authorities fail to perform their duties. Some respondents shared a similar opinion: when authorities (whether this is police or the government) fail their citizens, vigilante justice is more likely to exist in a society. One of the participants, for example, made a point that the reason *Anonymous* and other similar groups came to exist is because of an abuse of government and corporate power:

"On the one hand, you have corporations that are clearly breaking the law, and there's no legal framework or there's no legal pressure coming down to stop them… so, if you ask how I feel about the *Anonymous* and its legal grain is… I see it as a reflection, below the power structure it is a reflection of what's happening above the power structure … I mean, *Dexter* and this hacktivism or *Anonymous* phenomenon are both manifestations of that attitude developing…and, yeah, if you have corrupt cops, you're going solve your own problems in your own neighborhood 'cause cops aren't goanna help" (Participant #3, 2014).

"On the one hand, vigilante justice isn't good, um, and that's what that is – they are taking matters into their own hands – but, on the other hand, I guess, considering, um…from my personal standpoint, the complete lack of restraint that corporations have in their operations in this world, that I think *Anonymous* is only representative of a larger fervor that's growing in the public in the United States. And that's an indirect response to this creeping corporate control and just rigidity to that corporate reach that is expanding" (Participant #3, 2014).

The idea of using hacktivism as a last resort for social change, when all other means have proved ineffective, corresponds with the opinions of many *anons* on the message boards. Some *Anonymous* members stated that hacktivism came into place as a way of replacing traditional protest, which often fails or goes unnoticed. Many anons expressed the idea that the government and corporations have failed people and that traditional means of protest often lead to few results. Thus, hacktivism can be viewed as a phenomenon that is, to a certain degree, forced to exist.

In sum, most of the security professionals said that hacktivism stems from the idea of vigilante justice, which can be either good or bad. One of the benefits of vigilante justice is that groups like *Anonymous* give a voice or representation to a powerless group that would otherwise not have such a voice. However, some respondents also stated that vigilante justice or vigilante activism can be extremely dangerous and have a negative impact. One of the respondents illustrated an example by comparing *Anonymous* to a neighborhood watch group called the *Crips* that slowly turned into a violent gang:

131

"[*The Crips*] is one of the gangs in LA and it kind of actually franchised all across the nation. And they started as a neighborhood watch program by a couple of 17 year olds. And their idea was that there were so many gangs in neighborhood that they got a bunch of people together and instead of like calling the police or forming, you know, a peaceful protest, they went and started beating these gang leaders up, you know, the drug dealers that… but then it kind of turned into a feared gang in itself. They started with vigilante intentions, it started with good ideas but they weren't able to control where the group went…" (Participant #6, 2014).

In other words, because there was no forcible law or guidelines behind the actions of the *Crips*, the group could transform (and it, in fact, did change) easily into a different, more dangerous group. Similar to the *Crips*, *Anonymous* being a loose organization that has no forcible law behind its actions can be easily transformed into a potentially dangerous group. When there are no clear rules in a group, vigilante justice can go wrong, mistakes can be made, or groups co-opted by malicious leaders. Some of the potential effects of vigilante justice can be, among others, cyber-bullying and the targeting of an innocent person or organization. Many security professionals echoed this opinion, saying that all vigilante groups have the potential to become dangerous and/or harmful:

"…It's a vigilante sort of thing, and any type of vigilante actions …sometimes vigilante organization has the potential to become terroristic" (Participant #6, 2014).

"[Hacktivism sure] can save lives but the fact is members of Anonymous aren't trained in stopping crime, and so you get people… you end up with, you know, hacktivism turning into cyber bullying … They are uninformed for the most part and sometimes they get it right, sometimes they get it wrong" (Participant #6, 2014).

The idea that *Anonymous* makes mistakes from time to time was echoed by *Anonymous'* members, as well. Many *anons* on the forum stated that hacktivism can certainly go in the wrong direction when led by the ill-intentioned. *Anonymous* makes mistakes occasionally, many *anons* admitted. Because the group is all-inclusive, anyone

132

can commit bad acts on behalf of the group, and so *Anonymous'* reputation often suffers

as a result of such incidents.  However, members of *Anonymous* also pointed out that in a

number of cases where *Anonymous* has done something bad, it was carried out by "selfish

people who cause harm to massage their own egos" rather than true members of the

group.

Even though most security professionals agreed that hacktivism or vigilante

justice can go wrong or turn dangerous, *Anonymous* specifically does not represent a

threat to most people in a society. One of the security professionals noted that it is

important to differentiate between the terms "dangerous" and "threat":

> "Yes, *Anonymous'* members are absolutely dangerous but I think that
> there's an important distinction between are they dangerous and are they a
> threat, like, I know that they could do bad things but in general, like, I
> haven't really seen them doing bad things before." (Participant #5, 2014)

> "[*Anonymous*] always seem to be doing it for a good cause in general, I
> mean, sometimes they just go off and do crappy things but in general they
> always rally behind these good causes like supporting WikiLeaks,
> supporting truth and freedom and stuff like that, so do I consider them
> dangerous? Yes. But do I feel threatened by them? Not at all" (Participant
> #5, 2014).

> "For the most part people don't have to worry about a group like
> [*Anonymous*] because they aren't really gonna come after you, they are
> looking at more corporations that stand in the ways of what they believe…
> people have to watch out more for hackers, not hacktivists. Um,
> hacktivists…they tend to hack for a cause, they don't hack people for
> malicious intent" (Participant #4, 2014).

In other words, even though *Anonymous* can be dangerous to specific

organizations and/or individuals in a society, overall *Anonymous* does not represent a

threat to a society because most of the group's actions are well-intentioned. This opinion

was also echoed by *Anonymous'* members: many claimed that, even though many selfish

people exist who use the name of *Anonymous* to commit bad acts, the majority of the

group believes in ethical hacking and would never use hacking for personal agendas. In

other words, most *anons* seem to believe that the group is mostly composed of well-

intentioned hackers and activists, who do not represent a danger to society or the public.

Overall, when I discussed ethics behind hacktivism and/or *Anonymous*, security

professionals had nearly identical opinions, which can be summarized in the following

way:

**Table 3: Security professionals on ethics of hacktivism**

| **Is Hacktivism Ethical?** |
| --- |
| Hacktivism can be defined as hacking done with the purpose of bringing about social change. Such social change can be both positive and negative, depending on who is behind the cause. So, hacktivism can be either ethical or unethical; the ethics of it depends on circumstances. <br><br> Hacktivism can be considered ethical in cases when some harm is done to prevent even greater harm. Hacktivism stems from the idea of vigilante justice. |
| **Is Hacktivism Dangerous?** |
| Hacktivism has the potential to be dangerous and/or terroristic. It can turn into cyber-bullying; hacktivists often make mistakes and may target innocent people/organizations. |
| **Is Hacktivism is a Threat?** |
| Hacktivism and hacktivists can be dangerous but they do not represent a threat to society overall. There is a difference between being dangerous and being a threat. Most people should not fear hacktivists. Hacktivists are well-intentioned for the most part, since most of their intentions are about bringing positive change. |

**Theme Five: Hacktivism and Its Effects of Security Industry**

All of the respondents have said that hacktivism and/or groups like *Anonymous* have not

had any direct effect on the security industry. One of my respondents, for instance, noted

that the current methods of *Anonymous* are not going to change the face of the security

industry: "So it doesn't seem like [their main method, DDoS attacks] is going to be

something that's gonna change the face of security, unless they change their methods as

well" (Respondent #6, 2014). In other words, because *Anonymous* do not do a lot of

actual hacking, such methods do not have an effect the security industry, according to my

interviews.

However, all of the security professionals were in agreement that hacktivists and

groups like *Anonymous* have had an indirect effect on the security industry and society

overall: security companies and corporations in general have become more aware of

insecurities in the Internet because of hacktivists. Not only have groups like *Anonymous*

helped to bring about such awareness, hacktivist attacks have also helped to improve

websites and/or make them more functional and secure:

> "A lot of what happened with *Anonymous*… you know, once they started,
> um, hacking lots of people as a political thing and hacktivism in general
> has had… hacktivism in general has had a little effect that I've seen on the
> security industry but *Anonymous* was so high, especially *LulzSec*, was so
> high profile… and sort of aired of dirty laundry of everybody, like "hey,
> look, everybody's insecure, isn't that funny?", right? And, well, their goal
> was like the classic *Anonymous*, the old *Anonymous*, to just have some
> fun. They made a very good point, possibly unintentionally… um, and
> then there were sort of actors within *LulzSec*, which, you know, is a
> spinoff group of *Anonymous*, like Jeremy Hammond who was actually
> trying to make a difference. Jeremy Hammond has been a hacktivist for a
> long time, and, um, his hack of *Stratfor* was politically motivated. So,
> Jeremy Hammond, um, hacked *Stratfor* as a political move, um, and… I
> think, you know, so to get back to the actual question, I think a lot of
> people sort of had their eyes opened to just how insecure modern
> computer systems are, because of *LulzSec*" (Respondent #2, 2014).

> "WikiLeaks and *Anonymous* stuff – all of it brings awareness to the
> insecurities that are out there while at the same time screwing over those
> who got hacked" (Respondent #3, 2014).

> "Um, I don't know about the long-term effects of, you know, what some
> of their protests and hacks will have on society…um, what I will say is
> that it's probably helped to raise some security awareness, particularly for
> some companies out there, right, who think that they might be a target of
> something like that at some point. They might decide, you know what?

We should really review our security and make sure it's up to date, maybe get a pen test, have someone look at it" (Respondent #1, 2014).

Another point that was brought up in the interviews was that security companies and security professionals often feel pressure to close security loopholes. One of the respondents stated: "Security professionals feel big pressure in the sense that we need to make sure sites are secure, so hacktivists or just even hackers alone don't just come in and break people's websites or into their networks" (Respondent #4, 2014). Despite such pressure, some respondents said that although hacktivists constantly keep security companies busy, groups like *Anonymous* do not pose any threat to security companies themselves: "Hacktivists don't pose a threat to my company, we're a security company, we're fairly secure" (Respondent #1, 2014).

Another indirect effect of hacktivism that some security professionals mentioned was the growth of the security industry. Some of my respondents said now, more than ever before, companies want to purchase security tests and services. As a result of more online breaches, the demand for security services is increasing. Thus, hacktivism also promotes the expansion of the security industry: "There are more companies. Um, our company I feel is one of the bigger names and obviously there are other big names out there too, but you are seeing a lot more smaller names popping up, as well… The security industry is growing without a doubt" (Respondent #4, 2014).

Finally, some respondents stated that despite the fact that hacktivists often harm other companies, they have had a rather positive effect on the security industry, overall. One respondent, for instance, claimed that groups like *Anonymous* not only helped bring awareness about Internet insecurity, but also forced society to take security more

seriously. In other words, hacktivists and groups like *Anonymous* have changed the way people think about security:

> "Hacktivists have had a very positive effect. They are publicizing bugs that would otherwise either go undiscovered completely, or they would be privately disclosed to a vendor and they would never be made public. Um, the simple fact of the matter is that at the end of the day security is something that people try to ignore as much as they can. Nobody wants to deal with security, and when people like *Anonymous* go around with these high profile breeches, um, it forces people to take security seriously. And they…they are starting a different kind of conversation about security. Traditionally security… you know, you are preventing people from stealing credit card information or this or that or the other, but *Anonymous* operates in a completely different way targeting a completely different type of data than your…than cyber criminals, so they are making people think "What data do I have and is it valuable?," you know, it's not just about credit card numbers anymore. And, I mean, that's a very important thing that's pushing the security industry forward" (Respondent #5, 2014).

It is worth mentioning that even though members of *Anonymous* themselves did not discuss on their forum the ways in which hacktivism might affect security companies worldwide, security in general – including the fragility of the Internet and computer systems – was discussed by the *anons* very extensively. Most members of *Anonymous* seemed to take security very seriously, and it seemed that, overall, members of *Anonymous* were very aware of the insecurities in modern technology, including personal computers and the Internet. *Anons* on the forums often warned others about securing their computers and taking other precautionary measures, especially prior to engaging in any illegal activities (such as participating in a DDoS attack). It seemed that security was very crucial to members of the group. Many *anons* expressed fears of being spied on by the government, or even being identified and arrested. Securing one's personal computer and local network was an important step to avoid being tracked and/or arrested.

Overall, when I asked about the effects of hacktivism on the security industry, or how hacktivism and groups like *Anonymous* affected the respondents at work, answers

137

were mostly in agreement. Table 4 illustrates the opinions of the security professionals in this regard.

**Table 4: Hacktivism and its effects on security industry**

| **Direct and Indirect Effects of Hacktivism** |
|---|
| Hacktivism does not have a lot of direct effects on the security industry. However, hacktivists and groups like *Anonymous* have important indirect effects on the security industry: a) hacktivism has brought more awareness of Internet's insecurity; b) hacktivism encourages the expansion of the security industry; and c) hacktivism changes the way people think or conceptualize security – people now take security more seriously than before. |
| **Is Hacktivism a Threat to Security Companies?** |
| Hacktivism and hacktivists can be dangerous to some companies. However, hacktivists do not represent a threat to security companies or security professionals. |

**Theme Six: Importance of the Guy Fawkes Masks**

When I asked my respondents about anonymity and *Anonymous* (the question specifically asked "What are some possible reasons for hacktivists to hide their identity?"), the respondents named a variety of reasons. I have classified their answers into five broad categories: 1) hacktivists wear (Guy Fawkes) masks in order to be more inclusive; 2) hacktivists chose to wear masks because they want to avoid arrest and/or persecution; 3) hacktivists wear masks as a way of making a statement in regard to what they believe in; 4) hacktivists hide their faces and identities to avoid jeopardizing their careers and/or jobs; and 5) hacktivists hide their identities as a way of empowering their members. Some of these responses correspond with what members of *Anonymous* themselves have said in regard to hiding their identities and about wearing Guy Fawkes masks.

One of the most common reasons that a hacktivist may want to stay anonymous, whether in a live street protest or in online activism and/or hacktivism, is because they want to be more inclusive, according to the respondents. For example, one respondent stated that wearing the same mask serves as a way of promoting equality among members, and if members feel equal, they feel more united. In other words, wearing the same mask promotes a sense of unity among members of *Anonymous*:

> "And they all use the same mask. It's not just wear a mask, like protestors have in the past, it's all wear the same mask which plays into that idea that everyone and no one is *Anonymous*" (Respondent #3, 2014).

> "…it's to become more inclusive – if nobody has a face, anybody can be a part of it. You put your own identity on to the protestors, so they can be you. You know, I think it's just a way of being more inclusive" (Respondent #6, 2014).

One of my respondents noted that in order to promote collective group identity, it is important for *Anonymous* to hide individual identity, and this can be achieved through wearing the masks. Wearing the same mask, thus, promotes a sense of belonging among group members:

> "[Wearing the masks is] almost like a mob mentality – losing your individual identity to be part of the collective group identity, like, the whole point of the group is that you are not an individual but you are just a part of the group" (Respondent #5, 2014).

> "Wearing the masks is about maintaining sense of unity, while still being anonymous" (Respondent #4, 2014).

Many of the security professionals also named the desire to not face consequences for their activism/hacktivism as a reason that members of *Anonymous* want to hide their identities. Most respondents said that hacktivists and other members of *Anonymous* want to hide who they are for either, or both, of these reasons: a) they do not want to face retaliation from their 'enemies' (example: Scientology seeking revenge on *Anonymous* members), and b) they want to avoid being arrested and/or prosecuted by the authorities.

139

In other words, members of *Anonymous* face a serious threat on both sides. On the

one hand, from a government that is known for treating hacktivists harshly, and, on the

other hand, from the people and/or groups whom *Anonymous* targets. In regard to the

latter, many security professionals mentioned that the church of Scientology is known for

harassing individuals who stand up to them. Obviously, then, hacktivists want to avoid

harassment from the church, as well as avoid arrest and/or prosecution:

> "Um, of course, there are things we want to keep private, and, of course, if
> you're an activist, you face a very real threat of retaliation… and
> Scientology is known for retaliating against its enemies or perceived
> enemies. Clearly, *Anonymous* made itself an enemy of Scientology, very
> much so. So, it makes a lot of sense for them to hide their identities.
> Because Scientology will ruin your life if you mess with them, they will
> try very hard" (Respondent #2, 2014).

> "…There are things like when they protest scientology. Scientology is
> well-known for going after... right, so they'll go after you, um, and with
> the hacking stuff, it's fairly straight forward – you don't wanna go to jail,
> right?" (Respondent #1, 2014).

> "…it's very important to remember there's a difference between illegal
> and wrong. If you're doing something that's right that's illegal, you need
> to hide that. You need to maintain anonymity, you need to maintain
> secrecy, privacy, in order to keep from being prosecuted by what is unjust
> law, if that is really the case. So, I don't think that being *Anonymous*
> maintaining anonymity means you are doing something wrong"
> (Respondent #2, 2014).

> "[Why are they wearing the masks? I think the obvious answer [is] to
> avoid prosecution" (Respondent #6, 2014).

> "I mean, there's the obvious legal consequences, you know, they don't
> want to go to jail, and here's the way that it started, you know, with the B
> bulletin board. Um, so, that… that probably had a role in the formative
> nature of it but why did they continue to be *Anonymous*, it's, you know,
> like I said, the legal ramifications" (Respondent #5, 2014).

The idea of wearing masks as a way of protecting group members corresponds

with what *Anonymous*' members themselves stated on the message boards: many anons

said that the Guy Fawkes masks have a very specific function – to protect its members

from being identified, arrested, and/or prosecuted. Many *anons* talked about the police

taking pictures of protestors, as well as the U.S. government spying on people online.

Whether one chooses to engage in a traditional protest or digital activism, and especially

hacktivism, one should always wear a mask to secure his or her identity, according to

members.

Many security professionals, when discussing authorities prosecuting hacktivists

and activists, mentioned the government often treats protestors very harshly, especially

hacktivists or individuals committing a computer crime as a method of protest. As stated

in the quotes above, some of my respondents referred to the ways in which authorities

punish protestors as "unjust law." It felt as if many of my interviewees sympathized with

hacktivists and traditional activists. Many of my respondents expressed that hiding one's

identity from the authorities is something that everyone should do, regardless of if they

participate in a regular street protest (a legal activity), or in hacktivism (an illegal

activity). Furthermore, many security professionals mentioned that privacy is everyone's

right, and that hiding one's identity should not be thought of as doing something wrong.

The third reason, many respondents said, that members of *Anonymous* may want

to hide their identities named was that being anonymous sends a number of important

messages to society. One such message is an anti-establishment idea. It's known that

members of *Anonymous* wear a specific type of mask (Guy Fawkes masks), which are

commonly associated with the movie "V for Vendetta," and more specifically with the

historical figure known as Guy, or Guido, Fawkes. Guy Fawkes is known for his attempt

to blow up the British Parliament, and his attempt to do so symbolizes one person

standing up against the establishment:

"[Wearing Guy Fawkes masks] is about the anti-establishment idea. But if you think about it too, that's another stupid thing, the Protestants in England were anti-establishment. By breaking away from the Catholic church, the Roman Catholic church that was basically as big as Rome, you know, all over the continent, all over… a couple of continents, right? They broke away from it, they were the little guys, you know, and if you look at it in a way that England's looking at it, Guy Fawkes was the agent of the establishment, sent to bring them back, right, to undermine their revolution. He was a reactionary agent… But the symbols…and I don't know how controversial this is nowadays but the symbols have definitely changed over a few hundred years, and to the point where the establishment becomes, you know, the anti-establishment and things like that. And it's all just a point of view" (Respondent #6, 2014).

"People don't want to put themselves out there and, so, the Guy Fawkes mask, from… at least, from what I understand about it, um, it's pretty big mainly because of the "V for Vendetta" – it's one dude standing up for something" (Respondent #4, 2014).

The anti-establishment idea that manifests itself though wearing a Guy Fawkes mask was often discussed on the forums by members of Anonymous. Many members emphasized that it is not just any mask, but the Guy Fawkes mask that bears a special importance to members. Guy Fawkes, as a historical figure, encapsulates all of the values Anonymous aligns itself with – i.e., taking an "action against the totalitarian and fascists governments" (Anonnews.org 2013).

One security professional also noted that another reason hacktivists may want to stay anonymous, and consequently wear the Guy Fawkes masks, is because they want to send a message that everyone deserves anonymity and privacy. With the recent scandal over the National Security Agency spying on American citizens, and similar stories, hacktivists may feel that privacy is being taken away, according to my respondent. Anonymous' members, who often claim that their goal is to protect privacy and freedom of information, may wear the masks as a way of sending a message that privacy and anonymity are a basic human right:

"The idea of posting anonymously is where [the name of the group] came from, and that's why anybody can be part of [Anonymous], um, but that's also the masks… what they've done when they wore the masks in the public sphere, they've taken this term, this concept that didn't exist prior to that, that's this idea that we deserve certain amount of anonymity and they've sucked it out of the Internet and brought it into the physical world" (Respondent #3, 2014).

In other words, wearing the masks symbolizes the importance of having privacy in a society. While the Internet has, to some degree, always provided some privacy for its users, being private in the physical world is somewhat more challenging. Wearing the Guy Fawkes mask both online (as avatars) and in real life keeps members of *Anonymous* private at all times, while also giving the group something that people can recognize it by. Wearing the same mask, as many of my interviewees pointed out, is especially important because *Anonymous'* members want to stay private, but also let others know that it is *Anonymous* protesting.

Some security professionals also mentioned job security when asked about the possible reasons hacktivists may want to hide their identities. Many hacktivists and activists within *Anonymous* have jobs and/or careers that they need to maintain. One of my respondents noted that protests nowadays are something that people look down on, so a lot of people reasonably do not want to show their face if they participate in a protest:

"I can understand why privacy is important to [protestors] and staying anonymous, um…well, yeah, because you're protesting things that I think in modern society particularly… I think protesting is kind of frowned upon in general, right, so, for instance, if your boss sees you on the news at some protest, you might have some trouble at work. Um, I think we're living in a society where pretty much straight out of college you have a huge kind of debt burden, right, where as thirty-forty years ago you could kind of come out of college and protest for a year or do whatever else you wanted to, right… um, now there are some real world implications to that….um, where you have a debt that you need to maintain unless you want to go bankrupt." (Respondent #1, 2014).

143

In other words, activists and/or hacktivists may choose to hide their identity in order to keep their professional and personal lives separate. Stated differently, people who engage in activism, of any kind, need to also engage in impression management. This idea is mirrored by the concept of the impression management by Erving Goffman. According to Goffman, life represents a stage, and the world is the theatre. Every individual has "the front stage" – the behavior and image that people project onto others, as well as "back stage" – the things people want to keep private. Ritzer (2015:152) explains Goffman's theory the following way:

> "Continuing the theatrical analogy, Goffman (1959) argued that in every performance there is a front stage, where the social performance tends to be idealized and designed to define the situation for those who are observing it…Also of concern to Goffman is the back stage. In the back stage, people feel free to express themselves in ways that are suppressed in the front…The back stage plays a prominent role in our lives. For every one of our front-stage performances, there are one or more back stages where all sort of things happen that we do not want to be seen in the front stage."

It would be logical to assume that many activists/hacktivists have a life outside of their protests. They need to maintain their image in order to make their lives sustainable. Protests are something that one can do in his or her spare time. It is not surprising, then, that many members of *Anonymous* prefer to stay private as a way to maintain their lives outside of activism.

One of my respondents noted that everyone in the professional world nowadays have to hide something in order to save face. Hacktivists and members of *Anonymous* are not exceptions to this unspoken rule:

> "I'm hiding enough to control my impression management. So, I'm just trying to manage my impression like everybody does and put on a professional face, and I don't want you to know what I do at night and I don't want you to know, you know, maybe I'm in the middle of fight with

my girlfriend, and, maybe, even my fucking mom died. I don't want people to know that shit. So, there's a line that like... if you don't have anything to hide, then you shouldn't worry about it. Well, I argue that anybody who tries to put on a persona, professional or public persona, has something to hide. It's just not nefarious" (Respondent #3, 2014).

Lastly, some security professionals I interviewed said that privacy, for members of *Anonymous,* is important because it empowers the members of the group. It is empowering because: a) it promotes equality (if no one knows each other by face, people can have a sense of being more equal); b) if everyone is anonymous, the group can promote an image that it is easy for them to replace apprehended members; and c) being anonymous allows members of the group to join and leave at any time, without being judged or critiqued. Here is what some of my interviewees had to stay in this regard:

> "I think there's something powerful about not…a faceless adversary, I guess" (Respondent #5, 2014).

> "When they are all faceless, you are free to fill in a face" (Respondent #6, 2014).

> "Um, you know, if you are in a gang, right, you are not…I grew up in the crappier area of West Chicago suburb, you know, so I don't know if what I've heard is real or not, but the idea is when you're in a gang, you can never leave, you're in there for life, you know, that sort of thing. Like "Oh my god, why would you ever join a gang?" when I was a kid, but, you know, I assume they make it difficult to leave and, um, just because then other people will leave and, you know, god…but a…a group that you can do something justifiably illegal, that they can easily join, easily leave, you know… if you're part of it and you want to DoS a company that you hate, that's screwed you over maybe, right, a bank or something like that, you do it, you get in, you do it, "Okay, I'm done! That's it, I don't wanna do this anymore." You know, that's fine" (Respondent #6, 2014).

The idea of 'a faceless adversary' was frequently mention by *Anonymous* members themselves on the message boards. The idea that one can easily fill in a face or replace lost members is something that Anons seem to emphasize strongly. Members of *Anonymous* often use the metaphor of a hydra to explain how the group recovers. A

hydra, according to Greek mythology, is a monster with multiple heads; each time one of the hydra's heads is cut off, the creature grows two more to replace it. This metaphor seems to bear some significance to the members of *Anonymous*: members on the forum often said that if one is arrested, two will replace him or her. The hydra metaphor, in other words, conveys a sense of indestructibility and strength. No one can compromise *Anonymous*, because all members are equal and replicable. Wearing the same mask helps to support this notion of replaceability.

In sum, when I asked the respondents about possible reasons for *Anonymous'* emphasis on anonymity and never revealing one's identity, my respondents were all in agreement and suggested the following options (Table 5).

**Table 5: Why do members of *Anonymous* wear the same mask and/or conceal their identity?**

- To be more inclusive/promote a sense of unity among members

- To avoid prosecution, arrest, or retaliation.

- To send a message to the public: an anti-establishment ideal (represented through the image of Guy Fawkes) and the idea that one person can stand up against an oppressive regime; an idea that everyone deserves privacy.

- To empower members: being anonymous gives more freedom to the members, as well as promotes a sense of equality. On the top of this, wearing the same mask also sends a message that members can be easily replaced, since they all appear to be the same.

- Being anonymous means that members of *Anonymous* can join or leave the group without being judged and/or threatened.

**Theme Seven: Security Professionals on the Popularity of Hacktivism**

When I asked the respondents about possible reasons behind hacktivism's rise in popularity, all were in agreement and said that hacktivism, as well as digital activism,

146

represents, overall, a more effective form of political participation. My interviewees

suggested the following reasons that hacktivism/digital activism is more efficient: a)

people who want to protest can have greater effect, and reach, with hacktivism, while

simultaneously not harming anyone physically (i.e. financial instead of physical damage);

b) hacktivism is superior to traditional protest in many respects (e.g., a safe location,

hacktivism can be done from home); c) hacktivism, due to its antagonistic nature,

normally results in more attention than traditional protest; and d) hacktivism is more

effective than traditional protest because it is based in technology, and technology allows

protestors to fight for their cause in more flexible and efficient ways.

One of the most commonly stated reasons, by the respondents, for the rise in

hacktivism was the fact that hacktivism can do more damage to corporations, and other

targets, than regular protest. One respondent, for instances, noted that while hacktivism

can do serious harm to companies or individuals, hacktivism avoids physical damage:

> "[With hacktivism]… um, it certainly has less, you know, loss of life
> involved, if any loss of life. Um, you can do a lot of damage with hacking
> that doesn't involve hurting anybody, not physically" (Respondent #2,
> 2014).

> "I mean, traditional activism, if you were boycotting like, you know,
> *Hobby Lobby* with all the stuff that's going on… if you were doing a
> physical boycott, you could, maybe, slightly inconvenience one store, you
> know… you like, get a group of people, you block the entrance and it's a
> crappy protest that no one cares about. But it you are doing hacktivism,
> you could, you know, put back doors on their registers and steal all their
> credit card numbers, and do millions, or even billions, of dollars worth of
> damage. You could put them out of business with hacktivism. With
> activism, you are just going to slightly annoy one store manager, but with
> hacktivism you could turn the whole thing upside down. So, I think that's
> why people do it" (Respondent #5, 2014).

> "You can't shut down the business with a traditional protest like I was
> talking about earlier, right…Um, denial-of-service attack, that's not the
> case, right. If you shut down PayPal for two hours, that's two hours of
> business that were lost to PayPal, right, and so it's a much more, um…

antagonistic way of trying to approach things. You aren't just, um, trying to have your voice heard, right, you are actually kind of going for blood. You're looking to hurt a little bit as well." (Respondent #1, 2014).

The idea of not doing physical harm, or the anti-violence idea, was also voiced by members of Anonymous on the forum. Many *anons* on the message board claimed that while *Anonymous* should do everything possible to bring about positive change – including harming a business – members also emphasized that they preferred peaceful, non-violent methods to hacking. Hacking, in their words, should be used in extreme circumstances, when other measures have been proven to be ineffective. Most *anons*, however, thought of hacking for a political cause as a non-violent measure, because such hacking would only damage a business financially, without causing physical harm.

Another reason for the popularity and effectiveness of hacktivism, that many of my respondents commented on, was that hacktivism is superior to traditional protest in other ways, beyond being more damaging. One security professional stated, for instance, that traditional protests have become more dangerous for activists, since the government scrutinizes such protests heavily. Oftentimes, authorities may use physical violence towards protestors. Many activists are photographed at protests as they are assaulted by the police physically or through other means, such as tear gas or pepper spray. All of this can be avoided with hacktivism:

> "If you're protesting the government or if you're a Tea Party person, or if you're protesting marijuana laws… well, the things that the government has an issue of wanting to know who the dissidents are. So let's say, you doing an economy rally, that's the obvious one. Let's say you're saying Islamic people deserve more treatment…positive treatment in the U.S., that's gonna freak them out 'cause you said the word 'Islamic' or, if you are like, marijuana should be legalized… the federal… yeah, the... people who have, like, the… the marijuana… DEA that's who, the DEA would be there taking pictures of the pot protestors and then trying to identify their identity because now you have a list of people who could probably be randomly pulled over" (Respondent #3, 2014).

148

Members of *Anonymous* often discussed the issue of police brutality, on the forum. Many anons stated that they feared police brutality and arrest, and were therefore trying to avoid attending regular street protests. Some *anons* stated that they thought of traditional protests as too dangerous, and considered digital activism a safer option. Digital activism and/or hacktivism, according to many *anons*, represents an opportunity to make a change without taking the risk of being photographed by authorities or threatened by the police.

Another way in which hacktivism is superior to traditional protest, according to the security professionals, is that hacktivism is less time-consuming and can be done from one's home. It may be hard to balance one's work life with dedicated to activism. Taking to the streets and protesting takes a lot of time to plan and prepare for effectively, whereas hacktivism is not time-consuming and does not require one to travel or organize logistics. On the top of this, hacktivism, as mentioned previously, does not require one to be very computer-savvy. This means that anyone who is willing to engage in hacktivism can do so easily:

> "Anyone can do it…And I mean if you're gonna be doing any kind of activism in the real world, that involves the type of stuff you do with hacktivism, so where you are actually denying service to a business. The only way to do that in [physical life] is to get a bunch of people not let people into a storefront. And the police gets called, and the tear gas happens and you have to have a specialized equipment, you know, like a gas mask, you have to know how to get pepper spray out of your eyes, you have to, you know, wear…you know, padded jacket so rubber bullets don't hurt you so badly…but hacktivism is…you sit in your bedroom and you press a few buttons, I mean, what are you gonna choose?" (Respondent #6, 2014).

> "Hacktivism is safer and more effective, exactly. And…and lazier. You don't have to go outside" (Respondent #6, 2014).

149

Many members of Anonymous, when discussing hacktivism on the forum, mentioned the ease and convenience of using application like LOIC and HOIC. Anyone who wants to disrupt a business can learn to carry out a DDoS attack very quickly; most hacktivism that Anonymous participated in did not involve any "real" hacking. The instructions for uploading, installing, and launching LOIC/HOIC are posted on the message board and can be used by anyone who needs assistance using them. The convenience of using these applications, indeed, explains why some members of Anonymous may find hacktivism so attractive.

Lastly, hacktivism is superior to traditional protest, according to my interviewees, because it allows for a massive shift in power. Some respondents noted that hacktivism allows 'regular kids behind keyboards' to make a huge difference, which was not common previously, when the same demographics engaged in street activism. Thus, hacktivism gives power to individuals who otherwise would not have such power:

> "I think for a lot of cases, hacktivism isn't necessarily the right option but it certainly gives a lot of power to people who don't otherwise have power. You know, if you have no money, no voice, nobody's listening to you, and you can hack somebody with a big presence, well, that gives you a hell of a voice" (Respondent #2, 2014).

> "…no one had ever thought of using hacking as a tool for political change until one person tried it and then everyone's like "Oh, well, that's a really good idea, let's all do that." You know, these things just kind of happen, there wasn't really any reason that it wasn't happening, and now that people are realizing the effect that one person behind a keyboard in Pennsylvania can have, you know, they can bring down the government… people are like "Wow," you know, this changes the balance of power. So now everyones wants to do it" (Respondent #5, 2014).

Another big reason for which hacktivism is gaining popularity, according to security professionals, is that hacktivism attracts more attention than regular protest. When street activism becomes large enough, it also brings greater attention from the

media and from society, overall. However, in cases of hacktivism it seems that hacktivists

receive attention, regardless of the scope of the attack. Some of my respondents noted

that hacktivism is more effective at grabbing the nation's attention, possibly because

society feels more threatened by computer crime than by street activism, regardless of

size:

> "Opposed to putting yourself at risk, now you can hide behind your
> keyboard and actually make a difference. So it's becoming so much more
> convenient than actually having to go somewhere and have a rally. And,
> on top of that, so people have a rally, people aren't as threatened by a rally
> as they are by computer crime" (Respondent #4, 2014).

The main reason hacktivism receives such attention is because it can have a

shocking effect on society. When hacktivists strike, in many cases significant damage is

done, whether they attack a corporation, government, or private individual. Hacktivists

have been known to steal information, as well as publish or disclose private, or otherwise

sensitive, information to the public. It is no surprise, then, that hacktivists' attacks

typically attract more media attention. While a traditional street protest may attract the

attention of the local news, hacktivism typically captivates the news media, as well as

make worldwide headlines. Some of my respondents noted that one of the primary

methods used by hacktivists, a Distributed Denial of Service (DDoS) attack, is very

effective at attracting attention. It can be quite easy to crash a website or a server using a

DDoS attack, especially if many members of the group are using the Low Orbit Ion

Cannon/High Orbit Ion Cannon application simultaneously:

> "Instant gratification tool they have is the things like DDoS, like Low
> Orbit Ion Cannon, where if you're on a message board and they are like
> "We're going to raid these guys, we're going to attack these guys at this
> time." If you're actually gonna be doing things like, you know, things that
> actually will result in maybe millions of credit card numbers exposed or a
> compromise of an application, or a network or something like that. It takes

skilled people some time to do it, and you're gonna hold people's attention. And the whole idea of the protest, and this and that, is to bring as much attention to it as possible, bring as many people into it as possible. To do that you need something that results in spectacular-ness right away" (Respondent #6, 2014).

Lastly, some security processionals mentioned that hacktivism is gaining popularity because technology, overall, is gaining popularity. The world is becoming more digital, and people are becoming more and more reliant on technology. It is not surprising that activism is shifting online, as well. The World Wide Web is unavoidably becoming a new arena for activist, where they can engage in various ways to protest and promote social change: "I would say technology is, like, becoming more widely available… I guess everything's turning more digital now, so it's easier to do activism through hacking" (Respondent #4, 2014).

In sum, when I asked the respondents for their opinion on possible reasons behind hacktivism's rising popularity, they were in agreement that hacktivism, in comparison with traditional activism, is overall more effective. Hacktivism is more effective than traditional activism, in their view, for the following reasons (Table 6).

**Table 6: Why is hacktivism more efficient than regular protest?**

- Hacktivism does more damage than a regular protest, while simultaneously not doing harm to anyone physically.

- Hacktivism is more convenient than traditional street protest: it can be done from one's home; it gives power to otherwise powerless protestors; activists do not need to put themselves in danger of being assaulted or arrested by the police.

- Hacktivism does not just attract attention; hacktivists are capable of gaining immediate attention, and on a more global scale than traditional protest.

- Hacktivism is accomplished through technology, which allows for easier and more flexible methods of gaining the public's attention or accomplishing a goal.

**Theme Eight: Security Professionals on the Security of the Internet**

All of the respondents, at some point in the interview, mentioned that the Internet and software are inherently insecure. The fragility of modern communication is due to the fact that security has never really been taken seriously until recently. Both the World Wide Web and modern computers were built with no security in mind. This is how one of my respondents explained the lack of security when it comes to modern technology:

> "I think the problem… the reason that we have the security crisis that we do right now – and believe me it is crisis, everyone's owned, everyone's hacked, no one can stop it – is that we built all of this stuff but we didn't build on the foundation of security. Security has to be the first thing you think about, the last thing you think about and you have to be thinking about it the whole time in between. When we first did all of this Internet stuff, you know, it was just a bunch of researchers sending files back and forth, and they don't care about security because everyone on the network was trusted. And we've all been building on that really shoddy foundation for years, and still software today is developed when they don't even think about security until after the product is, you know, almost done and they're like "Okay, we've got it working, now let's add security," you can't add security. And all of the things that we use on a day-to-day basis were built with that in mind: let's do the development and then we'll add on security later. Security has to be the foremost consideration in your mind the entire time you're working on a product, or you'll never have it. You can't add on security, it's just not possible" (Respondent #5, 2014).

> "Computers and networks, including the Internet, are incredibly fragile. Much more than an ordinarily person would think" (Respondent #2, 2014).

> "…but we've never really had secure communication, basically. We've never had secure communication" (Respondent #3, 2014).

Since security has not been a priority for the technology industry until, possibly, very recently, as a result there are a great number of vulnerabilities in software, hardware, and in the Internet itself. These vulnerabilities are, inevitably, going to be exploited by others, and cannot be fixed easily, according to security professionals. One of my respondents described modern computer systems with the following metaphor: "You

can't go back and fix all the mistakes you've made and re-architect [the internet], you just

can't, it's not possible. You can't put a band-aid, you know, over an amputated leg"

(Respondent #5, 2014).

All of the security professionals interviewed agreed that even the most secure

companies, and even governments, can be vulnerable. In other words, because security is

inherent in modern technology, but rather added on afterwards, there is no completely

secure network. One of my respondents noted that if a hacker, or a hacktivist, has enough

time and patience, he or she will eventually gain access to their target:

> "And what I have learned working here is if you have enough time,
> anything breaks no matter what. And how…even if it's like the most
> locked down web app ever, the most locked down network, and obviously
> that's not practical and it's never a thing…you know that the saying goes
> "the most secure computer in the world in unplugged, locked up behind an
> armed guard, and even then it's not safe." Um, but the…just saying for
> fun, it's a completely secure everything, it takes two phone calls and
> showing up with a pizza box to their headquarters and now you're in, you
> know" (Respondent #6, 2014).

> "We'll find a lot of obvious vulnerabilities when we perform a security
> test. But if you spend fifty hours on a test you're still not gonna find
> everything because you get someone sitting in their basement with nothing
> to do for weeks, they'll find it. It's there, they'll find it, you know"
> (Respondent #6, 2014).

The insecurities of computer systems and the Internet, according to my

respondents, represents an opportunity to those who would like to take advantage of

them, for various reasons. Many respondents stated that hackers and/or hacktivists can be

considered opportunists who simply take advantage of such a fragile system. As hackers

and hacktivists take advantage of bugs in modern computer systems, in recent years the

security industry has been growing quickly.

The demand for security analysts and consultants has been growing, as well, since more companies have been targeted by both cyber-criminals and hacktivists. Many of my respondents agreed that, even though security professionals try to "put as many road blocks" as possible to prevent security breaches, there is little, if anything at all, that can be done to prevent targeted attacks. An example of targeted hacktivism is a DDoS attack, where hundreds, or even thousands, of people flood a website or a server with traffic, using programs like LOIC or HOIC. Many of my respondents noted that DDoS attacks are inherently impossible to prevent. DDoS attacks can be compared to a shopping mall, in this respect. Much like a shopping mall can be overcrowded, you can overwhelm a website. A bigger mall may require more people before becoming overcrowded, but if enough people decide to participate, it will eventually become overwhelmed. Similarly, websites have a limited amount of bandwidth and computing power to process requests. When too many requests are sent, too quickly, the server eventually crashes. One of my respondents explained a DDoS attack in the following way:

> "Imagine that you are a computer. And people are sending you packages through a big tube. One of two things can happen when too many packages come at once. Either the tube can get clogged with packages, or too many packages come in at the same time faster than you, the computer, can sort them. You can make the tube bigger – make more bandwidth – or you can get some friends help you sort through the packages. The fact remains that if too many packages are sent, things will break down. So all you've done is you increased the number of packages required before things break down. In the same way, a DDoS attack is inherently impossible to completely prevent. You may require more computers to participate in an attack, but at some point things still can become overwhelmed." (Respondent #1, 2014).

In sum, no matter what is done, in most cases a DDoS attack is impossible to prevent, and the only thing that can be done is to raise the number of attackers required to successfully bring down a network. As most hacktivists use DDoS as their primary

strategy, it is essentially impossible to stop the attack of a sufficiently large hacktivist group. One of my respondents stated that targeted hacktivism represents one of the most dangerous types of hacking. Unlike those who hack for a monetary purposes (credit card theft, etc.), and who often choose whichever target is easiest to attack, hacktivists pick their targets for moral and ethical reasons. As hacktivists have an agenda, and hack for moral rather than monetary reasons, they will often be more persistent with their target. Hacktivists, unlike typical hackers, may continue to chip away at the security of a target until they eventually find an exploit (i.e. successfully hack the target):

> "We best and, you know, there's not really that much, in my opinion, you can do against a targeted attack because that's not the way, you know, security is now…Most hackers would think: "Oh, I don't really know how to get that site, let's move on to the next one, they'll skip right past yours, if it looks like it's gonna be a pain in the ass to hack." I think some of my colleagues did a talk about broken windows. If you're gonna break into a building, you're desperate, you want some cash, you'll find the building that looks the easiest to break into. You know, not the one with guards outside, not the one that has actual locks and barbed wire, right? But if you really want what's in there, to teach them a lesson, you'll get past all the guards, you'll get past the barbed wires, you'll get past the dogs, you'll find a way to do it" (Respondent #6, 2014).

> "…if someone has a grudge against something and has the time, to…you know, and, the…need to do something about it, something will be done about it. And that's why presidents get killed. You know, that's gonna be like the most difficult job to pull off in the world…the most protected men in the world…but people who really need to do it, whether they are deranged, whether they've got a political agenda, will find a way to do it" (Respondent #6, 2014).

In sum, when I discussed the topic of security, in general, and how it relates to hacktivism, my respondents were in agreement, overall. The general issues that my interviews identified are summarized in Table 7, below.

**Table 7: Security Professionals on the Security of the World Wide Web**

- The Internet, and computer systems in general, are inherently vulnerable because security was not considered or built-in from the beginning. It is difficult to add security; security should be used as a foundation for new technology.

- Because the computer and the internet are inherently insecure and/or have security flaws, such vulnerabilities become opportunities for hackers and/or hacktivists who wish to exploit them.

- Targeted hacktivism (i.e., hacking directed at a specific target, for a specific purpose) is a serious threat. Targeted hacktivism is motivated by a political agenda, rather than potential monetary gain. Hacktivists are more likely to be persistent in their attempt to hack a target than cyber-criminals, who mostly search for easily identified vulnerabilities and move onto another target if unsuccessful.

- One of the most common strategies hacktivists employ is called a Distribute Denial-of-Service (DDoS) attack, which overwhelms a network with numerous requests. DDoS is impossible to prevent, due to the nature of the Internet the World Wide Web. Therefore, not much can be done to prevent DDoS attacks from sufficiently large groups.

- Most hacktivists use applications such as LOIC and HOIC to carry out DDoS attacks. DDoS is an extremely popular strategy among hacktivists because everyone can be taught to use such tools. Technical-savvy is not required to participate in a DDoS attack.

## Theme Nine: Alternatives to Hacktivism

When I asked the respondents about possible alternatives to hacktivism, all of my respondents said there are no good alternatives to hacktivism. In other words, they all agreed that hacktivism is almost forced to exist for a variety of reasons. Responses fell into one of two major categories: a) a handful of the respondents suggested that the only good alternative to hacktivism is having non-corrupt governments and corporations; and b) there are no alternatives to hacktivism, since it represents the most effective form of activism at the moment (i.e., hacktivism represents a superior form of activism compared to traditional, street activism).

157

As stated above, some respondents suggested that if governments and corporations were not corrupt, or did not overreach or overstep their power, hacktivism may have never come to exist. A number of security professionals also mentioned corruption as the primary reason that hacktivism evolved as a form of activism. When I asked the specific question, of whether there are any viable alternatives to hacktivism, I received the following types of answers:

> "Yeah, I think there's an alternative... to global computer insecurity, ecological problems across the globe and fair wages and economics and everything. We need a non-corrupt global governing body… considering, um, from my personal standpoint, the complete lack of restraint that corporations have in their operations in this world, that I think Anonymous is only representative of a larger fervor that's growing in the public in the United States. And that's an indirect response to this creeping corporate control and just rigidity to that corporate reach that is expanding" (Respondent #3, 2014).

> *"An alternative to hacktivism is if* we had a functioning government …but, let's be honest, everyone knows that the government is a bit of a farce. You know, they… they are not responsive to people's needs. I think hacktivism is a symptom of a deeper problem, that we feel like our governments and our corporations are not responsive to our needs and our demands. When we feel like the government, like the whole NSA spying stuff… the reason that those documents got leaked is because that person thought the government is doing something wrong, doing something illegal, and the reason everyone's so upset about it is because we agree. The government wasn't being honest with us, so hacktivism exist only, and as much as it's forced to exist, because of government corruption and corporate greed. Hacktivism… if those, if we didn't have a reason for hacktivism, it would not be here. Yeah, the alternative is to not have a corrupt government and a greedy corporate world" (Respondent #5, 2014).

Hacktivism, in other words, has evolved only as a response to problems of corporate greed and government corruption. Many respondents stated that government corruption served as the primary reason for hacktivism's rising popularity. Indeed, hacktivism has been a significantly more effective method to gain the attention of politicians and corporate leaders than traditional activism. Similar to my respondents,

members of Anonymous stated a similar idea on the forum: hacktivism is forced to exist. Anonymous and/or hacktivists would not occur, perhaps, if governments and corporations were not as corrupt, according to the forum participants. One anons said: "Anonymous exists because the world is in trouble… The freedoms people once had are gone, the government ruins the world, and the corporations run the government" (Anonnews.org 2013).

Other security professionals suggested that, when it comes to most things in life, whether it is technology or activism, people will almost always adopt the most effective methods, and hacktivism is currently one of the most efficient forms of activism. One security professional, for instance, compared hacktivism to the search engine, Google. Before Google had become the largest and most popular search engine, there were other popular search engines, such as Yahoo. Over time, however, Google has developed almost a monopoly on Internet searches. The reason for such success, the respondent stated, is that Google was easier to navigate, and easier to use effectively. Similar to search engines, hacktivism has grown because it allows for more effective results:

> "[Hacktivism is the most effective way because it is] the easiest, most convenient way of activism online is, you know, this sort of set-up that we've got going on, this paradigm right now. It will continue to exist until something better comes along… It's so hard to try think about what can be better because even think about, um, think about Google, right, when you need to search anything you go to Google. You know, why would you do anything else? We call it "googling", right? And there's…you can't imagine something more convenient than Google, but years ago, you know, you couldn't imagine anything more convenient than Yahoo, right? I mean you can't imagine the next thing that's gonna come along that you can't live without, the next big thing that's gonna make everything else look stupid… It's the same with hacktivism" (Respondent #6, 2014).

Other respondents offered a similar argument: hacktivism seems to be a good alternative in situations where traditional protest fails. Many recent protests – including

Occupy Wall Street (OWS) protests – have been met with brutality from the police. Many traditional activists' efforts have been suppressed, in other words. Unlike traditional civil disobedience, hacktivism employs much more aggressive measures (e.g., defacing or crashing a website) and can thus help hacktivist groups draw more attention to their causes while simultaneously avoiding police retaliation:

> "I don't see much replacing hacktivism, I find hacktivism is replacing other things. Um, yeah…I don't see it, I don't see…there are alternatives, I just don't know if those alternatives are as effective" (Respondent #4, 2014).

> "I think if the political system gets corrupt enough that engaging in street activism is no longer possible, right… it's no longer sort of possible to make your voice heard in the government and change something that's really bad. I think in really extreme cases, I guess that there's a morality to hacktivism… some protests are doomed to fail, right, maybe some are successful, right… I think traditional protests are less successful nowadays than they were, you know, twenty-thirty years ago" (Respondent #1, 2014).

In sum, security professionals were in agreement when I asked them about alternatives to hacking as a way of activism. They agreed that there are very few, if no, viable alternatives to hacktivism, at least currently. Hacktivism, they believe, exists because it is necessary, emphasizing that the only possible way to stop hacktivism is to stop government and corporate corruption. All respondents agreed that hacktivism is one of the most efficient methods for activists today. While some identified corrupt governments and corporations as the primary causes of hacktivism's popularity, other respondents suggested that hacktivism's high effectiveness is what makes it popular among activists (i.e., hacktivism will remain popular until a better method is identified).

**Interviews Analysis: Results**

My analysis of the interviews with security professionals reveals the following major findings:

1)       The first theme of the analysis explores the security professionals' familiarity with hacktivism, and more specifically with *Anonymous*. My respondents displayed a profound knowledge of both. It is worth noting that a few participants were involved with *Anonymous* at some point in the past, which they either stated directly or strongly alluded during their interviews. Their involvement with the group, however, was not tied to, or related to, any illicit activities. The knowledge that the respondents exhibited about *Anonymous* included, but was not limited to, the history and background of the group, as well as the group's structure.  The information that my respondents provided in this section is supported by peer-reviewed literature.

2)       The second theme focused on the security professionals' personal views of hacktivism. Considering that the security industry is commonly viewed as being in opposition to the hacker and hacktivist communities, I was surprised to discover that all of my respondents expressed sympathy and support toward the notion of hacktivism, as well as toward *Anonymous,* specifically.

3)       The third theme focused on *Anonymous* and their hacking skill: security professionals were united in their opinion that most members of the group have little to no hacking skill. Most attacks by *Anonymous* are accomplished through DDoS attacks, which do not require the participants to be tech-savvy individuals. The notion that *Anonymous* consists of mostly non-technical individuals is supported by both my content analysis and academic literature.

4)        Theme four explored the ethics behind hacktivism: security professionals stated that hacktivism can be considered both ethical and unethical. A respondent noted that if one considers hacktivism from a 'do no harm' position, hacktivism can ultimately be

considered unethical. However, hacktivism can be considered ethical, especially if we conceptualize hacktivism as 'vigilante justice'. A few of my interviewees suggested that in some cases it is justifiable to commit an act of violence or destruction in order to prevent an even greater harm. This conceptualization of *Anonymous* as vigilantes corresponds with the study by Serracino-Inglott (2013), who, similar to my respondents, conceptualized Anons as individuals using violence as a last resort for achieving positive social change (i.e., 'cyber vigilantes'). My interview respondents noted that while some vigilantes' actions may be seen as ethical, one should take vigilantism cautiously. Vigilante justice can be both beneficial to society and dangerous, depending on circumstance. Overall, the security professionals believed that hacktivism can be both ethical and unethical, and that it simply depends on circumstances. My respondents, however, did not view *Anonymous* as a threat to society. They saw *Anonymous'* actions as well-intentioned, for the most part.

5)      The fifth theme focused on the effects of hacktivism, and particularly of *Anonymous*, on the security industry.   My respondents stated that *Anonymous* did not cause any direct effect on the security industry; however, groups like *Anonymous* had a few important (positive) effects on security, in general. Groups like *Anonymous* have had an unintended effect: they helped raise awareness about the existing security vulnerabilities within modern computers and the Internet, and their (h)activism has contributed to greater security awareness, forced society to take security more seriously, and indirectly helped to expand the security industry.  My respondent's answers again correspond with academic literature. Mansfield-Devine (2011), similar to my

respondents, suggests that 'hacks' by *Anonymous* have helped to raise security

awareness.

6)      The sixth theme examines the importance of Guy Fawkes masks to members of

*Anonymous*.   My respondents suggested that the masks serve both a symbolic (e.g., an

anti-establishment message) and practical purpose (e.g., giving members protection from

the authorities and freedom to participate fully). My interviewees' responses are in

accordance with academic literature that examines the role of Guy Fawkes masks within

the *Anonymous* movement.

7)      In theme seven, my respondents explained why hacktivism, and groups like

*Anonymous* in particular, are rapidly gaining popularity. The security professionals

suggested that hacktivism has become a popular phenomenon because: 1) groups like

*Anonymous* are capable of doing greater damage to opponents, while also avoiding

physical harm; 2) groups like *Anonymous* give power to people who otherwise would not

have a voice,  as well as allows everyone to participate from the comfort of their home; 3)

groups like *Anonymous* are getting results fast and on a more global scale than members

of traditional civil disobedience; and 4)  groups like *Anonymous* use technology, which

allows for more diverse and creative forms of political participation.

8)      Theme eight dealt with the overall state of security for modern technologies (the

Internet and computer systems). All respondents noted that modern technology is

inherently vulnerable. Computer and Internet security was not viewed as important when

these technologies were first introduced. The vulnerabilities that exist in modern

technology are bound to be explored by hackers and/or hacktivists. In order to prevent

future attacks by hackers and/or hacktivists, it is important that society treats security as a

necessity in new technology, and adequately protect against security breaches in current technology. It is crucial that future technology is built with security in mind, to avoid the level of susceptibility present in current technology.

9)     Lastly, theme nine examines alternatives to hacktivism. My respondents agreed that hacktivism represents a new, powerful way of political participation that is unlikely to be replaced by other forms of protest in the near future. Hacktivism, according to my respondents, represents an effective method of activism.  Hacktivism, according to the respondents, is likely to continue gaining popularity in the future, which will require more research on this important social phenomenon.

## VI. CONCLUSIONS & STUDY LIMITATIONS

This study focused on analyzing the online community *Anonymous*, which is known for both cyber activism (i.e., hacktivism) and traditional activism (i.e., street protests). For more thorough examination of the group, the following was used: 1) content analysis of a message board where *Anonymous* members communicate with one another (used to examine the perspective of the group's members); and 2) interviews with security professionals about *Anonymous* and hacktivism (used to ascertain how others view the group). The two methodologies were intended to be complimentary, as well as reveal consistencies and/or inconsistencies between the responses of Anonymous' members and those of the security professionals. By analyzing both the interviews and the forum, I have discovered the responses of the two groups to be very consistent. The main points of agreement between the responses of the security professionals and the members of Anonymous were in regards to the following issues.

First, both members of Anonymous and security professionals agree that Anonymous does not represents a purely hacktivist group. In fact, most members of Anonymous are non-technical individuals. Secondly, both agree that Anonymous relies on critical mass, particularly DDoS attacks, to achieve its goals online. Interviews with the security professionals also discovered that DDoS attacks are a threat that is inherent to the architecture of the Internet, and are likely to remain a viable attack method. The respondents also all agree that DDoS attacks are an efficient, convenient method for the disaffected to protest safely, and that the phenomenon of hacktivism is unlikely to decline in the near future. Thirdly, both agree that the Guy Fawkes mask is used by Anonymous' members for both symbolic and practical purposes. Fourthly, both the security

professionals and the forum content view the actions of Anonymous positively, although

some security professionals expressed concerns about vigilantism and its potential

dangers.  Lastly, both members Anonymous and security professionals agree that

Anonymous, in general, represents a response to modern political and socio-economic

issues.

The correlation between interview responses and forum content over details such

as the history and structure of *Anonymous* lends credibility to the idea that it is a

decentralized, leaderless group. As both *Anonymous* members and security professionals

agree that *Anonymous* does not represent a threat to society at large, and both claim that

*Anonymous* does not represent a threat to individuals, it can be determined that one-on-

one interviews with members of *Anonymous* pose little risk and help clear the way for

further research using direct interviews.

Overall, this research has provided general knowledge of the group and how it

functions. However, one-on-one interviews with members of *Anonymous* are needed for

further exploration of this social phenomenon. The hacktivist/activist collective

*Anonymous* represents a unique social movement that is fundamentally different from

historical protest movements, and its influence cannot be ignored by either the scientific

community or society in general. Future sociological studies should focus on studying

*Anonymous* as a collective in even greater detail through one-on-one interviews with

members of the group, as well as by examining additional or new effects of the group on

society.

The greatest limitation of this research can be observed in the content analysis of

the message boards. Although the digital communications of the group, on the forum,

provide insight into the group's culture and activities, such analysis is not sufficient in itself to fully grasp *Anonymous* as a social phenomenon. In order to understand how members of the group identify, or see their role and goals within the group, it is important to conduct one-on-one interviews with members of the group. While analysis of the forum (non-participant observation) shows how members communicate with each other; in-depth, on-on-one interviews with members of *Anonymous* could reveal the individual opinions and beliefs of various members.

The anonymous nature of the forum prevents one from understanding the demographics of the group: more specifically, age, gender, race, and occupation are difficult, if not impossible to determine. In-depth, one-on-one, interviews with members would also help to better understand who *Anonymous* is composed of, or what types of individuals are attracted most to the group.  Interviews with members could also help us to understand how members use technology and the level of technological knowledge of different members. What also needs to be explored is the culture of the group: e.g., how members use humor and creativity, or how members connect with each other and the importance of such interpersonal communication. Interviews with the group's members could also yield more information on the structure of the group: is there any, however loose, hierarchy within the group? Coleman (2013), for example, suggests that even though a traditional leadership role may not exist within *Anonymous*, some form of labour division is likely to exist within the group (e.g., some members are responsible for editing videos, while other may be admins on social media sites, like Twitter, etc.).

Even though such one-on-one interviews may be difficult to obtain, most likely due to many members of *Anonymous* not wishing to be identified or have contact with

researchers, they are essential if one want to truly understand the social phenomenon of

hacktivism and the collective *Anonymous*.

## APPENDIX SECTION

## APPENDIX A

Hacktivism Glossary

The following is a list of the technical terms that I used throughout my thesis:

1. HOIC (High Orbit Ion Cannon) and LOIC (Low Orbit Ion Cannon) in this case refer to applications, through which Anonymous members often carry out their Denial-of-Service attacks (DDoS).

2. IP address can be defined as a combination of numbers separated by periods, which is assigned to a computer participating in a computer network over Internet.

3. VPN stands for Virtual Private Network. It is a network that uses public Internet space to connect to a private network.

# REFERENCES

Anonymous. 2010. "How to Join Anonymous - A Beginner's Guide Mobile." Youtube
    Website. Retrieved December 15, 2013 (https://www.youtube.com/watch?v=
    XQk14FLDPZg).

Anonnews.org (Anonymous Message Boards). 2013. Retrieved April 2013
    (http://anonnews.org/).

Arthur, Charles. 2011. "Hacking of Fox News Claimed by Group with Links to
    Anonymous." *The Guardian*, July 4. Retrieved April 30, 2014
    (http://www.theguardian.com/technology/2011/jul/04/hacking-twitter-feed-fix-
    news).

Bakioglu, Burcu S. 2013. "The Gray Zone: Networks of Piracy, Control, & Resistance."
    Social Science Research Network. Retrieved September 30, 2014
    (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2293105).

Beyer, Jessica L. 2014. "The Emergence of a Freedom of Information Movement:
    Anonymous, WikiLeaks, the Pirate Party, and Iceland." *Journal of Computer-
    Mediated Communication* 19: 141-154. Retrieved September 30, 2014
    (http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12050/abstract).

Bookchin, Murray. 2005. *Social Anarchism or Lifestyle Anarchism*. San Francisco, CA:
    AK Press. Retrieved April 15, 2014 (https://libcom.org/files/Social%20
    Anarchism%20or%20Lifestyle%20Anarchism.pdf).

Boone. Jeb. 2013. "FEMA Hacked: Anonymous Hacks US Server in Defense of
    Snowden and Government Transparency." *Global Post*, July 17. Retrieved
    December 1, 2013 (http://www.globalpost.com/dispatches/globalpost-blogs/the-
    grid/FEMA-hack-anonymous-retaliates-us-defense-snowden-transparency).

Coleman, Gabriella. 2013. "Anonymous in Context: The Politics and Power behind the
    Mask." Waterloo, CA: The Centre for International Governance Innovation.
    Retrieved September 30, 2014 (http://www.cigionline.org/sites/default/files/no3_
    8.pdf).

Conway, Maura. 2003. "Hackers as Terrorists? Why It Doesn't Compute?" *Computer
    Fraud and Security* 12:10-13. Retrieved April 15, 2013 (http://doras.dcu.ie/493/1/
    comp_fraud_12_2003.pdf).

Faris, Ellsworth. 1932. "The Primary Group: Essence and Accident." *American Journal
    of Sociology* 38: 41-50. Retrieved April 30, 2013 (https://www.brocku.ca/Mead
    Project/Faris/Faris_1932.html).

Fitri, Nofia. 2011. "Democracy Discourses Through the Internet Communication: Understanding the Hacktivism for the Global Changing." *Online Journal of Communication and Media Technologies* 1(2): 1-20. Retrieved April 15, 2013 (http://www.academia.edu/1344217/Democracy_Discourses_through_the_Internet_Communication_Understanding_the_Hacktivism_for_the_Global_Changing).

Fuchs, Christian. 2013. "The Anonymous Movement in the Context of Liberalism and Socialism." *A Journal For and About Social Movements* 5(2): 345-376. Retrieved September 30, 2014 (http://fuchs.uti.at/wp-content/Interface.pdf).

Fuchs, Christian. 2014. "Anonymous: Hacktivism and Contemporary Politics." Pp. 88-106 in Social *Media, Politics and the State*, edited Daniel Trottier and Christian Fuchs. NY: Routledge.

Gibbs, Samuel. 2012. "WhatsApp, AVG and Avira Attacked by Pro-Palestinian Anonymous Hackers." *The Guardian*, October 8. Retrieved December 1, 2013 (http://www.theguardian.com/technology/2013/oct/08/whatsapp-avg-avira-anonymous-hacked-palestine).

Gillen, Martina. 2012. "Human Versus Inalienable Rights: Is There Still a Future for Online Protest in the Anonymous World?" *European Journal of Law and Technology* 3(1): 1-19. Retrieved April 15, 2013 (http://eprints.uwe.ac.uk/21065/1/Gillen%20Human%20Rights.pdf).

Hampton, Noah C.N. 2012. "Hacktivism: A New Breed of Protest in a Networked World." *Boston College International and Comparative Law Review* 35(2): 511-542. Retrieved April 15, 2013 (http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr).

Hearn, Kay, Rachel J. Mahncke, and Patricia A. Williams. 2009. "Culture Jamming: From Activism to Hacktivism." Edith Cowan University. Retrieved April 15, 2013 (http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1002&context=isw).

Hai-Jew, Shalin. 2013. "Action Potentials: Extrapolating an Ideology from the Anonymous Hacker Socio-Political Movement (A Qualitative Meta-Analysis)." Pp. 51-107 in *Digital Democracy and the Impact of Technology on Governance and Politics: New Globalized Practices*, edited by Kayla Wolfe and Joel Gamon. Hershey, PA: Information Science Reference. Retrieved September 30, 2014 (http://krex.k-state.edu/dspace/bitstream/handle/2097/15352/Hai-JewIGI2013.pdf?sequence=1).

Himma, Kenneth Einar. 2005. "Hacking As Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?" Social Science Research Network. Retrieved April 15, 2013 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=799545).

Ifrah, Laurence. 2008. "'Hacktivism' – A New Threat?" Revue Défense Nationale. Retrieved April 15, 2013 (http://www.defnat.com/accueil.php).

Jensen, Michael J., James N. Danziger, and Alladi Venkatesh. 2007. "Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics." *The Information Society* 23: 39-50. Retrieved April 15, 2013 (http://www.tandfonline.com/doi/pdf/10.1080/01972240601057528).

Jordan, Tim and Paul Taylor. 1998. "A Sociology of Hackers." *The Sociological Review* 46(4): 757-780. Retrieved April 15, 2013 (http://onlinelibrary.wiley.com/doi/10.1111/1467-954X.00139/abstract).

Jordan, Tim. 2002. "Hacktivism: All Together in the Virtual." Pp. 119-137 in *Activism!: Direct Action, Hacktivism and the Future of Society*, edited by Barrie Bullen and Peter Hamilton. London, UK: Reaktion Books Ltd.

Kazmi, Ayesha. 2011. "How Anonymous Emerged to Occupy Wall Street." *The Guardian*, September 26. Retrieved December 1, 2013 (http://www.theguardian.com/commentisfree/cifamerica/2011/sep/27/occupy-wall-street-anonymous).

Knafo, Saki. 2011. "Occupy Wall Street and Anonymous: Turning a Fledgling Movement into a Meme." *The Huffington Post*, October 20. Retrieved December 1, 2013 (http://www.huffingtonpost.com/2011/10/20/occupy-wall-street-anonymous-connection_n_1021665.html).

Krapp, Peter. 2005. "Terror and Play, Or What Was Hacktivism?" *Grey Room and Massachusetts Institute of Technology* 21: 70-93. Retrieved April 15, 2013 (http://www.academia.edu/307639/Terror_and_Play_or_What_Was_Hacktivism).

Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution*. Sebastopol, CA: O'Reilly Media.

Manion, Mark and Abby Goodrum. 2000. "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic." *Computers and Society* 30(2): 14-19. Retrieved April 15, 2013 (http://www.csis.pace.edu/cis101/CIS_101_Fall_2007_Spring_2008/LearningPod Topics/SocialResponsibility/Terrorism-or-Civil-Disobedience.pdf).

Mansfield-Devine, Steve. 2011. "Hacktivism: assessing the Damage." *Network Security* 2011(8): 5-13. Retrieved April 15, 2013 (http://www.sciencedirect.com/science/article/pii/S1353485811700848).

Mansfield-Devine, Steve. 2011. "Anonymous: Serious Threat or Mere Annoyance?" *Network Security* 2011(1): 4-10. Retrieved April 15, 2013 (http://www.arifyildirim.com/ilt510/steve.mansfield.devine.pdf).

McGraw-Hill Online Learning Center. 2013. "Schaefer's Sociological Glossary." Retrieved April 2013 (http://highered.mheducation.com/sites/0072435569/ student_view0/glossary.html).

Milone, Mark G. 2003. "Hacktivism: Securing the National Infrastructure." *The Computer & Internet Lawyer* 20(3): 1-19. Retrieved April 15, 2013 (http://www.arifyildirim.com/ilt510/mark.milone.pdf).

Papadimitriou, Fivos. 2006. "A Geography of 'Notopia': Hackers et al., Hacktivism, Urban Cyber-Groups/Cyber-Cultures and Digital Social Movements." *City* 10(3): 317-326. Retrieved April 15, 2013 (http://www.tandfonline.com/doi/pdf/10.1080/ 13604810600982289).

Purkis, Jonathan and James Bowen. 2004. *Changing Anarchism: Anarchy Theory and Practice in a Global Age*. NY: Manchester University Press. Retrieved April 15, 2014 (http://books.google.com/books?id=etb2UFzCBv4C&dq=Jonathan+Purkis+ and+James+Bowen+2004&source=gbs_navlinks_s).

Ritzer, George. 2015. *Introduction to Sociology*. Thousand Oaks, CA: Sage Publications. Retrieved August 2014 (http://books.google.com/books?id=JVIXBAAAQBAJ& dq= goffman+back+front+stage&source=gbs_navlinks_s).

Serracino-Inglott, Philip. 2013. "Is It OK To Be an Anonymous?" *Ethics & Global Politics* 6(4): 217-244. Retrieved September 30, 2014 (http://www.ethicsandglobalpolitics.net/ index.php/egp/article/view/22527).

Sieczkowski, Cavan. 2012. "Anonymous Targets Westboro Baptist Church after Newtown Vigil Protest Threat." *The Huffington Post*, December 17. Retrieved April 30, 2014 (http://www.huffingtonpost.com/2012/12/17/westboro-baptist-church-hacked-anonymous-protest-newtown-shooting-victims-funerals_n_2315070.html).

Smith, Gerry. 2013. "Feds Charge 13 Members of Anonymous In 'Operation Payback' Attacks." *The Huffington Post*, October 3. Retrieved April, 2014 (http://www.huffingtonpost.com/2013/10/03/anonymous-charges-operation-payback_n_4039887.html).

Taylor, Paul. A. 2001. "Editorial: Hacktivism." *The Semiotic Review of Books* 12(1): 1-9. Retrieved April 15, 2013 (http://projects.chass.utoronto.ca/semiotics/srb/ Hacktivism.pdf).

Taylor, Paul A. 2005. "From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?" *New Media Society* 7(5): 625-646. Retrieved April 15, 2013 (http://atc.berkeley.edu/201/readings/PTaylor.pdf).

Van Laer, Jeroen and Peter Van Aelst. 2010. "Internet and Social Movement Action Repertories: Opportunities and Limitations." *Information, Communication & Society* 13(8): 1146-1171. Retrieved April 15, 2013 (http://www.academia.edu/262038/Internet_and_Social_Movement_Action_Repertoires_Opportunities_and_Limitations).

Wong, Wendy H. and Peter A. Brown. 2013. "E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One." *American Political Science Association* 11(4): 1015-1033. Retrieved September 30, 2014 (http://politics.utoronto.ca/wp-content/uploads/2013/12/wong-and-brown-2013.pdf).

Wray, Stefan. 1998. "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics." *Switch* 4(2):1. Retrieved April 15, 2013 (http://switch.sjsu.edu/web/v4n2/stefan/).

Yip, Michael and Craig Webber. 2011. "Hacktivism: A Theoretical and Empirical Exploration of China's Cyber Warriors." University of Southampton. Retrieved April 15, 2013 (http://eprints.soton.ac.uk/272350/).

Zetter, Kim. 2011. "Anonymous Hacks Security Firm Investigating It; Releases E-mail." *The Wired*, February 7. Retrieved April 30, 2014 (http://www.wired.com/2011/02/anonymous-hacks-hbgary/).