



# **Values and Symbolism in Anonymous's Brand Identity**

**by**

**Juanjuan Huang**

**Faculty Advisor: Amy Laura Hall**

**Divinity School**

**Date: July 2015**

This project was submitted in partial fulfillment of the requirements for the degree of Master of Arts in Graduate Liberal Studies in the Graduate School of Duke University.

Copyright by  
Juanjuan Huang  
2015

## **Abstract:**

Hactivism is a portmanteau of computer hacking and activism (Wikipedia). Coined in 1996 by Omega, a member of cDc, “hactivism” was linked to Article 19 of the United Nations Declaration of Human Rights (UNDHR), stating “everyone has the right to freedom of opinion and expression” (Shantz and Tomblin 63-64).<sup>1</sup> Among all the hacker collectives that associate themselves with hactivism, Anonymous, a leaderless and decentralized group of hackers, might be regarded as the most controversial one. This is because it dabbles in a series of whimsical pranks and publicity stunts but also deliberate digital attacks against government, religious, and corporate websites in the name of defending free flow of information and delivering social justice.

In this paper, I will use public media content regarding Anonymous for my primary sources, including Western mainstream media’s news coverage and Anonymous’s own social media posts, to analyze the contribution Anonymous has made to the hacker subculture. Anonymous commits itself to building a distinguishable brand identity as a defender of freedom of speech, hoping to use its symbolic values to “[contribute] to a wider political landscape” (Goode 84). Anonymous’s absence of hierarchy allows anyone who shares the same principles to partake in online/offline activities and claim its title. Its slogans take on the coloration of populism, denying self-promotion, demanding greater digital democracy and serving as an antidote to “cyber-imperialism” (Coleman 391). Plus, Anonymous excels at using social media to promulgate its values and create counter-narratives. Although, more often than not, Anonymous adopts legally ambiguous and morally debatable tactics to hack and expose “wrongdoers,” this leaderless and decentralized hacker collective has become an unorthodox political and cultural icon of civil resistance.

---

<sup>1</sup> cDc stands for “Cult of the Dead Cow”: a computer hacker organization founded in 1984 in Lubbock, Texas. See [http://www.cultdeadcow.com/cDc\\_files/cDc-0384.php](http://www.cultdeadcow.com/cDc_files/cDc-0384.php) for the origin of “hactivism.”

## Contents:

Abstract.....	iii
Introduction: The Mythmaking of Anonymous.....	1
Chapter One: Project Chanology—from Personal to Political.....	9
1.1 Targeting Scientology: Embarking on Free Information Battles.....	9
1.2 Logging onto Internet Relay Chat (IRC): The Formation of a Decentralized Anonymous Community.....	11
1.3 Involving YouTube: Visualizing “Call-to-Arms” Manifestos.....	14
1.4 Sparking Media Frenzy: A Double-edged Sword in Brand Identity Construction.....	19
1.5 Guy Fawkes Masks: Expanding Chanology from Online to Offline.....	24
Chapter Two: Operation Payback—from Rebellious to Resilient.....	30
2.1 Supporting WikiLeaks: Recapturing the White-hot Media Spotlight.....	30
2.2 Landing Twitter: Taking on the Coloration of Challenging Capitalist Hegemony.....	34
2.3 Countermeasure to Social Media Obstruction: Adopting a “Hydra Tactic”.....	40
2.4 Ethical Quandary: Participatory Democracy or Social Engineering?.....	44
Conclusion: Contemporary Significance of Anonymous’s Brand Identity.....	51
Appendix.....	54
Glossary.....	55
Cited Sources.....	56
Bibliography.....	58

## **Introduction: The Mythmaking of Anonymous**

### **The Uniqueness of Anonymous**

A newfangled phenomenon like Anonymous, born of the Internet itself, was something society would struggle to make sense of at first.

--Olson (409)

The Internet is the “protagonist” of our digital era, in which almost everything is being processed by computers, reduced to data and performed online, ranging from interpersonal communications, corporate trade to state control. From the 1960s, the growing web-based content and tantalizing secrecy encouraged the emergence of computer hackers, who exploited weaknesses in computers or networks to gain unauthorized access to data. Over the years, with the help of media representations, hackers have been typecast as socially awkward boys hiding in the “highly populated, youth-dominated, English-speaking online spaces” (Beyer 141) and secretly hacking others. However, Anonymous, a leaderless, decentralized, and loosely associated hacker collective, breaks this stereotype. Anonymous boldly seeks the media spotlight to fashion a recognizable identification as a defender of freedom of speech. To borrow a term from marketing, Anonymous is striving to form and develop its “brand identity.” According to BusinessDictionary, “brand identity” refers to the visible elements of a brand (such as colors, design, logotype, name, symbol) that together identify and distinguish the brand in the consumers’ mind.<sup>2</sup> As an unorthodox hacker collective, Anonymous’s attempt at building its brand identity is to fan media frenzy and engage in social media to make its logo, slogans, and manifesto identifiable in the politics of the Internet.

Unlike conventional hackers, Anonymous allows anyone who shares the same ideas to claim its title and partake in online/offline activities, blurring the line between age, gender, class

---

<sup>2</sup> See <http://www.businessdictionary.com/definition/brand-identity.html>

and region. It excels at using social media, notably YouTube and Twitter, to spread its values and coordinate its operations, including the digital attacks on a series of prominent websites such as CIA, FBI, ISIS, the Vatican, Visa, MasterCard, and PayPal in the name of defending free speech. This strategy may add some symbolic values to its moniker and make it the beacon of online civil disobedience, displaying “its potential contribution to a wider political landscape” (Goode 84). In the following two chapters, I will detail the process and importance of this hacker collective’s brand identity construction. I will first give a brief review of Anonymous’s history.

### **The Mythmaking of Anonymous**

Despite the high-profile brand identity pursuit, Anonymous’s membership and scale remain enigmatic. As the moniker itself suggests, all the participants of Anonymous (known as Anons) maintain anonymity either in online chats or real-life operations, making it nearly impossible to locate the key players and “measure the size of the [Anonymous] community” (Beyer 145). Such characteristics make Anonymous the most conspicuous yet mysterious hacker collective, defying an easy answer to a seemingly simple question: what is Anonymous? With no leaders and spokespeople in the picture, the media, especially the Western mainstream media, has played a vital role in consuming and (re)shaping Anonymous’s public image. The media portrayal of Anonymous oscillates from a group of juvenile pranksters to digital vigilantes, or even a horde of cyber criminals or terrorists. To a great extent, the Western mainstream media has contributed a kind of mythmaking of Anonymous, as evidenced by the following news coverage.

In July 2007, a Fox News affiliate in Los Angeles described Anonymous as “hackers on steroids” and an “Internet hate machine” (Olson 422), which relegated Anonymous as juvenile pranksters and stimulated nationwide media frenzy about Anonymous in the United States. In August 2014, in the wake of the killing of Michael Brown, the unarmed black teenager who was shot by a police officer in Ferguson, Missouri, Anonymous posted a YouTube video titled “Anonymous—Operation Shock Drop #OpFerguson #OpHandsUp #OpCopWatch,” trying to

draw national media attention towards this case.<sup>3</sup> Later, Anonymous exposed the name of the police officer, but the identity turned out to be wrong. In reporting the Ferguson case, the *Nation* quoted black feminist blogger Feminista Jones' words—"as a Black woman, I'm also used to the historical erasure of our work and theft of our labor"—to criticize Anonymous's propensity for media sensation at the expense of others' causes.<sup>4</sup> The magazine *America* likened Anonymous to "the online equivalent of a mob, an unaccountable collective that plays judge, jury and executioner."<sup>5</sup>

Furthermore, what dwarfed these negative media portrayals was a news report titled "Alert on Hacker Power Play" by Siobhan Gorman, published in the *Wall Street Journal* on February 21, 2012.<sup>6</sup> This article revealed that Gen. Keith Alexander, the director of the National Security Agency (NSA), made assessments about Anonymous in meetings at the White House, warning that "the hacking group Anonymous could have the ability within the next year or two to bring about a limited power outage through a cyberattack." The NSA's assessment alerted the public to Anonymous's potential of sabotaging the American power grid, which would be considered a national security issue. Although three years have passed, and Anonymous has never launched such a cyberattack, this piece of news is still being quoted as authoritative and even definitive by those who see and/or seek to portray to others that Anonymous is a threat to societal stability. In retrospect, this might be the NSA's attempt to use the media to spread fearmongering in the hope of preventing the public from participating in Anonymous's operations. Regardless of the reason, why was the United States government afraid of Anonymous?

Different from other "stereotyped hackers," Anonymous does not shun publicity and is eager to create counter-narratives. It makes significant use of the media attention to grow its popularity. And it uses social media to voice its own opinions. Although its rhetoric on social

---

<sup>3</sup> See <https://www.youtube.com/watch?v=2ppjvKPs4P4>

<sup>4</sup> See <http://www.thenation.com/article/190369/truth-about-anonymous-activism>

<sup>5</sup> See <http://americamagazine.org/issue/current-comment-21>

<sup>6</sup> See <http://www.wsj.com/articles/SB10001424052970204059804577229390105521090>

media might not be as extensive and influential as the reach of the mainstream media, it can offer the public with some new insights into the myth of Anonymous. How does a leaderless and decentralized hacker collective administer its social media content and build its brand identity?

## **The Brand Identity Construction of Anonymous**

According to Schmidt (the CEO of Google) and Jared (the Director of Google Ideas), social media, as a form of interconnected estate, is “a place where any person with access to the Internet, regardless of living standard or nationality, is given a voice and the power to effect change.” Social media gives Anonymous a chance to coordinate activities and rally support from its followers or sympathizers the world over. It uses the source code sharing website Pastebin.com to dump its hacked data; it uses YouTube to release its manifesto; it uses Facebook for information sharing, and it uses Twitter for updates, coordination and recruitment. Although Anonymous’s open nature gives permission for all the Anons to make manifestos via social media, there is a common thread running through the diversified creeds. The following are three web-accessed self-definitions of Anonymous, selected from hundreds of Anonymous-related social media accounts.

The Twitter account “@AnonyOps”, which has 347,000 followers, claims “this headless hydra supports whistleblowers, a free press, women, and is trans-inclusive.” On “Anonymous” Facebook webpage, its logo is a man in a suit with a question mark in the place of his head, representing its intentional leaderlessness and propensity for skepticism (Fig. 1). And on top of the logo floats the following words in bold “THE CORRUPT FEAR US, THE HONEST SUPPORT US, THE HEROIC JOIN US.” On the webpage of YouTube account “Anonymous Official,” its slogan goes as follows: “We Are Anonymous. We Are A Legion. We Do Not Forgive. We Do Not



**Figure. 1 Anonymous’s Logo on Facebook Page.**

Forget. Expect Us.”<sup>7</sup> This slogan has become the signature tagline of most Anonymous announcements.

Although these three self-definitions are not identical, they each emphasize Anonymous’s decentralization. In Greek mythology, a hydra is a many-headed serpent whose heads grow again as they are cut off, killed by Hercules eventually. But a “headless hydra” is a snake with no head to be chopped off, no vulnerability to be exploited. Thus, by likening Anonymous to a “headless hydra,” it implies that there are no leaders in Anonymous to be singled out, either for lionization or discredit. Moreover, the repeatedly used words “we” and “us” can create a sense of collectiveness and solidarity. This is because “identification and personalisation are instruments of control as they are applied in modes of centralised organisation” (Kaulingfreks and Ruud 422). Without personal interest at play, Anonymous has the potential to “channel the power of like-minded” (Beyer 149) allies from different walks of life. However, the Facebook and YouTube’s mottos such as “THE CORRUPT FEAR US” and “Expect Us” are rhetorically hyperbolic, setting no objectives. What is the self-appointed mission of Anonymous? Without a clear agenda, how does Anonymous build a distinguishable brand identity? At this point, a brief review of Anonymous’s origin will be useful.

Anonymous’s roots were in the imageboard 4chan—a simple image-based bulletin board created in 2003 where anyone could post comments and share images.<sup>8</sup> In particular, Anonymous rose up out of 4chan’s /b/ board, the forum reserved for “random” discussions which imposed anonymity on all the posts. This forced anonymity policy paved the way for the creation of Anonymous. As anthropologist Coleman quotes a former Anon:

The posts on 4chan have no names or any identifiable markers attached to them. The only thing you are able to judge a post by is its content and nothing else. This elimination of the persona, and by extension everything associated with it, such as

---

<sup>7</sup> See <https://www.facebook.com/ArmyAnonymous?fref=ts>;  
<https://www.youtube.com/user/AnonymousWorldvoce>; <https://twitter.com/AnonyOps>

<sup>8</sup> See <http://www.4chan.org/>.

leadership, representation, and status, is the primary ideal of Anonymous. (47)

Although, in this pseudonymous environment, elements of decentralization and equality begun to take shape, the modus operandi for early Anons involved “trolling” and “lulz.” As Internet slang, “trolling” means anonymously harassing or mocking others online with an aim to anger or humiliate them. “Lulz” is an alteration of the abbreviation LOL (laugh out loud). It means the enjoyment felt after pursuing a prank or online disruption that leads to someone else’s embarrassment (Olson 478). Users of the /b/ board treated the Internet as their playground and called themselves “/b/tards.” They posted pornography intended to be as shocking as possible to attract attention “as they also discussed data visualization strategies and traded coding tips. Nearly any appetite is acceptable, and nearly any weakness, technical or human, is exploited” (Norton). The frequently performed prank was Doxing—hacking and exposing others’ personal information as publicly and widely as possible. In order to seek “lulz,” users developed “all the tools of ‘ultra-coordinated motherfuckery’ that Anonymous practices today” (Norton), including massively choreographed pranks and Distributed Denial of Service (DDoS) attacks.<sup>9</sup>

As for the exact “birthday” of Anonymous, Coleman says that “it is almost impossible to pinpoint a day or event when trolling on 4chan was born. But by 2006, the name Anonymous was being used by participants to engage in trolling raids” (44). Such a background prompts burning questions: initially driven by “trolling” and “lulz,” is Anonymous a whimsical group of pranksters, or an awkward conglomeration of digital defenders, or a menacing gang of cyber terrorists? Or, perhaps, is this umbrella term “Anonymous” simply digital noise unworthy of media attention?

In retrospect, two operations changed Anonymous’s trajectory and pushed it to take on a political coloration. The first politically oriented action was the 2008’s Project Chanology,

---

<sup>9</sup> DDoS, a computer term, stands for Distributed Denial of Service. It is an attack on a website or networks carried out by a network of computers that temporarily knocks the site offline by overwhelming it with junk traffic (Olson 477).

targeting the Church of Scientology in the name of defending freedom of information as Scientology tried to suppress a leaked video.<sup>10</sup> Project Chanology was also the first time Anons decided to extend their activities from online to offline, donning Guy Fawkes masks to participate in street protests. The Guy Fawkes mask was designed by a British artist David Lloyd in 1982 for an anarchy-themed graphic novel *V for Vendetta*. The inspiration came from the story of Guy Fawkes, an important member of a group of “intransigent English Catholics,” who planned the

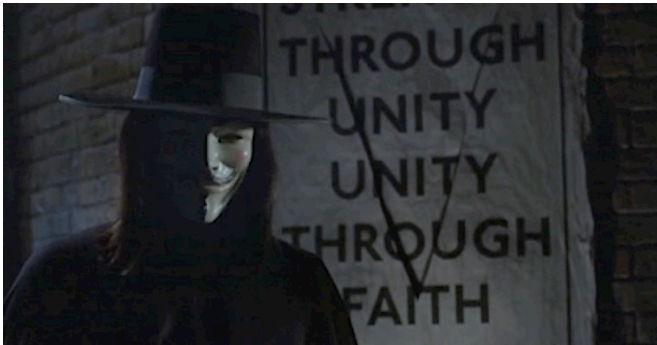


Figure. 2 A screenshot captured from the movie *V for Vendetta*.

failed Gunpowder Plot in 1605, attempting to blow up parliament in London to “restore Catholicism along with a Catholic monarch” (Oxford Dictionary of National Biography).

The stylized mask gained broader popularity after the release of the 2006

film adaptation of *V for Vendetta*, in which the Gunpowder Plot was the major storyline and the protagonist—an anarchist freedom fighter “V”—always wore the Guy Fawkes mask (Fig. 2). Over the years, Anonymous has adopted this mask to be its recognizable symbol for street protests.

From Project Chanology, Anonymous became increasingly associated with hacktivism, hacking and DDoSing government, religious, and corporate websites to deliver social justice. Another political watershed was Operation Payback (December 2010) in support of the whistleblower organization, WikiLeaks. Anonymous attacked the websites of three corporations that cut off their funding services to WikiLeaks under the United States government’s political pressure. This operation brought Anonymous massive media attention and earned it a reputation as an indomitable collective that use “weapons of the geek” (Coleman 107) to challenge Western capitalist hegemony and political authority.

---

<sup>10</sup> Chanology: a portmanteau of “4chan” and “Scientology” (Olson 476).

I will use these two operations—Project Chanology and Operation Payback—as case studies in this paper. I will underscore Anonymous’s collectiveness by not singling out any individuals. And I will elaborate on the process and significance of its brand identity construction by virtue of social media. Public resources such as media coverage and social media posts will be my primary sources, based on which I will undertake a content analysis—“a social research method appropriate for studying...not only communication processes but other aspects of social behavior as well” (Babbie 349). Along this line, I will center my analysis on the following question: given the collaboration of the NSA, Google, and other purportedly non-governmental entities, does Anonymous represent an alternative or protest to the intertwining of corporate and governmental opacity?

## **Chapter One: Project Chanology—from Personal to Political**

The last two years have been singular—never before have so many geeks and hackers wielded their keyboards for the sake of political expression, dissent, and direct action.

--Coleman (382)

### **1.1 Targeting Scientology: Embarking on Free Information Battles**

On January 21, 2008, a video titled “message to Scientology” was uploaded onto YouTube by Anonymous under the account “ChurchOfScientology.”<sup>11</sup> In the video, “a Stephen Hawking-style robotic voice” (Olson 72) announced,

Hello, leaders of Scientology. We are Anonymous. Over the years, we have been watching you. Your campaigns of misinformation; your suppression of dissent; your litigious nature, all of these things have caught our eye. (Timeline: 0:00 to 0:14)

In a hyperbolic yet playful way, Anonymous threw down the gauntlet to the Church of Scientology. It was the first time Anonymous used social media such as YouTube to announce its manifesto. Although it was just a two-minute video, it had a tremendous impact on Anonymous’s future strategy and trajectory. By posting it on YouTube, a video-sharing website open to everyone, Anonymous expanded its terrain from the hidden, secret hackers’ underground to the open public, allowing anyone who shared the same ideas to jump on board. By making public its mission of targeting the “suppression of dissent,” Anonymous started, intentionally or unwittingly, building a public image as a champion of the subdued and censored. The “message to Scientology” video had the potential “to mobilise people from the outside of the space of participation” (Gerbaudo 145). Or, at least, its provocative connotation might pique people’s interest and ask: What was this? Why did Anonymous declare a “war” on Scientology?

---

<sup>11</sup> See <https://www.youtube.com/watch?v=JCbKv9yiLiQ>

“Scientology emerged in the early 1950s as a movement that found its inspiration in the voluminous writings of L. Ron Hubbard (1911-1986)...[It] was soon serving as a religion for many of Hubbard's followers” (Davis). Hubbard was an American author best known for his science fiction, who developed a spiritual healing technology called Dianetics, through which practitioners re-experienced consciously painful or traumatic events in their past in order to be freed (Melton 28). Ever since its inception, Scientology has been controversial. Although it is legally recognized as a tax-exempt religion in eight countries including the United States, some still consider it to be evil and stifling. A piece in the magazine *Time* uses titles such as: “The Thriving Cult of Greed and Power. Ruined lives. Lost fortunes. Federal crimes. Scientology poses as a religion but is really a ruthless global scam—and aiming for the mainstream.”<sup>12</sup> However, the reason why Anonymous targeted the Church of Scientology had little to do with the latter’s contentious religious beliefs or its method of spiritual rehabilitation. As a matter of fact, the cyberwar between Anonymous and Scientology was sparked by a leaked video featuring an interview of Tom Cruise, “Scientology’s celebrity of celebrities” (Coleman 53).

The interview itself was conducted in 2004 and “shown exclusively to church members” (Olson 60). In 2007, an anonymous church member decided to leak the video and mailed it on a DVD to an anti-Scientology campaigner named Patty Pieniadz. She held the video and waited until early January 2008 when she reached out to NBC in the hope of coinciding with the release of Tom Cruise’s new biography. But, NBC got cold feet at the last minute of broadcast because the Church of Scientology was “notoriously litigious” (Olson 62). Around that time, some copies of this video were uploaded onto YouTube but promptly taken down for copyright violations. After some setbacks, the video finally found its way to *Gawker*. Despite Scientology’s intimidation, Nick Denton, the founder and the managing editor of *Gawker*, published a blog post titled “The Cruise Indoctrination Video Scientology Tried To Suppress” at 10:18 AM, January

---

<sup>12</sup> See <http://content.time.com/time/magazine/article/0,9171,972865-2,00.html>

15, 2008.<sup>13</sup> The interview was embedded in the post. Denton started the blog with a simple sentence “you have to watch this video” and made comments like “if Tom Cruise jumping on Oprah's couch was an 8 on the scale of scary, this is a 10.” Then, what exactly was in that video? What did Tom Cruise say? Why did the Church of Scientology go to great lengths to suppress it?

In this 9 minutes and 26 seconds video, Tom Cruise raved about the principle and merit of being a Scientologist in an incoherent and egotistic way. To quote some of his words:

We are the authorities on getting people off drugs. We are the authorities on the mind. We are the authorities on improving conditions. Criminal [*sic*], we can rehabilitate criminals. We are the way to happiness. We can bring peace and unite cultures. (Timeline: 2:37 to 2:54).<sup>14</sup>

Upon its release, the video went viral. So far, Denton’s blog post has received 114,274 page views. More importantly, *Gawker*’s publication paved the way for the video to be re-uploaded and eventually stayed on YouTube. The Church of Scientology was enraged and “about to furiously unfurl lawsuits” (Coleman 55) against publishers. For decades, Scientology’s inclination for legal coercion and information suppression had pushed a lot of journalists and activists to investigate it. In the face of the leaked Tom Cruise video, Scientology’s attempted repression offered a perfect opportunity for a neophyte like Anonymous to enter the stage of Internet politics. According to Coleman, the reason why Anonymous decided to get involved was because Anons “were undeniably, and royally, pissed off that Scientology dared to censor a video on ‘their’ Internet—especially such a hilarious one” (60). Hence, Anonymous voluntarily plunged into the confrontation with Scientology in the name of opposing Internet censorship.

## **1.2 Logging onto Internet Relay Chat (IRC): The Formation of a Decentralized Anonymous Community**

---

<sup>13</sup> See <http://gawker.com/5002269/the-cruise-indoctrination-video-scientology-tried-to-suppress>

<sup>14</sup> Ibid.

The premise for Anonymous to “win” this cyberwar and disrupt Scientology’s function was to establish a base where Anons could communicate and coordinate. But, as Williams (Assistant Professor of Sociology Department, CSU, Chico) puts it, “the Internet is likely the largest decentralized project in all of human history” (Shantz and Tomblin). Then, in this massive, decentralized, and sometimes mystifying Internet playground, where could Anons go? How could they carry out choreographed digital operations?

In this aspect, Anonymous demonstrated its knack of making good use of social media for the purpose of communication, message delivery, and mobilization. Kaplan and Haenlein (Professors of Marketing at ESCP Europe) define social media’s function as “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content” (61). According to them, the popular forms for ordinary netizens include collaborative projects (e.g., Wikipedia), blogs, content communities (e.g., YouTube), social networking sites (e.g., Facebook), virtual game worlds, and virtual social worlds.<sup>15</sup> As for hackers and geeks, however, their favorite social media tool is a little bit obscure in that their favorite “underground” communication device is Internet Relay Chat (IRC). It serves as a transnational platform offering virtual chat rooms, where people can have real-time text conversations with global users. IRC also allows users to create and name new chat rooms, or “channels (indicated as #),” in order to attract like-minded “virtual friends.” Unless a channel is set to be private or invite-only, anyone who has the IRC client—a program that runs on your computer and sends and receives messages to and from an IRC server—can enter the chat room, either joining in the conversation or merely observing.

Although participating in IRC networks requires a certain degree of technical knowledge, it is not so sophisticated that it deters users, evidenced by the data that “by 2008, a few million people were using it” (Olson 50). Against this backdrop, it is not difficult to imagine that Anons

---

<sup>15</sup> Netizen is a variant on citizen. It refers to a person who interacts with others on the Internet. In effect, anyone who uses the Internet becomes a netizen (Urban Dictionary).

chose IRC as their base for its instantaneity, relative privacy, and potential “comrades.” Olson, a writer with *Forbes* magazine, believes “IRC networks were helping Anonymous turn from an unpredictable, volatile mass of image board users into well-organized, sometimes-threatening groups” (52).

With the community construction underway, Anonymous named the operation “Project Chanology.” The word “Chanology” was created by an anonymous user of 4chan’s /b/ board as a portmanteau of “4chan” and “Scientology” (Olson 476).<sup>16</sup> This title could be understood as a way of paying homage to 4chan, the imageboard that gave birth to Anonymous and the mothership from which Anons frequently sought technical and moral support. However, as mentioned above, anyone could create a channel and start up a conversation on IRC. So, at times, there were hundreds of IRC channels under the same banner of Chanology. Although this could prevent Anonymous from being dominated by a handful of elite members, or infiltrated by FBI agents, the situation could be very confusing for newcomers. What’s more, there was an array of symbols—“~, &, @, %, and +”—used to show the status of each person in each IRC channel. For instance, someone labeled with “%” could kick out anyone below his/her status, and with the symbol “@” one could edit a channel topic and ban people (Olson 222). These signs implied that there were different organizational roles in terms of the infrastructure of Anonymous’s IRC channels. Then, did these organizers amount to opinion leaders and decision makers? Was this structure contrary to Anonymous’s public image of decentralization and leaderlessness?

It is safe to assume that these organizers’ words might carry more weight than the words of newcomers. But, it is highly unlikely for them to order or force others to engage in “unpopular” operations. After all, Anons are free, anonymous individuals sitting behind their own computers. They can create their own channels or come and go as they please. Thus, “one of Anonymous’s core principles is that it will not be anybody’s ‘personal army’” (Coleman 349).

---

<sup>16</sup> See *supra* note 10.

More often than not, a target will be chosen or an agreement will be reached by voting. To quote an Anon's description of a typical process of decision-making:

With any given operation there are always some who agree and some who disagree...Anonymous [*sic*] allows each person individually to vote on each operation, a yes vote means they participate, a no vote means they do not. Anyone is allowed to create an op and if others vote yes it will get traction and something may be accomplished. (Kelly)

Usually, it may take hours to vote but only minutes to attack a website. Although time-consuming, this horizontal form can make sure that everyone's voice can be heard. By rebelling against the vertical and hierarchical institutional structure, Anonymous aims to foster individualistic thinking and avoid internal power competition. To some degree, "what [Anons] have created is one of the most democratic systems in the world. In a sense, they have allowed anyone around the world to organize under an 'Anonymous' banner and allow for people to express unfiltered opinions" (Shantz and Tomblin 71). This "desire for leaderlessness and high democracy" (Coleman 48) may help Anonymous achieve solidarity out of multiplicity and make it one of the most irrepressible, diversified, and sometimes, whimsical hacker collectives.

### **1.3 Involving YouTube: Visualizing "Call-to-Arms" Manifestos**

Although decentralized, Anonymous somehow developed a concerted attitude about the importance of managing its public image. In Chanology IRC networks, Anons created two channels—"#xenu" and "#target"—to discuss tactics, coordinate actions, and boost morale.<sup>17</sup> As Project Chanology rapidly gained popularity, "#press" was created with the topic set as "here's where we're going to talk to the press" (Olson 71). This move was smart. On the one hand, extending an olive branch to the media might result in growing publicity, which would probably attract more like-minded people to join in Anonymous. For instance, on February 15, 2008, an article titled "Anonymous vs. Scientology: A Case Study of Digital Media" by Dan Schultz was

---

<sup>17</sup> According to Scientology's version of history, Xenu is the dastardly, evil alien overlord of the galaxy (Coleman 57).

published on pbs.org. Although Schultz did not directly mention IRC channels in his article, 6 out of 94 commenters introduced IRC in their remarks.<sup>18</sup> On the other hand, by inviting the media on board, Anons intended to take the initiative and feed the media the stories in their favor. As Kelly argues, “Anonymous is not defined as, and does not intend to be defined as, the traditional cast of voiceless, faceless hackers. Rather, Anonymous publicly leads the ‘hacktivism’ movement” (B. Kelly 1667). Whether or not Anonymous wanted to “publicly [lead] the ‘hacktivism’ movement” was uncertain, but it apparently refused to be “voiceless.” It was this desire to voice its political views that played a vital role in Anonymous’s brand identity construction and pushed it towards the path of online civil disobedience. But, Anonymous’s method of expressing its opinion and protesting against Scientology was unorthodox and debatable.

In the cyberwar against the Church of Scientology, Anonymous’s tactics featured “the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends” (B. Kelly 1668). The most commonly used methods were DDoSing and defacing the Church’s main website: Scientology.org.<sup>19</sup> DDoS is a computing term, standing for Distributed Denial of Service. A DDoS attack is using junk traffic to overwhelm targeted websites or networks in order to knock them offline temporarily. In the figurative sense, security writer Graham Cluley likened the effect of DDoS attacks to “15 fat men trying to get through a revolving door at the same time.”<sup>20</sup> Anons could partake in DDoS attacks on Scientology simply by downloading free software tools available on 4chan. Apart from these online attacks, Anons also ordered unpaid pizzas and escorts to Scientology churches across North America; they faxed images of their nude body parts to churches; they prank-called the Dianetics hotline (Coleman 5). Although some of those measures were disturbing and even illegal, Anonymous was bold enough to take credit for all the actions. Some media-savvy Anons in “#press” even wrote a press release titled the

---

<sup>18</sup> See <http://www.pbs.org/idealab/2008/02/anonymous-vs-scientology-a-case-study-of-digital-media005/>

<sup>19</sup> When used as a verb, deface means to vandalize a website (Olson 477).

<sup>20</sup> See <https://nakedsecurity.sophos.com/2009/08/06/fat-men-revolving-doors/>

“Internet Group Anonymous Declares ‘War on Scientology.’”<sup>21</sup> On January 21, 2008, they posted it on PRLog.org, a website offering free press release distribution service:

Anonymous announced their intention to combat the activities of the Church of Scientology on Monday. A spokesperson said that the group's goals include bringing an end to the financial exploitation of Church members and protecting the right to free speech, a right which they claim was consistently violated by the Church of Scientology in pursuit of its opponents...

At the end of this press release, it listed its source as Chan Enterprises, along with the company's email address and telephone number, all of which were feigned. Claiming the news was offered by “a spokesperson” was quite deceptive, because there had neither been leaders nor an official mouthpiece representing Anonymous. As an umbrella concept, Anonymous allows those who want to get on board to “call themselves Anonymous and rightfully claim the name” (Coleman 48). And, at the same time, it has strong anti-ego and anti-celebrity-seeking ethos. Those who seek self-promotion and personal fame will be labeled “namefags” or “leaderfags” as an insult, or be kicked out of channels. Although the suffix “fag” might be offensive, it is not generally a humiliation within Anonymous. It might be a rebellious way of ridding Anons of their ethnic, religious and sexual differences since “nearly every category of person, from old-timers to new-timers, is labeled a ‘fag’” (Coleman 42). To a great extent, such characteristics differentiate Anonymous from other hacker collectives because “this subsumption of individual identity into collective identity is unusual in Western culture” (Coleman 46). As a result, with no personal gain in the picture, Anonymous's goal is its collective celebrity and success.

The reason why “a spokesperson” appeared in this press release might be that Anons wanted to dupe the media. Although they enjoyed attention from the press, they could not resist the temptation of hoaxing the media for “lulz.” Goode's (Senior Lecturer, the University of Auckland) words shed some light on this phenomenon, “Anonymous hacktivism emerged at the intersection of pranksterism, or ‘trolling,’ and reaction against institutional practices perceived to

---

<sup>21</sup> See <http://www.prlog.org/10046797-internet-group-anonymous-declares-war-on-scientology.html>

impinge on the sanctity of free speech” (76). Despite the tongue-in-cheek style of the press release, however, the political message of defending “the right to free speech” was conveyed in a straightforward and provocative way. Surprisingly, this “dramatic and ominous” (Olson 71) press release inspired several other Anons to make a video. Piecing together “uncopyrighted footage and music,” accompanied by “an automated voice” (Olson 71-72), they finished the two-minute video “message to Scientology” and posted it on YouTube under the screen name of “ChurchOfScientology” on January 21, 2008.<sup>22</sup> A robotic voice declared Anonymous’s mission as the video unfolded:

For the good of your followers, for the good of mankind, and for our own enjoyment, we shall proceed to expel you from the Internet, and systematically dismantle the Church of Scientology in its present form. We recognize you as a serious opponent, and do not expect our campaign to be completed in a short time frame. However, you will not prevail forever against the angry masses of the body politic. Your choice of methods, your hypocrisy, and the general lawlessness of your organization have sounded its death knell... (Timeline: 0:29 to 0:57)<sup>23</sup>

In this video, there was no eye dropping or shocking nude images as Anons used to post on 4chan. Only “a drab corporate glass building stands against a backdrop of ominously racing dark clouds” (Coleman 61). Would an upload of an activism-oriented video be a smart or futile move? YouTube, as a video-sharing website, serves over 100 million videos per day. The video content has to be very intriguing, otherwise it would not be able to grab the attention of users. To Anons’ own surprise, this video went viral overnight. The next day, the Chanology-related “IRC network was crashing as thousands of new people tried piling into #xenu” (Olson 73). What on earth attracted these people? Who were they?

Although it was not very clear that, at this point, “was Anonymous simply trolling for its own lulzy amusement or was it earnestly protesting” (Coleman 60), the wildly circulated YouTube video “message to Scientology” added a strong political coloration on its moniker. At

---

<sup>22</sup> See *supra* note 11.

<sup>23</sup> *Ibid.*

the end of this video, the robotic voice claimed: “Knowledge is free. We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.”<sup>24</sup> Such a manifesto invoked the values of hacktivism in which many hackers and geeks had faith. “Hacktivism is the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking” (Jordan 1). But, against what are the “grassroots” protesting? What is the political end of their “self-activity”?

The answer of such questions may lie in the origin of the word “hacktivism.” Oxblood Ruffin, a member of cDc, pointed out in his article “Hacktivism, From Here to There” that “hacktivism” was coined in 1996 by Omega (also a member of cDc), “connecting technology and human rights” (64).<sup>25</sup> Omega linked “hacktivism” to Article 19 of the United Nations Declaration of Human Rights (UNDHR), which stated “everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” Although coined as “hacktivism,” it did not confine its practitioners to proficient hackers. Its aim was to raise awareness of those who were capable of using technology to fight for “the right to freedom of opinion and expression” and call upon them to rise to the challenge. This video indicated Anonymous had not only inherited this spirit but also tried to popularize it by visualization.

In visualizing its manifesto via the YouTube video, Anonymous turned a new page in building its brand identity while executing Project Chanology. This operation was regarded as the milestone of Anonymous transforming “from kids playing hacker to vigilante justice, to change the world” (Olson 133). It flew the “free information banner” under which those who believed “the potential of the Internet to change society” could rally. It brought to the fore “the need to

---

<sup>24</sup> See *supra* note 11.

<sup>25</sup> As I explained above, cDc stands for “Cult of the Dead Cow”: a computer hacker organization founded in 1984 in Lubbock, Texas; the article “Hacktivism, From Here to There” can be found on [http://www.cultdeadcow.com/cDc\\_files/cDc-0384.php](http://www.cultdeadcow.com/cDc_files/cDc-0384.php)

reform intellectual property laws” and “the evils of censorship of any kind” (Beyer 149). This rebellious, bold, vindictive yet mischievous spirit of Anonymous struck a chord with those hackers and geeks who had been waiting for a righteous cause around which to unite. As a matter of fact, from the 1990s, there had been constant friction between “netizens—wholly committed to free speech—and the Church of Scientology—wholly committed to stamping it out by any means necessary (legal or illegal) to censor criticism and prevent leaked documents from circulating online” (Coleman 58). Thus, in this sense, Anonymous was using Project Chanology to rekindle the old flame of hackers and geeks in protesting Scientology, in the hope of constructing its brand identity as a symbol of fighting against Internet censorship.

Apart from the video’s content, the YouTube account “ChurchOfScientology” also offered a link: <http://forums.whyweprotest.net> under its “About” tag in the hope of expanding its influence.<sup>26</sup> This site was an activism-oriented forum, which dedicated a whole section to “Anonymous vs. Scientology,” open to anyone who were interested in learning more about Chanology’s progress or wanting to contribute their own voice. Apparently, Anonymous was trying to use different social media forms to spread its ideas and expand its territory beyond the hackers’ underground, in that the enthusiastic response to the YouTube video made Anonymous recognize the high potential of netizens. Despite government or big corporations’ constant attempt at control of information and mass surveillance, the Internet and social media could still “empower individuals to take part in the creation of new narratives. Thus, in an era when crass perversions of populism, and exaggerated calls for national security, threaten the very premises of representational democracy and free discourse, interactive technologies offer us a ray of hope for a renewed spirit of genuine civic engagement” (Rushkoff 6).

#### **1.4 Sparking Media Frenzy: A Double-edged Sword in Brand Identity Construction**

---

<sup>26</sup> ChurchOfScientology is the account that posted the video onto YouTube.

As mentioned previously, the media, especially the Western mainstream media, has played a crucial role in mystifying and branding Anonymous. As Douglas Thomas (Associate Professor of Communication, USC Annenberg) points out, “hacker identity and mainstream representation, often reflect on each other, blurring the lines between fact and fiction” (ix). But, the mythmaking was a win-win situation for Anonymous: the media received audience growth and Anonymous “[received] an enormous PR boost” (Phillips 500) from frenzied news coverage. The media propelled Anonymous’s cause in that the aura of mystery attracted more people to pay attention. As can be seen with the Fox 11 News Report, which dubbed Anonymous “the Internet hate machine,” even negative coverage helped push Anonymous into the national spotlight. As a result, “what once has been an underground site, known only to the few thousand active participants, had become a household name” (Phillips 501).

The Church of Scientology recognized the power of the media as well. Scientology hit back by telling *Newsweek* that Anonymous was “a group of cyber-terrorists...perpetrating religious hate crimes against Churches of Scientology and individual Scientologists for no reason other than religious bigotry” (Braiker). But, to Scientology’s dismay, the more it attempted to criticize Anonymous and suppress the Tom Cruise interview video, the more viral the video was spread. This was a classic case of the Streisand effect, “whereby an attempt to hide, remove, or censor a piece of information has the unintended consequence of publicizing the information more widely, usually facilitated by the Internet” (Wikipedia).<sup>27</sup> To date, the video “message to Scientology” has received 5,183,094 views. Another video titled “Tom Cruise Scientology Video (Original Uncut)” has been viewed 10,508,931 times.<sup>28</sup>

The Streisand effect fanned Anonymous’s passion as Project Chanology proceeded. On January 19, 2008, the Church of Scientology’s main website was hit by 488 attacks from different

---

<sup>27</sup> Streisand effect is named after American entertainer Barbra Streisand, whose 2003 attempt to suppress photographs of her residence in Malibu, California, inadvertently drew further public attention to it. (Wikipedia)

<sup>28</sup> See [https://www.youtube.com/watch?v=UFBZ\\_uAbxS0](https://www.youtube.com/watch?v=UFBZ_uAbxS0)

computers. On January 24, 2008, Anonymous launched a bigger assault on Scientology.org, taking the site offline (Olson 423). Such news hit the Western mainstream media, American media outlets in particular. Fox attributed such online disruptions to a “small clique of super hackers” (Olson 80). The media and Anonymous had different agendas. For the media, “these kinds of events [made] headlines not for their political motivation but merely for the spectacle of vigilante computing” (Krapp 87). By categorizing Anonymous into a “small clique of super hackers,” such news negated the elements of decentralization, collectivity, openness and populism—the core values of Anonymous’s brand identity. Although sometimes Anonymous would play with societal stereotypes of hackers to foster a sense of danger around their actions and tactics (Sauter 989), it did not play along at this time. On the contrary, Anonymous tried to use social media to constitute counter-narratives. First, it posted another press release titled “Internet Conflict with Scientology Expands” on PRLog.org on January 27, 2008.<sup>29</sup> With its source still listed as Chan Enterprises, the post claimed:

Recently, Anonymous caught the attention of news networks such as Fox News, KNBC, and Sky News. Their message spread to popular social media sites, such as Digg, Reddit, and Slashdot... We are not merely a small clique of “super hackers” as some portray us, but a collective of individuals from all walks of life.

And then, on the same day, the account “ChurchOfScientology” uploaded another video titled “Call to Action” onto YouTube.<sup>30</sup> A robotic voice further explained what Anonymous was:

Anonymous is a collective of individuals united by an awareness that someone must do the right thing, that someone must bring light to the darkness, that someone must open the eyes of a public that has slumbered for far too long. (Timeline: 0:15—0:26)

To a great extent, Anonymous’s active engagement in using social media to brand itself implied that “the Internet platform has allowed users to be both consumers and *prosumers* of messages”

---

<sup>29</sup> See <http://www.prlog.org/10047683-internet-conflict-with-scientology-expands.html>

<sup>30</sup> See <https://www.youtube.com/watch?v=YrkchXCzY70>

(Berenger 511-12). Anonymous's method of producing "messages" was to de-individualize itself and seek the collective fame. By defining Anonymous as "a collective of individuals from all walks of life," it negated the sense of achievement of those who initiated and penned these announcements. It also conveyed such a message to viewers that Anonymous's actions were self-motivated operations and the participants did not have to be skilled hackers. Anyone could contribute to its cause if they shared the same sense of social justice with Anonymous.

Moreover, Anonymous's usage of social media could not only publicize its own motive but also feed the media more materials to debate. To a great extent, "the use of social media...played a role in mobilization of supporters and setting the agenda for mass media" (Berenger 511). When Fox called Anonymous the "Internet hate machine" (Olson 422) in 2007, Anonymous posted a video titled "Dear Fox News" onto YouTube on July 29, 2007.<sup>31</sup> It ridiculed Fox by claiming "we are everyone and we are no one...we are the face of chaos and the harbingers of judgment...you have now got our attention." As expected, this video stimulated Fox to keep condemning Anonymous. "As a consequence, the terms 'hackers on steroids,' 'hacker gangs,' and 'the Internet hate machine' were immediately integrated into the trolling lexicon" (Phillips 500). In a sense, Fox and Anonymous "worked" jointly, snowballing the Anonymous phenomenon. This case might confuse some, since Anonymous's "trolling" on FOX seemed to go against "the broad principles underlying Anonymous" (Olson 244):

1. Choosing targets because they were oppressors of free expression;
2. Not attacking the media.

For Anons, the term "attack" might be understood as Distributed Denial of Service (DDoS) attack; "trolling" the media was for "lulz," rather than an offensive action.<sup>32</sup> There were two reasons why Anonymous would not DDoS the media. First, launching DDoS attacks on the

---

<sup>31</sup> See <https://www.youtube.com/watch?v=RFjU8bZR19A>

<sup>32</sup> As I explained earlier, a DDoS attack is using junk traffic to overwhelm targeted websites or networks in order to knock them offline temporarily.

media amounted to silencing it, contrary to Anonymous's fundamental principle of freedom of speech. Second, Anonymous needed media attention. Unlike those hackers who hacked for monetary theft or personal gain, Anonymous set the political end of its hacktivism-oriented operations as hijacking and exposing "wrongdoers" in the name of delivering social justice. Therefore, Anonymous would use social media sites, such as YouTube, Facebook, Twitter, IRC channels, "whyweprotest" forums, and PRLog website, as vehicles to voice its opinions, in the hope of sparking the media frenzy rather than attacking the media. It proved to be the best way to reinforce its brand identity and maintain its political momentum by constantly remaining in the mainstream media spotlight. The more intensive the media attention, the better for Anonymous's causes, in that it could steer the public attention towards the alleged "wrongdoers" and their "wrongdoings."

On the flip side of the coin, however, Anonymous itself might be labeled as "wrongdoers" and consumed by the media. Anonymous's open nature allows anyone to act on its behalf and make announcements via social media; but, at the same time, it makes it extremely difficult to defend itself if something goes south. Since "there are no agreed-upon mandates to uphold" (Coleman 17), Anons are bound by their free will and personal morality, which might end up in internal conflicts. The fracture between "moralfags" and "lulz-seekers" is a good case in point.<sup>33</sup> "Moralfag" is someone who does not appreciate or partake in the extreme or humiliating activities designed for malicious "lulz" or "trolling." As Project Chanology advanced, activist-oriented Anons viewed themselves as defenders of free information, becoming more and more concerned about the morality and ethics of the operations. But, there were some non-activist Anons not ready to abandon "lulz," the thing that brought them together in the first place. As their infighting intensified, lulz-seekers derided moralfags in IRC channels. The following is an excerpt from a chat log of a lulz-seeker nicknamed "CPU" (Coleman 69):

---

<sup>33</sup> As explained previously, the suffix "fag" is not generally a humiliation within Anonymous.

<CPU>: Internethatemachine is for those sick of the moralfags and the lovefags am i rite lol?

<CPU>: We should just hit a random forum for the lulz. Anyone remember the emetophobia raids?

[...]

<CPU>: Or we could find an epilepsy forum and spam it with flashing gifs or something?

Then, on March 22, 2012, someone invaded “the homepage of the American epilepsy association” (Gerbaudo 107) and posted bright flashing images, inducing seizures among some of the forum’s members. No one knew for sure whether or not CPU did it since nobody took the credit for this intrusion. But, “every piece of reporting incorrectly attributed the attack to Anons fighting Scientology” (Coleman 69). For instance, *Wired* reported, “circumstantial evidence suggests the attack was the work of members of Anonymous, an informal collective of griefer best known for their recent war on the Church of Scientology” (Poulsen).<sup>34</sup> Drawing such a conclusion might be because the media got wind of the infighting and the verbal threat. Despite Anonymous’s claim that it was not behind this “morally reprehensible and notorious” (Coleman 69) intrusion, it was hard to change the mainstream media’s narratives. After all, how could a leaderless, non-membership and decentralized collective disassociate itself from some shadowy operations? Nevertheless, this trolling “left a dark stain on the name of Anonymous” (Coleman 69).

## 1.5 Guy Fawkes Masks: Expanding Chanology from Online to Offline

Actively using social media to build and reinforce its brand identity made Anonymous a high-profile activism-oriented hacker collective. In Project Chanology, it went a step further as it extended their operations from online to offline. The proposal of expanding the cyberwar against Scientology to the streets was spurred by the unexpected massive influx of newcomers, who were

---

<sup>34</sup> See <http://archive.wired.com/politics/security/news/2008/03/epilepsy>. A griever is a player in a multiplayer video game who deliberately irritates and harasses other players and derives pleasure from annoying others.

inspired by the YouTube Video “message to Scientology.” “#marblecake”—the channel responsible for organization during that time—computed that on IRC there were “140 to 145 different Chanology channels and participants in forty-two countries in total” (Olson 80-81) only four days following the video’s release. Suggested by a French Anon, “#marblecake” decided to work on the idea of confronting Scientology in the real world because they “honestly thought the funniest thing [they] could do to Scientology was get in front of their buildings” (Olson 81). But how could they send out this message and call upon Anons to step out of their underground and participate in street protests? The answer was at the end of the YouTube Video “Call to Action”.<sup>35</sup>

Be very wary of the 10<sup>th</sup> of February. Anonymous invites you to join us in an act of solidarity. Anonymous invites you to take up the banner of free speech, of human rights, of family and freedom. Join us in protest outside of Scientology centers worldwide. We are Anonymous. We are Legion. We do not forgive. We do not forget. We will be heard. Expect us.  
(Timeline: 1:38 to 2:02)

By releasing this video, Anonymous announced the date of their first street protest against Scientology on YouTube. This call-to-arms video, viewed 853,628 times to date, aimed to reach Anons on a transnational scale via the world’s largest video-sharing website. Such ambition indicated that “social media have had a transformative effect on how leaders lead, and, to a greater extent, how followers follow” (Berenger 511). Anonymous did not rely on the hierarchical structure and the administrative pressure to organize its operations. It depended on the power of words, waving “the banner of free speech, of human rights, of family and freedom” to invoke viewers’ empathy and encourage them to “follow” in Anonymous’s footsteps.

Although it was hard to predict how many people would answer the call and partake in the street protest, “#marblecake” prepared another YouTube video titled “Code of Conduct,” hoping to infuse necessary activist experience into potential protest neophytes—“Internet nerds, geeks, hackers, and trolls” (Coleman 63). Once they hit the street, they would be hidden in the

---

<sup>35</sup> See *supra* note 30.

plain sight. The aim of this video was to teach them how to demonstrate peacefully and engage in civil disobedience. On February 1, 2008, the five-minute video “Code of Conduct” was posted on YouTube under the same screen account “ChurchOfScientology,” elaborately listing 22 rules to guide Anons through their first real life public demonstration.<sup>36</sup> Among all the rules, three of them (Rule #2, Rule #17, and Rule #22) were of great importance.

Rule #2: Stay cool, especially when harassed. You are an ambassador of Anonymous. Although individuals trying to disrupt your demonstration will get on your nerves, you must not lose your temper. Doing so will harm the protest and tarnish the reputation of Anonymous. (Timeline: 0:50 to 1:09)

This rule highlighted the collective identity of Anonymous by prioritizing “the reputation of Anonymous” and asking Anons to serve as “an ambassador of Anonymous.” The question is: would the denial of individualism and the anti-celebrity ethos facilitate or halt the momentum of Anonymous? On the one hand, the absence of charismatic leaders might make it difficult to build a mass basis speedily. But, conversely, it might reinforce Anonymous’s brand identity of collectiveness and equality. This was because “media attention was a resource for the movement as a whole, but the sum of it was limited, and therefore individuals were thrown into competition for something intrinsically scarce. And because the movement elite understood the spotlight as a resource, leaders not chosen often resented the chosen ones” (Gitlin 162). Against this backdrop, announcing Rule #2 to encourage fellow members to resist the temptation of self-promotion and act as “an ambassador of Anonymous” might create and preserve cohesion among Anons. Rule #17 went as follows:

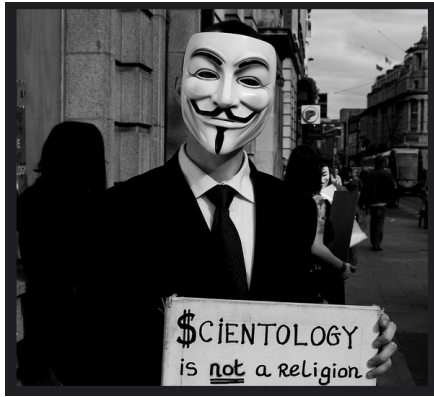
Rule #17: Cover your face. This will prevent your identification from videos taken by hostiles, other protesters or security. Use scarves, hats and sunglasses. Masks are not necessary, and donning them in the context of a public demonstration is forbidden in some jurisdictions. (Timeline: 3:27 to 3:46)

The initial purpose of this rule was to protect Anons from being captured by high-definition cameras and subsequently harassed by Scientologists. Surprisingly, this rule inspired Anons to

---

<sup>36</sup> See <https://www.youtube.com/watch?v=-063clxiB8I>

don Guy Fawkes masks when they hit the streets. As mentioned earlier, the Guy Fawkes mask symbolizes an anarchist fighter named “V” in the graphic novel “*V for Vendetta*” and its film



**Figure. 3 Anonymous protests against the Church of scientology. Flickr.com.**

adaptation (2006). The protagonist “V” is a man who advocates anarchism and prefers using violence to expose government’s evil. Over the years, “V,” along with his mask, has become a pop cultural icon, featuring violent defiance against a dystopia. In Project Chanology, it was highly unlikely to pinpoint the person who suggested donning Guy Fawkes masks in the first place. But on February 10, 2008, thousands of Anons

answered the call of the YouTube video and made the protest a transnational phenomenon. A lot of them wore the mask while protesting outside of Scientology’s buildings in cities like Sydney, London, Los Angeles, and so on (Fig. 3).<sup>37</sup> Pictures of Anons wearing the Guy Fawkes masks appeared in the mainstream news, conjuring up a bizarre and mysterious impression that a lot of faceless people were peacefully protesting in public spheres. In this regard, Anonymous adapted the symbolic values of the Guy Fawkes mask to suit civil disobedience instead of violent actions.

Additionally, the use of Guy Fawkes masks also had some impact on the collective identity construction of Anonymous. According to Coleman, “by cloaking markers of the self, like ethnicity, class, and age, all sorts of different possibilities are opened up” (174). The negative possibility was that since anyone could don a mask and engage in the protest, it made the operation not immune to infiltration. It could not prevent some pro-violence people from participating, who might physically assault Scientologists and sabotage the operation. But, the positive possibility was that this “mask strategy” made it difficult for the Western mainstream

<sup>37</sup> See <https://www.flickr.com/photos/lacylisa/5032761601/in/photolist-8EJdFK-8EMp97-4rjJz8-8EMp5w-4rp1uA-8EJswr-4rjPXc-4rknLg-4rk9pg-4rpeGs-4rpeBJ-4rk91P-4yonj6-4ysyVN-sy1sbH-4roTpf-7wne8L-4yrKzZ-4rpeiQ-4rpeDW-7weqDw-4roSql-4roPNm-4rjCV6-8EMAYS-4rjNQk-8EJu6x-4roL7N-4roWT9-4rjMDv-4ysHwJ-4roN1E-4roQbh-8EJgyt-51QK8p-4roSMU-61cue8-5Cbvq3-4rqn6B-4rurHo-c292dQ-4Wam2t-4yw2S7-4rezlX-4roQx1-4roY93-4roLvj-4rjNkt-8EMfTQ-4yoaBg>

media to locate a leader or an organizer. Sociologist Gitlin—the then President of Students for a Democratic Society (SDS)—believes “the media were always searching for prominent personalities, attractive and articulate by media standards, and then, having made them prominent, continued to cover them *because* they were prominent, celebrity piled up for some leaders and eluded others” (162).<sup>38</sup> With a leader in the picture, members would either have someone to adore or a target to discredit. The internal conflicts might cause “stimulation of competition and envy within the movement. That was one of the most destructive elements within the movement. Everyone secretly wanted the attention, and everyone could see that the people getting the attention were really no better qualified than anyone else” (Gitlin 162). In this line of logic, donning Guy Fawkes masks denied Anons the chance to take credit for themselves and compete for the media spotlight. And then, the last but not least rule was Rule #22:

Document the demonstration. Videos and pictures of the event may be used to corroborate your side of the story if law enforcement get involved. Furthermore, posting images and videos of your heroic actions all over the Internet is bound to generate win, exhorting other Anonymous to follow your glorious example. (Timeline: 4:24 to 4:43)

This rule revealed Anonymous’s eagerness to make use of the power of social media. Posting “images and videos of [Anons’] heroic action” could feed the mainstream media with headline-grabbing stories. It might also attract more people to engage in the fight against Scientology, either in cyberspace or the real world because “the video uploads on YouTube, where an interested viewer can watch an actual event unfold in a relatively unmediated format” could be very convincing. After all, “seeing *is* believing, unless there is evidence that the video had been altered or mashed-up” (Berenger 516). Rule #22 was to remind Anons that they should see their street protest not only as a participatory action but, more importantly, as a media resource.

---

<sup>38</sup> Students for a Democratic Society (SDS) was a student activist movement in the United States that was one of the main representations of the New Left. The organization developed and expanded rapidly in the mid-1960s before dissolving at its last convention in 1969. (Wikipedia)

In a nutshell, by announcing those 22 rules, Anonymous was trying to “train” its nerdy hackers and geeks into well-prepared activists before they hastily jumped into the real world. This video has received 320,932 web views so far. Although it is hard to tell to what extent it had impacted on the social mobilization of Project Chanology in 2008, it made apparent Anonymous’s keenness to take advantage of modern technology and actively engage social media in its brand identity construction and counter-narrative creation. Understandably, there must be some Anons behind the production of these videos—“message to Scientology,” “Call to Action,” and “Code of Conduct.” But nobody knew their identity except the fact that a pseudonymous account “ChurchOfScientology” was used to post these videos. In this sense, social media fit in with Anonymous’s brand identity construction featuring leaderlessness and equality because “social media have become a means through which leadership is exercised while at the same time concealed, so as to maintain an impression of absolute spontaneity and fulfill the criteria of horizontalism” (Gerbaudo 144).

Immediately following the release of those videos, the media witnessed Anons’ growing passion for participating in the cyberwar against Scientology and protesting in front of its buildings in many cities. But, by the summer of 2008, the momentum of Project Chanology halted because “infighting among organizers” (Olson 85) occurred and a lot of Anons gradually lost interest in this cause. Afterwards, Anonymous had been trying to stay in the media spotlight but had not launched another landmark action until 2010’s Operation Payback.

## Chapter Two: Operation Payback--from Rebellious to Resilient

Pushing hard against rules and boundaries may often lead to entrapment or demise, but the entity's core animating idea—Anonymous if free for anyone to embody—positions it well for resurrection and reinvention.

--Coleman (399)

### 2.1 Supporting WikiLeaks: Recapturing the White-hot Media Spotlight

After two years of intermittent trivial operations, Anonymous launched Operation Payback in September 2010 as revenge on an Indian software company Aiplex because the latter DDoSed websites that offered pirated copies of Bollywood films for downloading.<sup>39</sup> But, as in other operations, Anons lost their interest very soon again. The opportunity presented itself two months later when WikiLeaks released to major Western news outlets, including the *Guardian* and the *New York Times* hundreds of confidential diplomatic cables that exposed the United States government's dark deeds. This leaking incident grabbed the attention of Anonymous and significantly changed the trajectory of Operation Payback. By playing the role of a vehement supporter of WikiLeaks, Anonymous made a comeback to center stage.

As a matter of fact, WikiLeaks began disclosing diplomatic cables and secret documents of the United States government from early 2010. On April 5, 2010, an article titled "Video Shows U.S. Killing of Reuters Employees" was published in the *New York Times*. It reported that the WikiLeaks leaked video "showing an American helicopter shooting and killing a Reuters photographer and driver in a July 2007 attack in Baghdad."<sup>40</sup> In October 2010, around 400,000 documents regarding the Iraq War were released. On October 23, the BBC titled its report as "Huge Wikileaks release shows US 'ignored Iraq torture'."<sup>41</sup> The pinnacle came on November 28, 2010, WikiLeaks coincided with five major newspapers—the *New York Times* (the U.S.), the

---

<sup>39</sup> Although controversial, Anonymous believed in free information even if it was pirated or secret content.

<sup>40</sup> See <http://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html>

<sup>41</sup> See <http://www.bbc.com/news/world-middle-east-11611319>

*Guardian* (the UK), *El País* (Spain), *Le Monde* (France), and *Der Spiegel* (Germany)—to publish simultaneously the first 220 of 251,287 leaked documents labeled confidential.<sup>42</sup> For instance, the article “Leaked Cables Offer Raw Look at U.S. Diplomacy,” written by Scott Shane and Andrew W. Lehren in the *New York Times*, revealed that the Yemeni government had sought to cover up the American role in missile strikes against the local branch of Al Qaeda.<sup>43</sup> A cable’s account of a January meeting between the Yemeni president, Ali Abdullah Saleh, and Gen. David H. Petraeus, then the American commander in the Middle East, recorded Mr. Saleh saying “we’ll continue saying the bombs are ours, not yours.” The *New York Times* stated that “the disclosure of the cables is sending shudders through the diplomatic establishment, and could strain relations with some countries, influencing international affairs in ways that are impossible to predict.”

It is not difficult to imagine that the revelation of these confidential cables humiliated and enraged the United States government. And then, “a trio of powerful companies—Amazon, MasterCard, and PayPal (among others)—bowed to its influence, refusing to process donations or provide website hosting for the embattled organization” (Coleman 119). On December 4, online payment service company PayPal announced suspending the WikiLeaks account that the organization used to collect donations.<sup>44</sup> On December 6 and 7, MasterCard and Visa blocked payments to WikiLeaks respectively.<sup>45</sup> On top of that, the United States government was trying to investigate social media users associated with WikiLeaks. According to Glenn Greenwald, a Subpoena was served on Twitter on December 14, 2010.<sup>46</sup> It was “actually an Order from a federal court that the DOJ requested” seeking information of scores of individuals currently or formerly associated with WikiLeaks, including Julian Assange, Bradley Manning and WikiLeaks

---

<sup>42</sup> These documents were not top-secret and dated from 28 December 1966 to 28 February 2010.

<sup>43</sup> See <http://www.nytimes.com/2010/11/29/world/29cables.html?pagewanted=1>

<sup>44</sup> See <http://www.reuters.com/article/2010/12/04/wikileaks-paypal-idUSN0415723720101204>

<sup>45</sup> See <http://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/>

<sup>46</sup> Glenn Greenwald is the journalist who first exposed PRISM (the US and British global surveillance programs) in the *Guardian* in June 2013, based on classified documents disclosed by Edward Snowden.

Twitter account.<sup>47</sup> Greenwald further explained that the information demanded by the DOJ (Department of Justice) included users' mailing addresses, IP addresses, as well as the means and source of payment, including banking records and credit cards. Thus, after the leaking, WikiLeaks was facing not only political pressure and financial difficulties but also legal troubles.

It was against this backdrop that Anonymous re-directed Operation Payback to defend WikiLeaks, hoping to use its spirit of defending free information to rekindle Anons' passion and use the victimization of Wikileaks and Julian Assange to invoke sympathizers' support. On December 5, 2010, Anonymous released a statement on its website, mapping out its plan ("Operation", Pandasecurity.com).<sup>48</sup>

- ❖ Offer WikiLeaks an additional mirror and have it Googlebombed.<sup>49</sup>
- ❖ Create counter-propaganda, organizing attacks (DDoS) on various targets related to censorship (time, date and target will be published by that time).
- ❖ Contact media entities, inform them that Operation: Payback has come out in support of Wikileaks, and has declared war on the entities involved in censoring there [*sic*] information; we will seek public support in a campaign against censorship.
- ❖ We will find and will attack those who stand against Wikileaks and we will support WikiLeaks in everything they need.

Some media outlets dubbed this action "Operation Avenge Assange" and began probing into the reason why Anonymous eagerly jumped on board even without the invitation from WikiLeaks.

---

<sup>47</sup> Julian Paul Assange, the co-founder of WikiLeaks. He has been under investigation by the US government for the leak. He has also been investigated by Sweden regarding the alleged sexual offences. In 2012, he was granted political asylum by the Embassy of Ecuador in London to escape extradition to Sweden; Bradley Manning (now known as Chelsea Elizabeth Manning), a U.S. Army soldier, was sentenced in August 2013 to 35 years' imprisonment and to be dishonorably discharged from the Army in violations of the Espionage Act and other offenses, after disclosing to WikiLeaks classified or unclassified but sensitive military and diplomatic documents.

<sup>48</sup> See <http://www.pandasecurity.com/mediacenter/news/operationpayback-broadens-to-operation-avenge-assange/>

<sup>49</sup> Google bomb is the practice of causing a web page to rank highly in search engine results for unrelated or off-topic search terms by linking heavily.

On December 10, 2010, CNN conducted an online interview with some Anons. The following is part of their conversation:<sup>50</sup>

**CNN:** So, how did you come together over WikiLeaks? Was this spontaneous? Tell me how it started.

**Anon:** Operation Payback started as a demonstration against all things people were unable to change using legal means. Our primary goal is freedom of information. Any and all information. At first we were focused on issues concerning piracy (and we still are), but once the WikiLeaks fiasco occurred it was obvious we had to help. Our initial goal specifics were different, but we all share the common idea of free information.

This interview conveyed twofold meanings. Politically, the cause of supporting WikiLeaks was consistent with Anonymous's self-claimed mission of defending free information. Strategically, by stating that Operation Payback was aimed to address issues that "people were unable to change using legal means," Anonymous publicly acknowledged it would not exclude "illegal or legally ambiguous digital tools" (B. Kelly 1668) in support of WikiLeaks. In terms of law, participating in a Distributed Denial of Service (DDoS) attack is illegal in many countries, "breaking the Computer Fraud and Abuse Act in the United States as well as the 2006 Police and Justice Act in the United Kingdom; in both countries, perpetrators face a maximum penalty of ten years in prison" (Olson 64). However, this high stake did not seem to deter Anons. To a great extent, their heroism derived from the lack of awareness of the legal risk. Many Anons were under the false impression that there was strength and protection in large numbers, so "they were immune to arrest, or well hidden from the authorities" (Olson 86).

Nevertheless, associating itself with the heated topic WikiLeaks enabled Anonymous to come out of two years' obscurity and back into the media spotlight. On IRC channels, "the people who set up AnonOps...were angry at PayPal, but, more than that, they saw an opportunity. The victimization of Wikileaks, they figured, would strike a chord with Anonymous and bring hordes of users to their new network. It was great publicity" (Olson 109). When it came to choosing

---

<sup>50</sup> See <http://www.cnn.com/2010/US/12/09/hackers.wikileaks/>

targets to launch Distributed Denial of Service (DDoS) attacks, Anonymous, once again, demonstrated its media savvy. It decided to prey on PayPal, Visa and MasterCard instead of the United States government and the DOJ in case the daunting idea of attacking American authorities would deter many Anons from participating.

Targeting those three global financial services companies had high potential to make headline news in that “the world is getting the impression that unless western economic interests are involved, our media does not care to report upon it” (Coleman 153). For Anonymous, PayPal, Visa and MasterCard were perfect targets since they represented the world’s largest electronic payment service. According to *Forbes* magazine, in 2010, MasterCard, ranked #53 in the list of the World’s Most Valuable Brands, generated \$9.47 billion revenues. Visa was rated #30 of the World’s Most Valuable Brands with \$12.93 billion revenues. PayPal would notch \$20.8 billion in payment volume and its revenues would reach \$723 million.<sup>51</sup> For such financial services companies, their core competence was to guarantee safe transactions and create a sense of security for customers. If Anonymous could launch Distributed Denial of Service (DDoS) attacks on those three companies’ websites and take them offline, it would be devastating to their reputation of trustworthiness. More importantly, it would create a sensational effect in the mainstream media.

Therefore, driven by the belief in free information and the desire for “great publicity,” Anonymous chose PayPal as its first target and launched a fierce DDoS attack.

## **2.2 Landing Twitter: Taking on the Coloration of Challenging Capitalist Hegemony**

Unlike Project Chanology, Anonymous relied more on Twitter in addition to Facebook, YouTube and IRC channels in Operation Payback. This change might be because of Twitter’s instantaneity, interactivity, and growing popularity. To date, “over 500 million subscribers are on Twitter, generating billions of tweets every day” (Ayish xix). Surprisingly, Twitter’s 140-

---

<sup>51</sup> See <http://www.forbes.com/companies/mastercard/>; <http://www.forbes.com/companies/visa/>; <http://www.forbes.com/2010/04/19/paypal-online-auctions-technology-cio-network-ebay.html>

character limit policy even pushed Anonymous to develop a concise, catchy and provocative manner to socialize with its followers.<sup>52</sup>

On December 4, 2010, Anonymous launched Distributed Denial of Service (DDoS) attacks on ThePayPalBlog.com, on which PayPal made its announcement of discontinuing the financial services for WikiLeaks. The blog went down as of 4 a.m. PST (“’Tis the Season of DDoS”, Pandasecurity). Subsequently, an Anonymous Twitter account “@AnonyWatcher” posted: “TANGO DOWN— thepaypalblog.com—Blog of Paypal, company that has restricted Wikileaks’ access to funding.” According to Urban Dictionary, “TANGO DOWN” is military slang that refers to a target especially a terrorist being eliminated. There has been wide pop culture usage in video games and movies, mainly by characters in tactical squads engaging terrorists. The rhetoric of such a military jargon subtly situated Anonymous in the righteous position of the champion for social justice. In the same tweet, “@AnonyWatcher” also called upon its Twitter followers to “join in the #DDoS if you’d like.” Although it was hard to find out how many people responded to that tweet, statistics on Pandasecurity.com showed that ThePayPalBlog.com underwent 77 times of interruptions with a total downtime of 8 hours and 19 minutes.

This victory, although minor, served as a big advertisement for Operation Payback. Within four days, “the number of visitors to AnonOps IRC had soared from three hundred to seventy-eight hundred” (Olson 113). Thrilled and emboldened, Anonymous decided to launch another Distributed Denial of Service (DDoS) attack on PayPal’s main website on December 8 and set the attack time at 2:00 p.m. GMT. The message “FIRE AT 14:00 GMT” was spread out through IRC channels, forums, websites, YouTube videos, Facebook pages, and Twitter feeds. At around 1 p.m. ET, Operation Payback Twitter account “@Op\_Payback” tweeted:<sup>53</sup>

Target is: api.paypal.com \_Status: seems to be down :)

---

<sup>52</sup> According to Twitter, each tweet can contain no more than 140 characters. See <https://dev.twitter.com/overview/api/counting-characters>

<sup>53</sup> See [http://www.huffingtonpost.com/2010/12/09/paypal-api-down\\_n\\_794557.html](http://www.huffingtonpost.com/2010/12/09/paypal-api-down_n_794557.html)

Instructions: <http://pastehtml.com/view/1c8i33u.html> #ddos  
#payback #wikileaks

At 1:52 p.m., the *New York Times* updated that Operation Payback's attacks on PayPal would begin in a few minutes.<sup>54</sup> "When 2:00 p.m. finally came around, the IRC channels, Twitter, and 4chan exploded with \*FIRE FIRE FIRE FIRE\* and FIIIIIRE!!!" (Olson 114). A lot of followers re-tweeted this message. For instance, Twitter account "@anonymous1901" posted "ALL ANONS FIRE ON PAYPAL!!!! We have received the order by Op\_Payback to fire. ALL ANONS FIRE ON PAYPAL!!!!"<sup>55</sup> Thus, in the full glare of worldwide publicity, PayPal site went down and stayed offline for a full hour.

In this DDoS attack, Anonymous made the most use of Twitter, communicating and coordinating in a mobile, instant, interactive yet still anonymous way. It even used Twitter to feed the media the updates. Gerbaudo, a lecturer in Digital Culture and Society at King's College London, thinks that for many contemporary social movements, social networking sites like Twitter and Facebook "constitute a platform for political organising and mass mobilisation" (144). He also believes that Facebook is often used by leaders, organizers or activists to mobilize people from the outside of the space of participation, in the hope of recruiting and training a following among a largely un-politicized youth. And Twitter is important for purposes of the internal organization (144). The case of Operation Payback had a similar dynamic. Anonymous used Facebook, the social networking site with "more than 175 million active users" (Kaplan and Haenlein 59), to promulgate its activities and boost morale, through such means as posting "we need a new target!" to show off its performance, which might have the potential to galvanize some "un-politicised youth" into action.

Compared to its Facebook Page, Anonymous's primary Twitter accounts, especially "@Op\_Payback," were frequently used for updates or posting call-to-arms tweets. On December

---

<sup>54</sup> See [http://thelede.blogs.nytimes.com/2010/12/06/latest-updates-on-leak-of-u-s-cables-day-9/?\\_r=0](http://thelede.blogs.nytimes.com/2010/12/06/latest-updates-on-leak-of-u-s-cables-day-9/?_r=0)

<sup>55</sup> See <https://twitter.com/anonymous1901>

8, 2010, the same day it took down PayPal main site, Anonymous also steered its resource to carry out DDoS attacks on the websites of MasterCard and Visa. On Twitter, “@Anon\_Operation” took responsibility for the attacks, tweeting: “We are glad to tell you that [Mastercard.com] is down and it's confirmed. Operation: Payback (is a bitch!).” Just before the attack on Visa, it also tweeted: “TARGET: WWW.VISA.COM :: FIRE FIRE FIRE!!! WEAPONS.” (“MasterCard, Visa”, CNN). These capital letters and exclamation marks exuded a sense of rebellious youth energy and flagrant provocation. It seemed to mock these global corporations that their billion-dollar assets could not protect them from being DDoSed by an anonymous collective of hackers and geeks.

Some may wonder whether or not those Distributed Denial of Service (DDoS) attacks on PayPal, MasterCard, and Visa would affect cardholders’ purchases or transactions. According to Sauter, a Research Assistant at MIT Center for Civic Media, these corporate homepages rarely serve a vital role in the companies’ operations. Or, to put it in a metaphorical way, “one does not go to [www.starbucks.com](http://www.starbucks.com) to get one’s morning latte” (987). Actually, these homepages “serve a placeholder or trademark-defense purpose. To briefly tear down the online poster of these organizations may serve a symbolic purpose and be a good way to attract attention, but it often has little effect on their practical, day-to-day operations” (987). Sauter’s theory was evidenced by MasterCard spokesman James Issokson’s statement. He told CNN “the hack attack did not affect the use of credit cards or financial security. The networks used to run credit card transactions operate independently from corporate websites.”<sup>56</sup> As Anonymous desired, these “symbolic” attacks made Operation Payback the headline news, promoting Anonymous’s self-claimed mission of defending free information and delivering social justice.

For Anonymous, such a result was a win-win situation. On the one hand, it took revenge on the world’s three largest financial services corporations in defense of WikiLeaks. James Ball wrote an article “The Bankers’ Blockade of Wikileaks Must End” in the *Guardian*, saying that

---

<sup>56</sup> See [http://money.cnn.com/2010/12/08/news/companies/mastercard\\_wiki/index.htm](http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm)

“unlike many of the country’s leading corporations, WikiLeaks has neither been charged with, nor convicted of, any crime at either state, federal, or international level.”<sup>57</sup> In this aspect, “the blockade by Visa, Mastercard, Paypal and others is a sinister attack on free speech” rather than cooperation with law enforcement. Anonymous’s response to the blockade indicated a way that a computer-savvy younger generation would rebel. As media theorist Gauntlett points out, “we are seeing a shift away from a ‘sit back and be told’ culture towards more of a ‘making and doing’ culture. The ‘sit back and be told’ position is forcefully introduced in schools, and then gently reinforced by television and the magic of the glossy, shiny, and new in consumer culture” (8).<sup>58</sup> Rising from the “sit back and be told” position amounts to rebelling against authority, aiming to take back one’s own mind and voice. But, the almost ubiquitous “consumer culture” implies that big corporations are trying to use their economic resources to collaborate with government and influence political decision-making. Against this backdrop, Operation Payback added another layer of political coloration upon Anonymous’s brand identity: challenging authority and seeking social change. Although Anons might be lulz-driven occasionally, they would undertake a political cause and use social media to mobilize support; they would also use “computer hacking, the internet, and technology to try to effect social change or spread a message” (Shantz and Tomblin 4).

On the other hand, Operation Payback helped Anonymous make a swift comeback to the center of media attention. On December 8 and 9, 2010, there were at least nineteen Western mainstream media outlets covering the stories, including the BBC, CNN, the *New York Times*, the *Guardian*, and *Wall Street Journal*. Even now, typing in the keywords “December 8, 2010, operation payback” in Google search will generate 35 pages and 345 results. The article “Web Attackers Find a Cause in WikiLeaks,” by Noam Cohen in NYtimes.com, said “while the attacks on such behemoths as MasterCard, Visa and PayPal were not nearly as sophisticated as some less

---

<sup>57</sup> See <http://www.theguardian.com/commentisfree/2011/oct/24/bankers-wikileaks-free-speech>

<sup>58</sup> David Gauntlett is a Professor of Creativity and Design in the Faculty of Media, Art and Design, University of Westminster, UK. See <http://davidgauntlett.com/>

publicized assaults, they were a step forward in the group's larger battle against what it sees as increasing control of the Internet by corporations and governments."<sup>59</sup> It further quoted John Perry Barlow, an advocator for civil liberties, stating that "this is kind of the shot heard round the world—this is Lexington."<sup>60</sup> Although likening Operation Payback to "Lexington" was somewhat exaggerating, it acknowledged Anonymous's role in challenging authority.

Conversely, amplifying Anonymous's heroism might allow the media to "characterize companies like [Paypal, MasterCard and Visa] as victims 'crippled' by the dastardly work of 'vandals'; it did not matter that no permanent damage was done to these sites" (Krapp 72). News accounts such as "computer hackers have sent two of the world's biggest credit card companies into meltdown in revenge for cutting off payments to the WikiLeaks website" might give the impression that big financial companies were vulnerable even defenseless in the face of "the dastardly work of" Anonymous.<sup>61</sup> Moreover, many media outlets "reported the payments blockade but refrained from critical editorial comments" (Pieterse 1921) about the legitimacy of the banking blockade. Pieterse, Professor of Global Studies and Sociology at UC Santa Barbara, further points out that in such news reports "Washington's reservations come up but the ethical and legal problems that the banks' blockade poses do not. This illustrates a culture of compliance and conformity that is routine in the USA, to the point that one hardly notices it" (1921). In this regard, it was a lose-lose situation for PayPal, MasterCard, and Visa. These companies subjected their economic decisions to the political pressure of the United States government, which gave Anonymous a perfect excuse to launch Distributed Denial of Service (DDoS) attacks and sway public opinions. On the surface, it was the capitalists in the United States that suffered reputational damage. But, in the long run, "the public loses confidence in their governments as

---

<sup>59</sup> See [http://www.nytimes.com/2010/12/10/world/10wiki.html?\\_r=1](http://www.nytimes.com/2010/12/10/world/10wiki.html?_r=1)

<sup>60</sup> Lexington: the place where the first shot of American Revolution War was fired in 1775.

<sup>61</sup> See <http://www.dailymail.co.uk/news/article-1336806/WikiLeaks-hackers-Operation-Payback-cyber-war-targets-Swedish-Government.html>

they churn out truthiness. But maybe it's a good thing. Perhaps the masses of information available to us are paving the way for the Age of the Awakened" (Shantz and Tomblin 70).

### **2.3 Countermeasure to Social Media Obstruction: Adopting a "Hydra Tactic"**

While Anonymous just started enjoying the long lost frenzied mainstream media attention, it began suffering on the social media side. *Forbes* magazine published an article titled "Facebook and Twitter Suspend Operation Payback Accounts" on December 8, 2010, at 2:14 p.m.—the same day Anonymous DDoSed PayPal main site.<sup>62</sup> The reporter Mike Isaac said Operation Payback's Facebook fan page was shut down earlier that day, on which users posted updates about the operation including a link to CNN's news "Visa website down after threat from WikiLeaks supports."<sup>63</sup> Then, approximately as of 3:09 p.m. PST, Twitter suspended Operation Payback's major account "@Anon\_Operation" too, which had over 20,000 followers. Facebook and Twitter issued official statements respectively to explain the reason they banned Anonymous's accounts. Facebook claimed:

Your Page "Operation Payback" has been removed for violating our Terms of Use. A Facebook Page is a distinct presence solely for business or promotional purposes. Among other things, Pages that are hateful, threatening, or obscene are not allowed...If your Page was removed for any of the above reasons, it will not be reinstated.<sup>64</sup>

Besides, according to Fox News, "some WikiLeaks supporters accuse Twitter of preventing the term 'WikiLeaks' from appearing as one of its popular 'trending topics.' Twitter denies censorship, saying the topics are determined by an algorithm."<sup>65</sup> It was hard to know whether or not Facebook and Twitter did this after bowing to the same political pressure of the United States government as PayPal, Visa, and MasterCard did. In the face of the suspension, the burning

---

<sup>62</sup> See <http://www.forbes.com/sites/mikeisaac/2010/12/08/facebook-and-twitter-suspend-operation-payback-accounts/3/>

<sup>63</sup> Ibid.

<sup>64</sup> Ibid.

<sup>65</sup> See <http://www.foxnews.com/tech/2010/12/08/wikileaks-supporters-launch-hack-attacks/>

question was: did Facebook and Twitter's reaction, along with the DOJ's Subpoena on Twitter, mean that "big media companies and governments dominate the digital public sphere to the extent that it is impossible for the tail of individual users, however long it may be (Anderson, 2006), to form any substantial and sufficiently homogenous counterpublic sphere" (Lindgren 50)? Is there a way for netizens to get around or even challenge their dominance?

In the exploration of constituting the counternarrative in "the digital public sphere," Anonymous might carve out space for the construction of their brand identity. Compared to the social media giants Facebook and Twitter, Anonymous was a moneyless, faceless and leaderless collective. And now, with its Facebook and Twitter accounts banned, it became voiceless and hence powerless. However, "in the emerging social media landscape, the notion of a passive audience has proven to be rather odd and antiquated as intelligent and self-motivated users take control of their online communications" (Ayish xx-xxi). The countermeasure Anonymous adopted was a "hydra tactic" as Anons created different yet Anonymous-related Facebook or Twitter accounts to replace the banned ones. They moved like a hydra, whose heads would grow again after being cut off. For instance, after Twitter account "@Anon\_Operation" was banned, other screen names such as "@Anon\_Operationn" and "@Anon\_Operations" were set up as its variant. This "hydra tactic" exhibited Anonymous's strong point of being leaderless, decentralized and flexible: it allowed those who were interested in Anonymous's cause to create Anonymous-related accounts anytime, anywhere.

Admittedly, the phenomenon of a "hydra-like account" (Isaac) would probably dilute the momentum of Operation Payback in social media. This is because users might be baffled about which account to follow or whose words to trust, which made "mobilization efforts [drop] off quickly after initial surges" (Beyer 142). Plus, critics of hacktivism might equate the loose cooperation to "the lack of a clear agenda," which "made it a politically immature gesture" (Krapp 87). But, conversely, this tactic could make it very difficult for "big media companies and governments" (Lindgren 50) to ban completely Anonymous from participating in social media. In

this regard, Anonymous embodied “a vital oppositional space of politics and culture in which a wide diversity of individuals and groups have used emergent technologies to help produce creative social relations and forms of democratic political possibility” (Kahn and Kellner 34).

Now, on Twitter, Facebook, and YouTube, accounts associated with Anonymous have exploded into a kaleidoscope mode. For instance, there are at least 91 Twitter account names related to Anonymous or Anons. Some focus on updating Anons’ global news such as “@YourAnonNews,” which has 1.44 million followers; some center on activities in a particular country or area such as “@AnonUK” (584,000 followers) and “@TurkeyAnonamous” (445,000 followers). And some have famous scholars or activist followers such as “@USAnonymous” (509,000 followers) is being followed by Gabriella Coleman, the author of the book *Hacker, Hoaxer, Whistle-Blower, Spy: the Many Faces of Anonymous*; “@Anon\_Operations” (295,000 followers) is being followed by Glenn Greenwald, one of the winners of the 2014 Pulitzer Prize for Public Service.

Despite their different foci, the common thread is that the vast majority of these accounts are accompanied by the variants of Anonymous’s signature logo—a man in a suit with a question mark in the place of his head—or the Guy Fawkes mask. For instance, the avatar of Twitter account “@AnonUK” (Fig.4) is a headless man in a suit wearing shorts resembling the national flag of the UK.<sup>66</sup> This feature not only neatly situates “@AnonUK” within the larger context of Anonymous’s cause but also highlights its locality. By combining generality with particularity, this avatar brings to the foreground the symbolic values of Anonymous’s brand identity: openness, decentralization and adaptability. The avatar of another Twitter account “@GroupAnon” (Fig. 5) is a man wearing the Guy Fawkes



Figure. 4 A screenshot of Twitter account @AnonUk

---

<sup>66</sup> See <https://twitter.com/AnonUK>

mask, with two circles of rosy blushes on the mask's cheeks.<sup>67</sup> The mask, another "signature icon" (Coleman 64) of Anonymous, conveys an important message of the 2006 movie "*V for Vendetta*," in which the protagonist "V" says "beneath this mask is an idea; and ideas are bulletproof." The blushes on the mask may serve as an indicator of youth and passion; they might also signify the face paint of a clown, thus referencing the prankish, "trolling" side of Anonymous. By adding such features to the mask, this avatar may aim to attract the pro-democracy youth group.



Figure. 5 A screenshot of Twitter account @GroupAnon

These examples indicate that, over the years, the avatars accompanying Anonymous's social media accounts have become carriers of the symbolic values of its brand identity. As Anonymous's "digital-native culture and net-freedom ideology" (Sauter 989) contribute to its global recognizability, they have also "helped entrench the idea of 'the internet' as an anonymous but powerful 'we' demanding freedom from interference and encroachment by government or big business" (Goode 80). Although these hydra-like Facebook and Twitter accounts may allow someone to "hijack" Anonymous's moniker for other purposes, it is an efficient way for Anonymous to survive control of information. Once adapted to the virtual eco-political geography, it could commit itself to "political and cultural resistance" ("the Electronic Disturbance" 3). Therefore, "whether or not Google is making us stupid, Facebook is commoditizing our privacy, or Twitter is chopping our attention into microslices" (Rheingold 1), these similarly-themed social media accounts may serve as a constant reminder for Anons that they are not fighting alone. The use of social media may create a sense of transnational solidarity. Moreover, by disseminating Anonymous's iconography into numerous corners of the Internet, the "hydra tactic" can further strengthen Anonymous's brand identity. Anonymous may

---

<sup>67</sup> See <https://twitter.com/GroupAnon>

play the role of online freedom fighters against Internet censorship in a leaderless and decentralized manner.

## **2.4 Ethical Quandary: Participatory Democracy or Social Engineering?**

The umbrella concept of Anonymous was prone to give such an impression that Anons voluntarily participated in all operations with full transparency and informed consent. However, Coleman's evaluation of Operation Payback is intriguing. She describes it as "a mixture of manipulation, false information, good intentions, and rampant uncertainty" (126). Her statement touches upon the protracted ethical question surrounding Anonymous's Distributed Denial of Service (DDoS) attack strategy. As mentioned earlier, deliberately launching a DDoS attack is deemed illegal in many countries including the United States. Why, then, did Anonymous insist on this tactic? What kind of manipulation was attempted and what "false information" was fed? Could Anonymous's DDoS attacks be justified in the name of defending freedom of speech and fighting against Internet censorship?

Anonymous's cyberattack strategies included Distributed Denial of Service (DDoS) attacks, defacing websites, stealing and dumping targets' data on the Internet. Among all the methods, the most frequently used and also the most controversial one was DDoS attacks. The aim of DDoSing was to use junk traffic to overwhelm websites to slow them down or even to take them offline. Anonymous believed DDoS attacks fell in the category of legit "virtual sit-ins" and electronic civil disobedience. Opponents argued that blocking websites amounted to "muting" them, asserting that a DDoS attack was an unethical assault or even a violent intrusion. Thus, Anonymous's heavy reliance on DDoS attacks, along with its high-profile propaganda of calling on a larger population to partake in DDoS attacks, made it a heated topic. Some old school hackers were often strongly opposed to the deployment of DDoS attacks. Oxblood Ruffin, a

member of Cult of the Dead Cow (also known as cDc), a veteran hacker group in the United States, defined DDoS attacks as follows:<sup>68</sup>

Denial of Service attacks are a violation of the First Amendment, and of the freedoms of expression and assembly. No rationale, even in the service of the highest ideals, makes them anything other than what they are—illegal, unethical, and uncivil. One does not make a better point in a public forum by shouting down one’s opponent. (Jordan 98)

This version placed Distributed Denial of Service (DDoS) attacks against the backdrop of the First Amendment to the United States Constitution, which guarantees freedom of religion, speech, the press, and the right to peaceably assemble or petition. By defining DDoS as “a violation” that “[shouted] down one’s opponent,” Ruffin repudiated its legitimacy. In response to such doubts, Anonymous once again used social media to construct a self-defense narrative. On December 9, 2010, at the early stage of Operation Payback, Anonymous posted a video titled “A Letter from Anonymous” on YouTube, stating:<sup>69</sup>

During the Civil Rights Movement in the 1960s, access to many businesses was blocked as a peaceful protest against segregation. Today much business is conducted on the Internet. We are using the LOIC to conduct distributed denial of service attacks against businesses that have aided in the censorship of any person. Our attacks do no damage to the computer hardware. We merely take up bandwidth and system resources like the seats at the Woolworth’s lunch counter. (Timeline: 5:10 to 5:43)

In this statement, Anonymous shunned the head-on ideological conflict with old school hackers and tried to justify Operation Payback in a metaphorical way. As can be seen that it likened Distributed Denial of Service (DDoS) attacks to the sit-in “at the Woolworth’s lunch counter.” Such an analogy had the potential to evoke the audience’s memories and compassion of the Civil Rights Movement. On February 1, 1960, four freshmen—Franklin McCain, Ezell Blair Jr. (later known as Jibreel Khazan), Joseph McNeil, and David Richmond—from the Agricultural and Technical College of North Carolina (now North Carolina A&T State University) sat down at

---

<sup>68</sup> See *supra* note 25.

<sup>69</sup> See <https://www.youtube.com/watch?v=WpwVfl3m32w>

the lunch counter inside the Woolworth store and stayed until the store closed (“The Greensboro Four”).<sup>70</sup> This action was a political gesture of protesting against the store’s segregation policy and set a series of nonviolent protests in Greensboro in motion, resulting in the Woolworth department store removing its policy of racial segregation eventually. Thanks to the considerable local and nationwide media attention, Woolworth became a symbol of civil disobedience in the history of the United States, despite the fact that it was not technically the first sit-in of the Civil Rights Movement.

In the attempt to justify its cause morally, it was a smart move for Anonymous to place Operation Payback in the larger context of the Civil Rights Movement and liken Distributed Denial of Service (DDoS) attacks to occupying the seats at the Woolworth’s lunch counter. “By invoking this metaphor, they seek to take advantage of the cultural capital and symbolism of historical sit-in campaigns” (Sauter 987). In the West, especially in the United States, the Civil Rights Movement had been one of the richest “cultural capital” that inspired and nurtured activists, either online or offline. It was like an inexhaustible network of voices and stories, from which practitioners could mine tactical guidance and encouragement. In addition, it was also a sensitive topic that would be easily picked up by the media in that whether or not some contemporary activists were inheriting, expanding or exploiting its symbolic values was always debatable. Sauter thinks Anonymous’s DDoS attacks on the homepages of big corporations like Paypal, MasterCard, and Visa should be deemed as “valid online protest” because more often than not these companies “use established press channels to communicate with the public” (987) rather than their homepages. As a result, Anonymous’s DDoS attacks were flooding these publicly accessible websites rather than silencing its opponents.

However, “as a series of highly publicized arrests show, groups such as Anonymous may frame their actions in terms of online protest, but governments frame them in terms of

---

<sup>70</sup> See <https://web.archive.org/web/20110125173028/http://www.ncmuseumofhistory.org/collateral/articles/Greensboro.Four.pdf>

criminality” (Beyer 148). In the United States, the key element to proving a DDoS attack illegal under the Computer Fraud and Abuse Act (1984) is the attacker’s intentionality. Although sometimes it may be difficult for authorities to prove executors’ intentionality, it still can be precarious to launch DDoS attacks. Then, why did Anonymous insist on employing the DDoS strategy and wandering in this ethical and legal grey area? In the same YouTube video, it also claimed:

Anonymous’ campaign will defend against any individual, organization, corporation, and/or government entity that seeks to hinder the free flow of information on the Internet and beyond. Our methods may appear to be unjustly burdening our targets, but we argue that in this moment when the Freedom of Speech is under attack by the very institutions which are supposed to support it, drastic measures must be taken. (Timeline: 4:33 to 5:10)

This segment gave a hint that some media-savvy Anons were behind this video production because they knew what to feed the public. By assaulting “the very institutions,” it tactfully shifted viewers’ attention away from further discussions of Distributed Denial of Service (DDoS) attacks’ legality and legitimacy. Its hyperbole could probably stir up the audience’s anger as it alleged that the authorities—the protectors of freedom of speech—had become perpetrators that obstructed the free flow of information. By announcing that “drastic measures” were underway, it made public that they were going to adopt radical, harsh, even relentless methods to fight for “the Freedom of Speech,” thereby portraying Anonymous as a courageous collective challenging authority and advocating for the oppressed. Moreover, this rhetoric might help Anonymous “continually [play] with societal stereotypes of the hacker” (Sauter 989) and conjure up an impression that “Anonymous is as merciless as it is clandestine” (Phillips 500).

To date, this video has been viewed 246,423 times. The popularity and the accompanying hyperbole caused a sensation in corporate media outlets and steered their focus to this spectacle rather than the ethical questions. Few Western media outlets discussed the moral issue of DDoS attacks when they covered the story of Operation Payback. More often than not, the media

consumed the eye-catching story without reminding readers of the legal risks of DDoS attacks. Or, sometimes the news coverage even offered deep linking to webpages “where one could download LOIC, join an IRC channel, or find information on scheduled raids” (Sauter 1001).<sup>71</sup>

A group of anonymous Internet activists announced on Monday that they will launch an attack on PayPal in retaliation for the service’s decision to stop collecting money for WikiLeaks. According to [the Twitter feed](#) of the group, [Operation Payback](#), the attack will begin in a few minutes, at 7 p.m. GMT (2 p.m. ET).

(LOIC stands for Low Orbit Ion Cannon, whose

Figure. 6 An excerpt from the article “Updates on Leak of U.S. Cables, Day 9 (NYTimes.com). The underlined blue words are deep links.

function I will elaborate in the following paragraph.) Figure 6 is a case in point. It is a screenshot of an article “Updates on Leak of U.S. Cables, Day 9” published on NYTimes.com.<sup>72</sup> When readers click on the underlined blue words “[the Twitter feed](#)”, they will be re-routed to Anonymous’s Twitter page “@Anon\_Operation.” Clicking on “[Operation Payback](#),” the Wikipedia page of “Operation Payback” will come up. To a lesser extent, the deep linking embedded in the major news coverage “provided a sheen of endorsement to the linked materials, for why would a news organization or blog make it so easy to access these materials if it did not believe them worthy of the resultant attention and influence?” (Sauter 1001). Such a media effect was the combination of Anonymous’s attempt to manipulate the media by feeding it things to see and many media outlets’ negligence of social consequences by uncritically cooperating. In this context, Anonymous and the media were facing the similar ethical puzzle: whether it was acceptable to use legally ambiguous DDoS attacks to draw public attention or not?

As a matter of fact, “Anonymous did not create DDoS as an activist tactic but rather innovated on the history of experience, skills, and code of activists and hackers who came before” (Sauter 1003). Anonymous’s innovation was to adopt software named “LOIC” in its Distributed

<sup>71</sup> “In the context of the World Wide Web, deep linking consists of using a hyperlink that links to a specific, generally searchable or indexed, piece of web content on a website, rather than the home page” (Wikipedia).

<sup>72</sup> See <http://thelede.blogs.nytimes.com/2010/12/06/latest-updates-on-leak-of-u-s-cables-day-9/?hp#operation-payback-plans-attacks-on-paypal>

Denial of Service (DDoS) attacks to lower the technological threshold for inexperienced netizens. This move made Anonymous's already controversial DDoS strategy more contentious. Why? What was LOIC? LOIC stands for Low Orbit Ion Cannon, a program whose function is to "send out useless requests or 'packets' to a server" (Olson 76). With enough people using LOIC altogether, it can "overload [the server] with enough junk traffic to take it offline" (Olson 77). Sometimes it is used by technicians to stress-test websites. But, as an open-source application, it is free to download and easy to learn even for "less technically able individuals" (Sauter 998). During Operation Payback, LOIC was even improved to a point that it added the Hive Mind automated attack mode, which "allowed the tool be controlled remotely, through the IRC protocol. During Hive Mind mode, the user was essentially volunteering his or her machine to be part of a botnet" (Sauter 997).<sup>73</sup> This made newcomers' contribution to DDoS attacks much easier, even enabling them to "go to school, work, sleep, or anywhere while still participating in DDOS actions as they arose" (Sauter 998).

What made LOIC's usage contentious was not the program itself, but the way Anonymous promulgated it. As Operation Payback's popularity grew, many netizens were instigated by the media frenzy of Anonymous's Distributed Denial of Service (DDoS) attacks on PayPal, MasterCard, and Visa. In the face of the massive influx of newcomers, some Anons posted several LOIC tutorials on YouTube, intending to train these "newfags" to use LOIC to partake in DDoS speedily. These tutorials did not tell users that their IP addresses would be exposed and easily traced if they did not take additional security measures such as using a proxy. On the contrary, the tutorials reassured users that the risk of being caught was minimum and even if, in the worst case scenario that they were caught, they could easily deny it by claiming their computer was compromised by a virus. It is hard to tell whether the Anons who produced these tutorials were also novices or experienced hackers who knew the legal risk but chose to feed the

---

<sup>73</sup> The word botnet is a combination of the words "robot" and "network." A botnet is a number of Internet-connected computers communicating with other similar machines in an effort to complete repetitive tasks and objectives such as DDoS attacks (Wikipedia).

newcomers the “false information” (Coleman 126). Nevertheless, it enabled Anonymous to “expand its participant community dramatically” (Sauter 998). But, at the same time, it also landed some “unwitting young adults on the wrong side of the law” (Goode 77). On December 15, 2010, PayPal offered the FBI with a long list of 1,000 individuals’ IP addresses who had used LOIC to attack PayPal. On January 27, 2011, British police arrested five men in connection with Operation Payback cyberattacks.

Apart from this, Olson also claims that the actual determining factor in Anonymous’s Distributed Denial of Service (DDoS) attacks on PayPal, MasterCard, and Visa was not the participation of these LOIC users but some botmasters. A botmaster was someone who remotely controlled “zombie computers,” which were infected by a virus or links to bogus software updates. She asserts, “around 90 percent of all the firepower from the attack on PayPal.com had come not from Anonymous volunteers but from zombie computer” (117). But she further points out that those who knew the truth chose to lie to the media, aiming to romanticize “this new powerful phenomenon of a hive that nobody seemed able to quantify” (122). This incident raised another moral issue: whether it was fair to “deceive” the volunteers “who had considered themselves to be an audience in the world of politics and industry to become actors, strengthened by the invisible yet palpable presence of thousands of their new comrades-in-arms” (Sauter 998), in the name of creating a public image of mass participation and social solidarity?

Although Anonymous has managed to establish its brand identity as a vehement defender of free information and a courageous fighter against authority and hegemony, its symbolic values will be compromised by these ethical questions. Anonymous’s open nature makes its leaderless and decentralized structure adaptable to various situations, but it also makes it difficult to supervise the intentionality of all Anons. In this sense, the moral issues resonate with an old question “can the end justify the means?”—the answer remains elusive.

## **Conclusion: Contemporary Significance of Anonymous's Brand Identity**

“Since the 1983 release of the movie *WarGames*, the figure of the computer hacker has been inextricably linked to the cultural, social, and political history of the computer” (Thomas ix). But, whether or not Anons can be considered as hackers has been a heated topic. Many of them do not have sophisticated hacking skills. I argue that the Anonymous phenomenon should be analyzed as a microcosm of hacker culture. It is not the tools—complex hacking software or automated mode LOIC—that characterize the political coloration of Anons' actions. It is their acknowledgement of the symbolic values of Anonymous's brand identity, around which they rally and participate in Distributed Denial of Service (DDoS) attacks. “Although they violate the law by gaining unauthorized access to personal computers or to computer networks, hackers have their own code of ethics, namely the principle that all information should be free” (Turgeman-Goldschmidt 9).

“The classic if simplistic distinction in hacker culture is between legitimate ‘white hats’ (hackers hired to locate security vulnerabilities) and ‘black hats’ or ‘crackers’ with malevolent motives. ‘Gray hats’ execute unauthorized hacks with a benign motive to expose security flaws, though reputation and status may also be at stake (Goode 77). I do not think Anonymous fits into any of those three stereotypes. Although there are “many faces of Anonymous” (Coleman) and many Anons do not have a clear political agenda, their actions made Anonymous's moniker take on a political coloration. This is because Anons' motive is not about monetary theft or pure security exploitation. In the past five years, people who paid attention to the work of Anonymous have noticed this collective more frequently engaging itself in the self-claimed mission of defending freedom of speech, hacking “wrongdoers” and revealing imperfections of the social mechanism. The legally and morally debatable Distributed Denial of Service (DDoS) tactics win it massive media coverage and help it swiftly construct its brand identity as a fearless defender of free information. In this sense, I would suggest that Anonymous be categorized as “yellow hats.”

Yellow is a dazzling color that grabs people's attention and denotes a warning of the danger that might shatter the social order. Anonymous's case exhibits the importance of building a progressive hacktivist icon because it offers a ray of hope that "a new equilibrium will arise between the traditional holders of power and unexpected influencers arising from the grassroots" (Cohen et al. 37).

It is undeniable that the desire for "trolling" and "lulz" is still running in Anonymous's blood, so occasionally it will add some mischievous or provocative elements in their operations. As a result, sometimes the public has difficulty comprehending how Anonymous can dabble in delivering social justice and also "trolling." Perhaps Anonymous's style is like Charlie Chaplin's movies. Consider, for example, *Modern Times* (1936), which narrates a worker's struggle and rebellion in the face of a modern and industrialized world in a ridiculously hilarious, exaggerated manner. Similarly, Anonymous combines hacktivism and "trolling," aiming to become an unorthodox political and cultural icon featuring online civil disobedience, and, like it or not, a mordant sense of humor. According to Kemp, Emeritus Professor of the History of Art at Oxford University, "an iconic image is one that has achieved wholly exceptional levels of widespread recognizability and has come to carry a rich series of varied associations for very large numbers of people across time and cultures" (3). I argue that Anonymous's brand identity carries important political and cultural values and can be regarded as an icon that advocates freedom of information and delivers social justice in Internet politics, thereby attracting "very large numbers of people across time and cultures."

As a widely recognizable symbol, Anonymous's brand identity has significant contemporary values as well, as evidenced by news stories about the cyberwar between Anonymous and the Islamic State militant group (also known as ISIS).<sup>74</sup> For instance, on March 24, 2015, *The New York Times* ran an article titled "Behind a Veil of Anonymity, Online

---

<sup>74</sup> The Islamic State militant group is a marauding army gobbling up chunks of the Middle East (WSJ.com). See <http://www.wsj.com/articles/assad-policies-aided-rise-of-islamic-state-militant-group-1408739733>

Vigilantes Battle the Islamic State” by Rick Gladstone. In this piece, “loosely knit hacking organizations like Anonymous” were depicted as a centripetal force attracting many hacktivists to subvert ISIS’s aggressive use of social media, particularly Twitter, for recruitment and spreading images of brutalities.<sup>75</sup> It was the spirit of delivering social justice—derived from Anonymous’s brand identity—that rallied those online activists to unite under the same banner. They strove to cripple ISIS’s ability of propaganda by hacking their websites and reporting suspect accounts of “Islamic State fighters, recruiters and fund-raisers” to Twitter’s violations department. Their effort pushed Twitter to suspend ISIS-related accounts “at the rate of 2,000 per week.” By using words like “the battle of Anonymous vs. ISIS” (also known as OpISIS), Gladstone situated Anonymous on the high moral ground as an agglomeration of hackers fighting for a righteous cause, omitting mention of the possibility that Anonymous might use illegal hacking skills. In the face of ISIS’s rampant expansion of social media notably Twitter, the United States government and Twitter did little to halt its momentum. So there were some media outlets even talking about the possibility of the United States government cooperating with Anonymous, such as the SFGATE article titled “Why the U.S. should but won’t partner with hacktivists Anonymous.”<sup>76</sup> Admittedly, it would be absurd for the United States government to “outsource justice” to Anonymous, but such news coverage implied that some American mainstream media organizations were welcoming and even encouraging hacktivists’ intervention.

Anonymous’s brand identity construction heralds “a newfangled phenomenon” (Olson 409) in our digital era that there is a niche for what I would term “yellow hats” hackers in Internet politics. Despite the ethical tensions, the symbolic values accompanying progressive hacktivists’ brand identity have a high potential to promote social justice and shift the state-society power balance, at present and well into the future.

---

<sup>75</sup> See [http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?\\_r=0](http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html?_r=0)

<sup>76</sup> See <http://www.sfgate.com/news/article/Why-the-U-S-should-but-won-t-partner-with-6235020.php>

## Appendix:

### The Clarification of Anonymous's Usage of the Suffix "fag"

With the help of Professor Amy Laura Hall, a source offers the clarification of why Anonymous uses the seemingly offensive suffix "fag" as follows:

"It's not generally an insult (though sometimes is) within Anonymous. Everyone is considered a "fag" of some sort or another. Part of that comes from several original Anons being queer, part of that comes from a commitment to free speech that's intentionally transgressive. So there are old fags, new fags, moral fags, summer fags, fame fags, lulz fags, occu fags, etc. Some of them are derisive, but it is the first word in whichever term that is derisive."

## Glossary<sup>77</sup>

**4chan:** an English-language imageboard frequented by 22 million users a month, featuring forced anonymity on all the posts. The topic is very diversified, including anime and online pranks.

**Botnet:** a combination of the words “robot” and “network.” A botnet is a number of Internet-connected computers communicating with other similar machines in an effort to complete repetitive tasks and objectives such as DDoS attacks.

**Botmaster:** someone who remotely controlled “zombie computers,” which were infected by a virus or links to bogus software updates.

**Deep linking:** in the context of the Internet, it consists of using a hyperlink that links to a specific, generally searchable or indexed, piece of web content on a website, rather than the home page.

**DDoS:** a computer term, standing for Distributed Denial of Service. It is an attack on a website or networks carried out by a network of computers that temporarily knocks the site offline by overwhelming it with junk traffic.

**Google bomb:** the practice of causing a web page to rank highly in search engine results for unrelated or off-topic search terms by linking heavily.

**Griever:** a player in a multiplayer video game who deliberately irritates and harasses other players and derives pleasure from annoying others.

**IRC:** a term stands for Internet Relay Chat. It serves as a transnational platform offering virtual chat rooms, where people can have real-time text conversations with global users.

**LOIC:** a term stands for Low Orbit Ion Cannon, a program whose function is to send out useless requests to a server. With enough people using LOIC altogether, it can overload the server with enough junk traffic to take it offline.

**Lulz:** an alteration of the abbreviation LOL (laugh out loud). It means the enjoyment felt after pursuing a prank or online disruption that leads to someone else’s embarrassment.

**TANGO DOWN:** as military slang, it refers to a target especially a terrorist being eliminated. There has been wide pop culture usage in video games and movies, mainly by characters in tactical squads engaging terrorists.

**Trolling:** as Internet slang, it means anonymously harassing or mocking others online with an aim to anger or humiliate others.

---

<sup>77</sup> The definition of these terms is based on Wikipedia, Urban Dictionary, and Parmy Olson’s book *We Are Anonymous*.

## Cited Sources

- "Hackers Target Wikileaks 'Enemies': Mastercard, Twitter, Paypal, Even Foxnews.Com." FoxNews.com. Web. 06/24/2015.
- "Huge Wikileaks Release Shows Us 'Ignored Iraq Torture'." BBC.com. Web. 06/25/2015.
- "Internet Conflict with Scientology Expands." PRLog.org. Web. 06/22/2015.
- "Internet Group Anonymous Declares War on Scientology." PRLog.org. Web. 05/26/2015.
- "Operation:Payback Broadens to "Operation Avenge Assange"." Pandasecurity.com. Web. 06/24/2015.
- "Paypal Suspends Wikileaks Donations Account." Reuters.com. Web. 06/23/2015.
- "The Greensboro Four." *Civil Rights*. North Carolina Museum of History. Web. 07/25 2015.
- "'Tis the Season of Ddos--Wikileaks Edition." Pandasecurity.com. Web. 06/01/2015.
- Aaron, Smith, . "Mastercard, Visa Targeted in Apparent Cyberattack." CNN.com. Web. 06/23/2015.
- Aleteuk. "Tom Cruise Scientology Video - ( Original Uncut )." YouTube. Web. 06/20/2015.
- Anonymous, A letter from. "A Letter from Anonymous, 9th of December 2010." YouTube. Web. 06/24/2015.
- Ball, James. "The Bankers' Blockade of Wikileaks Must End." Guardian. Web. 06/20 2015.
- Behar, Richard "The Thriving Cult of Greed and Power." Time.com. Web. 06/21/2015.
- Bosker, Bianca "Pro-Wikileaks Hackers' Latest Target: Paypal." Huffingtonpost.com. Web. 06/24/2015.
- Bumiller, Elisabeth. "Video Shows U.S. Killing of Reuters Employees." NYTimes.com. Web. 05/31/2015.
- Chen, Adrian. "The Truth About Anonymous's Activism." The Nation. Web. 03/17/2015.
- ChurchOfScientology. "Call to Action." YouTube. Web. 06/23/2015.
- . "Code of Conduct." YouTube. Web. 06/23/2015.
- . "Message to Scientology." YouTube. Web. 06/20/2015.
- Cohen, Noam. "Web Attackers Find a Cause in Wikileaks." NYTimes.com. Web. 05/31/2015.
- dearfoxnews. "Dear Fox News." YouTube. Web. 06/23/2015.

Denton, Nick. "The Cruise Indoctrination Video Scientology Tried to Suppress." Gawker.com. Web. 05/25/2015.

Editors. "Current Comment." Americamagazine.org. Web. 06/20/2015.

Fantz, Ashley and Atika Shubert. "Wikileaks 'Anonymous' Hackers: 'We Will Fight'." CNN.com. Web. 06/23/2015.

Fernandez, Colin and Laura Caroe. "Army of Hackers Targets the Swedish Government, Sarah Palin and Credit Card Giants in Wikileaks 'Operation: Payback'." Dailymail.co.uk. Web. 06/25/2015.

Gladstone, Rick "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State." NYTimes.com. Web. 06/24/2015.

Gorman, Siobhan. "Alert on Hacker Power Play." WSJ.com. Web. 06/15/2015.

Greenberg, Andy. "Visa, Mastercard Move to Choke Wikileaks." Forbes.com. Web. 06/24/2015.

Isaac, Mike. "Facebook and Twitter Suspend Operation Payback Accounts." Forbes.com. Web. 06/24/2015.

Mackey, Robert "Updates on Leak of U.S. Cables, Day 9." Blogs.NYTimes.com. Web. 06/23/2015.

Owen, Taylor "Why the U.S. Should but Won't Partner with Hacktivists Anonymous." SFGATE.com. Web. 06/24/2015.

Poulsen, Kevin. "Hackers Assault Epilepsy Patients Via Computer." Wired.com. Web. 05/28/2015.

Ruffin, Oxblood. "Hacktivism, from Here to There." cultdeadcow.com. Web. 07/25 2015.

Schultz, Dan. "Anonymous Vs. Scientology: A Case Study of Digital Media." PBS.org. Web. 05/26/2015.

Shane, Scott and Andrew W. Lheren "Leaked Cables Offer Raw Look at U.S. Diplomacy." NYTimes.com. Web. 06/25/2015.

## Bibliography

- "Fawkes, Guy." Oxford Dictionary of National Biography. Web. 08/02 2015.
- Ayish, Mohammad Ibrahim. "Forward." *Social Media Go to War : Rage, Rebellion and Revolution in the Age of Twitter*. Ed. Berenger, Ralph D. Spokane, Wash.: Marquette Books, 2013. Print.
- Babbie, Earl R. *The Practice of Social Research*. Belmont, CA: Wadsworth Cengage Learning, 2013. Print.
- Berenger, Ralph D. "Introduction: Social Media Go to War." *Social Media Go to War : Rage, Rebellion and Revolution in the Age of Twitter*. Ed. Berenger, Ralph D. Spokane, Wash.: Marquette Books, 2013. Print.
- . "Social Media Go to War: Summary and Conclusion." *Social Media Go to War : Rage, Rebellion and Revolution in the Age of Twitter*. Ed. Berenger, Ralph D. Spokane, Wash.: Marquette Books, 2013. Print.
- Beyer, Jessica L. "The Emergence of a Freedom of Information Movement: Anonymous, Wikileaks, the Pirate Party, and Iceland." *Journal of Computer - Mediated Communication* 19.2 (2014): 141-54. Print.
- Braiker, Brian. "'Anonymous' Takes on Scientology." Newsweek.com. Web. 05/27/2015.
- Cohen, Aaron M., et al. "The Best Predictions of 2011." Washington: World Future Society, 2012. 28. Vol. 46. Print.
- Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy : The Many Faces of Anonymous*. London ; Brooklyn, NY: Verso, 2014. Print.
- Critical Art Ensemble. *The Electronic Disturbance*. Brooklyn, NY: Autonomedia, 1994. Print.
- Davis, Derek H. "The Church of Scientology." *Book Review*. Vol. 42. Oxford: J. M. Dawson Institute of Church-State Studies of Baylor University, 2000. 851-52. Print.
- Gauntlett, David. *Making Is Connecting : The Social Meaning of Creativity from Diy and Knitting to Youtube and Web 2.0*. Cambridge, UK ; Malden, MA: Polity Press, 2011. Print.
- Gerbaudo, Paolo. *Tweets and the Streets [Electronic Resource] : Social Media and Contemporary Activism*. London: Pluto Press, 2012. Print.
- Gitlin, Todd. *The Whole World Is Watching : Mass Media in the Making & Unmaking of the New Left*. Berkeley: University of California Press, 1980. Print.
- Goode, Luke. "Anonymous and the Political Ethos of Hacktivism." *Popular Communication* 13.1 (2015): 74-86. Print.

- Jordan, Tim. *Hactivism and Cyberwars : Rebels with a Cause?* Ed. Taylor, Paul A. London ; New York, N.Y.: Routledge, 2004. Print.
- Kahn, R., and D. Kellner. "Technopolitics, Blogs, and Emergent Media Ecologies." *Small Tech : The Culture of Digital Tools*. Eds. Hawk, Byron, Ollie O. Oviedo and David M. Rieder. Minneapolis: University of Minnesota Press, 2008. Print.
- Kaplan, Andreas M., and Michael Haenlein. "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons* 53.1 (2010): 59-68. Print.
- Kaulingfreks, Femke, and Ruud Kaulingfreks. "Open-Access Communism." *Business Ethics: A European Review* 22.4 (2013): 417-29. Print.
- Kellner, Douglas. "Media Culture and the Triumph of the Spectacle." Intellect, 2005. 23. Print.
- Kelly. "Anonymous to Destroy Facebook on November 5th (Update: Well, Probably Not)." gizmodo.com. Web. 05/26/2015.
- Kelly, Brian B. "Investing in a Centralized Cybersecurity Infrastructure: Why "Hactivism" Can and Should Influence Cybersecurity Reform." *Boston University Law Review* 92.5 (2012): 1663. Print.
- Kemp, Martin. *Christ to Coke : How Image Becomes Icon*. Oxford ; New York: Oxford University Press, 2012. Print.
- Krapp, Peter. "Terror and Play, or What Was Hactivism?" *Grey Room*.21 (2005): 70-93. Print.
- Lindgren, Simon. *New Noise : A Cultural Sociology of Digital Disruption*. Digital Formations ; V. 88. New York: Peter Lang, 2013. Print.
- Melton, J. Gordon. *The Church of Scientology*. Vol. 1.; 1. Salt Lake City: Signature Books in cooperation with CESNUR, 2000. Print.
- Norton, Quinn. "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down." *Wired*. Web. 05/25/2015.
- Olson, Parmy. *We Are Anonymous : Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and Co., 2012. Print.
- Phillips, Whitney. "The House That Fox Built: Anonymous, Spectacle, and Cycles of Amplification." *Television & New Media* 14.6 (2013): 494-509. Print.
- Pieterse, Jan Nederveen. "Leaking Superpower: Wikileaks and the Contradictions of Democracy." *Third World Quarterly* 33.10 (2012): 1909-24. Print.
- Rheingold, Howard. *Net Smart [Electronic Resource] : How to Thrive Online*. Cambridge: MIT Press, 2012. Print.

- Rushkoff, Douglas. *Open Source Democracy [Electronic Resource] : How Online Communication Is Changing Offline Politics*. [S.l.]: Project Gutenberg, 2004. Print.
- Sauter, Molly. "'Loic Will Tear Us Apart': The Impact of Tool Design and Media Portrayals in the Success of Activist Ddos Attacks." *American Behavioral Scientist* 57.7 (2013): 983-1007. Print.
- Schmidt, Eric, and Jared Cohen. "The Digital Disruption." *Foreign Affairs* 89.6 (2010): 75. Print.
- Shantz, Jeff and Jordon Tomblin. *Cyber Disobedience : Re://Presenting Online Anarchy*. Winchester, UK ; Washington, USA: Zero Books, 2014. Print.
- Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002. Print.
- Turgeman-Goldschmidt, Orly. "Hackers' Accounts: Hacking as a Social Entertainment." *Social Science Computer Review* 23.1 (2005): 8-23. Print.