

Introduction

In the last few years WikiLeaks has enjoyed considerable amount of attention from the press, as well as from the academia. Whilst the press concentrated mainly on the portrayal of Julian Assange -either as a villain or a misunderstood nerd hero- scholars have analyzed WikiLeaks as a phenomenon relating to a new form of journalism enabled by the Internet (Benkler, 2011). What is generally overlooked in these academic discussions is the vast amount of support WikiLeaks and Julian Assange have received from those Internet users, who associate themselves with the “hacker ethic”.

The relationship between Anonymous and WikiLeaks manifested itself in December 2010, when WikiLeaks came under intense pressure to stop publishing secret United States diplomatic cables. In order to force the organization to stop their activities, companies such as Amazon, PayPal, BankAmerica, MasterCard and Visa either stopped working with or froze donations to WikiLeaks (Wikipedia, 2010).

Although, WikiLeaks was supported within communities where Anonymous users emerged from (4chan, reddit..etc.) their support never manifested itself until these corporations stopped offering their services to WikiLeaks. In December 2010 Anonymous organized Operation Payback: Avenge Assange and launched Distributed Denial of Service (DDoS) attacks against these corporations in their support for WikiLeaks.

The Operation Payback: Avenge Assange members used IRC channels to manage communications and Facebook and Twitter have also been widely used to coordinate the attacks (P2Pnet, 2010), but the latter two suspended the accounts of Operation Payback (Forbes, 2010). However, further Twitter accounts were established and widely used later on.

Operation Avenge Assange

"The first serious infowar is now engaged.
The field of battle is WikiLeaks.
You are the troops."
- John Perry Barlow

Julian Assange defies everything we hold dear. He despises and fights censorship constantly, is possibly the most successful international troll of all time, and doesn't afraid of fucking anything (not even the US government).

Now, Julian is the prime focus of a global manhunt. In both the physical and virtual realms. Governments across the world are baying for his blood, politicians are up in arms about his recent leak, and even his own country has abandoned him to the wolves. Online, WikiLeaks is a focus of mass DDoS attacks, legislation and downright pandering to the corrupt incumbents which would silence this man.



Therefore, Anonymous has a chance to kick back for Julian. We have a chance to fight the oppressive future which looms ahead. We have a chance to fight in the first infowar ever fought.

1. Paypal is the enemy. DDoS'es will be planned, but in the meantime, boycott everything. Encourage friends and family to do so as well.

2. Spread the current leaked cables as much as possible. Save them to hard drives, distribute them on CD's, mirror them to websites and seed them on torrents. The end goal is a human DNS - something that can only be stopped by shutting off the entire internet.

3. Upvote Julian on the Times 2010 Person of the Year. While this might not aid his cause, it will get him much needed public exposure. (<http://tinyurl.com/2wb7ju8>)

4. Get vocal! Twitter, Myspace, Facebook and other social networking sites are critical hubs of information distribution. Make sure everyone you know is aware of what is happening. If you can convince just one person to tell one other person every day, the spread of info will be exponential.

5. If you're up for it, print out cables which are relevant to your area and distribute them. Post them on bus stops, train stations, street lamps. Be creative and catch people's attention. Using graffiti to spread the WikiLeaks website is also a great idea.

6. Complain to your local MP, mayor, or whichever political figure you can contact. Ask him for comments about the leaks. Record every word that is said.

7. Protest! Organise community marches, send around petitions, get active. This cannot happen without numbers.



TL;DR:
Protest.
Inform.
Enquire.
Fight.



The future of the internet hangs in the balance
We are Anonymous.
We do not forgive; we do not forget.
Expect Us.

Figure 1.: Flyer for Operation Payback: Avenge Assange, 2010

The Operation Avenge Assange flyer, retrieved from an IRC discussion, summarizes the movement's goals (see Figure 1.): 1.) DDoS, 2.) Spreading the cables, 3.) Voting for Julian Assange on the Times 2010 Person of the Year, 4.) Spreading information on Twitter, Myspace, Facebook and other social networking sites, 5.) Printing out and distributing cables, 6.) Complaining to local political figures, and 7.) Protesting.

It is evident from the flyer for the Avenge Assange operation that Anonymous wanted to concern itself with launching DDoS attacks on the companies who actively do not support WikiLeaks, as well as the distribution and analysis of the released cables. However, most of the attention shifted from the latter to the former and a new movement named Operation:Leakspin was conceived for the purpose of sorting through WikiLeaks releases to identify and raise awareness of potentially important and previously overlooked cables (Wikipedia, 2010).

**Gentlemen,
we have, at best, given them a black eye.
The game has changed. When the game changes,
so too MUST our strategies.**

OPERATION: LEAKSPIN

**Begin searching through Wikileaks.
Find only the best, least exposed leaks
you can get your hands on. Post summaries of them, along with
the complete source. Encourage the reader to read more.
Make one-to-two minute YouTube videos reading the leaks.
Use misleading tags, everything from "Tea Party" to "Bieber".
Post snippets of the leaks EVERYWHERE. News comments, fan forums, etc.**

They don't fear the LOIC.



**They fear exposure.
The fun begins, at 9:00 P.M. EST**

ROFL101

Figure 2.: Flyer for Operation:Leakspin, 2010

It is hard to ascertain how much support Operation Leakspin has garnered in the Anonymous community and what its status is at the time of writing this paper; a year after the operations in support of WikiLeaks were launched. Whilst DDoS attacks against the corporations seem to have ceased, there still are cables that haven't been analyzed yet (ABS-CBN news, 2011).

The organizational characteristics of Anonymous is one that we have not seen so explicitly played out until now. Anonymous, at its core, is the collective

Internet behind the same non-name, there are no central entities, it is decentralized and there is no single group working towards one goal, it consists of multiple “operations” running simultaneously (Davies, 2008). Each of these characteristics in Anonymous poses a new interpretation of not only online activism and hacktivism but also of online communities.

This study relies on data gathered from IRC and Twitter during and after Operation Payback was launched. It begins by looking into the importance of data in Internet research and introduces the data sets used in this thesis. The paper goes on to look into the structure of communication within the IRC channels and Twitter, asking questions such as: Who is dominating the conversation? Who gets heard? Who is talking to who? What are they talking about?

The aim of this paper is to shed light on how these operations are organized and co-ordinated, whether the myths surrounding Anonymous' anti-leadership and anti-hierarchy ethics are mirrored in the data. The study is also concerned with how Anonymous' support for WikiLeaks evolved over time and how it manifests itself today.

A comprehensive analysis of Anonymous is long overdue in Internet studies, since it has become a fairly stable and important part of our web ecology. Through the rigorous, data-driven study of the movement, this study would like to confirm or debunk myths surrounding Anonymous.

IRC and LOIC: The symbiosis

Main method of action with respect to Anonymous operations consists of Distributed Denial of Service (DdoS) attacks. Such attacks attempt to make a website unavailable to its intended users by saturating the target server with external communication requests, leading to server overload. DdoS attacks are carried out either by botnets (a collection of compromised computers) or through applications that can be downloaded to voluntarily engage in such attacks.

During the operations against the Church of Scientology, a Norwegian hacker and 4chan regular known as Praetox created the Low Orbit Ion Cannon (LOIC), an open source network load testing tool, that Anonymous utilized to put load on servers. The LOIC was specifically designed for users of 4chan (Norton, 2011). When enough people download LOIC and point it at the same target, it is possible to make the server deny access to its legitimate users.

This is akin to many people visiting the same webpage at the same time, the server becomes too saturated. Since the server cannot handle traffic beyond a certain limit, users who would legitimately want to visit the website are also denied access, since the server either slows down or stops responding. The result is that the webpage becomes unavailable for a short while.

When LOIC was first created, users would copy paste the URL of a target from a list of multiple possible targets and launch attacks via point-and-click. However,

since LOIC is only efficient when enough amount of people point the application to a common target, later versions added a way to automate targeting. Anonymous members could put the LOIC in “slave mode” and collectively point and fire at one target. When the program is in slave mode, those who are running the LOIC can point it at an IRC channel, where the admins of the channel can direct and fire the LOIC by issuing commands in the channel's topic header.

Internet Relay Chat (IRC) is a protocol that enables conversations to take place in real time through written language. IRC allows multiple users to write messages over the Internet, it is mainly designed for group communication in discussion fora, called channels (Wikipedia, 2006).

Anonymous set up various servers to enable conversations via IRC and channels were established in order to serve as a topic-based discussion forum on these servers. Each channel operates by a keyword and usually contains a description of the chat room's activities, called a topic. These channels served different purposes ranging from general discussion (#Forum) to providing help to those wishing to join the DDoS attacks (#Target). The largest channel during the first weeks of December 2010 was the main channel, #OperationPayback, sometimes having over 4000 users (Lyon, 2010).

The **regulative pillar** of IRC is very distributed, which makes it a great choice for Anonymous. Basically, channel and server administrators have the ultimate power to set up and enforce regulations. There are no central rules that everybody must adhere to, what is unacceptable in one channel might go unregulated in another. Which ties back to the **technical pillar**, since generally channels on IRC servers have operators, who are responsible for setting up and enforcing rules. They have the power to kick, ban or silence a user. This technical infrastructure leads to an uneven distribution of power, with obvious hierarchies within a channel.

There are two groups of privileged users on IRC: IRC Operators and IRC Channel Operators (Oikarinen and Reed, 1993). An IRC Operator may have access to an entire network of servers or to one server in particular. They may disconnect or ban users from accessing any of the servers they are in charge of among other things. An IRC Channel operator may apply these same actions to the channel they are in charge of, as well as set up and enforce rules that are channel-specific, such as making sure that only Channel Operators can change the topic of the channel (Oikarinen and Reed, 1993).

The privilege granted to the channel operators when it comes to setting the topic of the channel is one of the most important **technical** decisions of this multi-platform setting of Anonymous.

One of the most important technical attributes of LOIC is the one that ties it to IRC, as well as making it a centrally controlled tool. Since LOIC is at its most efficient form, when enough amount of people point the application to a common

target, the users are asked to set the target to hive-mind mode. When in the hive-mind mode, the tool directs the attacks from everyone who is using it, to the target that is specified in the topic of the main IRC channel (Your Anon News, 2011).

Obviously, with such centralized control within a group that claims to be decentralized, the question “Who is setting the targets for the tool?” arises naturally. Which directs us back to IRC, where we have a hierarchy of lurkers, regular users and channel operators, with the latter minority defining who gets to be the target and who doesn't.

Another clash of the **socio-normative** ideals of Anonymous, and the way the tools and platforms used by them operate is the question of anonymity with regards to LOIC. LOIC doesn't mask the IP addresses of those who are engaging in a DDoS attack with the use of the tool. Your Anon News, one of the websites that is used to distribute information, has an FAQ page where the answer to the question: 'Will I get caught/arrested for using it?' is: 'Chances are next to zero. Just blame you have a virus, or simply deny any knowledge of it.'¹ Furthermore, it states that the tool doesn't work through a Proxy, however, using a VPN (Virtual Proxy Network) is an option. However, it is safe to assume that DDoS'ing through a VPN is generally discouraged (see: Figure 3.)

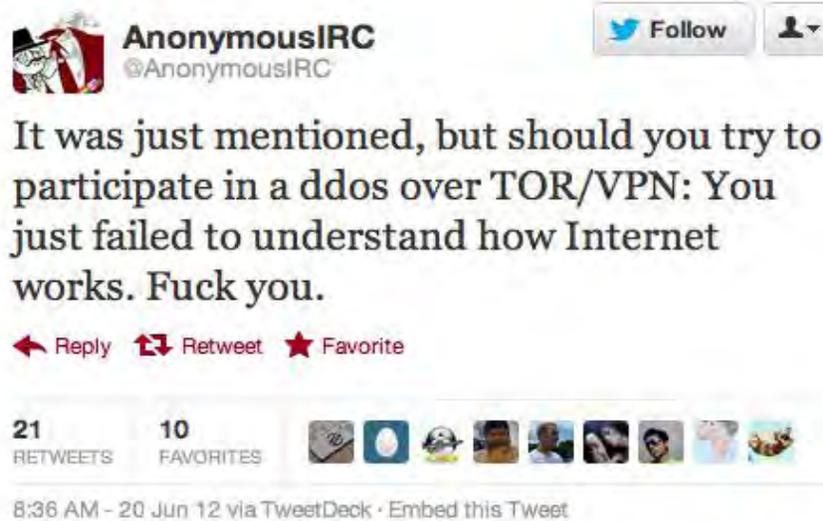


Figure 3.: A tweet by one of the Anonymous related accounts discouraging users from using VPN whilst launching DDoS attacks. Retrieved from Twitter on June 21, 2012.

¹ The number of people who have been arrested due to DDoS'ing as part of Anonymous operations shows how much of a misdirection this statement is. In fact, one of the first Operation Payback related arrests was made in the Netherlands (Openbaar Ministerie, 2010).

Thus, there is no anonymity with LOIC². In a 2011 article in Ars Technica, Nate Anderson proposes that Anonymous is divided into two groups, a small minority that is able to remain anonymous, and less tech-savvy users who are “shepherded” by the former, who use LOIC in an insecure manner and who, eventually, get caught by authorities.

One line of argument used to suggest that Anonymous was shepherded by hackers who knew how to cover their own tracks, but who had no qualms about inciting groups of preteen hacker wannabes to participate in DDoS attacks, with little attention paid to security. This narrative, which may have some truth to it, suggested that the authorities could only pick up low-level LOICers in their raids. (Anderson, 2011).

This argument is further supported by the very low technical barrier to entry that Anonymous raids and LOIC presuppose from the participants. George V. Hulme calls launching an attack on LOIC “mind-numbingly easy” (Hulme, 2010). The tool provides a way to engage in “point and click” hacking, and the graphic user interface is a testament to the ease with which it can be used (see Figure 4.) Furthermore, there are countless pastes, blog posts and YouTube videos explaining how to set up the tool, as well as IRC channels that are created for this purpose only. Thus, the tech-savvyness involved in these attacks is on par with downloading any simple tool and clicking on a button.

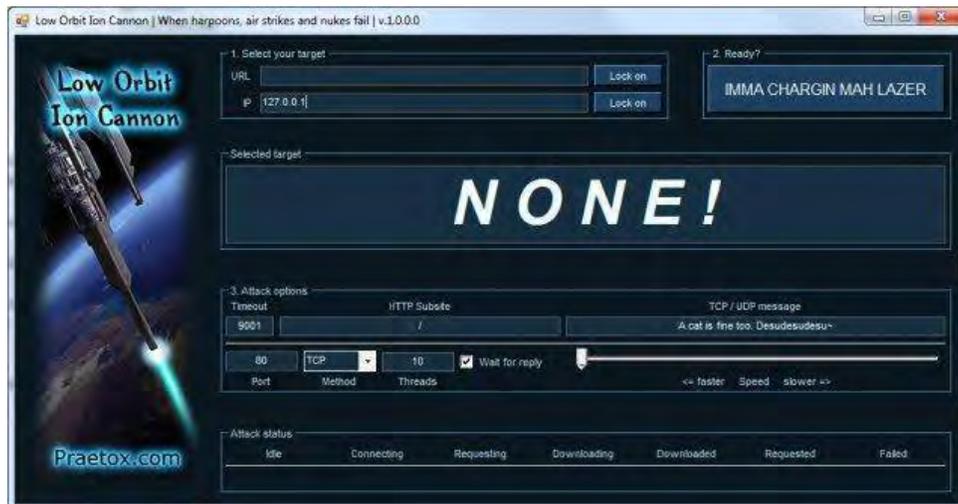


Figure 4.: The graphical user interface of the Low-Orbit Ion Cannon.

2 Which is one of the main findings of the article titled 'Attacks by “Anonymous” WikiLeaks Proponents not Anonymous' by Barbosa et al. (2010).

New Media and the era of Big Data

Since each action of the Anonymous idea/meme is rooted in diverse ethical norms and tactics, a good way of approaching Anonymous would be to analyze it on the sub-level of operations carried out by the group. However, since these projects do not rely heavily on central nodes, but operate in a chaotic way, employing multiple platforms for various reasons, it is also important to take the platform into consideration when analyzing these operations.

When it comes to studying a phenomena or a movement/community through platforms, there are mainly two schools of thought occupying this area, they differ mainly in their methodologies. In his paper "#IranElection: Quantifying Online Activism" Devin Gaffney provides a classification of these two methods. He distinguishes the "manual curation" of Web 1.0 from the "automatic collection" of Web 2.0.

The Web 1.0 methodology is described as anthropological, it involves becoming part of an online community and manually analyzing some subset of this network of websites/users/groups. In such methodologies the researchers' emphasis is placed on groups, websites and entire entities. In contrast, in the Web 2.0 methodology, data is machine-accessible and in most cases it is tagged to the level of users. Actors within this network are not only websites or entities, but also individual users. Twitter as a case study is a perfect example, where it is possible to quickly identify the exact communication transmissions of interest through the use of related hashtags.

This study will look into two qualitatively different data sets: IRC chat logs and tweets. The purpose of this chapter is two-folded, first, it aims to demonstrate the kind of questions that can be asked of different datasets with the Web 2.0 methodology. Second, it would like to ground or refute the claims made by the mainstream media as well as the academia, relating to the structure and organization of the group.

It is also important to note that when doing research with data mined from various platforms, the question of what is being studied, the case study or the platform, always remains relevant. In this chapter, the assumption is that we are studying both. When studying hashtags on platforms and how various networks evolve over time, the findings don't only answer questions regarding Anonymous, but also those that seek to answer how the platform itself organizes information.

Datasets

The following tables provide an overview of the datasets I will be using for the quantitative analysis of Anonymous. Table 1. shows the IRC data, I have chat logs from three channels during the time of the DDoS attacks. The first channel, #operationpayback, is the main channel, and #setup and #propoganda are specialized channels. The logs were assembled from different online sources, due to the efforts of those, who logged the communications during the attacks³.

IRC	<i>Name of channel</i>	<i>Time frame</i>	<i>Number of lines</i>
1)	#operationpayback	2010-12-09, 13:00-18:00	38572
2)	#setup	2010-12-09, 15:30-1730	1372
3)	#propaganda	2010-12-09, 14:45-18:00	965

Table 1.: Datasets for IRC

Table 2. provides an overview for the Twitter datasets. The datasets are grouped into three sections, based on the three different sections that the Twitter analysis is structured into in this chapter. The first grey area looks into two Twitter datasets, the tweets in 1a) and 1b) are from a 30-day period starting on December 8, 2010. The tweets in the white areas, tweets in 1c) and 1d), are from a one-week period, starting on December 1, 2011.

Finally, the second grey area denotes the tweets tagged with #Anonymous, over a one year period. The tweets were retrieved from archives in Twapper Keeper, a discontinued online tool that lets users create their own Twitter archives.

3 <http://www.blyon.com/anonymous-irc-logs/>

Twitter	Name of hashtag	Time frame	Number of tweets
1a)	#leakspin	2010-12-08 - 2011-01-08	4265
1b)	#operationpayback	2010-12-08 - 2011-01-08	3512
1c)	#Anonymous #wikileaks ⁴	2011-12-01 - 2011-12-08	547
1d)	#cablegate #wikileaks ⁵	2011-12-01 - 2011-12-08	398
2)	#Anonymous	2010-12-08 - 2011-01-08	306709

Table 2.: Twitter datasets.

IRC

IRC: #Operation Payback

Gabriella Coleman states that “To understand the dynamics of power and authority in Anonymous one must confront what is one of the most interesting, prevalent, and socially-vibrant norms within Anonymous: its anti-leader and anti-celebrity ethic. This ethic that modulates, even if it does not fully eliminate, the concentration of power.” (Coleman, 2011). With the quantitative analysis of almost five hours of IRC chat logs captured on December 9, 2010, I aim to look into the structure of mobilization efforts during Operation Payback: Avenge Assange. For each specific question that I will be asking of my dataset, I will first detail the methods that I applied, then provide a visualization of the data relating to the question and finally, discuss the implications of the findings.

The dataset consists of 38.572 lines and is formatted in the following way:

```
[2010-12-09 13::22:19] tranz1uc3nt: watchmouse: cant ping api.paypal.com
```

[TIME when the line was sent] USERNAME1: USERNAME2: message

USERNAME1 is the person who sends the line and if it is intended as a means to

⁴ Tweets tagged with #Anonymous **and** #wikileaks.

⁵ Tweets tagged with #cablegate **and** #wikileaks.

directly communicate with another user of the channel, then that user's name (**USERNAME2**) comes next followed with a colon.

There are also lines that indicate that a user has joined or left the chat room or was kicked out of the channel:

```
[2010-12-09 13::22:10] watdo joined the chat room.  
[2010-12-09 13::22:10] sj60 left the chat room.
```

The dataset itself is one of the many captured chat logs from the Operation Payback efforts in the first two weeks of December 2010. The reason for choosing this specific timeframe of December 9, 2010; between the hours of (approximately) 13:00-18:00 is the fact that this specific slice in date and time captures the hours when the DdoS attack against `api.paypal.com` was going on. Thus, I believe that this is one of the most interesting data sets, one that has the potential to reveal the underlying organizational characteristics of the movement.

Who gets heard?

One of the most interesting aspects surrounding the Anonymous movement is its presumed de-centrality and anti-leader ethic. However, so far, no quantitative analysis has been done to support this claim. In order to look into these claims, I have applied a user-based analysis to the 13.059 instances of communication lines within the IRC chat logs. It was revealed that during the timeframe when the chat log was captured, 2073 members joined the conversation.

The distribution of users based on how many lines they had indicates that a very large majority of people only contributed one line to the conversation and there wasn't a large group of people governing the flow of information:

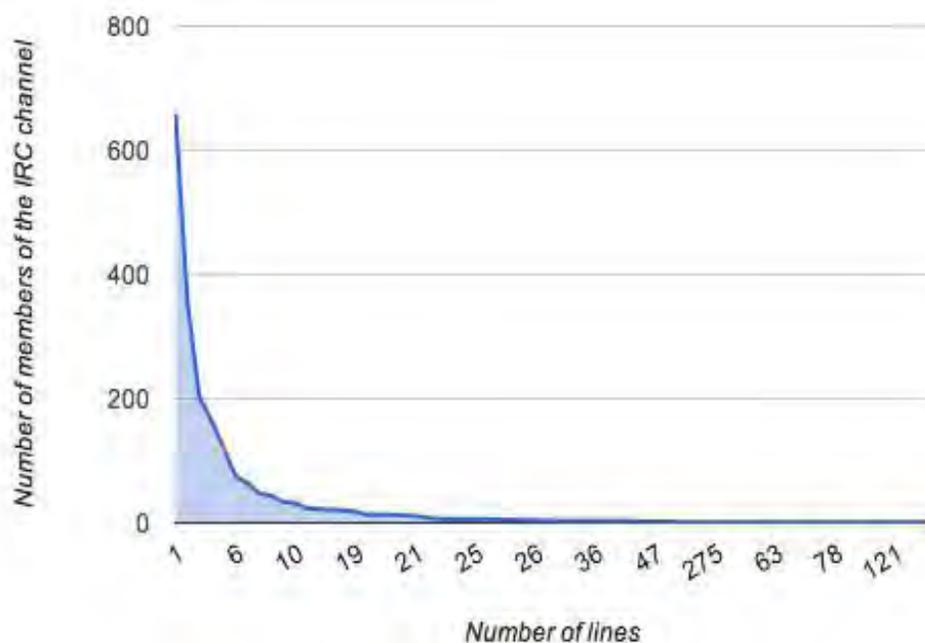


Figure 5.: Chart depicting the number of lines on the X-axis and the amount of users who had that many lines on the Y-axis.

I have separated the Top 10 users with the most amount of lines from the rest and found that they are only responsible for 11.3% of the conversation. The case of Wikipedia serves as a basis for comparison; Wikipedia is celebrated as a great example of Web democracy (Wilson, 2008), yet it was revealed that top 1% of Wikipedia users were responsible for almost half of the total amount of edits on the site (Chi, 2007). The chart shown above (Figure 5.) poses an entirely different and certainly more democratic distribution.

Within the Top 10 users, I have looked into the distribution of lines and found an even distribution, that supports the idea that there were no leaders in the IRC channel during the action/reaction phase of the operation:

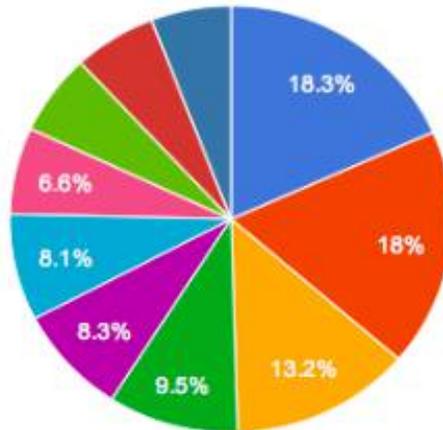


Figure 6.: Distribution of lines amongst the Top 10 most active participants.

However, most striking finding came from looking into users who had more than 20 lines, which only amounted to 133 users, the rest of the 2073 members had less than 20 lines. The distribution of lines between the top 133 users further grounds the claim that there were no central entities leading the conversation:

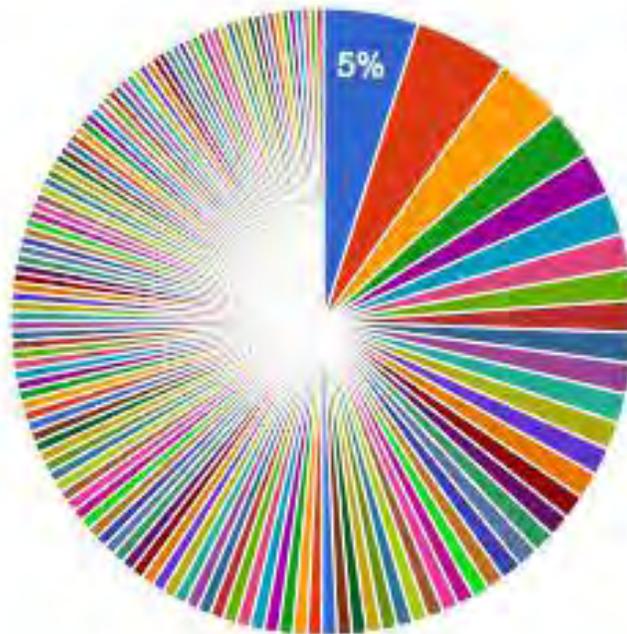


Figure 7.: Distribution of lines between the Top 133 most active users.

The mention network

In order to further analyze the issue of decentralization, I have gathered the instances when one user mentions another. Mention network are centralized if a large majority of nodes are connected to few selected nodes. During this part of the analysis, nodes are only those users in the #OperationPayback channel, who have mentioned another user or are mentioned by someone. If a user mentions another, then an edge is established between them and nodes are weighted according to how many times they get mentioned.

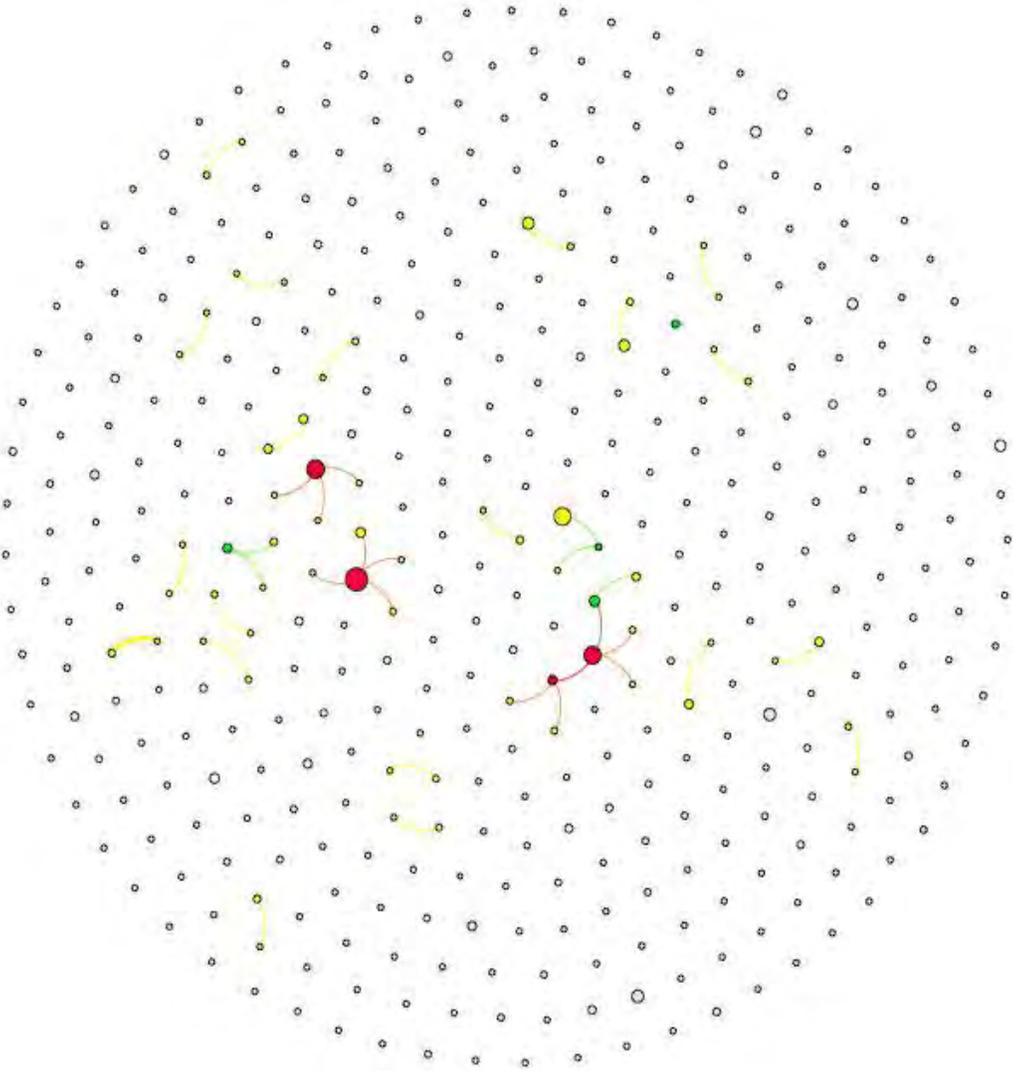


Figure 8.: The mention network of IRC's #OperationPayback channel, with nodes sized and colored based on their average weighted degree.

The nodes are sized and colored based on their prominence within the network (in this case, prominence is understood as average weighted degree). Only those edges that have a weight of more than one are shown. What can be observed in this graph (Figure 8.) is a very sparse network, with loosely connected nodes and a lack of dominant nodes.

Most 'conversations' consisted of one user mentioning another, but there were very few users who got mentioned more than once. There are no prominent authority figures, a few users got more mentions than others, but this is an extremely decentralized and anti-hierarchic mention network.

Dynamics within the chat room

In order to gain an insight into the dynamics of the chat room, I separated the instances of people communicating, joining and leaving the chat room, as well as the instances of people being kicked out. I looked into the ratio of these three forms of action and compared them to the whole.

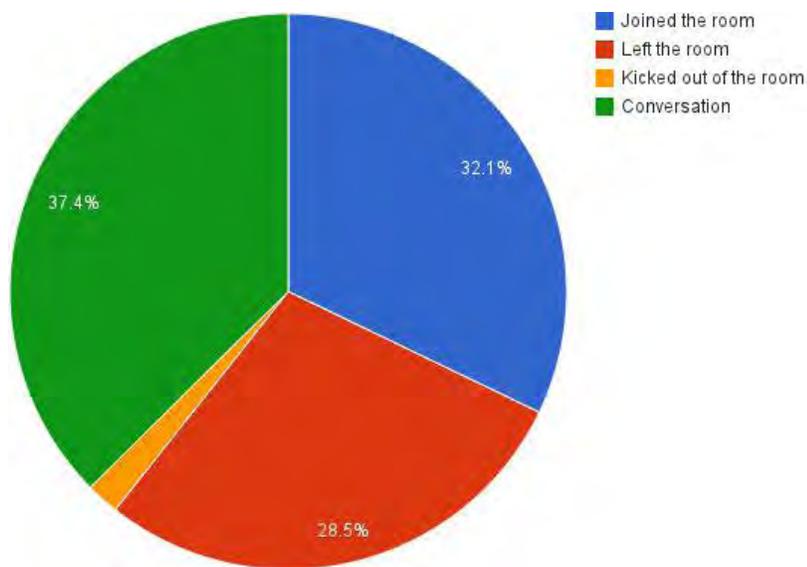


Figure 9.: Distribution of activity showing the ratio of lines that relate to communication and those that depict people joining, leaving and getting kicked out of the chat room.

I then plotted the instances of people joining, leaving and talking in the

chatroom by looking into the exact time (HH:MM) that these instances happened.:

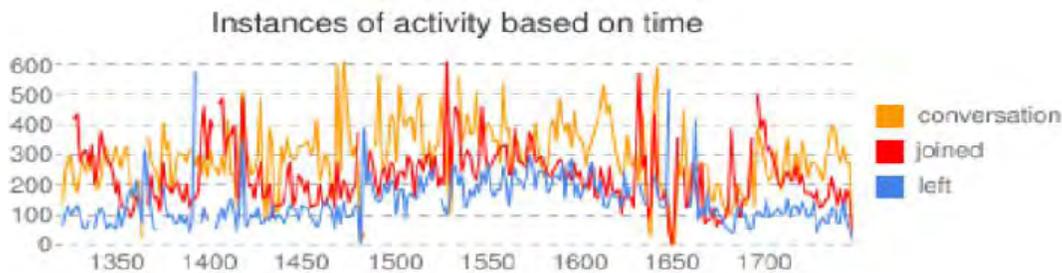


Figure 10.: Instances of the three classes of activity with number of lines on the Y-axis and time on the X-axis.

One of the most trivial observations from the above presented data is the vast amount of communication and action happening in a time frame of under five hours. However, assuming that the chat room wasn't empty when the logging started (which is safe to assume, since the first few lines of the chat log seem to be continuing a topic that has started earlier) and based on the number of people joining the chat room compared to the number of instances of communication, it can be inferred that a considerable amount of users remained silent and as mere observers.

However, the second graph (Figure 10.) shows a mild temporal correlation between the peaks within instances of communication and people joining the room. The visualizations also indicate that these few hours in the life of Anonymous were packed with action, with more people joining than leaving.

Anonymous and forms of cyborg control and power

When the separate instances of people getting kicked out of the chat room were analyzed, it was revealed that one account, EvilBoat, was responsible for a large majority (91.1%) of these instances as shown in Figure 11. Furthermore, the reasons for getting kicked out of the channel by EvilBoat mainly consisted of writing in all caps, posting the same line multiple times or 'flooding' the chat room (sending too many lines one after the other). At this point, I decided to further analyze this account by querying it in Anonymous-related IRC logs posted on Pastebin and similar services. Upon further investigation, it became obvious that EvilBoat was a bot⁶.

⁶ Bots perform automated functions and are very common in IRC channels (see the Wikipedia article: Internet Relay Chat Bots for more information).

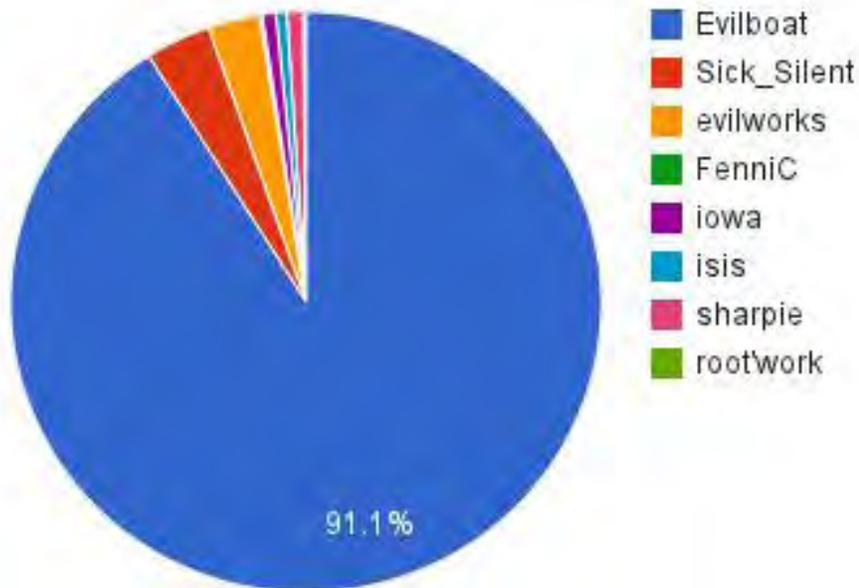


Figure 11.: Pie chart showing which channel operators kicked people out of the chat room, and out of all the instances of people getting kicked out of the room, what percentage each operator was responsible for.

One of the logs published on Pastebin is formatted in a way that when EvilBoat kicks a person out of the channel, then it publishes the reasons for doing so instantly (see Figure 12). Another document posted on a site similar to Pastebin lists the bots of the Anonymous servers, with EvilBoat's name included on the list (see: Appendix 2). Thus, it is safe to assume that EvilBoat was indeed one of the bots in the channel, who had channel operator privileges and was programmed to kick out users, who didn't adhere to the IRC etiquette.

```
[19:31] <goldn> how do i make sure iim safe?
03[19:31] * Joins: adega
[19:31] <goldn> how do i make sure iim safe?
03[19:31] * Joins: fernando
03[19:31] * Joins: BeHeadR
[19:31] <Daedalus> #setup
03[19:31] * Joins: Serpentine
[19:31] <goldn> how do i make sure iim safe?
03[19:31] * goldn was kicked by EvilBoat (Stop repeating yourself!)
```

Figure 12.: Excerpts from logged #operationpayback IRC chats depicting EvilBoat kicking people out for various reasons.

The delegation of moderation tasks to a bot is an interesting and telling characteristic of Anonymous operations. Anonymous is deeply rooted in the chan-culture, especially the /b/ board of 4chan. The /b/ board is known for its loose moderation and regulative conventions. A bot that picks up on communication patterns (such as the number of duplicate lines and the pace of posting) rather than on the content of communication, reflects the often emphasized ideals of the movement's support for freedom of speech.

Furthermore, Operation Payback is an interesting object of study for data-driven researchers, since everything involved in this issue is related to technology and internet. The movement was conceived due to a website (Wikileaks) getting censored and denied its rights. The mobilization efforts were done purely online, pamphlets and videos were distributed in various online platforms. Coordination efforts were all digital, and most importantly, one of the main protest tactics of the operation, namely the DDoS attacks, were done online. Everything is material in the sense that data is material. The movement and its efforts (and -arguably- even its ideals) are all mediated through the technical infrastructures of the Internet. There is no offline component of this particular operation, and the purely human elements are the people who participated in it.

The fact that power in the IRC channels is most dominantly practiced via pieces of code reveals a futuristic form of protest and organization, where each member of the community is judged by the same criteria in a somewhat objective manner. However, it is important to note -before sounding too enamored with this particular notion of objectivity- that bots can be programmed to not kick out channel operators (see: Appendix 3.) however, it isn't clear whether EvilBoat's code contained such a rule. Which, of course, leads us to the very valid argument that just because it is a bot that does the human's task, doesn't mean that it is neutral. The second chapter of this thesis makes the argument that algorithms and technical infrastructures are not neutral, but that they may carry within themselves various socio-normative values that they then enforce on those who interact with them.

This particular bot, and those similar to this one, were programmed by a channel operator, who infused it with his or her own values of what is acceptable and what is not. Furthermore, power and control within the IRC channels is practiced via at least one bot, and various human channel operators. Although, as Figure 11. reveals, human operators weren't as involved in direct moderation as the bot. Thus, interestingly, we see a cyborg form of power and control within the Anonymous IRC channel.

It is made up of human channel operators, who can kick out people from the channel (or even ban them, thus ensuring that they can't participate in the conversation any more) based on their own, subjective, personal ideals⁷

7 At least one instance of a user being kicked out of the room for criticizing the moderators was

to show whether there is any overlap in their narrative or userbase during the first month of the operations.

Since Twitter is frequently used for coordination efforts within Anonymous, an interesting question to ask these datasets would be whether coordination occurs in a centralized way, with few actors having disproportionate amount of power. Twitter as a basis of quantitative research forms a very good candidate platform where such questions may be answered, e.g. with the help of ReTweet or mention network analysis (boyd et al., 2011).

Furthermore, two datasets (1c and 1d) are also briefly discussed. These datasets contain tweets with the hashtags '#wikileaks *and* #anonymous' (1c) and '#wikileaks *and* #cablegate' (1d) from the first week of December, 2011. Since Anonymous imitates the learnt behaviors from 4chan (Dagdelen, 2012), which are enforced by the technical infrastructure of the platform, it shows a fascination with the 'spectacular'. Thus, in this section, the questions that I will be asking are directed along the lines of: After a year has passed since the attacks were launched, where does Anonymous concentrate its efforts in support of WikiLeaks?

The concluding section of the Twitter analysis will provide an overview of all of the top hashtags for the 365 days of #Anonymous. The top hashtag for each day in the dataset of over 300.000 tweets are retrieved and visualized, in order to show 1.) What are the topics Anonymous associated itself with? 2.) What can we say about the attention span of Anonymous?

Thus, this section provides a detailed analysis of the relationship between Anonymous and WikiLeaks and how the operations payback and leakspin were organized and coordinated. It then goes on to examine how Anonymous' support for WikiLeaks has evolved and how the support manifests itself today. Finally, this section concludes with a brief overview of the topics Anonymous associated itself with.

WikiLeaks and Anonymous: Then and Now

Then: Datasets #operationpayback and #leakspin from December 08, 2010 until January 08, 2011

In order to understand whether there were any Twitter users who dominated the discourse, a *user-based analysis* was employed. All of the users who tweeted with the hashtag #operationpayback were retrieved, as well as the amount of tweets they have posted. The same was done for the hashtag #leakspin. The pie chart in Figure 16. shows how most of the people involved in the conversation posted one tweet, the results are very similar for both hashtags.

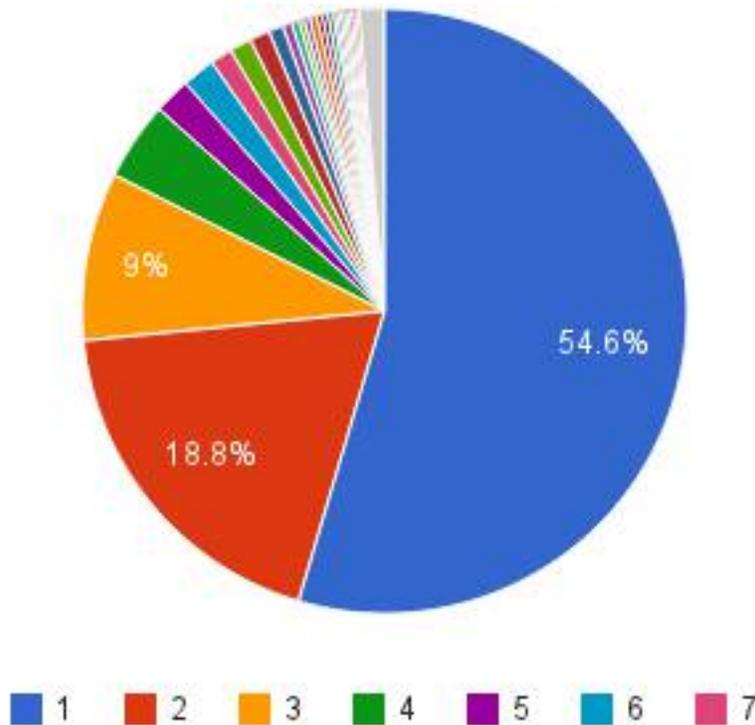


Figure 16.: Pie chart depicting what percentage of users had how many lines under the hashtag #leakspin.

In the next step, the same data is plotted on an area chart, to compare the user statistics and make the differences or similarities between the structure of these two hashtags more visible. The chart (Figure 17.) depicts the number of lines that a user had on the y-axis and the usernames on the x-axis. However, to make the visualization less clustered, the username labels are not shown, but each point on the horizontal axis can be thought of as one user.

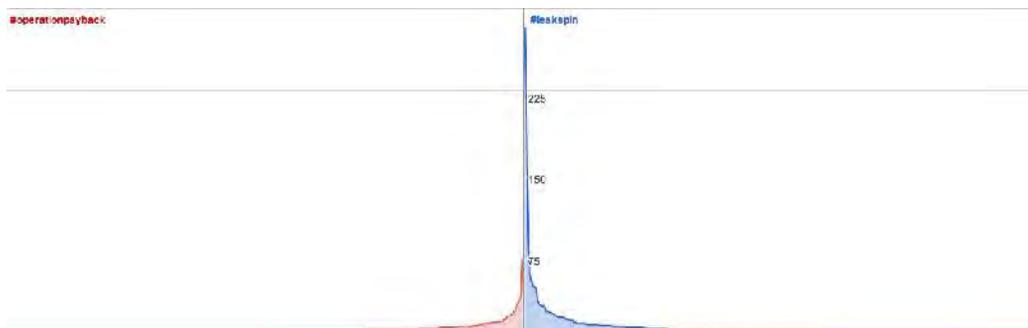
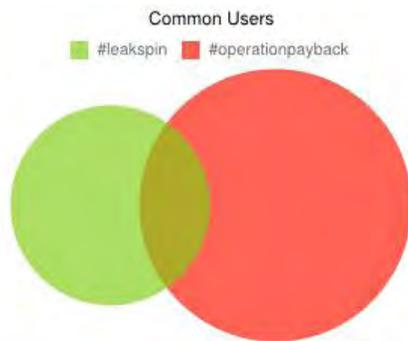


Figure 17.: Area chart depicting #operationpayback on the right and #leakspin on the left. The Y-axis shows the number of lines, and the X-axis shows the user who had that many lines, however the user labels aren't depicted.

Thus, we can see how #operationpayback had one user posting around 75 tweets, whereas #leakspin's maximum 'tweet posted per one user' count depicted on the graph is 283. However, the user '@gnudarwin' who posted 1425 tweets under the hashtag #leakspin was not shown in the graph, but it is worth a mention due to the amount of posts it has made. However, besides the extremities, the users who were responsible for the two accounts shared a similar posting pattern; very few users who were engaged with the topic in a disproportionate amount and



many users who only posted a few times. Despite the similar engagement behavior (and the fact that both operations were launched by Anonymous in support of WikiLeaks, thus shared the same goal), the users producing these two accounts don't have a huge overlap, as can be observed in Figure 18.

Figure 18.: Venn-diagram of users.

In order to answer the same question -as the one discussed above- about whether there were certain entities who dominated the discussion, a very different approach was taken, namely a *network-scientific method* was employed. With the help of the Twitter Analytics Tool, developed by the Digital Methods Initiative (University of Amsterdam), graph files of the mention networks were created from the two Twitter datasets. A mention network features Twitter users as nodes, and if a Twitter user mentions another or Re-Tweets an other user, then a directed edge is created between these users. The edges are then weighted based on how many times these users mentioned each other. I visualized the graph file by employing the built-in force-based graph drawing algorithms in Gephi.

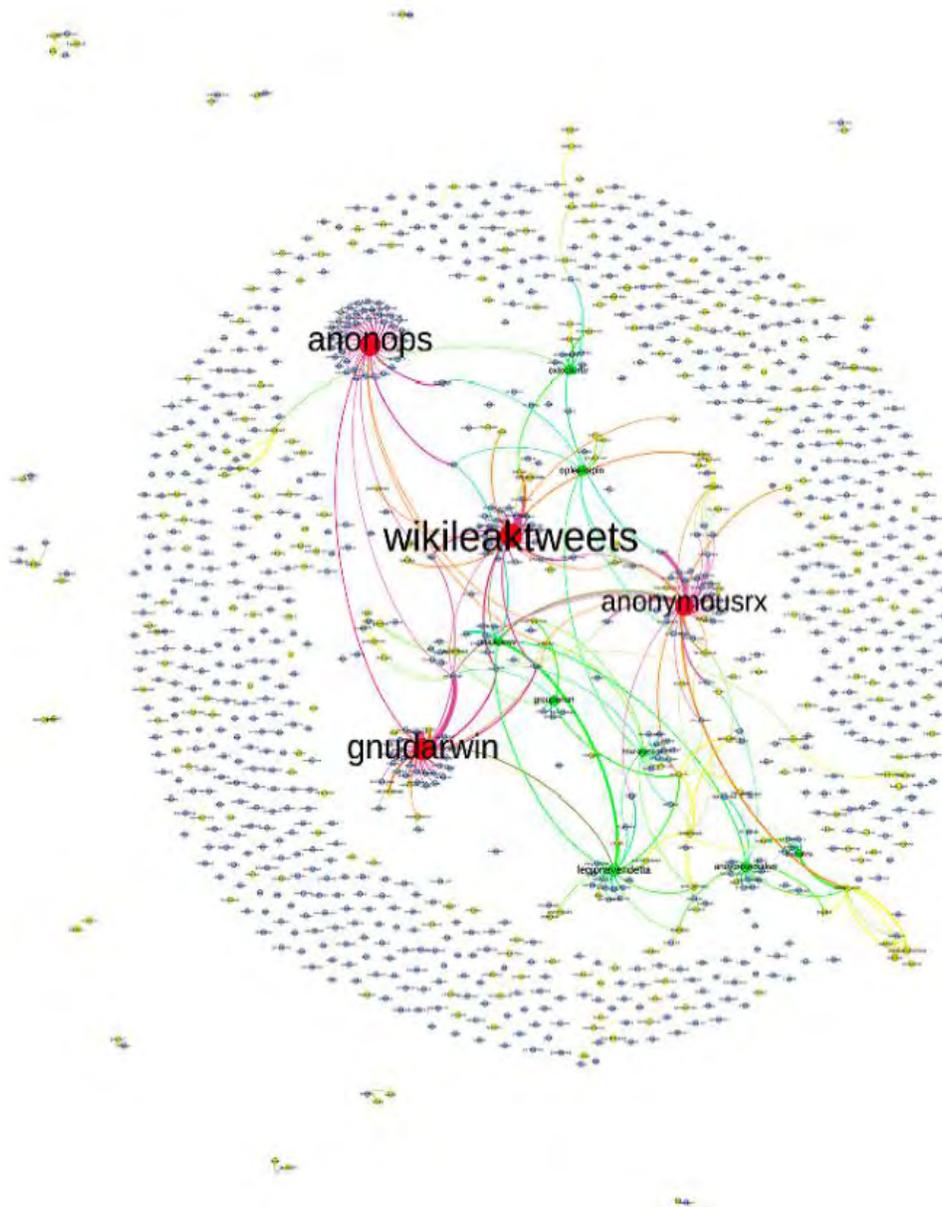


Figure 19.: Mention network for #leakspin, with nodes colored and sized based on their average weighted degrees. The graph is visualized with Gephi's built-in Force Atlas layout algorithm.

Figure 19. shows the **mention network** for #leakspin. It is surprisingly decentralized, with only four major hubs, two of which are Anonymous accounts. Once again, GNU Darwin's deep engagement with the issue can be observed, the

account received many interactions. However, the majority of the nodes have edge weight degree of less than two, thus their edges aren't even depicted. This means that most people either replied to a user or Re-Tweeted a tweet only once, which is very similar to how the people who tweeted under #operationpayback behaved (see Figure 20.)

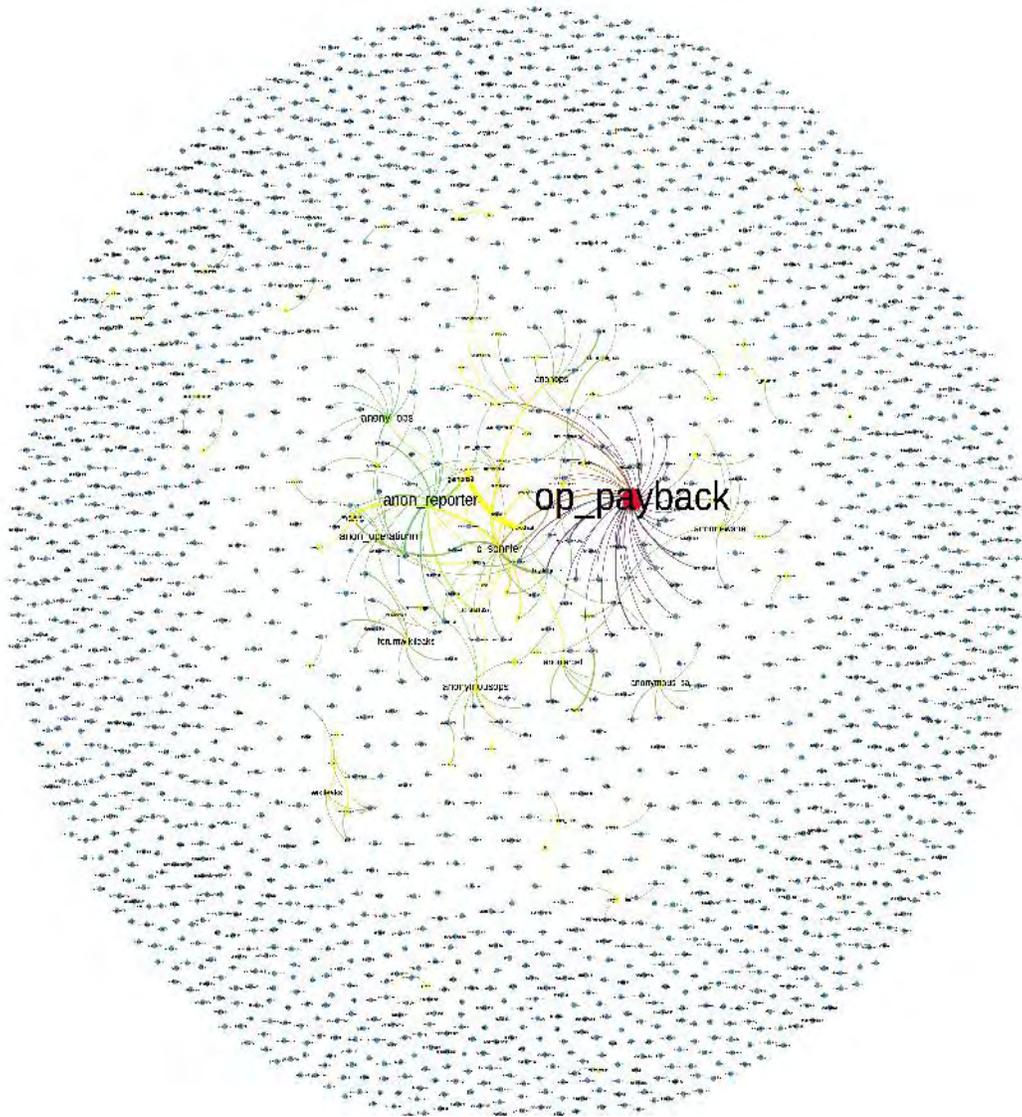


Figure 20.: Mention network for #operationpayback, with nodes colored and sized based on their average weighted degrees. The graph is visualized with Gephi's built-in Fruchterman-Reingold layout algorithm.

As the above graph shows, the **mention network** for #operationpayback was very sparse and decentralized as well. The accounts that were more dominant are solely those that were created by various people in support of the operation for the sake of this issue only. The operations form issue-based communities, with specialized accounts producing the accounts of the movement, and many people who choose to engage with it a few times. I believe that these graphs further ground the claim that Anonymous is a very decentralized movement. The lack of clusters is even more surprising when one takes into account how Twitter privileges clusters, by showing only the tweets of people registered members follow in the Twitter feed. However, this is also a testament to the fact that hashtags bring together various people, who may not engage with each other as much as they presumably do with the people they are following, but who are joining in on the conversation nevertheless.

The above presented data and findings give us an insight into the structure of the operations. We now know *how* the people involved with the operations were communicating, the next obvious question to ask is: What were they communicating about? I will be using two approaches to answer that question. First, I will be looking into the **hashtag networks** that formed around the two hashtags #operationpayback and #leakspin. Second, I will be looking into the different spheres that these two narratives link to and provide an Issue Map of the **link-network** that formed around these tweets.

Hashtags are crucial objects within the Twitter space. It is a form of metadata tag, which helps users specifically denote a dimension to the discussion. The use of hashtags provides us with a way to “isolate categories employed across the data set in order to get a better idea of the substance of the tweets at large” (Gaffney, 2011). Thus, it serves as a means to employ quantitative research to Twitter data in order to get an insight into the contents of the datasets. For this part of the study, hashtag networks were created with the help of the Twitter Analytics Tool (DMI, University of Amsterdam) and Gephi visualization tool. Here, hashtags serve as nodes. If two hashtags appear in the same tweet, then an undirected edge is created between them, the edges are weighted according to the number of times the two hashtags appeared together.

observed the operation would expect to see. This further grounds the claim about how Twitter hashtag analysis can serve as a valid alternative to manual, coarse-grained content analysis (although, it of course doesn't replace in-depth content analysis).

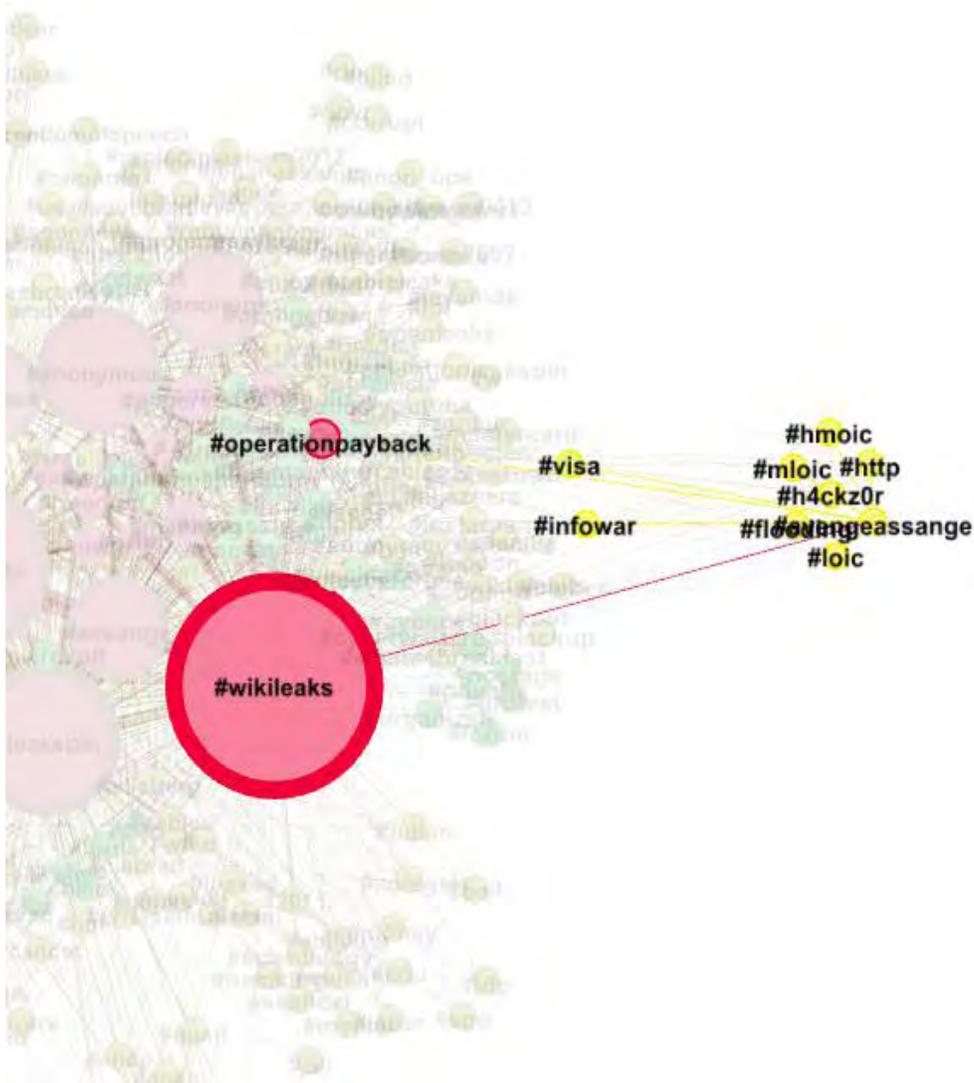


Figure 22.: An excerpt from the #leakspin hashtag network.

Figure 22. depicts an excerpt from the #leakspin hashtag network, it shows the clusters that #wikileaks and #operationpayback were together associated with. Operation Payback's fascination with the spectacular resulted in hashtags that depict notions of hacking and information war.

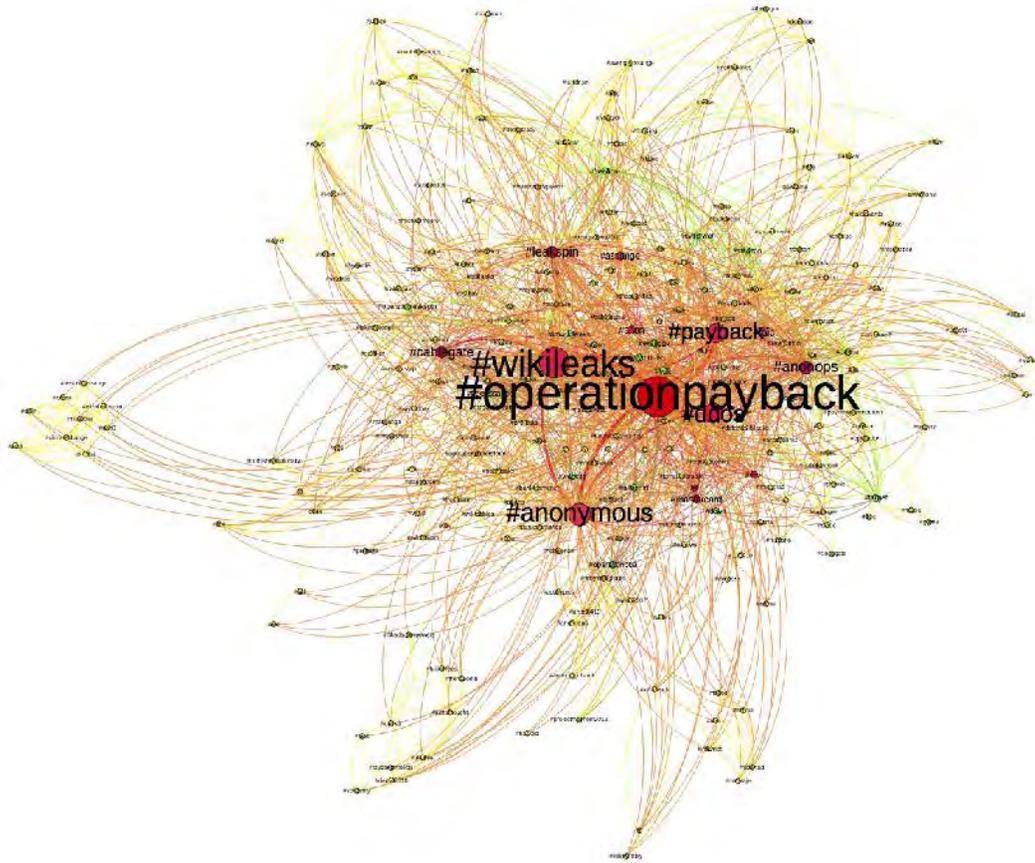


Figure 23.: Hashtag network for #operationpayback, with nodes colored and sized based on their average weighted degrees. The graph is visualized with Gephi's built-in Force Atlas 2 layout algorithm.

On the **hashtag network** of #operationpayback, a very similar pattern to the one above can be observed. The image basically covers the themes associated with #operationpayback: wikileaks, anonymous, ddos, mastercard, amazon, cyberwar, paypal, target revolution and of course, leakspin.

When we zoom in and enhance only the main cluster of the network, these notions are even more apparent and coherent (this, and further detailed views of the graph can be found in Appendix 6.)

As evidenced by the above presented data and findings, hashtag network analysis can be a viable alternative to coarse content-analysis. However, since Twitter has a character limit of 140, many studies show that it is used for awareness efforts rather than mobilization or coordination processes (Borra and Poell, 2011; boyd et al., 2011; Gaffney, 2011). Apart from the platform specific objects, like the hashtag, the RT or the reply, an important thing that a tweet may contain is links to other websites. **Link-analysis** may deepen our understanding of

the subject matter by providing us with one more sphere to study.

All links from the two Twitter datasets were retrieved. 94.9% of #leakspin, and 52.1% of #operationpayback tweets contain links. I used Issue Crawler to crawl the links that were posted with the #leakspin hashtag. **Issue Crawler** was developed by the Govcom.org Foundation, Amsterdam. The tool is used to depict a network of websites around a particular issue.

I used the co-link analysis of the tool, with two iterations and two crawl depths. What this results in is the tool crawling the entry point websites that were found in the #leakspin dataset and fetching the websites that these entry points link to. Then, for the second iteration, the tool crawls the new websites and fetches the links that those point to as well. Finally, only those websites are retained that received at least two links from any of the nodes in the network. The nodes in the network are sized based on their indigree count (the number of links they received from other nodes).

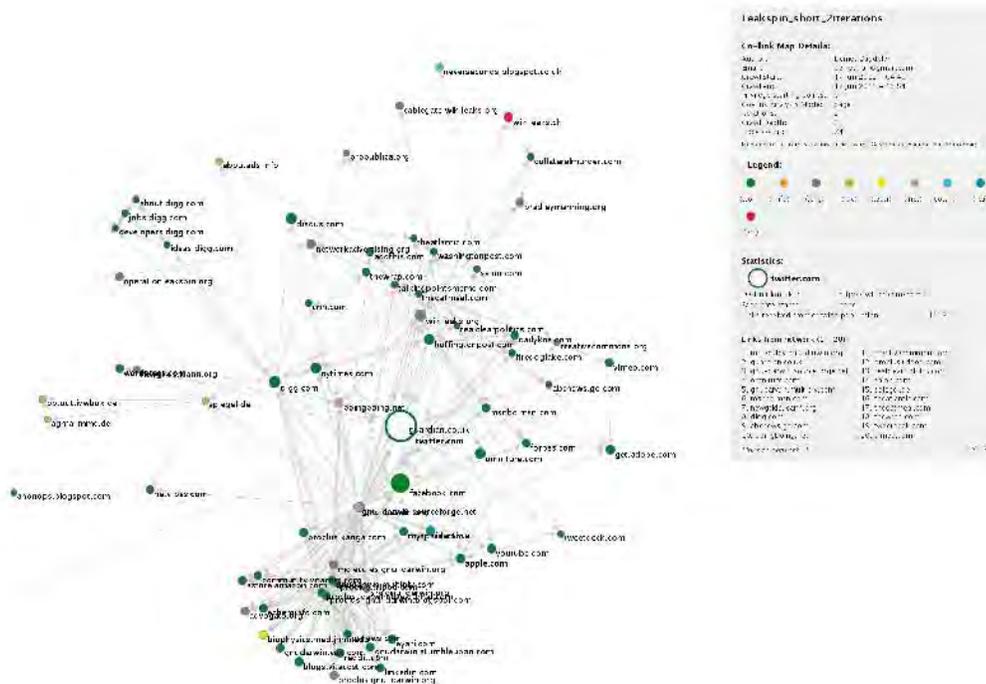


Figure 24.: Issue Crawler map for links retrieved from #leakspin. For a bigger image, see Appendix 7.

The **network map** shows the centrality of mainstream media websites, which are then mixed in with WikiLeaks related webpages. The newspapers that published the cables are also very visible and prominent. An interesting cluster is the bottom cluster around the centre, it depicts the network of gnu-darwin.org and associated websites. It is interesting to see how this open-source movement foundation has shown a very strong support of and engagement with WikiLeaks and #leakspin that was apparent in all of the steps of the Twitter analysis.

The **issue map** for #operationpayback exhibits very similar general patterns, such as the prominence of the mainstream media and WikiLeaks-related websites. However, the Issue Map, in this case, also includes Anonymous webpages, such as: anonops.blogspot.com. It can be viewed in Appendix 8.

Now: Datasets #anonymous and #cablegate from December 01, 2011 until December 08, 2011

In order to pinpoint the status of the Anonymous movement within the WikiLeaks discussion a year after Operation Payback and Operation Leakspin were launched, this analysis will focus on the 16.123 tweets that contain the hashtag #wikileaks retrieved between 01 December 2011-08 December 2011. Tweets containing the hashtag #Anonymous were retrieved from the database of all #wikileaks tweets.

All hashtags that appeared more than twice within the #wikileaks dataset were retrieved and manually browsed to see those that might relate to the distribution of the diplomatic cables, out of these hashtags #cablegate was chosen as the basis for comparison, because it was the hashtag contained in most tweets that presumably relate to the diplomatic cables. Tweets containing #leakspin were also retrieved (for it is the name of the Anonymous operation that deals with raising awareness of the disclosed cables). However, it was revealed that there were only 72 tweets that contained the hashtag #leakspin in the dataset, all of which formed a subset of the #cablegate tweets, thus only the #cablegate and #Anonymous tweets were analyzed.

These datasets were compared in various ways in order to ascertain how much overlap they have, since this would give an insight into whether tweeters still associate the analysis and distribution of diplomatic cables (#cablegate) with Anonymous (#anonymous) with regards to #wikileaks.

As a starting point, **related hashtags** for #Anonymous and #cablegate were analyzed and visualized with the Triangulation tool (developed by the Digital Methods Initiative) to determine the commonalities amongst them and observe the degree to which the contents of these two datasets overlap.

browsed manually. The reason for analyzing the tweets as opposed to solely looking at the hashtags was that the dataset revealed that many of the Twitter users utilize a substantial amount of hashtags per tweet and not all of them are related to the content they are linking to or are writing about.

During the process of coding only one category name was created (“awareness”), for the rest, the names of the coding categories all emerge either from the tweet itself or from the content of the webpage that the tweet links to.

Not all tweets containing the aforementioned keywords were put under the mentioned categories, the content of the tweet and/or the webpage that the tweet linked to was given more importance than the hashtags mentioned in the tweet. However, except for the “awareness” category, all tweets that were placed under a category had the one or more of relevant keywords in its content.

Categories	Keywords from the tweet or webpage that is linked to
Assange	“extradition” and “Assange” and/or “#assange”
awareness	No content but lots of hashtags and/or tweets about WikiLeaks in general as opposed to particular deeds of WikiLeaks.
cables	Links to discussions about any of the cables or webpages containing the cables themselves. Keywords: “cables” or “cablegate” or “cable”.
DDoS	Tweets containing the hashtag DDoS or tweets mentioning MasterCard, Paypal, Amazon or any of the other formerly DDoS'd corporations. Keywords: “DDoS” or “operationpayback” or “mastercard” or “visa” or “opvisa”.
Egypt	Tweets that specifically mention Egypt in context or that link to content related to Egypt. Keywords: “Egypt”.
spyfiles	Tweets mentioning the “Spy Files” release of Wikileaks or that link to content mentioning it. Keywords: “Spy files” or “surveillance”.
manning	Tweets mentioning Bradley Manning. Keywords: “Manning”

news	News articles that mention issues related to WikiLeaks, but don't focus on WikiLeaks.
occupy	Tweets about the occupy movement. Keywords: "Occupy" or "99percent" or "99%"
support	Keywords: "Thank you WikiLeaks.", "donate", "support"

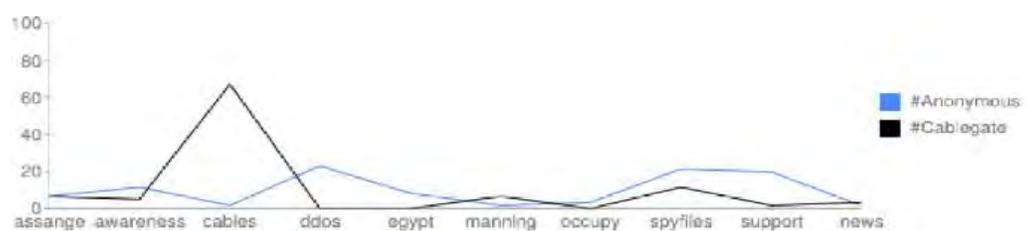


Figure 26.: Line chart visualization of 100 random tweets from the #Anonymous and #Cablegate datasets: The Y-axis shows the number of times the category appeared within the datasets and the X-axis shows the categories.

Results of the content analysis further ground the claim that whilst there still are people and organizations working on the analysis and distribution of the diplomatic cables leaked by WikiLeaks in 2010, Anonymous is not associated with these activities anymore. The two operations that Anonymous started in support of WikiLeaks in December 2010 barely have anything in common by December 2011. In the context of WikiLeaks, Anonymous is still associated with the DDos attacks launched in December 2010 and Operation Leakspin has merged with Cablegate (the name that is widely used to refer to the WikiLeaks' disclosure of the cables). Furthermore, Anonymous is still discussing the DdoS attacks, presumably due to their spectacular nature, as opposed to the dry nature of topics pertaining to the leaked cables.

The evolution of #Anonymous: from December 2010 until December 2011

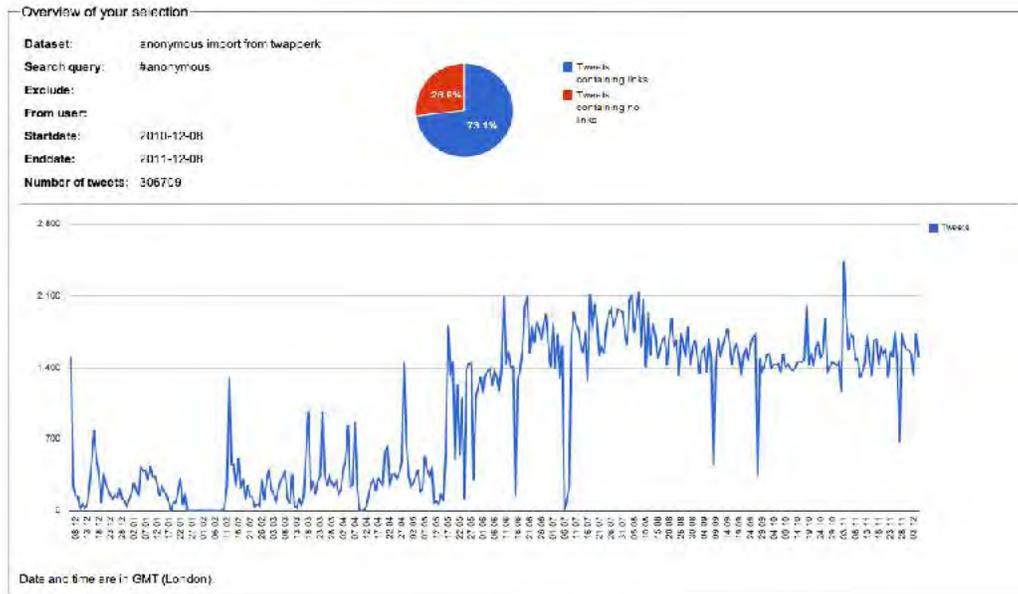


Figure 27.: Overview of the #Anonymous dataset, via the Twitter Analytics Tool (DMI, University of Amsterdam).

The concluding section of this chapter looks into over 300.000 tweets with the hashtag #Anonymous in order to provide an overview of the topics that Anonymous has associated itself with in the span of a year. The method applied in this section involves retrieving the top hashtag for each day of the year, beginning from December 08, 2010 until December 08, 2011. Thus, each day corresponds to one hashtag. These are then plotted on an arc diagram, as hashtags/days corresponding to nodes. If two days have the same top hashtag, then an edge is created between those two nodes.

Furthermore, since this section would also like to gain an insight into the 'attention span' of Anonymous, only the first occurrence of an edge is plotted. Thus, if day 35, day 37 and day 39 all have the same top hashtags, then an edge is created between day 35 and day 37, as well as between day 35 and day 39, but not between day 37 and day 39.

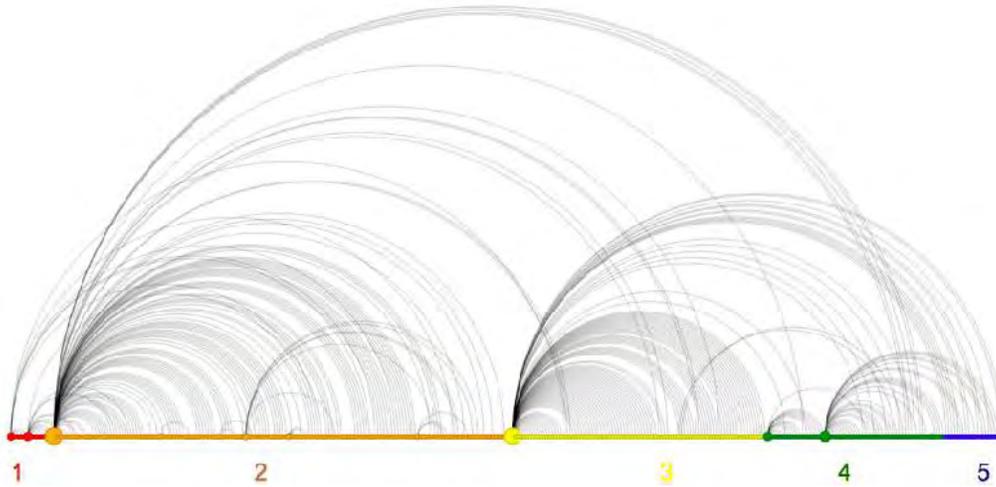


Figure 28.: An arc diagram depicting the co-occurrence of top hashtags for 365 days, in the #Anonymous dataset.

The nodes are put into five groups, each group starts with a large node, that depicts the beginning of an era of a new topic for Anonymous.

Group	Time frame	Top hashtags
1	2010-12-08 - 2010-12-31	#operationpayback and #wikileaks (the two bigger red nodes)
2	2011-01-01 - 2011-06-19	#anonops (the big orange node)
3	2011-06-20 - 2011-09-16	#antisecc (the big yellow node)
4	2011-09-17 - 2011-11-17	#occupywallstreet and #ows (the two bigger green nodes)
5	2011-11-18 - 2011-12-08	#antisecc and #ows

The nodes are sized according to their out-degrees, one of the biggest node is the orange node depicting #anonops, which is a general hashtag related to Anonymous operations. The other large node is the yellow #antisecc node. What is made visible by the visualization Figure 32., is the attention span of Anonymous. Whilst the largest operations were paid attention to for a quarter of a year on average, there are many smaller arcs, that don't go beyond a few weeks or days. The general hashtag #anonops is the only node that generates arcs that span over

almost a year, whereas topical hashtags with the smaller arcs depict Anonymous' short attention span when it comes to engaging with a specific issue.

Conclusion

We've tried hacker group, notorious hacker group, hacktivists, the Internet Hate Machine, pimply-faced, basement-dwelling teenagers, an activist organization, a movement, a collective, a vigilante group, online terrorists, and any number of other fantastical and colorful terms. None of them have ever really fit. Anonymous has constantly forced us to reach for the thesaurus — revealing that as a whole, we in the media have no idea what Anonymous really is or what it means.
(Norton, 2011)

The above quote by Quinn Norton -as part of a special series about Anonymous in the *Wired* magazine- demonstrates the difficulty of capturing Anonymous as an object of study, as well as the need to open up the topic for academic discussion.

The cases of actions taken by Anonymous or by online communities that are commonly associated with Anonymous represent a wide variety of motivations and methods of action. Prior to 2008, Anonymous was widely represented as Internet trolls and pranksters. danah boyd wrote in 2010: “I would argue that 4chan is ground zero of a new generation of hackers – those who are bent on hacking the attention economy. While the security hackers were attacking the security economy at the center of power and authority in the pre-web days, these attention hackers are highlighting how manipulatable information flows are.”

It is important to realize that motivations of Anonymous range from enjoyment derived from other people's or communities' misery to expressing legitimate political and societal concerns. Whereas the acts of trolling memorial pages are beyond the realm of defending, expressing their distrust of authority and desire to keep the Internet a space, where freedom of speech is not limited could be accepted as a valid political stance. However, since operations and actions carried out under the name Anonymous include both ends of the spectrum and many things in-between, Anonymous cannot be defined as an *activist group*, since Anonymous as a collective doesn't share a common goal.

The line between online activism and hacktivism is drawn with respect to the methods applied by the groups. Whereas activists employ non-disruptive methods, hacktivists incorporate recent technology as a tool for change and can be

defined as the nonviolent use of legal and/or illegal digital tools in pursuit of political ends (Samuel, 2006). Online activism utilizes the Internet as a means to enable faster communications and to deliver information to a large audience. Whilst most of the methods applied by Anonymous fall under the category of hacktivism, in the case of e.g. Project Chanology and Operation Leakspin, some arms of the movement utilized technology solely as a means to spread information. Once again, there is a tension when classifying Anonymous as a *hacktivist* collective. Internet activists and hacktivists both enjoy a place under the Anonymous umbrella.

Even though it can be argued that Anonymous shares some values with the culture of the image-board communities at its core, it is important to distinguish between Anonymous and these online communities. *Online communities* are usually defined as a group of people centered around a platform or a website, occupying the same online space (Preece and Maloney-Krichmar, 2005). In the case of Anonymous, even though it started out from such online communities, it has evolved into what Gabriella Coleman calls a “political gateway”, Coleman notes that for many people Anonymous is a path to engage in political action (Coleman, 2011). One of the attributes that sets Anonymous apart from online communities is the fact that with Anonymous, communities are formed with respect to operations. There are multiple operations that run simultaneously, some that are centered around a cultural or a national region, thus different operations have different users, and, generally, the users remain within the “community” for the duration of the operation only.

Anonymous manages to coordinate actions and communication, without relaying on any central website or platform. The major platforms that are associated with Anonymous are known, but it is not a guarantee that the next operation organized by them will employ all or any of these platforms. Anonymous sometimes establishes central nodes of communication for various operations (e.g. in the case of Operation Payback anonops.net served this role). However, Anonymous by nature is decentralized, resulting in the establishment of temporary central nodes for the sake of an operation only, as opposed to as a means to represent Anonymous as a whole.

Anonymous, as demonstrated above, is not a group of people brought together by a shared set of values or goals. Anonymous is also not a community of people using the same websites. In the context of online activism/hacktivism, it can be most accurately described as a tool to engage in action. However, in the wider notion of the Internet ecology, it should be thought of as an idea or a meme.

Anonymous is the constantly remixed meme of acting online in a collaborated manner towards a goal under the guise of anonymity. The process of collaboration, the motivations behind the goals and the methods to achieve the goals are constantly remixed and re-interpreted, but the importance of anonymity

is always agreed upon.

Anonymous' more political operations inarguably fall under the category of activism, whether they utilize hacker techniques or not. However, considering the fact that since June 2009, LOIC has been downloaded almost 630.000 times solely from Source Forge (it is also hosted on GitHub), Anonymous is able to mobilize a large amount of people, in a very short time, without relying on any specific platform.

The success of the coordination of their efforts in a very decentralized web, with such a fast response time, is not only interesting but might provide useful to study. Just as the fruitful collaboration techniques of the open source community is studied in order to apply these techniques elsewhere, Anonymous might serve as an online political activism model to build on.

This paper provided a fine-grained analysis of Anonymous and its support for WikiLeaks. Most of the findings support the claims made about Anonymous in the past with regards to its decentralized and anti-hierarchical nature. It was possible to observe how Anonymous is fascinated with the spectacle and the fast-paced, it forms issue-based communities that dissolve as soon as they act. Furthermore, Anonymous can be thought of as a meme; a behavioral pattern that adapts to its environment (that is made up of various platforms) without losing its core mechanisms.

Anonymous is a thoroughly mediated “group”, and one of the challenges for Anonymous was to navigate within an ad-hoc assemblage of a multitude of platforms, some of which clash with their anti-hierarchical and pro-privacy ideals. Not only is Anonymous mediated by 'external' circumstances, such as the platforms and the communication channels they use, the act of practicing the group's values and forms of power and control are delegated to non-human actors as well. Anonymous' values are expressed mainly through what they choose to protest, and the act of protesting is generally done with the LOIC tool, which turns individuals into members of a protesting group, that are executing virtual sit-ins. The communication in one of the most important mediums to the movement, IRC, is moderated largely by bots, who are infused with the values of the platform itself. With the multitude of tools, platforms and bots that Anonymous juggle, Anonymous forms a path to *cyborg* political action.

Despite its low barrier to entry, its love for the spectacular and its failure to reach any of the goals it has so far set up for itself, Anonymous -and similar, purely political online activism attempts- present a *behavioral pattern* (that include raising awareness, collaborating on manifestos, taking action, mobilizing, coordinating, setting goals) and forms of civil engagement that is very important for the well-being of any democracy.

Bibliography

Anderson, Nate. "Exclusive: How the FBI Investigates the Hacktivities of Anonymous." *Ars Technica*. Ars Technica, Aug. 2011. Web. 1 June 2012. <<http://arstechnica.com/tech-policy/2011/08/exclusive-how-the-fbi-investigates-the-activities-of-anonymous/>>.

Barbosa Et Al. "Attacks by "Anonymous" WikiLeaks Proponents Not Anonymous." *CTIT Technical Report 10.41*. University of Twente, 10 Dec. 2010. Web. 20 Dec. 2011. <<http://doc.utwente.nl/75331/1/2010-12-CTIT-TR.pdf>>.

Benkler, Y. (2011). A Free Irresponsible Press: WikiLeaks and the Battle over the Soul of the Networked Fourth Estate. Harvard Civil Rights-Civil Liberties Law Review (forthcoming). 28 August, 2011 <http://www.benkler.org/Benkler_WikiLeaks_current.pdf>.

boyd, danah. "for the lolz!: 4chan is hacking the attention economy." zephoria. June 12, 2011. 18 December, 2011. <<http://www.zephoria.org/thoughts/archives/2010/06/12/for-the-lolz-4chan-is-hacking-the-attention-economy.html>>

Chi, H. "Long Tail of user participation in Wikipedia". May 15, 2007. February 2, 2012. <<http://asc-parc.blogspot.com/2007/05/long-tail-and-power-law-graphs-of-user.html>>.

Coleman, G. "Anonymous — From the Lulz to Collective Action." *The New Significance*. May 9, 2011. December 14, 2011. <<http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/>>

Dagdelen, D. "Anonymous, WikiLeaks and Operation Payback: A Path to (Cyborg) Political Action." MA Thesis. University of Amsterdam. 2012. <<https://docs.google.com/open?id=0B6KeRZYpmpk7VU12Nnh0WVBiaHM>>.

Davies, S. "The internet pranksters who started a war." ninemsn. May 8, 2008. December 7, 2011. <<http://news.ninemsn.com.au/article.aspx?id=459214>>.

Gaffney, D. "#iranelection: Quantifying online activism." Web Science.2010.

Hulme, George. "LOIC Tool Enables 'easy' WikiLeaks-driven DDoS Attacks." *CSO*. CSO Online, 15 Dec. 2010. Web. 25 May 2012. <<http://www.csoonline.com/article/646813/loic-tool-enables-easy-wikileaks-driven-ddos-attacks>>.

Isaac, M. "Facebook and Twitter Suspend Operation Payback Accounts." *Forbes*. December 8, 2010. December 7, 2011. <<http://www.forbes.com/sites/mikeisaac/2010/12/08/facebook-and-twitter-suspend-operation-payback-accounts/>>.

Latour, B. (1992): Where are the Missing Masses? *Sociology of a Few Mundane Artefacts*. In *Shaping Technology, Building Society: Studies in Sociotechnical Change*. Wiebe E. Bijker and John Law (edit.). Cambridge, MA: MIT Press, 225-258.

Lindgren, S. and Lundstrom R. (2011). *Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter*. New Media and Society. Published online before print June 27, 2011. doi:10.1177/1461444811414833 September 2011 vol. 13 no. 6 999-1018. December 7, 2011. <<http://nms.sagepub.com/content/13/6/999.short>>.

Lyon, Barrett. "Anonymous IRC Logs: A Moment in Time". December 16, 2010. January 24, 2010. <<http://verbophobia.blyon.com/anonymous-irc-logs/>>

Morozov, E. "Parsing the impact of Anonymous". *Net Effect*. December 9, 2010. October 27, 2011. <http://neteffect.foreignpolicy.com/posts/2010/12/09/parsing_the_impact_of_anonymous>.

Norton, Quinn. "Anonymous 101: Introduction to the Lulz." *Wired*. November 8, 2011. December 20, 2011. <<http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1>>

Oikarinen, J., and D. Reed. "RFC 1459 - Internet Relay Chat Protocol." Network Working Group, May 1993. Web. 15 May 2012. <<https://tools.ietf.org/html/rfc1459>>.

P2P. "p2pnet talks with Operation Payback." *P2P*. November 18, 2010. December 8, 2011. <<http://www.p2pnet.net/story/45762>>.

Parket, Landelijk. "16-jarige Jongen Aangehouden Vanwege WikiLeaks-aanvallen." Openbaar Ministerie, 9 Dec. 2010. Web. 15 May 2012. <http://www.om.nl/actueel/nieuws-_en/@154591/16-jarige_jongen/>.

Pastebin. "[ddos] LOIC Tutorial." *Pastebin*. Pastebin, 26 Feb. 2012. Web. 20 May 2012. <<http://pastebin.com/A0tUTHA2>>.

Preece J. and Malone-Krichmar, D.(2005). Online communities: Design, theory, and practice. *Journal of Computer-Mediated Communication*, 10(4), article 1. <<http://jcmc.indiana.edu/vol10/issue4/preece.html>>.

Protovis: A Graphical Toolkit for Visualization. Michael Bostock, Jeffrey Heer. *IEEE Trans. Visualization & Comp. Graphics (Proc. InfoVis)*, 2009

Samuel, A. "Hacktivism and the Future of Political Participation." Harvard University, Cambridge, Massachusetts. 2006. December 13, 2011. <<http://www.alexandrasamuel.com/dissertation/pdfs/index.html>>

Schwartz, Mattathias. "The Trolls Among Us." *The New York Times*. August 3, 2008. December 18, 2011. <<http://www.nytimes.com/2008/08/03/magazine/03trolls-t.html?pagewanted=all>>

Smythe, Elizabeth, and Peter J. Smith. "New Technologies and Networks of Resistance." *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*. (2002): 48-82. Print.

Sourceforge. "Download Statics." December 20, 2011. <<http://sourceforge.net/projects/loic/files/stats/timeline?dates=2009-06-24+to+2011-12-20>>.

TorrentFreak. "Behind the Scenes at Anonymous' Operation Payback". November 15, 2010. January 24, 2012. <<http://torrentfreak.com/behind-the-scenes-at-anonymous-operation-payback-111015/>>.

Vegh, S. "Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank." 2003. Pp. 71-96 in *Cyberactivism*, edited by Martha McCaughey and Michael D. Ayers. New York, NY: Routledge.

Wikipedia. "Operation Leakspin". Wikimedia Foundation. 2010. December 6, 2011. <http://en.wikipedia.org/wiki/Operation_Leakspin>.

Wikipedia. "Operation Payback". Wikimedia Foundation. 2010. December 6, 2011. <http://en.wikipedia.org/wiki/Operation_Payback>.

Wilson, Chris. "The Wisdom of Chaperones: Digg, Wikipedia and the myth of Web 2.0 democracy". *Slate*. February 22, 2008. January 25, 2012. <http://www.slate.com/articles/technology/technology/2008/02/the_wisdom_of_the_chaperones.html>.

Appendices

Appendix 1.: Anonymous Press Release

ANONYMOUS PRESS RELEASE

December 16, 2010



FREE-THINKING CITIZENS OF THE WORLD,

In the middle of this mass uprising amongst humanity over the censorship of Wikileaks, ANONYMOUS has made its voice heard among the cries for justice and freedom. Many people think they understand ANONYMOUS, but as an amorphous, opt-in entity, ANONYMOUS is - if we might understate ourselves - fractitious at best and anything but unanimous.

Individuals within ANONYMOUS believe many often contradictory things, even within that same individual. Such is humanity. Humans argue, disagree, fight, bicker, and often say hurtful things specifically to hurt one another. As a group of humans (at least to our knowledge - there may be a few dogs on the internet these days) ANONYMOUS holds many of these human qualities.

It may then seem odd to try to characterize or explain ANONYMOUS at all. Among this buzzing hive of thoughts, ideas, and dreams, the only common characteristics that one might perceive are only the ideas that hold the most traction among humans at large.

Many people will follow certain battle standards in the fight for greater justice. Some will fight those who prey upon children. Others will fight empires and kingdoms who do wanton violence against their own people.

The battle standard that ANONYMOUS follows, however, is the freedom of information.

Without information, one cannot fight for any other cause. Children will remain abused if their plight remains unknown. Nations will rage wars against their own people if cloaked in secrecy. Crimes will go unpunished, victims will go uncomforted, and walls will remain undefended.

As Thomas Jefferson put it, "Information is the currency of democracy." But we would go further and say that information is the life-blood of society. Humanity as a great mass of people is constantly transmitting and receiving a treasure-trove of information: sights and sounds, textures and tastes. We love, we hate, we laud, we lament - sometimes to only ourselves but often to others, and we take great comfort in the mere act of communication.

As humanity has pushed the boundaries of technology, we realize now that this act of sharing information acts as a kind of collective processing - fashions,

conventional wisdom, and even the scientific method itself are all the product not of a single genius but of countless humans laboring together.

A trillion times a trillion programs are running simultaneously in our little organic computers that are our brains, networking together through text, through speech, and through pixels. Not all these programs have immediate applications to the tasks we face every single day, but when it does pertain we are grateful that thousands of man-hours have been applied to refine great works of art and thought itself.

As beautiful as the collective dreaming of mankind may be, there are nevertheless those who wish to stifle the free exchange of information. The reasons for this are numerous: expression of political dissent is often repressed in autocratic regimes, and those offended by certain types of communication seek to have the offending material removed.

Indeed, not all information is beautiful or inspiring. Words of hurt and words of hate can and often do damage relationships, families, and individuals. But the crime committed, if any at all, is not the fault of communication itself. We can no more blame the act of speech for harming another as we can fault one's beating heart for spreading a cancer.

Instead, we affirm in the strongest possible sense that the solution to bad speech is more speech, not less. The indiscriminate use of censorship damages the human collective response to bad speech and makes it less capable of responding effectively when bad speech actually does occur.

When information is hidden from view for any reason, its sudden and inevitable revelation is necessarily shocking and cause for alarm. Without a precedent to relate to it and without open dialogue to communally process it, the information becomes harmful due to the censorship itself.

Furthermore, we warn free peoples everywhere of the dangers of private censorship on behalf of government. Government is necessarily slow of action as it reacts to the free expression of men and women. It is thus sad to note that the only effective method of pre-emptive censorship known to man is when the gatekeepers of information censor on behalf of governments.

If information channels are to be useful as methods of collective processing, then they must be agnostic to the message sent. Information is necessarily an enabler of crime, but it also an enabler of comfort. We warn that the hand used to censor must be watched at all times and questioned without ceasing, lest it be abused to cover the crimes of the censor.

We challenge the citizens of democracies everywhere to hold their governments accountable to the people. As the past century has progressed, we have seen governments expected to do more for their people, including the provision of

public pensions and the pursuit of national interests abroad through military interventions. Insofar as the public is aware of what is being done in their name, then we leave it to the institutions of law and the ballot-box to decide what is best for these nations.

Insofar as the people are kept in ignorance about what is done in their name, though, we object in no uncertain terms to elected officials covering up crimes to avoid scrutiny. Knowledge of one's own government's dealings are the responsibility of the people, and with great power in the state must come great scrutiny. We thus work for a radical transparency in governments everywhere, to hold them accountable for crimes committed in the state's name.

We call also for a public and open debate over the issues of copyrights and patents. For too long, we have watched private companies abuse these legal channels as a form of litigational capital. Software copyright firms, for example, exist for the primary purpose of buying copyright claims to harass others. Pharmaceutical firms spend a significant quantity of their monopoly profits not on research and development but on defending their patents.

Indeed, Kiss bassist Gene Simmons is on record as having said, "Make sure your brand is protected... Make sure there are no incursions. Be litigious. Sue everybody. Take their homes, their cars. Don't let anybody cross that line." We have come to a sad impasse as a society where the law is a battlefield of giants where the mere threat of legal action can cause financial crisis.

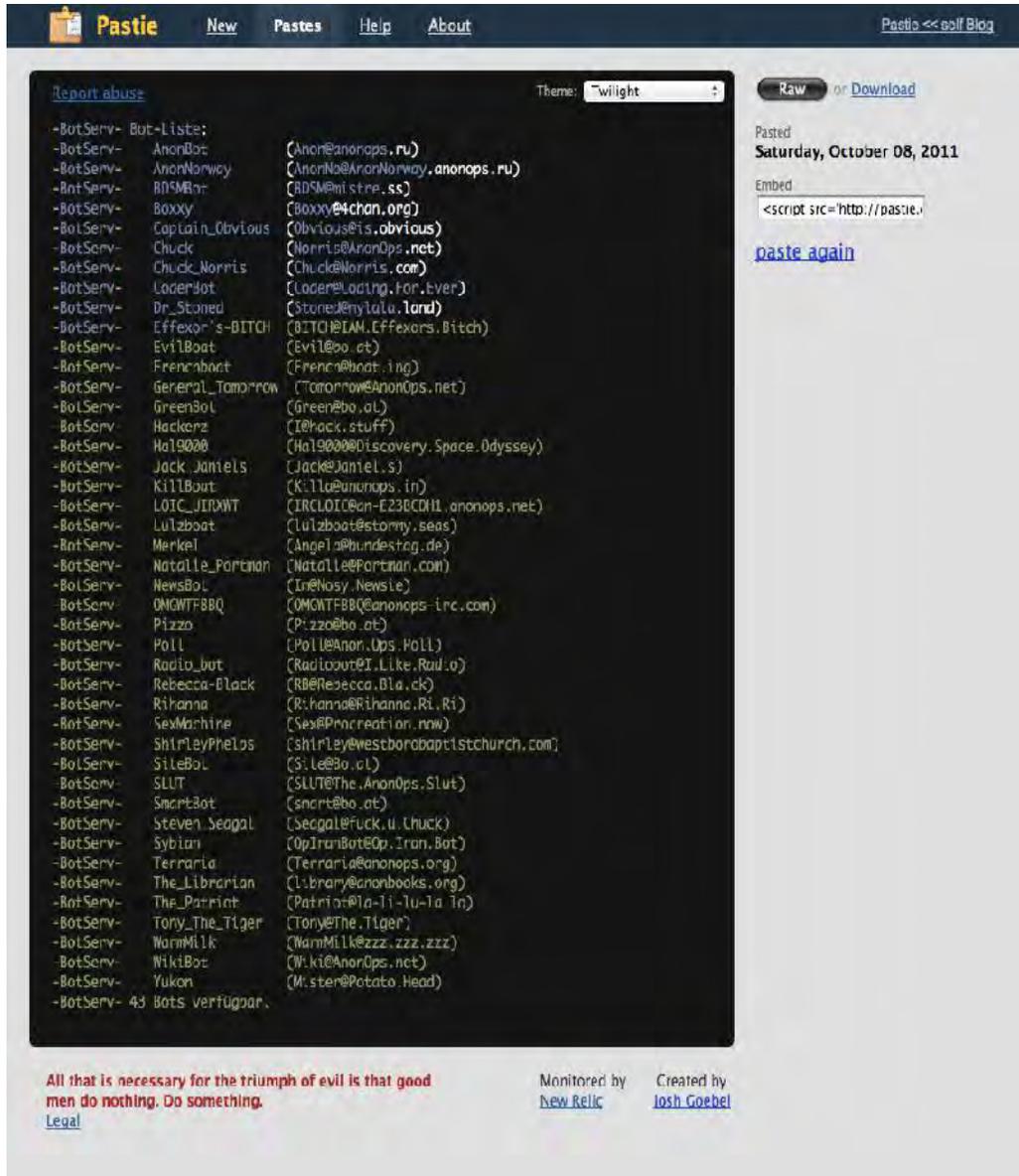
We thus cannot in any way support any business models which rely on the slavery of information for its own sustenance. If the freedom of information requires that the laws be changed, then we work towards those ends in a peaceful and reasoned manner. We will not stand idly as the law is used to protect the strong and to persecute the weak.

We understand that money is required to promote the arts and sciences, but we cannot allow the law to be used to enforce an empire of tyranny, harassment, and abuse. If the people decide to promote the arts and sciences, then we call for governments everywhere to promote them directly rather than through the creation of enforced monopolies.

If the law does not adapt to the new realities brought by new technologies and the Internet, then the march of technology will rob them of the ability to uphold the law. We thus call for governments everywhere to promote freedom of information whatever, wherever, and however it may arise. Governments which refuse to change with the changing world risk being left behind by it.

**WE ARE ANONYMOUS
WE ARE FREE
AND WE WISH YOU WOULD BE TOO**

Appendix 2.: Anonymous bots: from Pastie



The screenshot shows a Pastie page with a dark theme. The main content is a list of 43 bots, each with a name and an email address in parentheses. The list is titled "43 Bots verfügbar." and is preceded by a "Report abuse" link. The page also features a "Raw" or "Download" button, a "Pasted" date of "Saturday, October 08, 2011", and an "Embed" section with a script tag. At the bottom, there is a quote: "All that is necessary for the triumph of evil is that good men do nothing. Do something." followed by a "Legal" link. The page is monitored by "New Relic" and created by "Josh Goebel".

Report abuse Theme: `twilight` [Raw](#) or [Download](#)

Pasted **Saturday, October 08, 2011**

Embed
<script src='http://pastie.'

[paste again](#)

```
-BotServ- Bot-Liste:
-BotServ- AnonBot (Anon@anonops.ru)
-BotServ- AnonNorway (AnonNo@AnonNorway.anonops.ru)
-BotServ- BDSMBot (BDSMB@mistre.ss)
-BotServ- Boxy (Boxy@tchan.org)
-BotServ- Captain_Obvious (Obvious@is.obvious)
-BotServ- Chuck (Norris@AnonOps.net)
-BotServ- Chuck_Norris (Chuck@Norris.com)
-BotServ- LoaderBot (Loader@loading.for.ever)
-BotServ- Dr_StoneD (StoneD@nylala.lard)
-BotServ- Effexor's-DITCH (DITCH@IAM.Effexors.Bitch)
-BotServ- EvilBot (Evil@bo.at)
-BotServ- FrenchBot (French@botting)
-BotServ- General_Tomorrow (Tomorrow@AnonOps.net)
-BotServ- GreenBot (Green@bo.at)
-BotServ- Hackerz (I@hack.stuff)
-BotServ- Hal9000 (Hal9000@Discovery.Space.Odyssey)
-BotServ- Jack_Janiels (Jack@Janiels)
-BotServ- KillBot (Kill@anonops.in)
-BotServ- LOIC_JIRXWT (IRCL0IC@an-E23DCMIL.anonops.net)
-BotServ- LulzBot (LulzBot@stompy.seas)
-BotServ- Merkel (Angel@bundestag.de)
-BotServ- Natalie_Portman (Natalie@Portman.com)
-BotServ- NewsBot (In@Nosy.Newsle)
-BotServ- OMCWTFBBQ (OMCWTFBBQ@anonops-irc.com)
-BotServ- Pizzo (Pizzo@bo.at)
-BotServ- Poll (Poll@Anon.Ops.Poll)
-BotServ- Radio_bot (Radio@out.I.Like.Rad.o)
-BotServ- Rebecca-Black (RB@Rebecca.Black)
-BotServ- Rihanna (Rihanna@Rihanna.Ri.Ri)
-BotServ- SexMachine (Sex@P@n@cre@tion.new)
-BotServ- ShirleyPhelps (Shirley@westborobaptistchurch.com)
-BotServ- SiteBot (Site@bo.at)
-BotServ- SLUT (SLUT@The.AnonOps.Slut)
-BotServ- SmartBot (Smart@bo.at)
-BotServ- Steven Seagal (Seagal@Fuck.U.Chuck)
-BotServ- Syrian (OpIranBot@Op.Iran.Bot)
-BotServ- Terraria (Terraria@anonops.org)
-BotServ- The_Librarian (Library@anonbooks.org)
-BotServ- The_Patriot (Patriot@i-li-tu-ia.in)
-BotServ- Tony_The_Tiger (Tony@The.Tiger)
-BotServ- WarmMilk (WarmMilk@zzz.zzz.zzz)
-BotServ- WikiBot (Wiki@AnonOps.net)
-BotServ- Yukon (M.stem@Potato.Head)
-BotServ- 43 Bots verfügbar.
```

All that is necessary for the triumph of evil is that good men do nothing. Do something.
[Legal](#)

Monitored by [New Relic](#) Created by [Josh Goebel](#)

Appendix 3.: Anonymous bots: from Pastebin “DONT KICK OPS”



PASTEBIN | #1 paste tool since 2002 | create new paste | tools | api | archive | real-time | faq

PASTEBIN | Follow @pastebin | search...

create new paste | trending pastes | sign up | login | my alerts | my settings | my profile

AnonOps Dump #1

BY: ANONYMOUSDOWN ON NOV 15TH, 2011 | SYNTAX: NONE | SIZE: 317.65 KB | HITS: 2,007 | EXPIRES: NEVER

DOWN_CAD | RAW | EMBED | REPORT ABUSE

```
1. 0200 #noruk
2. - password: 4e97bca5e690a3793a1ca093c5c:8523f [MD5]
3. - founder: noruk
4. - descrip: noruks channel
5. - register: Wed Sep 7 16:38:15 2011
6. - last used: Wed Nov 9 14:18:35 2011
7. - flags: KEEPTOPIC, PEACE, SECURE, SECUREFOUNDER, SIGNKICK, XCP
8. - mlock: -ntr
9. - irc!serv: Rihanna
10. - bs flags: DONTKICKOPS, FANTASY, SYMBIOSIS
11. - access levels:
12.         NUM  LEV  NICK
13.         1    10  xy
14.         2     5  chenyue
15.
16. 0201 #opera1 ircpaybank
17. - register: Fri Dec 10 20:04:24 2010
18. - flags: FORBIDDEN
19. - forbidden: by Token, reason: This channel has been closed by network administration
20.
```

Public Pastes

- Untitled 3 sec ago
- 3x members.twitst... 22 sec ago
- Untitled 3 sec ago
- Untitled 7 sec ago
- Untitled 8 sec ago
- Untitled 8 sec ago
- Untitled 10 sec ago
- Untitled 13 sec ago

Appendix 4.: #propaganda word cloud with users

Appendix 7: Issue Crawler map for links from #leakspin

