**The Guy Fawkes Effect:**
**Wikileaks, Anonymous, and U.S. Policing of the Internet**

December 2013
Barnard College
Undergraduate Thesis (Political Science)

A/N: The only version of this I could still locate on my email did not include full citations or a works cited page. I am too lazy now to go back through and properly reference the material (I may at some point). If you have any questions on research or source material, get in touch and I will do my best to track down the books and articles I used.

## I. Introduction

"This will be the September 11th of world diplomacy," said Italian Foreign Minister Franco Frattini on the eve of what has come to be known as Cablegate (**Reuters, Sun, Nov. 28, 2010. http://www.reuters.com/article/2010/11/28/italy-wikileaks-idAFLDE6AR0D420101128**). Later that day, the online whistle-blowing and media organization WikiLeaks began releasing 251,287 United States Embassy diplomatic cables in the largest leak of classified information in history. Since a triumphant year of high-profile releases in 2010, WikiLeaks has become a shell of the organization it once was, due largely to a sweeping campaign by the United States government to shut down the organization as a whole.

The retaliatory measures taken by the United States government against WikiLeaks were unprecedented, but WikiLeaks was not the only target. The nebulous hacktivist collective and fair-weather WikiLeaks friend, Anonymous, also came under heavy fire from government officials and fell victim to a series FBI raids and arrests. In December 2010, the United States government began a large-scale, across-the-board crackdown on hacktivism the likes of which Western industrial democracy had never before seen. The reaction is troubling, particularly coming from the United States, the bastion of free speech and individual liberty itself. We must ask ourselves, why did the U.S. government begin cracking down on hacktivism in 2010?

I argue that the current wave of hacktivism is a social movement as well as a strategy. The simplest understanding of hacktivism is as a method of political protest that not only organizes online, but uses the Internet as the platform to engage in political action through a variety of tactics (many of which fall under the umbrella of illegal hacking). However, this definition does not pin down the ideological currents that bind current hacktivist groups together into a social movement. Today's hacktivism, which coalesced into a movement in 2008, has

become a worldwide social movement advocating for Internet freedom, freedom of information, institutional transparency, and individual privacy.

While hacktivism has existed in various forms since the 1980s, most notable hacktivist groups of the 1990s and early 2000s are now defunct. The two most important hacktivist groups still making headlines are WikiLeaks and Anonymous. Founded in 2006 and nebulously formed in 2004, respectively, the two organizations have grown up together as occasional partners and loose allies in a global movement for information freedom. Despite their differences, both groups organize and engage in political action entirely online, and share a unifying ideological commitment: transparency for institutions, free speech and privacy for individuals. [1]

Yet the use of the Internet as the platform for implementing this ideology has consequences that many governments fear. Understanding why the U.S. government has cracked down on WikiLeaks and Anonymous requires an understanding of the complicated relationship between the Internet and the state. At the center of this relationship is the question of anonymity. Anonymity is anathema to state sovereignty; when you do not know who someone is, laws cannot be exercised against them. I argue that it was the fear of anonymity, and not the actions taken by WikiLeaks and Anonymous themselves, that explains the U.S. government's unprecedented behavior. Anonymity was always a potential of the Internet, but the extent of its use in hacktivism was not solidified until WikiLeaks and Anonymous emerged on the global stage in 2010.

---

[1] WikiLeaks' mission statement describes the group thus: "The broader principles on which our work is based are the defence of freedom of speech and media publishing… WikiLeaks is an independent global group of people with a long standing dedication to the idea of a free press and the improved transparency in society that comes from this" (**WikiLeaks.org, 2013**). Anonymous has no localized mission statement, however much of the media it produces can shed light on the group's ideology. A recent YouTube video titled "What is Anonymous" describes Anonymous as, "an idea… citizens bearing witness to tyranny. We seek transparency of government and institutions, and individual freedom" (**https://www.youtube.com/watch?v=I7uxOhqdgzA**).

**II. A Unique Threat to Security or a Broad Threat to Sovereignty?**

The threat of cyber warfare, or more specifically cyberterrorism, has been a fear of governments around the world since the inception of the Internet. As businesses and governments move their operations online, protection of those interests becomes key. This is the viewpoint put forward by many within the U.S. government apparatus, from the State Department, to the Secretary of Defense, to the FBI, CIA and NSA. The frame of cyberterrorism is used to explain their unprecedented retaliation against hacktivists. When these groups are viewed to present a new and serious threat to national security, by putting personal and government information at risk and compromising the government's ability to perform its duties, dealing harshly with hacktivists is a necessary part of the maintenance of public order.

The argument harkens back to long-held views about counter-terrorism. As Christopher Corpora **(2006)** argues, modern terrorism does not obey conventional rules of engagement, and previous practices of combating terrorism will not stand up to the new threats posed. An appropriate response to terrorism would require a comprehensive strategy amounting to an "ideological war" against all levels of the terrorist threat **(Corpora, 2006).** Internet security must be strict and dealings with violations must be severe, as the possibility of what then-Defense Secretary Leon Panetta called a "cyber-Pearl Harbor" is imminent **(Panetta, 2012).** Hacktivist organizations such as Anonymous and WikiLeaks may not yet be capable of launching an attack of that magnitude, but their technical know-how is constantly increasing. The actions they have already undertaken have been damaging to national security and corporate interests, and those actions will continue to be a threat until such a time as the organizations are stopped. Cracking down on such organizations is a necessary step to ensure that their capabilities do not grow to

include the ability to launch a deadly cyberterror attack.

However, there are many within the scholarly world who view the U.S. government's response to hacktivism as entirely unrelated to hacktivists' actions. The fearful response to hacktivism has nothing to do with the attacks these groups pull off, and everything to do with the anarchic nature of the Internet. Glorel Curran and Morgan Gibson (2013) argue that anonymity on the Internet threatens state sovereignty by creating an anarchic space of organization **(Curran and Gibson, 2013: 297).** It is not the hacktivists' actions at all, but the nature of the Internet itself, that the U.S. government seeks to change.

Efforts to dominate hacktivist groups, the argument runs, should be viewed in a larger context of creating what Rita Zajacz dubs an "Internet minus the anonymity" **(Zajacz, 2013, 500).** WikiLeaks' and Anonymous' pose threats to the government's sovereignty due to their anonymity and non-territoriality **(Zajacz, 490).** The actions taken by the U.S. government against these groups is not directly related to their actions, but is simply one part of an attempt to remove anonymity from subversive action. The threat that the government seeks to minimize is thus not to national security, but to sovereignty. The retaliation against these threats signifies not an attempt to ward off future attacks, but to bring the Internet as a whole under the state's control.

## III. The Guy Fawkes Effect: A Unique Threat to Sovereignty

I believe that both of these arguments fail to account for serious issues in the WikiLeaks and Anonymous cases. On the one hand, the view of hacktivism as cyberterrorism does not stand up to the lack of on-the-ground damage done by either of these groups' actions. The threat to national security was never great enough for hacktivists to truly present a terrorist threat.

Furthermore, the actions taken by these groups were not themselves new, and thus an unprecedented response is illogical. On the other hand, viewing the treatment of WikiLeaks and Anonymous through the lens of a wider attempt to remove anonymity from the Internet does not account for the temporality of these cases. There was a clear shift in the U.S. government's treatment of hacktivism before and after the WikiLeaks Cablegate release in 2010. If anonymous organizing on the Internet was always the threat to sovereignty that it is now, the timing of the U.S. government response makes little sense.

The true impetus for the crackdown on hacktivism lies between these two arguments, in something I have termed the "Guy Fawkes effect." The lack of impact on national security had by either of these two groups shows that they are not truly terrorist threats akin to Al Qaeda or similar organizations, yet the threat they pose is certainly something new and serious. That threat is their anonymity. Despite the Internet's potential for anonymous action since its inception, true anonymous hacktivism began in earnest with WikiLeaks and Anonymous. The use of anonymity as a strategy to avoid capture and retaliation from governments was always a possibility, but was not used in large-scale activist demonstrations until 2008. The U.S. government in turn did not recognize the full scale of the new breed of anonymous hacktivism until 2010.

The Guy Fawkes mask worn by the character "V" in the 2006 film *V for Vendetta* has become a global symbol of resistance. It has particularly been adopted as a symbol by Anonymous, but has also been seen at protests around the world. What I have termed the Guy Fawkes effect is something like more traditional anarchist black bloc protests moved into the online sphere: anonymity is used as a tool to make repressing individuals' actions within the group more difficult. If the state is defined by a monopoly on the legitimate use of violence within a territory, that violence only has power insofar as it can be exercised upon the populace

as a tool to keep them obedient to certain laws and social customs. State sovereignty cannot be enforced on anonymity. It is in differentiation of people that state power can be exercised – a police line-up of Guy Fawkes masks would be impossible to convict.

While this argument runs very similar to the one posited by Zajacz (2013) and Curran and Gibson (2013), I believe the fundamental difference to be in viewing the particular threat of anonymity in Internet activism to be new and specific to Anonymous and WikiLeaks. On the one hand, the tools used by these groups are not new. The distributed denial-of-service (DDoS) attacks, information theft and website defacement popularly used by Anonymous have been staples of Internet activism since the 1990s, but Anonymous was the first to place Anonymity at the heart of its agenda **(Sauter, 2012; etc).** Likewise, leaks of classified information to the public are certainly not unique to WikiLeaks, but WikiLeaks was the first to provide a platform specifically focused on maintaining anonymity of the whistleblower and non-territoriality of the publisher.

It is the fear of the uncontrollability of these groups, rather than a fear of their past or future actions, that has caused the U.S. government to deal with hacktivist action so harshly. The potential was always there, but the realization of anonymous mobilization online is new and unique to these two groups. As a result, the retaliatory measures taken by the U.S. government since 2010 mark an attempt to set a new precedent for establishing state control over the Internet by removing anonymity from the equation.

## IV. Hacktivism and its Discontents: A Brief History

*The Early Days – 1980s to early 2000s*

What we now know as computer hacking has a long history, pre-dating the beginnings of

the Internet. The original hackers were Tech Model Railroad enthusiasts at MIT between the 1950s and 1980s, who coined the term to describe their endeavors to play with track circuitry **((McCormick, 2012: 1).** Hacking came to describe interference with technology systems, usually as a prank or practical joke, though it was not long before hacking expanded to become a tool of political dissidence. The Internet itself came into existence in its most basic form in 1969, while the World Wide Web, the Internet that we today access through browsers, has been in existence since 1989 (**http://www.latimes.com/business/hiltzik/la-fi-mh-internet-20131029,0,745156.story#axzz2mqGqTvn5**).

The first piece of anti-computer hacking legislation in the U.S., the Computer Fraud and Abuse Act (CFAA) was adopted by Congress in 1986, prior to the invention of the World Wide Web. The CFAA in its initial iteration focused mainly on federal computer crimes, namely those which involved hacking of a federal government or financial institution computers **(OLE, 2).** In 1991, Robert Tappan Morris, a Cornell student responsible for an early Internet malware worm, became the first person to be convicted under the CFAA **(US v. Morris).**

Political hacking dates back to 1989 and the mysterious incident of the WANK worm. In October 1989, the second major malware worm in computer history, adapted from the Morris worm, was launched against computers at NASA and the U.S. Department of Energy during the Galileo Probe launch. The worm defaced computer login screens at both organizations with the blast "WORMS AGAINST NUCLEAR KILLERS… Your System Has Been Officially WANKed" **(McCormick, 2012: 1)** No damage was done to the programming of the launch. Though the perpetrators of the attack were never caught, the worm was tracked to Melbourne, Australia, and many suspect that a notorious Australian hacker known then as Mendax (known now as Julian Assange) was among those responsible **(Manne, Cypherpunk Revolutionary).**

The Intervasion of the UK, a 1994 takedown of British government websites, introduced the world to distributed denial-of-service (DDoS) as a protest tactic **(McCormick, 2012: 2).** A favorite tactic among modern hacktivists, DDoS attacks knock out targeted websites by bombarding their servers with communication requests, so much so that the sites shut down and become inaccessible to legitimate users.

In 1996, the term "hacktivism" was coined by members of the Texas-based hacking group Cult of the Dead Cow (cDc). cDc, like hacking itself, began mostly as a practical joke, an organization bent on "global domination through media saturation" **(McCormick, 2012: 2).** cDc spun off into a group called Hacktivismo, which focused on helping activists around the world evade Internet censorship (**McCormick, 2012: 2).** Both cDc and Hacktivismo are now defunct.

At the same time that cDc and Hacktivismo were advocating for an end to Internet censorship, the Electronic Disturbance Theater (EDT) was co-opting Internet censorship for anti-establishment purposes. EDT was a group of four activists, all of whom were open about their identities, that began using DDoS as a tool for political mobilization in defense of the Zapatista movement **(Dominguez, ??)**. EDT created a tool called FloodNet that allowed for individuals to engage in DDoS attacks against a select list of opponents, in their case certain websites of the Mexican government **(Sauter, 988).** The source code for FloodNet was released in 1999, and spawned numerous offshoots, most notably the Low Orbit Ion Cannon (LOIC) that has become the staple of Anonymous' DDoS attacks. No members of Electronic Disturbance Theater were ever arrested as a result of their actions.

Anonymous itself began between 2003 and 2004 in the early days of the un-moderated image board 4chan, the birthplace of lolcats and most Internet memes. In traditional hacker fashion, Anonymous did not begin as an activist organization. Rather, it was centered on pranks

and what one early Anonymous member called "ultra-coordinated motherf***ery" **(McCormick 2012: 2).** Anonymous' political activism did not begin in earnest until 2008.

In 2006, the domain name WikiLeaks.org was registered **(Domscheit-Berg, 2011, ???).** Founded by the aforementioned Julian Assange, WikiLeaks was intended to be "a not-for-profit media organization… provid[ing] an innovative, secure and anonymous way for sources to leak information to our journalists" (**WikiLeaks.org**). WikiLeaks' first major leak came in 2007 with the publishing of the Guantanamo Bay handbooks **(Domscheit-Berg, 2011).** This was quickly followed by hundreds of documents from the Swiss bank Julius Baer in January 2008, indicating corruption and tax evasion in the bank's Cayman Islands branch (WikiLeaks.org).

*2008: Anonymous Hacktivism on the Global Stage*

Julius Baer immediately filed a lawsuit against WikiLeaks, marking the first legal action taken against the website, excluding a previous case in which WikiLeaks was banned in China (WikiLeaks.org). As a result of the legal injunction, Dynadot, the server hosting WikiLeaks' website, was forced to remove the website until the lawsuit was dropped on March 8, 2008 (WikiLeaks.org).

Meanwhile, Anonymous was beginning its first foray into coordinated political action. Dubbed Project Chanology (a portmanteau of 4Chan and Scientology), the first Anonymous operation was a reaction to the Church of Scientology's attempt to remove an interview with Tom Cruise from the Internet (**http://news.cnet.com/8301-10789_3-9857666-57.html**). The project heralded the beginnings of what are now common Anonymous tactics: declarations and press releases regarding the coming operation and threatening retaliation to the target, mass horizontally-organized action facilitated by anonymous Internet Relay Chat (IRC) message boards, videos posted to anonymous YouTube accounts describing the project, and a coordinated

use of DDoS attacks. Most notably, Project Chanology saw the introduction of LOIC, Anonymous' DDoS coordination tool of choice, as a user-friendly program allowing individuals to volunteer their computers to be used as part of planned DDoS raids **(Sauter ???)**. LOIC varies markedly from the EDT's FloodNet tool; the differences will be elaborated upon later.

As a result of Project Chanology, two members of Anonymous were arrested. Dmitriy Guzner, a 19-year-old hacker from New Jersey, became the first member of Anonymous to be arrested and charged with crimes under the CFAA. In May 2009, Guzner plead guilty to charges that he illegally hacked the Church of Scientology's website and was sentenced to 366 days in federal prison and a fine of $37,500 (**http://www.huffingtonpost.com/2009/11/18/dmitriy-guzner-teen-sente_n_362713.html**). Brian Thomas Mettenbrink, another Anonymous member involved in Operation Chanology, was likewise sentenced to one year in prison and a fine of $20,000 (**http://www.theregister.co.uk/2010/05/25/second_scientology_ddoser_jailed**/).

By early 2008, both groups had established their modus operandi for engaging in cyber activism. WikiLeaks would publish information it saw as relevant to the populace regardless, or perhaps because of its negative impact on the institution it targeted. Its whistleblowers' identities would be protected, to the point that those in WikiLeaks did not know where the leaks came from (**WikiLeaks.org**), its journalists and volunteers would remain anonymous to the outside, and its headquarters and web server would remain unfixed and easily duplicable. Anonymous cemented itself as a mass mobilization of anonymous individuals with varying degrees of computer expertise, with no central command or leadership. Their branded use of the Guy Fawkes mask as a symbol of their members' perpetual anonymity became solidified, as did their use of LOIC for DDoS attacks. Furthermore, by 2008 both groups had coalesced into allies in a definitive social movement. Internet activism became synonymous with the ideology of freedom

of information and transparency, and both Anonymous and WikiLeaks used activism on the Internet to further their activism on behalf of these goals.

2008 also marked the most recent series of amendments to the CFAA. The 2008 amendments greatly expanded the scope of the CFAA and allowed for the prosecution of a much greater number of domestic computer crimes. Requirements that attacks be carried out across state or national lines were eliminated, as was the previous requirement that more than $5,000 in damages must have resulted from the attacks for the crimes to be prosecuted (**OLE 2**). Whether or not these changes were a reaction to the growing influence of hacktivist groups remains unknown, however the increase in the government's ability to prosecute computer crime had a substantial impact on further retaliations to hacktivist groups.

Thus, in the 20 years between the WANK worm and Chanology and Julius Baer, hacktivism has grown and changed dramatically. What started as a tactic for political advocacy in a new and barely understood Internet morphed into a strategy and finally an ideology. While EDT, cDc and Hacktivismo used hacktivism as a tool for a variety of political causes, the modern wave of hacktivism begun with Anonymous and WikiLeaks shows the beginnings of a true social movement using subversive Internet tactics to advocate for freedom of information and institutional transparency. The two groups were also the first of their kind to make anonymity a key to their identities. While the laws on the books caught up with the shifting patterns of subversion on the Internet in 2008, what I have dubbed the "crackdown" on hacktivism had not yet begun.

## V. 2010: Cablegate, Payback, and a New Precedent Set

While WikiLeaks and Anonymous may have made names for themselves in 2008, it was

2010 that marked a turning point in the way these two groups were treated by the U.S. government. For WikiLeaks, 2010 saw the release of their biggest disclosures of classified information to date (and the biggest in history). It also saw an unprecedented retaliatory response on the part of the U.S. government that crippled the organization's ability to function and dealt more harshly with whistleblowing than U.S. history had ever seen. For Anonymous, the retaliation to operations conducted in 2010 turned over a new era in equally unprecedented treatment of hacktivists in the criminal justice system. The convictions of and charges against Anonymous actors after 2010 dwarfed those of Guzner and Mettenbrink. The arrests of Anonymous members signified a marked campaign by the FBI against Anonymous as a whole, rather than a sporadic attempt to punish a few lawbreakers. The crackdown on hacktivism begun in 2010 fundamentally redefined how the Internet could be used as an activist space.

On April 5, 2010, WikiLeaks released *Collateral Murder*, a classified US military video showing a 2007 air strike in Baghdad in which American soldiers fired on civilians, many of whom were unarmed, and killed two Reuters reporters (**http://www.collateralmurder.com/**). Chelsea Manning (then Bradley Manning), an Army private, was arrested on May 26 under suspicion of leaking the video to WikiLeaks after she claimed responsibility for the leak on an online message board (**http://www.wired.com/threatlevel/2010/06/manning-detainment/**). Also included in Manning's dump of information to WikiLeaks were the Afghan War Diaries (released on July 26), the Iraq War Logs (released on October 22), and the "Cablegate" U.S. Diplomatic Cables (released on November 28).

After the Cablegate incident, the United States government[2] launched a massive

[2] I say that the U.S. government as an undefined body was behind the retaliation because pressure on WikiLeaks (and Anonymous as well) came from a variety of government sectors, many of whom operated behind closed doors whose involvement is not fully understood. These include but are not limited to: President Obama, the Secretaries of State and Defense, the FBI, the CIA, the NSA, and

campaign against WikiLeaks. The WikiLeaks website was DDoSed and taken offline by an attacker whose identity remains unknown, however "the scale and sophistication of the attack points to a state sponsor" (**Zajacz, 497-8**). Under pressure from the U.S. government, WikiLeaks' domain name provider dropped the website, its web hosting service stopped allowing access to the site, and numerous banks and credit card companies refused to process donations (**Zajacz, 496**). WikiLeaks managed to get back online fairly quickly, though the banking blockade crippled WikiLeaks' funds (**wikileaks.org**). WikiLeaks maintains that the attack on their entire website amounted to an unconstitutional "prior restraint" by the U.S. government, and many have criticized the informal pressures exerted by the U.S. government as an attempt to skirt around the Constitution (**Benkler, 2011; Elias, AP, 2008**). In addition to the WikiLeaks website, Julian Assange found himself in a legal battle as Interpol attempted to extradite him to Sweden on rape charges barely a week after the diplomatic cables were published (Benkler, 2011). Some within the U.K. government have speculated that Assange was framed in apparent retaliation for the leaks, though whether or not this is true remains unknown (**http://www.telegraph.co.uk/news/uknews/10070597/GCHQ-staff-scolded-over-emails-claiming-Julian-Assange-was-framed.html**). In either case, it forced Assange into house arrest at the Ecuadorian Embassy in London and greatly diminished his ability to organize WikiLeaks.

In retaliation to the banking blockade against WikiLeaks, Anonymous entered the fray in December 2010 and began Operation Avenge Assange (**Sauter 991**)**.** Prior to coming to WikiLeaks' aid, Anonymous had been involved in Operation Payback, a campaign to target and DDoS websites of groups and organizations that supported copyright law and led to the 2010 DDoS campaign against the torrenting website The Pirate Bay (**Sauter 991**)**.** Operation Avenge

---

Senator Joseph Lieberman. Furthermore, in discussing the impact of anonymity on the state, it is the state apparatus as a whole, rather than a specific section of the government, that is threatened.

Assange DDoSed numerous websites Anonymous deemed culpable, including those of senator Joseph Lieberman (who had been instrumental in pressuring for the banking blockade), MasterCard, Visa, PayPal, and Amazon.com (**Pegoraro, Wash Post; Sauter 991**).

Following Operation Payback, Anonymous underwent a similar set of counter-attacks both on its websites and online infrastructure and its members. Citing pressure from the FBI, Anonymous' web hosts removed their servers, causing their websites to be unusable (**Mansfield-Devine, 7).** Its Twitter and YouTube accounts were likewise booted, and Anonymous was forced to scramble to put itself back online. New accounts continued to crop up, but the game of cyber whack-a-mole ultimately distracted Anonymous' resources from focusing on future attacks (**Mansfield-Devine, 7).** Additionally, fourteen Anonymous members were arrested for their involvement in Operation Payback, allegedly picked arbitrarily from a list of over one thousand participants (SOURCE?). The FBI issued an additional 21 search warrants in connection with attacks on PayPal (**Haag**). The so-called Paypal 14 may serve up to five years in federal prison on charges of conspiracy, and an additional ten years on charges of damaging a protected computer under the CFAA (**http://uk.reuters.com/article/2011/07/19/us-usa-fbi-hacking-idUKTRE76I4E320110719; http://freejeremy.net/prisoner-solidarity/paypal-14/**). As of the writing of this paper, the PayPal 14 still await sentencing.

Yet the PayPal 14 were not the only targets of the crackdown on Anonymous. On June 7, 2011, a key Anonymous member known as Sabu (real name, Hector Monsegur) was arrested by the FBI. He faced up to 124 years in prison for his actions with Anonymous and LulzSec (an anonymous spin-off different more in name than in character from Anonymous).[3] The next day,

[3] LulzSec, an abbreviation of Lulz Security, has been called a spin-off group from Anonymous. LulzSec was active during much of 2011 and 2012, and has claimed responsibility for numerous high-profile hacktivist actions. LulzSec and Anonymous were nominally different entities for a time, to the extent that either of these groups can be thought of as entities given their amorphous and transitory natures.

Monsegur was released on bail, under the condition that he become an informant for the FBI (**Olson, 388**). Monsegur continued to be a popular voice in Anonymous, and facilitated the coordination of several more attacks **(Olson, 390)**. Numerous arrests were made of other Anonymous members as a result.

Among these was Jeremy Hammond, a computer programmer from Chicago, who was arrested in March 2012 for his involvement with Anonymous. Hammond leaked information from the private intelligence firm Stratfor, which supporters of Hammond claim "revealed that Stratfor had been spying on human rights activists at the behest of corporations and the U.S. government" (**http://freejeremy.net/who-is-jeremy-hammond/**). Hammond was sentenced to ten years in federal prison on November 15, 2013.

In September 2012, Barrett Brown, a journalist and self-proclaimed Anonymous spokesperson, was also arrested for his connections to Anonymous. Brown has not been sentenced yet, though he has already spent more than a year in jail. If convicted, he could face up to 105 years in federal prison (**http://www.rollingstone.com/culture/news/barrett-brown-faces-105-years-in-jail-20130905**). After his arrest, Brown attested that the FBI's arrests of Sabu, Hammond and others amounted to Anonymous' "de facto leadership" (**http://www.businessweek.com/articles/2012-03-08/barrett-brown-on-the-arrests-of-five-of-anonymouss-hackers**). In the same interview, Brown noted that the FBI's crackdown on Anonymous was unprecedented compared to their treatment of the group in the past (**http://www.businessweek.com/articles/2012-03-08/barrett-brown-on-the-arrests-of-five-of-anonymouss-hackers).**

The FBI's retaliation against Anonymous began a new way of dealing with hacktivists

---

However, as both groups' tactics and members were essentially the same, the differentiation is somewhat moot. As far as my research into the matter has shown, LulzSec was essentially a sub-sect of Anonymous whose members were particularly loyal to Sabu.

through a practice of targeting and attempting to destroy the entire group. After the arrest of Sabu, Brown and others, the FBI declared "victory" over Anonymous, claiming they had rendered the collective unable to carry out further operations (**Boone, Anonymous to FBI, 1**). The key members, according to Brown, had been put behind bars. Additionally, the FBI believed that the exposure of Sabu as an informant "bred fear and distrust within Anonymous, deterring hackers from continuing with their operations" (**Boone, Anonymous to FBI, 1**). The goal in the FBI's dealings with Anonymous was clearly to destroy the entire organization by destroying their loose leadership structure and by inflicting such harsh punishments on captured members so as to deter others from engaging.

The attempts to destroy the entire organization's ability to mobilize did not begin until after Operation Payback. Prior to this, the FBI showed tactics of simply holding hacktivists responsible for their particular illegal actions. Even more so, the retaliations against Anonymous as a whole showed a marked difference from the way the FBI had dealt with hacktivism in the past. Despite their similar use of illegal hacking for political purposes, no member of cDc or Hacktivismo was ever arrested, though the openness with which the groups shared their member lists would have made them easy to track down (**Riga, Andy. The Gazette. Feb. 3, 1999**). Likewise, the worst punishment inflicted on those who participated in Electronic Disturbance Theater's DDoS attacks was a temporary crashing of their computer system, but no jail time (**McKenzie, on EDT, 1999**). Clearly, there was something about Anonymous that law enforcement found significantly more threatening than previous iterations of hacktivism.

Anonymous was not alone in facing a new threat to their existence. On August 21, 2013, Chelsea Manning was sentenced to 35 years in federal prison, having been convicted of 17 charges under the CFAA and Espionage Act. Manning's sentence was the longest sentence ever

imposed upon a whistleblower in U.S. history which many feel has fundamentally changed the legal landscape for whistleblowers in the U.S. (**NYTimes Editorial; McAskill, the Guardian**). Manning's punishment was a far cry from the treatment previously given to whistleblowers, such as Daniel Ellsberg, the whistleblower behind the release of the Pentagon Papers in 1971. Ellsberg was also charged under the Espionage Act, but all charges against him were later dropped (**NYTimes Archive – Pentagon Papers).** Additionally, Manning's sentence is distinct from that of Thomas Drake, an NSA whistleblower who criticized the NSA's Trailblazer project to the New Yorker in 2011. Drake was similarly charged under the Espionage Act, but the charges against him were dropped (**http://america.aljazeera.com/articles/2013/12/5/jailed-whistleblowerstoedwardsnowdendonatcomehome.html**).

Between the retaliation against the WikiLeaks website itself and the disproportional punishment of Chelsea Manning compared to other whistleblowers, a clear difference in government policy towards whistleblowing can be seen. Likewise, the intensity of the FBI's crackdown on Anonymous began a distinctly different treatment of hacktivism. When the cases of the two groups are taken together, one can clearly see a new precedent being set for how the U.S. government deals with Internet activism, from the inklings of a shift in 2008 to a full-blown crackdown after 2010.

## VI. Hacktivists as Cyberterrorists: Breaking Down the Argument

The harsh treatment of hacktivists would be understandable if their actions posed a new and serious threat to national security. As such, the groups would be considered cyberterrorists, using unprecedented tactics to bring harm to the United States, and would therefore require unprecedented reprisals to prevent against future harmful actions.

Embedded in this argument are two separate claims. The first is that the actions of WikiLeaks and Anonymous presented a serious threat to national security. For the claim to be true, assets important to the United States must have been directly compromised in a serious and meaningful way by the actions taken by these groups. The second is that these groups presented a *new* threat, unlike any previous threat, and as such must be dealt with in an unprecedented fashion. For this claim to be true, it must be proven that these groups' *actions*, not the groups themselves, were unlike those of other groups before them. I argue that both of these claims are resoundingly untrue. Neither WikiLeaks nor Anonymous ever posed a serious threat to national security, nor were their *actions* novel or unique compared to other hacktivist actions.

*Threats to National Security*

When Italian Foreign Minister Franco Frattini likened the WikiLeaks diplomatic cables to September 11th, he echoed a common assertion made by many in the U.S. government prior to the release of the cables. As Secretary of State, Hilary Clinton warned that WikiLeaks "puts people's lives in danger, threatens our national security and undermines our efforts to work with other countries" (**Jackson, USA Today, 2010**). Manning herself was criticized for not realizing that her disclosures to WikiLeaks would be of interest to terrorist organizations who could benefit from the new information about the government (**Tate, Londono, Washington Post**). While the most serious claims of damage to national security were levied against WikiLeaks, Anonymous undertook its fair share of fire as well. NSA director Keith Alexander argued that the group could soon orchestrate a widespread power outage through a cyber attack, and in 2011 the U.S. Department of Homeland Security released an official warning about Anonymous (**Benkler, Hacks of Valor, Foreign Affairs, 2012**).

Despite these claims, the damage inflicted by both of these groups turned out to be

minimal. The WikiLeaks diplomatic cables were certainly an embarrassment, but like the Afghan and Iraq war logs before them, no real harm was done to national security. On the subject of the Afghan War Diaries, President Obama himself said that the WikiLeaks releases "don't reveal any issues that haven't already informed our public debate" (**Obama, speaking in the Rose Garden, July 27, 2010**)**.** No lives were put in danger as a direct result of the WikiLeaks Afghanistan or Iraq releases (**Christian Science Monitor, Oct. 27, 2010**). While the Cablegate release was certainly embarrassing to U.S. diplomats, Defense Secretary Robert Gates reported that the cables did not have a big impact on U.S. assets (**VOA News, Nov. 30, 2010**). Notably, Manning was not convicted of the most serious charge levied against her – aiding the enemy – showing that the charge that her leaks had seriously endangered U.S. national interest could not be proven (**http://articles.washingtonpost.com/2013-08-21/world/41431547_1_bradley-manning-david-coombs-pretrial-confinement**). Likewise, the actions undertaken by Anonymous during 2010 and 2011 similarly posed no serious threat to national security. Anonymous' tool of choice, DDoS attacks against websites, is unsophisticated in terms of cyber attacks (**Shahani, Al Jazeera America, 2013**). While many of the sites Anonymous targeted experienced downtime, their entire Operation Payback campaign mounted to "little more than an irritation" (**Mansfield-Devine, 9**). The kind of cyber attacks that Alexander warned against never occurred. On the whole, U.S. national security was not threatened by the actions undertaken by hacktivists in 2010.

Despite the lack of damage inflicted by hacktivist actions so far, the terrorist argument also hinges on the potential for these groups to become more serious threats in the future. The threat of a cyber-Pearl Harbor might likewise account for the crackdown. Yet despite this fear, many in the academic community studying cyberterrorism believe that the threat is overblown,

and that "Pearl Harbor-type cyber attacks don't happen outside terrible Bruce Willis movies" (**http://www.washingtonpost.com/blogs/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/**). At best, the belief in the threat of a cyber-Pearl Harbor coming from hacktivist groups is misguided. The goals of WikiLeaks and Anonymous have been clearly shown to center around freedom of information and institutional transparency. These are political organizations, not Internet militias. Hacktivist groups aim to cause "disruption, not destruction" (**Benkler, 2012**). Launching a full-scale cyberterror attack to destroy U.S. government assets would do nothing to further their goals.

Furthermore, the way that the U.S. government responded to these groups' actions did not show a specific concern for national security. In response to claims that the diplomatic cables would put lives at risk, WikiLeaks requested more information about the individuals in question to aid in targeted redactions of the documents. These requests were denied (**Chiacu, Reuters, 2010 (possibly find better article for this)**). The unprecedented sentence to be served by Chelsea Manning, along with the U.S. government pressuring credit card companies to ensure WikiLeaks' finances were crippled, shows the U.S. government taking an offensive, rather than defensive, strategy. Likewise, the targeted arrests of Anonymous show a marked attempt to disrupt the entire organization, rather than to protect specifically against a massive cyber attack. Clearly, national security was not the only priority.

*A New Breed?*

The second claim made by the argument that hacktivistm amounts to a new breed of cyber threat must likewise be put to scrutiny. The newness of these groups' actions would make an unprecedented response understandable. However, just as neither group posed a serious threat to national security, so too did they not engage in new actions outside the existing repertoires of

online contentious politics.

While Anonymous occasionally uses multiple tactics such as information theft and website defacement, by far its most commonly used method of action is the DDoS attack. DDoS is nothing new. As previously mentioned, DDoS' historical use in hacktivism dates back to 1994. Likewise, Anonymous' use of mass organized DDoS tools such as LOIC is similarly not new, as EDT made its FloodNet tool famous in hacktivism as early as 1998. Anonymous' tactics were the most recent iteration of a long history of hacktivist contentious politics, and their innovations in tactics and tools were "incremental" (**Sauter, 988**). Anonymous has faced unprecedented reprisals for its actions compared to all previous hacktivist groups, yet its actions are not unique.

The tactic of whistleblowers leaking classified information to inform the public and bring about social change is nothing the U.S. has not seen before. WikiLeaks has certainly tried to make itself seem novel. It boasts on its website that it "has released more classified intelligence documents than the rest of the world press combined" (**WikiLeaks.org**). However, the difference between WikiLeaks' information and the information provided by previous whistleblowers is one of quantity, not quality. The Afghan War Diaries have been likened to simply a newer version of the Pentagon Papers, chronicling a different war (**http://www.pbs.org/pov/mostdangerousman/legacy.php**). Yet some within the press have argued that the distinct differences between the Afghan War Logs and the Pentagon Papers prove that WikiLeaks' releases are far more dangerous and reckless than previous leaks.

The qualitative distinction often levied against WikiLeaks is that, unlike traditional whistleblowing through the news media, WikiLeaks has no oversight to ensure that its releases do not endanger lives. While a more traditional press would comb through the documents to ensure that no lives were put at risk, and in essence act as "gatekeepers," with the advent of

WikiLeaks, "there are no gates" (**Greenfield, CBS, 2010**). This has been shown to be untrue. In releasing the Afghan War Logs, WikiLeaks withheld 15,000 of 91,000 documents to ensure further review and appropriate redaction of any information that could endanger lives (**http://online.wsj.com/news/articles/SB10001424052748704407804575425900461793766**). As previously stated, no lives have been lost as a direct result of the WikiLeaks cables. WikiLeaks has proven itself to be no more reckless than the traditional press in its release of classified information.

WikiLeaks and Anonymous have been shown not to be serious threats to national security. The actions they have undertaken have not been unprecedented. Furthermore, it is incredibly unlikely that either group would endeavor to engage in a cyber-Pearl Harbor that would legitimately damage national security. Therefore, the idea that these groups' actions have resulted in a new and unique cyberterrorist threats to national security is unfounded.

**VII. Hacktivist Anonymity: A New Threat to Sovereignty**

It is not the actions of WikiLeaks and Anonymous that are perceived to be a threat: it is their nature as anonymous organizations. Their anonymity poses a danger to national sovereignty rather than national security. While the potential impact of Internet anonymity on national sovereignty has been debated for decades, the central use of anonymity in hacktivism is a new phenomenon that began with WikiLeaks and Anonymous. Since 2008, there has been a growing recognition on the part of the United States government that these groups' anonymity poses a unique threat by creating an activist space outside the state's control. This recognition crystallized into a concerted crackdown on hacktivism in 2010, the goal of which has been to remove anonymity from Internet activism and destroy anonymous hacktivist networks entirely.

On the one hand, anonymity can be crucial to democracy by allowing the Internet to become a free commons of debate and expression. Curran and Gibson (2013) view anonymity as instrumental in creating an anarchic space on the Internet, though they see this anarchism as a positive movement towards social emancipation. Anonymity creates what Curran and Gibson have called "crypto-anarchism," using anonymous organization as a tool to "allow for the eventual triumph of individual freedom over state-sanctioned violence and domination" (**Curran and Gibson, 306**). The furthering of anonymity-enhancing technologies in Internet activism is crucial to allowing for the realization of this democratic potential (**Curran and Gibson, 307**). Anonymity on the Internet creates a space for true democracy to flourish without the fear of reprisal.

On the other hand, the anarchism of the Internet can pose a critical threat to state sovereignty. Anonymity of a population means that law and order cannot be enforced. In removing a person's definable identity and locatability, behavior cannot be regulated by the state (**Zajacz, 492**). Crypto-anarchism may herald a new era of true democracy, but its inability to be checked by the state is anathema to the entire idea of state sovereignty. Regardless of any national security threat, truly anonymous political activism poses an existential threat to the state itself by creating a space where state power is null and void.

This is the point of the Guy Fawkes effect: hacktivist groups represent masses of uncontrollable people whose behavior cannot be confined under the existing rules for exerting state dominance. The Internet provides a space for mass anonymous mobilization to organize, and hence poses a new threat to state sovereignty. However, while the potential for anonymous mobilization has existed since the formation of the World Wide Web in 1989, it was not until Anonymous and WikiLeaks rose as political activist networks that that potential was realized.

Anonymous differed significantly from earlier hacktivist groups in its emphasis on anonymity. Groups such as EDT and the Electrohippies participated in similar kinds of attacks to Anonymous – such as DDoS and website defacement – but did not do so behind the mask of Anonymity (Sauter, 989). Rather, these groups believed in a "radical transparency" wherein their true identities would be openly tied to their online actions **(CNET: http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/)** These groups had clear leaders whose real identities were widely known. By contrast, Anonymous has no centralized leadership or organized structure. Its members go to great lengths to keep their identities hidden, and each of Anonymous' new operations are launched via a random and horizontal series of conversations in anonymous IRC channels (**Mansfield-Devine, 5**). While tools such as LOIC turned out to be easily traceable, the intent on the part of Anonymous' members was always to maintain their anonymity. Having learned from the arrests of Anonymous members linked back to the use of LOIC for DDoS attacks, Anonymous members have begun to take greater precautions in hiding their identities from authorities (**Mansfield-Devine, 7**). Despite these shortcomings, the emphasis on anonymity is clear right down to the group's name: Anonymous.

While its founders' identities are now known the world over, WikiLeaks has similarly created a new kind of activism bound by anonymity. WikiLeaks' anonymous online drop-box was a unique and new invention that allowed users to submit information without the possibility of their identities being traced (**Zajacz, 492**). Those who leak information to WikiLeaks are so well-hidden through WikiLeaks' layers of onion routing[4] and encryptions that even WikiLeaks'

[4] Onion routing is a popular and highly effective method for encrypting online communications. Messages are encrypted in layers upon layers of data that must be unpeeled like an onion. Onion routing is important because it allows messages to be passed between parties in a way that no intermediaries would be able to discern the message's origin, destination or content.

editors do not know the true identities of their leaks (**Cammaerts, 423**). It was not until Chelsea Manning declared herself responsible for giving WikiLeaks the Collateral Murder video and other information that those within WikiLeaks knew who she was (**Cammaerts, 423**). Additionally, WikiLeaks' lack of a physical headquarters puts it outside any state's sphere of influence. It lacks territoriality, and hence the ability for territorial laws to be exerted over it (**Zajacz, 494**). While WikiLeaks centers its actions around a long-used tool of subversion (leaking classified information), it was novel in its focus on maintaining absolute anonymity for its sources.

WikiLeaks and Anonymous heralded a new era of anonymous hacktivism that posed an existential threat to state sovereignty. Anonymous' use of DDoS attacks has been likened to a more extensive virtual sit-in, as an Internet space is rendered inaccessible through protesters flooding it with their own traffic (**Sauter, 984**). However, as DDoSing is done anonymously, the risks posed that would ordinarily prevent a person from engaging in a physical sit-in (such as bodily harm and arrest) are not present **(CNET: http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line/)**. Anonymity changes the game. When there is no fear of reprisal, activists can engage in unchecked civil disobedience. Likewise, WikiLeaks' anonymity creates a method of "indestructible publishing" where sources cannot be traced and intimidated, and content cannot be removed (**Zajacz, 490**). Due to its lack of territoriality, the Internet as a whole cannot be controlled by a single retaliatory action; Internet content can be duplicated and mirrored across websites, and thus any attempt to remove WikiLeaks' content would mean an attempt to "dismantle the Internet itself" (**Zajacz, 491**). Both groups have used the Internet's inherent anonymous capabilities in a new way that makes them virtually impossible to for the U.S. government to regulate.

Because the U.S. government cannot exert influence over the Internet as a whole, it has turned to a system of cracking down on individuals found to be members of anonymous hacktivist networks who live within its territory. By regulating what Rita Zajacz (2013) dubs "intermediaries," the U.S. has been able to exert control over average Internet users and circumvent the Internet's anarchic potential (**Zajacz, 491**). In this case, the actions taken by the U.S. to target website hosts, companies that process donations, and group leaders shows an attempt to control average users by controlling intermediaries. The banking blockade against WikiLeaks crippled its finances, while the severity of Chelsea Manning's sentence acted as a warning to others that leaking to WikiLeaks would bring dire consequences. Likewise, the "whack-a-mole" style shutdown of Anonymous' myriad of online locations compromised the group's ability to organize effectively, and the severity of the punishments inflicted on identified Anonymous members acted as a deterrent to discourage others from joining the group. Thus, the U.S. government made a concerted effort to stop the ability of anonymous organizations to function by disciplining the portions of the groups that could be identified, located, and controlled.

In the crystallization of these groups into anonymous activist movements online, the anonymous, and hence anarchic potential of the Internet was realized. The Internet's ability to act as an anarchic space posed a serious threat to the sovereignty of the U.S. government. When political action can be taken against the state without fear of reprisal, the state's power is diminished. However, it has already been shown that neither of these groups posed a legitimate threat to national security. Rather, WikiLeaks and Anonymous acted fulfillments of the emancipatory potential of the Internet, but were wrongfully perceived as a threat. Whether the crackdown on hacktivism represents a noble but misguided attempt to reduce the threat of

cyberterrorism, or a more sinister targeting of legitimate protest remains to be seen.

## VIII. Conclusions

It is the threat of anonymous mobilization on the Internet, rather than the specific actions taken by WikiLeaks and Anonymous, that caused the U.S. government to crack down on these groups. The treatment of hacktivism before and after WikiLeaks and Anonymous became globally notorious in 2010 shows a concerted effort to change the precedent for dealing with hacktivism in the U.S. The U.S. government apparatus showed a clear attempt to eliminate these groups as a whole, in keeping with a broader attempt to wipe out anonymity on the Internet. Certainly, the efforts to hinder Anonymous and WikiLeaks have proved at least partially successful.

Many of Anonymous' core organizers have now been imprisoned. Despite the group's horizontal and amorphous structure, the incapacitation of these de facto leaders is certainly a blow. The revelation that Sabu was an FBI informant struck fear into the group, and Anonymous has made a conscious effort as of late to ensure its members are capable of preserving their anonymity. Anonymous vows it will continue its struggle, but to this day there have been no Anonymous operations on the scale of Operation Payback (**Boone, Global Post, Aug. 21, 2013**). Anonymous is not yet defunct, but at the same time it does not possess the influence that it did at the high point of Operation Payback. What becomes of the PayPal 14 may change its actions in the future and decide once and for all whether Anonymous is here to stay.

WikiLeaks too has been noticeably weakened by the retaliation it faced after 2010. Though the WikiLeaks website is up and running, it has released few important leaks in recent years. The anonymous online submission platform is inaccessible from most Internet browsers

(**WikiLeaks.fdn.fr**). Assange's house arrest at the Ecuadorian Embassy in London has hindered his ability to mobilize the group as a whole, as have the internal struggles that led to the departure of WikiLeaks second-in-command Daniel Domscheit-Berg in 2011. However, WikiLeaks released a classified portion of the Trans-Pacific Partnership Agreement (TPP) as recently as November 2013 (**WikiLeaks.org**). The controversial act is still under negotiation, but WikiLeaks' revelations of the treaty's Intellectual Property Rights chapter has sparked widespread public debate and opposition to the agreement. The importance of the TPP release on the one hand shows WikiLeaks' renewed power, though with Assange under house arrest and anonymous online submission still impossible, WikiLeaks has not yet returned to its former glory.

The extent to which anonymity has been removed from the Internet certainly can be debated as well. Edward Snowden's leak of the PRISM program in June 2013 showed a history of the NSA collecting individuals' data directly from the websites and services they frequently use (such as Microsoft, Apple, Google, Yahoo!, Facebook, YouTube, and Skype) dating back to 2007 (**The Guardian, PRISM**). The extent of NSA surveillance over both domestic and foreign users on these platforms is still being discovered. Reports from December 2013 show that U.S. intelligence agencies have begun trying to collect data on what they believe to be potential "terrorist or criminal networks" operating in online role-playing games (**http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html?ref=international-home**). As Snowden's releases continue to be disclosed, it seems the web of de-anonymizing the Internet is only being cast wider.

While the World Wide Web may have been around since 1989, the rules of engagement on the Internet are still being decided upon. PRISM, the TPP, and proposed amendments to the

CFAA will all have an effect on what the Internet becomes. Anonymous hacktivsm may prove to be an easily subdued blip or the new wave of political contention for the next several decades. Anonymity on the Internet can be both threatening and emancipating, and both sides have been thoroughly debated. Whether it should be eliminated altogether is likewise a question that the public has yet to answer.

It is my personal opinion that anonymity on the Internet should be protected. I believe that anonymous hacktivism is crucial to checking state power in a new political space whose rules are as yet undefined. I hope that future laws governing Internet action take into consideration the political motivations behind hacktivism, and open up the Internet more to a sphere for political contention. As human society as a whole becomes embedded in the Internet, so too will political activism. Hacktivism is a natural extension of political activism, and should receive the same protections as more traditional forms of demonstration. I have argued that WikiLeaks and Anonymous do not pose a threat to national security. Despite the current dubious legality of their tactics, their goal is to serve the public good. As such, the retaliation against them sets a precedent that is both disturbing and antithetical to human rights to free speech, assembly and expression.