Ad Captandum: The Efficacy of Information Operations on Electoral Interference

Kevin Zhang
New York University
Brooklyn, NY
zhang.kevin@nyu.edu

***Abstract*—**Globally, foreign Information Operations (IO) with the goal to disrupt local and national elections have drastically increased, creating new challenges for the privacy and national security landscape. Utilizing social media companies as their main vector for distribution, foreign information operations misinformed and biased popular opinion through sharing by state-sponsored news organizations. In the aftermath of the 2016 US Election's Special Counsel investigation, Russia had definitively US voters through a strategy built by disinformation and social media campaigns to cause social discord. As a main takeaway, there have been increasing efforts from social media companies to staunch the rate of foreign involvement in electoral manipulation. In doing so, these companies have begun culling the tide of fake and state sponsored accounts.

This paper provides a comprehensive analysis of the differing strategies state actors use for their information operations. Using political transparency information data sets, this paper aims to explore whether there is a statistical correlation between when an account becomes "active" and when it is removed from Twitter. In this study, I explore publicly released banned accounts data from Twitter's Transparency Report on Russia, China, and Iran IO accounts during the period before the 2016 US election to the present day. The strategies examined include account dormancy, hashtag and follow usage, and geotagging as main strategies employed to interfere directly with target audiences. In determining which strategies were effectively deployed, I found that my hypotheses for following metrics and geotagging ranked high as tactics for either increasing social media spread. However, increasing IO account dormancy to obfuscate themselves from a censor was proven statistically insignificant, and did not play a large factor in intervention strategy.

Keywords: Information operations, Fake accounts, Misinformation, Electoral interference, International relations

I. Introduction

Electoral interference is by no means a new concept; it is generally accepted that countries will exert political influence through intelligence networks. However, with the advent of social media and a globally connected world, it becomes much easier for foreign agents to broadcast messages to specifically influence target audiences. As stated within the 2016 election report by the US Senate Select Committee on Intelligence, "The Russian government directed extensive activity…against U.S. election infrastructure' at the state and local level" [1]. The report later indicates that Russia was not directly involved in vote tampering, with the second volume of the report displaying evidence that Russia's extensive social media influence was a side-channel attack on the U.S. population.

These foreign entities attempted to sow discord amongst the American electorate by using false social media accounts and targeted data, and creating division within political parties to weaken the institutions and erode the integrity of the presidential election[2]. This is magnified by the increasing trend to create organizations similar to the Internet Research Agency (IRA) and "Fancy Bear" and "Cozy Bear" units (elements of Russia's GRU military intelligence units), seeking to exploit any advantage to seize the upper hand in the political arena. Increasingly, military, intelligence, and information security divisions are being formed, with battle lines and strategies forming. The front-line soldiers, however, are a vast army of bot accounts. For example, the IRA prepared hundreds of thousands of accounts to disseminate fake news and engender what is referred to as "chaos."

This strategy, though crude and considered by some as "sloppy," would prove effective in pulling attention away from major foreign policy events through indiscriminate targeting, the integrity of the electoral process and Americans' trust in the system would erode significantly; this strategy, though crude and considered by some as "sloppy," would prove effective in pulling attention away from major foreign policy events [3].

However, it is important to note that foreign electoral intervention in the US began far before the 2016 electoral cycle, and was not limited in scope to Russia. Although not all these IO campaigns are directed towards the United States, the principal reagent that precipitated in Twitter discovering these accounts were the studies by the US Congress and the Special Counsel post-2016 election. Present within Twitter's Information Operations Data Set are accounts from a variety of global regions.

The success of the IRA and GRU's platform manipulation during the 2016 electoral cycle raises significant challenges for these social media companies; how best to defend against a side-channel attacker? What techniques have evolved between the last election cycle and the present one? As defenses have improved on both the social media company and governmental level, to what degree are the companies responsible for filtering misuse?

II. Approach

A. Twitter Data Set

Twitter maintains extensive data sets on IO user accounts, tweets, and accompanying media to systematically examine how the platform is utilized for external state influence. The data set [4] is available through Twitter's Trust and Safety and Transparency teams, which provides data to researches in

hopes of improving automated detection. This data set includes not only examples of Russian IOs, but also interference from China, Spain/Catalonia, Iran, Venezuela, and Russia, among eight other country sets.

My approach largely examines the aforementioned data set, containing information specifically regarding suspended and removed Twitter accounts related to foreign IOs. This data is divided into three portions: the user information, tweet information, and media associated with the tweet. Additionally, tweet and user metadata are available for analysis as well.

The data sets themselves are divided per country and distribution date (Twitter continues to update the Transparency Report quarterly with freshly banned account information), with April 2020 as the most recent date. Although released recently, these data sets contain accounts discovered as early as 2008. Additionally, each release of banned accounts is accompanied by either a blog post or tweet thread from the Twitter Trust and Safety team outlining exact reasons why these accounts had been removed (e.g. electoral manipulation operation targeting specific countries).

In selecting the data, I sought to locate a sample of accounts with the highest volume of tweets, while also preserving the distinct foreign policy goals laid out by the accompanying Twitter blog. Specifically, I identified China, Russia, and Iran as countries of interest that would best fit my model, and provide interesting differences in IO procedure. The Chinese data sets were captured in August of 2019, tailored to counter the Hong Kong protest and growing democracy movement present at the time [5, 9]. Meanwhile, the Russian data sets document interference by the Internet Research Agency (IRA), a designated member of Russia's extensive "web brigades" that targeted the US 2016 Presidential and 2018 Congressional elections[6, 7] Finally, the Iranian data sets demonstrate a clear attempt to push Iranian ideals and foreign policy to regional neighbors and provides interesting insight; the created accounts did not aim to counteract a specific individual event or election, but rather to distribute pro-Iranian views[6, 7, 8] . Both the Russian and Iranian data sets were released during a period from late 2018 to mid-2019.

Figure-1: Please see Appendix A

B. *Problem Questions and Hypotheses*

After de I was fascinated by the methodology in which these IO accounts sought to attack institutions of civil society. Numerous data points and classifiers within the data revealed different avenues by which a skilled attacker could maximize their misinformation spread, while also remaining eluding the Twitter censor. Consequently, I bound my analysis by two principal questions that would determine the efficacy of IOs on elections:

1) What strategies are used on Twitter by foreign IOs teams and how are they implemented?

2) Did these strategies successfully maximize spread while remaining undetected by Twitter?

In the literature review, I was able to identify that various IO groups use targeted tactical maneuvers to ensure maximum impact upon a population. Primarily, they mimic popular accounts and hashtags to associate with political movements such as Black Lives Matter (e.g. from the Ghana data - African Lives Matter). Additionally, to avoid detection by the proper authorities, the accounts adopted dormancy strategies, with Russian accounts waiting for an average 177 days before creating a single tweet or retweet [10]. Additionally, the accounts put on the façade that their accounts and tweets originate in their target country to manipulate the spread from fake accounts to legitimate ones [12].

I wanted to explore three distinct strategies mentioned above (dormancy, hashtag and following metrics, and geolocation) that IO accounts could utilize to mask their actions and increase their efficiency in spreading false information. To ensure that I could robustly define the problem statement and tactics outlined above, I developed hypotheses regarding the three strategies in use:

1) Dormancy: As IO accounts have longer dormancy periods between their account creation and their first tweet, their overall lifespan would increase (along with their capacity to spread misinformation). This is chiefly due to Twitter potentially viewing longer living accounts as more likely to be human.

2) Hashtags and Follow Metrics: Primarily, hashtags for IO accounts will reflect current political trends present during when the tweet is published. Additionally, I believe that as the number of accounts the IO account follows increases, so too will its own following count. This perpetuates the idea that increasing a users' audience will assist in adding you to other users' suggested accounts or follow lists.

3) Geolocation: Geotagged location will affect the spread of both IO accounts and their tweets, as individuals from that location may retweet or share. This also serves as some form of obfuscation, as the IO account will falsifying its geolocation.

C. Limitations

In evaluating the data set using the above methodology, I may encounter some limitations with either the scope of the project or the data itself.

This approach's main weakness is that it relies on statistically significant values to provide insight on whether strategies are fruitful for IO accounts to pursue. If the analysis returns high p-values or low correlation coefficients, there exist the possibility that I may not be able to draw any substantive results from the data set. Though, this may serve in identifying a conclusion to a null hypothesis from a low correlation value (the variables may not contribute to IO's spread or obfuscation); however, other statistical analysis can be used to potentially study the data.

Finally, it is possible that the data sets I specifically chose by country(or the methodology of choosing variables within the data sets) are sound applicable for this type of analysis, and our correlated values to not provide us valuable understanding of the data. If the datasets themselves do not provide conclusive data, some subjective questions can still be answered simply from working through the data itself (e.g. number of bot accounts). In this capacity, I did identify the lack of a variable (the exact date in which the accounts were removed or taken down) and proceeded to use existing data to form a proxy variable.

D. Summary of Contributions

This report's findings can be itemized as follows:

- Utilizing Twitter's Transparency report datasets, I was able to identify three principle strategies IO accounts were using to further their goal of electoral manipulation.
- Using a cross-country analysis between Russia, China, and Iran, I was able to differentiate different approaches to electoral interference. The analysis revealed that all the accounts tend to follow more accounts to increase their visibility and spread.
- Using hashtag word clouds, I was able to analyze the topic of the IO tweets, and determine that these accounts benefitted from joining in on the conversation regarding controversial political and social-cultural topics trending at the time
- Additionally, the data proved the null hypothesis for dormancy and indicated that dormancy did not affect the speed in which Twitter identifies and removes its accounts as bots.
- Finally, I discovered that Russia, Iran, and China engage in falsification of geographic tagging to create the appearance that the IO accounts are real individuals within their target countries.

III. Evaluation

A. Dormancy Test

Analysis of dormancy strategy uses a combination of calculating important key dates within the lifespan of the IO accounts and conducting a correlation analysis using Pearson correlation coefficient (PCC) [11].

Initially, I tested my approach with a single partition of the Iranian dataset as all the datasets contained within the Twitter Transparency Report are uniform. Using the Pandas library, I identified important metadata and element headers within the Comma Separated Values (CSV) file that would best examine whether the strategy account dormancy proved effective.

Specifically, I sought to retain the *userid*, *tweetid*, *account_creation_date*, and *tweet_time* variables, as my analysis explicitly dealt with date and time related data. Both *userid* and *tweeted* assisted in differentiating unique accounts and tweets. Additionally, with each portioned dataset, I included a self-created column identified as "*TwitterReleaseDate*". This column indicated the date in which the banned accounts in that dataset had been released in the Transparency Report. Additionally, in order to identify the first and last times the accounts had tweeted, I used a *min()/max()* function as part of the NumPy library [20] to scrape the data and pull the *tweet_time* at the extremes.

Three values were of importance: the takedown date, the dormancy period, and the overall lifespan of the account. The data itself did not contain the exact date when the accounts had been suspended or banned. As a proxy, I calculated the takedown date by averaging the "*TwitterReleaseDate*," and 2) the last tweet sent out by the account (the NumPy.Max operation on *tweet_time*). Both dormancy period and overall lifespan could be measured by length of days; I calculated the dormancy period by measuring the time difference between the *account_creation_date* and the first tweet, and determined the lifespan of the account by processing the time delta of the just-computed *Takedown_Date* subtracted by the *account_creation_date.*

Following, I ran Pearson Correlation tests specifically to conclude whether a longer dormancy period would affect the overall lifespan of the account. The variables I used as potentially correlated values were *Dormancy_Period* and *Account_Lifespan*. Additionally, I used the matplotlib library [12] to visually represent this data in a scatterplot, as shown for the Russian dataset below in Figure 1. Both the plots for Iran and China are included in Appendix B.1 and B.2.

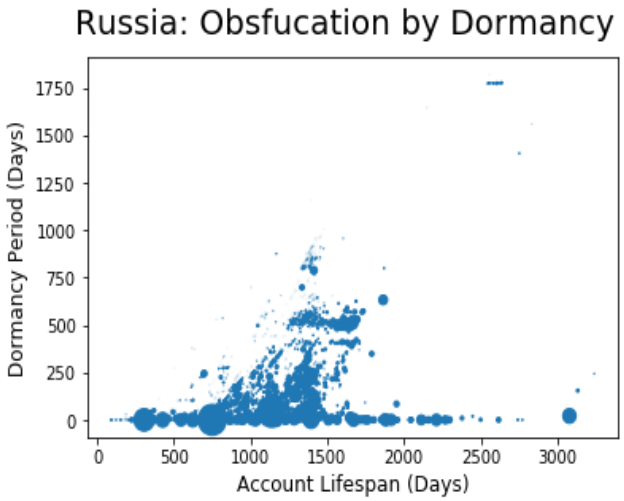


Figure-2: Please see Appendix B

B. *Dormancy Results*

In examining the results in closer detail, I realized that none of the values were correlated when The Pearson Correlation Coefficient was applied to dormancy period and account lifespan. Russia had the highest correlation value, with a PCC value ≈ 0.53186, while both China and Iran had values of ≈ 0.47867 and ≈ 0.40687, respectively. These indicated that for the most part the data was not highly correlated, and thus did not serve as an effective strategy. This is further demonstrated in the scatterplots, included above in Figure-2 and in Appendix B.1 and B2.

Russia's distribution does have some mild statistical significance, as there exists a "cluttered" – normal distribution. The fact that many accounts do have both larger dormancy periods and longer lifespans lends some credence to the theory that dormancy may help with obfuscation; however, the data itself is skewed by the high number of active accounts with close to no existing dormancy period.

Interestingly, there also exists a slight linear correlation in the Chinese dataset. However, China's accounts differ in that there exist chiefly two distinct groups of accounts. Firstly, there were a large portion of accounts that were extremely active (number of tweets), that did not have a period of dormancy. Additionally, there was a subset of accounts that did remain relatively dormant and I did see a linear trend between the two values; however, these accounts were comparatively less active.

Potentially running this test again and dropping the values for which no dormancy period exists may provide further insight as to whether dormancy plays a role. However, this also runs the risk of skewing the data even further. Ultimately, the null hypothesis is satisfied for the dormancy strategy: dormancy period has no affect on the overall lifespan and subsequent take down rate of these IO accounts.

C. *Hashtag and Follow Metrics Test*

In order to analyze the contents of a tweet message and potential to spread, I examined two distinct metrics: frequency of hashtags used per tweet, as well as overall twitter following data. Ultimately, I ran another PCC correlation test on the follower/following metrics to determine whether either would affect the other. I began my analysis by identifying the key variables: *follower_count*, *following_count*, *tweet_language* and *hashtags*. Additionally, I retained *userid* and *tweetid* to distinguish unique accounts from each other.

To best analyze the hashtags, I presented the data in a visual format that would indicate the trending topics explored over the entire period of data. I filtered the NaN values out and sorted the tweet hashtags based on *tweet_language* to match the language utilized in this report and created a dictionary titled *word_cloud_dict* to contain all the tweet hashtags. Using the wordcloud library, I proceeded to plot the dictionary in a cluster, where larger words would indicate higher frequency of use within the dataset. It is important to note that the values represented are categorized per *tweetid* and not *userid*.

In analyzing Follow metrics, I chose to group the *follower_count* and *following_count* metrics by *userid*. It is important to make a clear distinction between the two main variables: *follow_count* specifically refers to the number of Twitter followers an account may have, whereas *following_count* refers to the number of accounts that unique account is subscribed to at the time. Both values are captured at the moment of account deletion (in this example, the *Takedown_Time*). Utilizing PCC, I correlated the two values for each country, examining whether users who follow more people will in turn have higher follower counts. In doing so, I also used matplotlib library [12] to create a scatterplot to represent the data best visually (see below Figure 3 and Appendix C.1 and C.2).

Figure 3: Please see Appendix C

D. *Hashtag and Follow Metrics Results*

Through my hashtag analysis and follow metric correlations, I was able to identify popular topic trends during the timespan of all three countries' datasets. Additionally, for the Chinese and Russian datasets, I was able to find a high correlation between the number of followers an account has as compared to the number of accounts that unique account is subscribed to (i.e. following).

With the Russian dataset, I found two distinct groups of hashtag topics: those related to news sites, and those related to US political issues. The first set of hashtags contains values like "news", "sports", "politics", "world", and "business," all of which can be inferred as column headings for a news site. This fits with the trend indicated by other sources that many of these Russian accounts were instrumental in the proliferation of news stories favored by state-sponsored news companies (e.g. Russia Today) [17]. A secondary cluster of hashtags containing values like "Blacklivesmatter," "MakeAmericaGreatAgain," and "StopimportingIslam" touch upon controversial political and cultural movements, specifically in the United States.

This does differ in the case with Iran and China, as both countries may have different goals in mind when tweeting. For example, Iran's primary hashtag cluster center on geopolitical issues, with constant reference to other countries in its region (e.g. "Palestine," "Gaza," "deleteIsrael," "letkashmirbefree," "grouppalestine.").

After performing correlation test on following and followed account values, I found that Russian accounts have a highly correlation value of ≈ 0.85287. This indicates that accounts that follow more accounts will have larger following

counts themselves. It is important to note that there is very low causal interference in this test, as the act of following another account (*following_count*) is actively controlled by the user.

Although this may seem relatively standard for twitter accounts, it is important to note that this may not be a target strategy for all IO accounts. This correlation is consistent in the Chinese dataset, with a measured correlation coefficient of ≈ 0.79109. However, this trend is not shared by the Iranian dataset, as its correlation coefficient sits at ≈ 0.06378. This is indicative that Iran may be utilizing a varied approach in Tweet distribution.

Initially, I believed that the best way to demonstrate the importance of the topics was to utilize a natural language processing system to categorize and count related hashtags. However, due to hardware constraints of my personal system, I was unable to see this method through. Instead, I opted to display the hashtags visually in a word. Although maneuvering away from an empirical analysis, a word cloud would allow me to best identify trends IO accounts would best take advantage. This visual representation of the data would provide a good steppingstone for future research using natural language processing methods.

E. Geolocation Test

As tweets of various countries had differing degrees of reach and strategy involved, geo-tagging of tweets can provide insight into the IO strategy. I examined the five most popular and distinct geo-tagged locations within the Russian, Iranian, and Chinese datasets. My key goal was to assess whether those geo-tags affected that number of retweets a tweet received.

When partitioning the data, I focused my evaluation on the *user_reported_location* column header, which indicates the location where the tweet was tagged. This value is self-generated, as the user can fill the location with whichever location they choose (as opposed to being tied to the device's location sharing application or GPS). Geotags are also not exclusive to exiting cities or countries; non-existent places, such as "somewhere on earth," can also be tagged. Additionally, I chose to examine *retweet_count* as a measure of spread, as tweets with higher retweet numbers will reach larger audiences. Finally, as I was examining individual tweets, I chose to group these values using the *tweetid* variable.

In processing the data, I dropped all accounts that did not contain locations. For the Russian Dataset, this was around 15% of the data, as the majority of tweets contained geotagging. I then grouped the data in ascending order based on the locations with the highest number of tweets. For each dataset, I picked there top five locations to run further tests on. These locational distributions (or tags) were distinct in that I attempted to avoid repetitive values (e.g. in Russia's data set, the two most popular tags are "USA" and "United States"). Additionally, I attempted to vary the geographic distribution of locations selected to see differences in retweet counts.

For each location, I produced a histogram detailing the frequency (total number of tweets) and number retweets for that specific location. Finally, I used ANOVA [14] to determine the variance distribution among the five discreet locations, per Iranian, Chinse, and Russian data sets. Using this, I determined whether there was a statistically significant value in the relationship between geotagged location and retweet count. I also included a histogram indicating the number of retween compared with the total number of unique tweets per each country-geolocation (Figure 3 as seen below, or Appendix D.1-D.14)

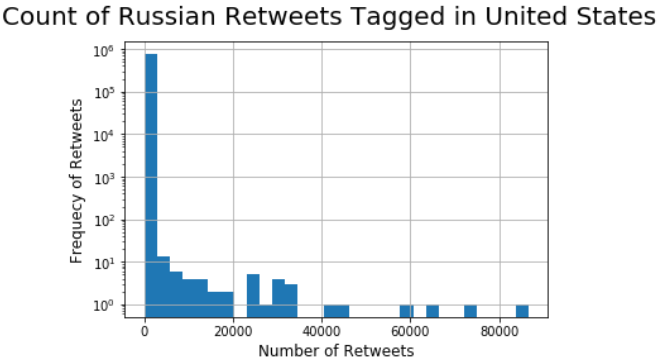


Figure 3: Please see Appendix D

F. Geolocation Results

In examining tweets from different geotagged locations and their varying degrees of reach, I selected the most popular geotagged locations. The locations provided some clarity and insight into the country datasets, as they built on the strategic narrative examined in the other strategies. Specifically, the popular geotags differ greatly between Iranian, Chinese, and Russian datasets.

Specifically, for the Russian data set, common geotags revolved around United States and Russian cities, such as New York and Moscow. The Russian cities had both their Cyrillic and English Romanticized versions of the names appear frequently. An interesting outlier was the geotag "USA #Islamistheproblem #Wakeup," which incorporated both a hashtag and geotagging as a strategy (see previous section on hashtag use). Curiously, this geotag was one of the top five most used hashtags among Russian IO accounts.

Iran and China differ in that they focused more on different geographical regions. Iran's geotags tend to revolve around Middle Eastern locations (e.g. Pakistan, Kingdom of Saudi Arabia). China has an interesting distribution, with many values being in the United States (e.g. San Francisco). However, China's top five geotagged locations contain two locations in simplified Chinese script: Bronx, NY, and the People's Republic of China.

Additionally, using ANOVA variance analysis, I identified that geolocation does play a role in retweet count for all three of our country models. Regarding parameters for use of ANOVA, the assumption for comparison of population parameters within ANOVA is satisfied, as each data distribution resembles a log-normal distribution. Utilizing the five distinct locations indicated above, I was able to output ANOVA p-values for each country data set. Russia maintained an ANOVA p-value of $1.541e^{-137}$ and f, and f-statistic of ≈ 160.42. Its p-value which is very close to zero. Iran's and China's p-values were similar, with p-values extremely close to zero (represented by a literal p-value output of zero) and f-

statistics ≈ 4948.45 and ≈ 3919.38, respectively. As each fall below the statistical significance p-value of < 0.01, this statistical significance in difference of retweets helps us arrive at the conclusion that geo-tagging was instrumental in extending the reach of tweets

IV. Related Work

Throughout my literature review, I was unable locate empirical studies on the effects of IO accounts and the various strategies that they utilize to engage in platform manipulation. Twitter itself publishes blog posts and data dumps regarding its own data; however, they rarely delve deep into statistical analysis. Additionally, I found few papers that provide analysess and recommendations to these social media companies on how to better curate and adjust their transparency settings. Many of these papers conduct an ex post facto view on electoral interference, without providing guidance on how best to combat foreign IOs.

Much of the existing work on this topic is legal in nature, focused on the legality of the issue, while addressing the social culture effects of the intervention. The analyses provided are namely of a high-level, governmental opinion, largely relying on claims made by foreign policy analysis units and governmental bodies [15]. Many of these papers are opinion pieces crafted in response to governmental actions, such as the release of the Mueller Report in late 2019. This is even true of some papers published within technical journals, such as "Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election," [18] a paper which outlines a modicum of techniques foreign interventionists used to disrupt the election.

Many papers tend to focus strictly on Russian intervention; on the contrary, data pulled from the Twitter Transparency Report [4] details that that numerous countries engaged in this IO platform manipulation, both against the United States and other countries. My work focuses on how these foreign IOs differ in regards to strategy, payload, and target.

A subset of this also exist, as I was unable to identify a paper that had utilized Twitter's election transparency report [4]. Twitter has released other information in the past; however many articles examine specific advertisements paid for by potential IO counterparties, rather than social media accounts.

Nevertheless, some papers come close to the work done within this project. Specifically, papers analyzing doctored social media posts and building tools to identify future troll farm posts. Adam Badawy's paper [16] demonstrate that interference can be exacerbated by natural spread via social media (tweets and events were retweeted and shared by senior, bipartisan pundits and interest groups).

The Hamilton Dashboard [17] provides one such service: using machine learning to aggregate and identify informal Russian soapboxes on social media through their re-sharing of Russian state-sponsored news. However, the dashboard does come with an important caveat: "'These channels and accounts often engage with topics...that are in no way affiliated with the Russian government. It would therefore be INCORRECT to, without further analysis, label anyone or anything that appears on the dashboard as being connected to Russian propaganda.'" While the Hamilton Dashboard is still in their adolescent phase and therefore conclusions cannot be precisely drawn from their data, research does demonstrate that there are certain patterns and trends when dealing with botting and IO accounts.

V. Conclusion

As the nature of our election cycles change and increasingly, we look to social media as our news outlets, platform manipulation by IO accounts will continue. These information operations act as force multipliers, allowing foreign entities increased access to new angles of attack.

The goal of this project was to determine which strategies IO accounts employ successfully to both increase their information dissemination and evade Twitter's detection. Successfully, I was able to identify key strategies that contributed to further platform manipulate by IO accounts. Specifically, false geolocation tagging and influencing of follower metrics were statistically significant strategies that assisted IO accounts to further the audience for their false information, while decreasing their chances of being detected.

For future work, I plan on exploring more of Twitter's Transparency dataset; I wish to see if their strategies hold up with the countries I examined in this report. Additionally, comparing different social media companies and their responses to information operations may also reveal varying counter-information operation strategies. Twitter maintains that they are "committed to providing a platform that fosters healthy civic discourse and democratic debate" [19]. However, the battle between social media platforms and IO accounts progressively takes the appearance of a cat and mouse game, consistently stuck in the same feedback loop.

Although the results in this paper do point towards certain strategies that may have been used in the past, IO accounts have the advantage in that they simply need to adopt a new modus operandi to evade Twitter's censor. In all three datasets examined in this project, single use accounts with single tweets exist alongside accounts that may have 200,000 tweets under their belts. The goals remain the same, but the strategies are increasingly modified. The identification and removal of these accounts does not limit further platform abuse, nor does it discourage a motivated, resourceful attacker. The principle of "who's responsibility is it to curate/filter" continues to serve as an important question that will need an answer, sooner rather than later. Thus, the real collective action problem emerges: whose role is it to determine the truth?

Acknowledgment

Thank you to NYU Professor of Computer Science Rachel Greenstadt and NYU Ph.D Candidate Janith Weerasinghe, who guided me in crafting this privacy study. An un-hashed version of Twitter's Data Set was also generously provided by Twitter's Trust and Safety Team. The full dataset can be found in the reference section [4].

REFERENCES

[1] United States Senate Select Committee on Intelligence. Report Of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 1. Washington: GPO, 2019. Print.

[2] United States Senate Select Committee on Intelligence. Report Of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 2. Washington: GPO, 2019. Print.

[3] Rosenberg, Matthew, et al. "'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020." The New York Times, The New York Times, 10 Jan. 2020, www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

[4] Twitter,``Transparency Report - Information Operations," https://transparency.twitter.com/en/information-operations.html

[5] Twitter Safety. (2019, August 19). Information operations directed at Hong Kong. Retrieved May 3, 2020, from https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html

[6] Gadde, V., & Roth, Y. (2018, October 17). Enabling further research of information operations on Twitter. Retrieved April 10, 2020, from https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html

[7] Twitter Safety. (2019, December 20). New disclosures to our archive of state-backed information operations. Retrieved March 31, 2020, from https://blog.twitter.com/en_us/topics/company/2019/new-disclosures-to-our-archive-of-state-backed-information-operations.html

[8] Roth, Y. (2019, June 13). Information operations on Twitter: Principles, process, and disclosure. Retrieved May 1, 2020, from https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html

[9] Gadde, V., & Roth, Y. (2018, October 17). Enabling further research of information operations on Twitter. Retrieved April 10, 2020, from https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html

[10] Twitter Safety. (2019, September 20). Disclosing new data to our archive of information operations. Retrieved April 23, 2020, from https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html

[11] Starks, Tim, et al. "Russia's Manipulation of Twitter Was Far Vaster than Believed." POLITICO, 5 June 2019, www.politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543.

[12] Strangman, G. (2002). Scipy.stats.pearsonr Python Library. Retrieved April 18, 2020, from https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.pearsonr.html

[13] Matplotlib Python Library. (202, April 8). Retrieved May 10, 2020, from https://matplotlib.org/3.2.1/contents.html

[14] Wordcloud Python Library. (2020, May 2). Retrieved May 3, 2020, from https://pypi.org/project/wordcloud/

[15] Analysis of Variance (ANOVA) - Python for Data Science. (2018, November 15). Retrieved May 3, 2020, from https://pythonfordatascience.org/anova-python/

[16] Trenin, Dmitri. "Collision Rather Than Collusion: Issues in Russian-U.S. Relations." Asia Policy, vol. 24, 2017, p. 33-38. Project MUSE, doi:10.1353/asp.2017.0041.

[17] A. Badawy, E. Ferrara and K. Lerman, "Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign," 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Barcelona, 2018, pp. 258-265.

[18] SchaferMedia, Bret, and Bret Schafer. "Hamilton 2.0 Methodology & FAQs." Alliance For Securing Democracy, German Marshall Fund of the United States, 4 Sept. 2019, securingdemocracy.gmfus.org/hamilton-2-0-methodology-faqs/.

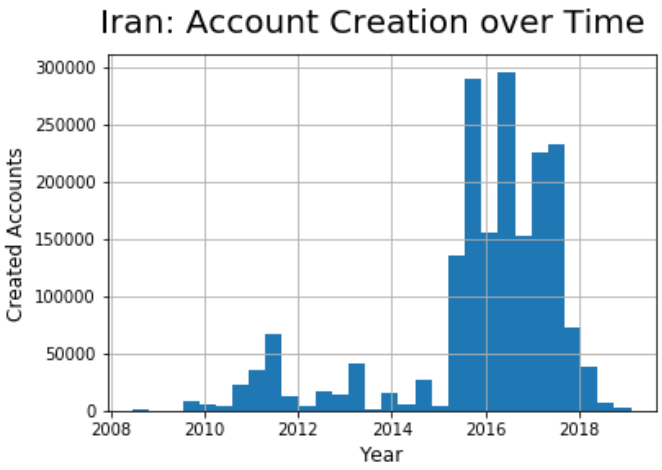
[19] H. Berghel, "Oh, What a Tangled Web: Russian Hacking, Fake News, and the 2016 US Presidential Election," in IEEE Computer Society: Computer, vol. 50, no. 9, pp. 87-91, 2017.

[20] "Update on Twitter's Review of the 2016 US Election." Twitter, Twitter Public Policy, 19 Jan. 2018, blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.

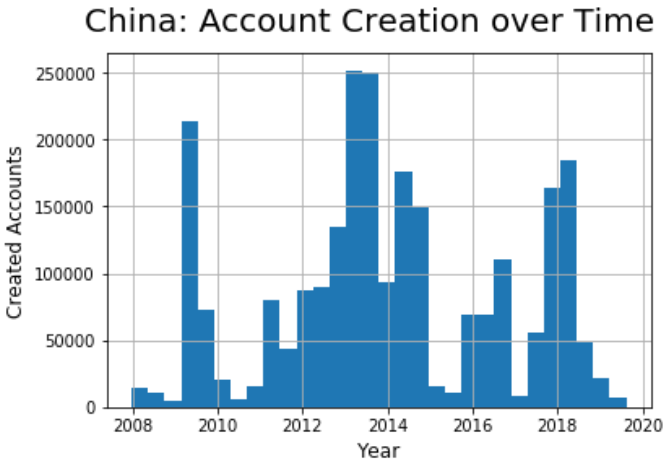
[21] Numpy.loadtxt — NumPy v1.19.dev0 Manual. (2020). Retrieved May 3, 2020, from https://numpy.org/devdocs/reference/generated/numpy.loadtxt.html?highlight=loadtxt

[22] T. (2018, October 17). Today we are releasing all the content associated with previously disclosed information operations that we have found on our service since 2016. Our goal is to enable further independent academic research and investigation: Https://t.co/rBJNiCjjif. Retrieved May 1, 2020, from https://twitter.com/Policy/status/1052543582199050240

APPENDIX A

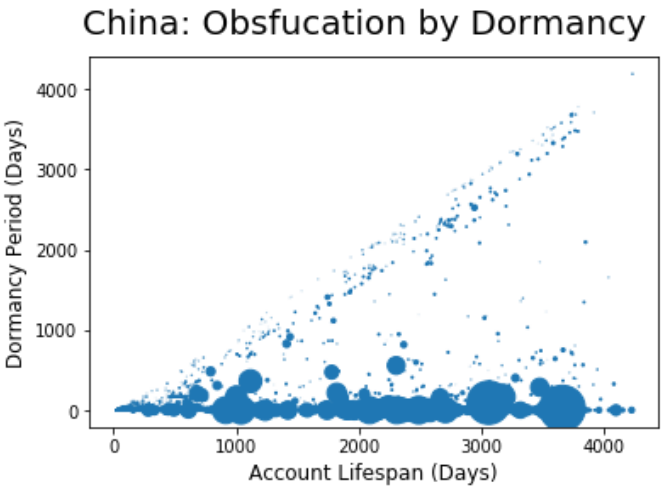


Appendix A.1

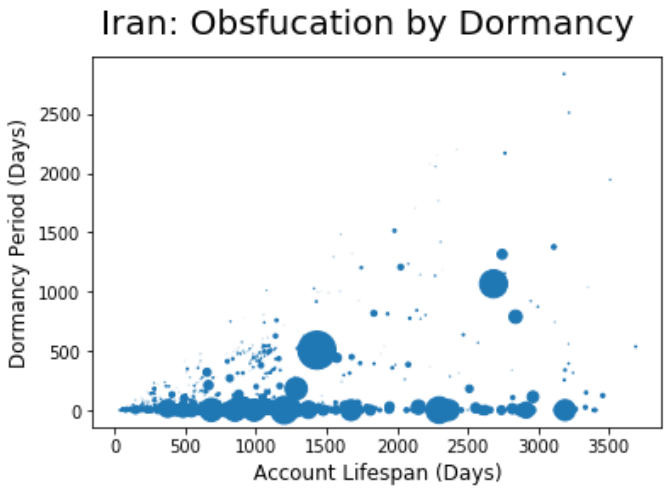


Appendix A.2

APPENDIX B

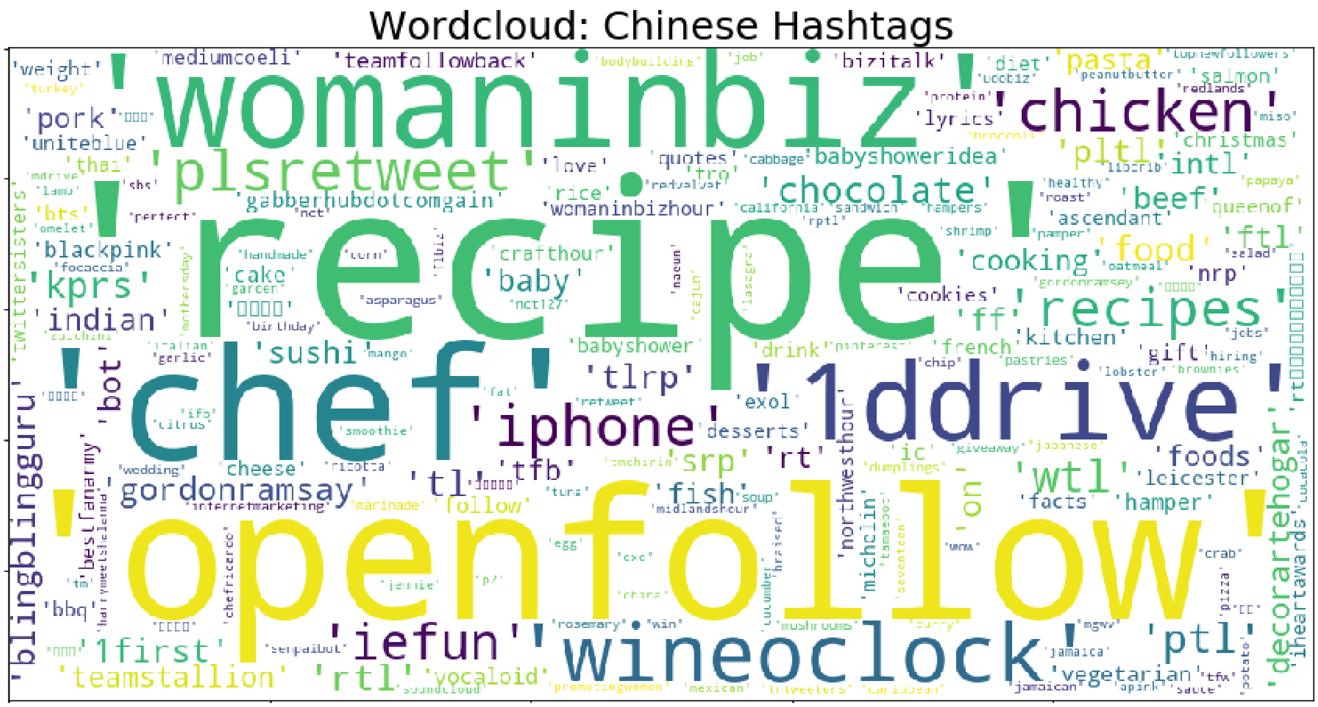


Appendix B.1

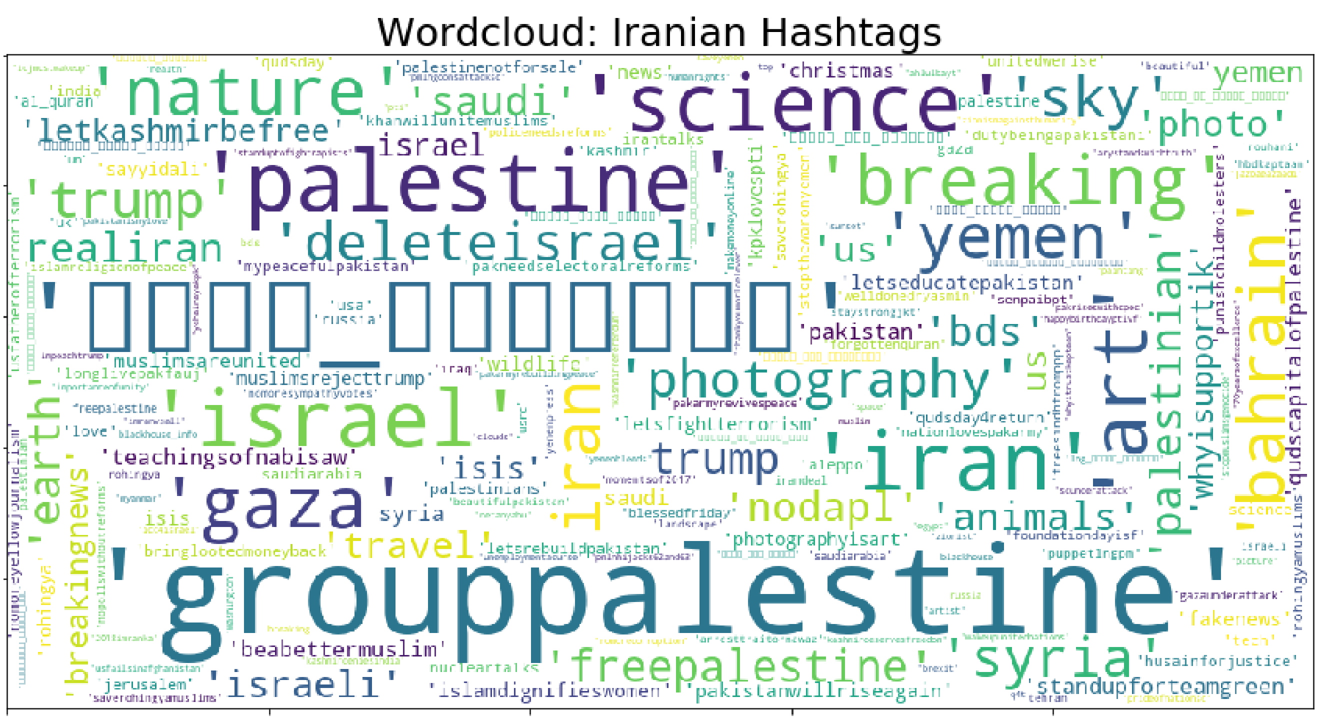


Appendix B.2

APPENDIX C

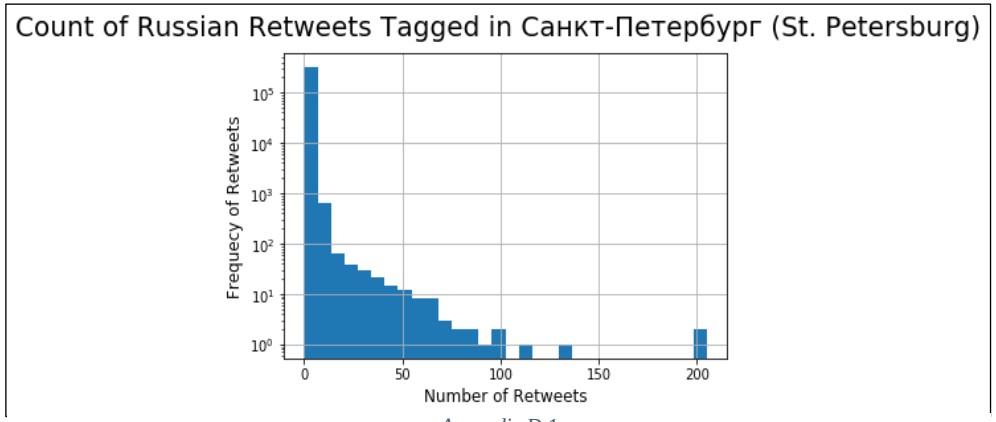


Appendix C.1

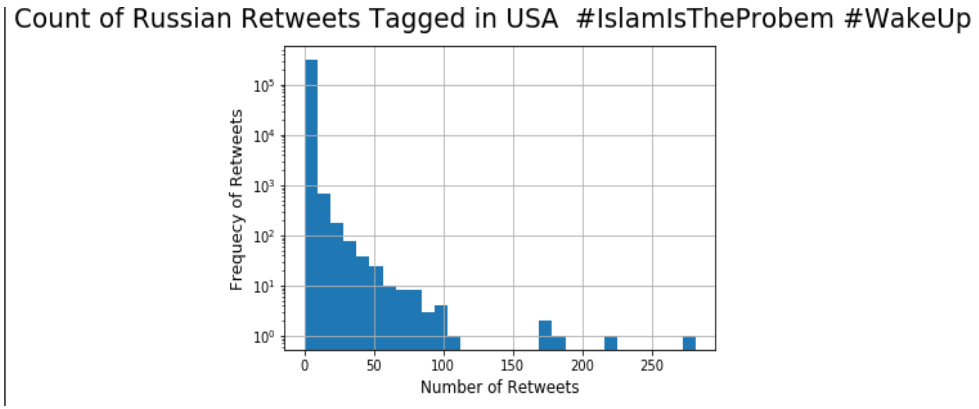


Appendix C.2

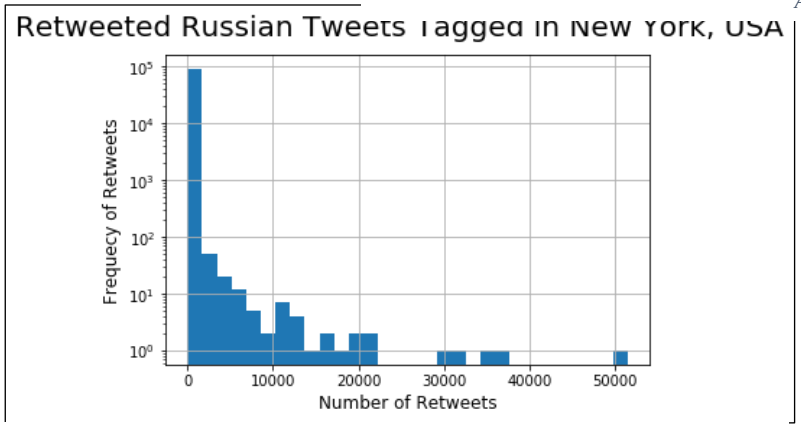
APPENDIX D



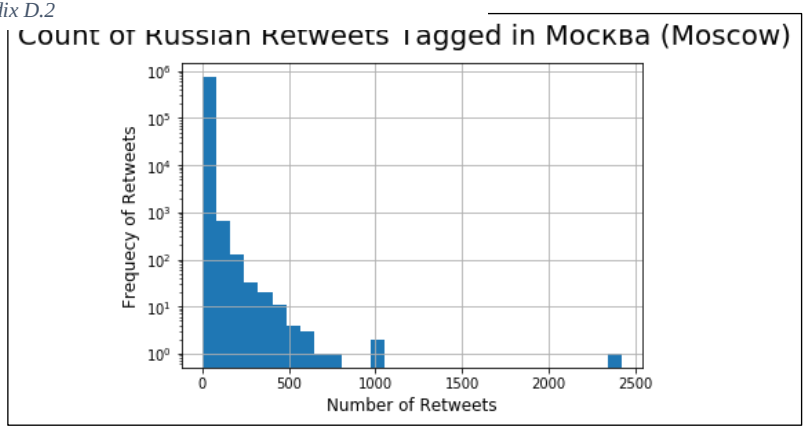
Appendix D.1



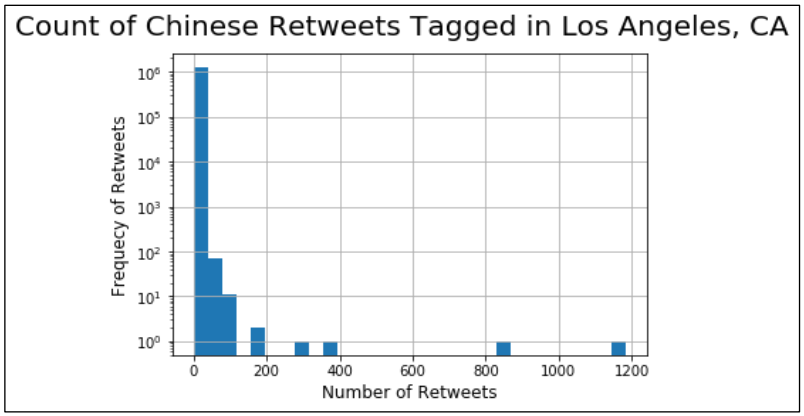
Appendix D.2



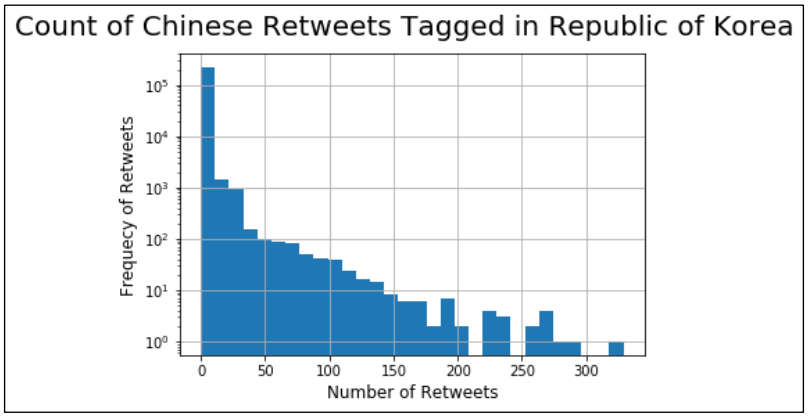
Appendix D.3



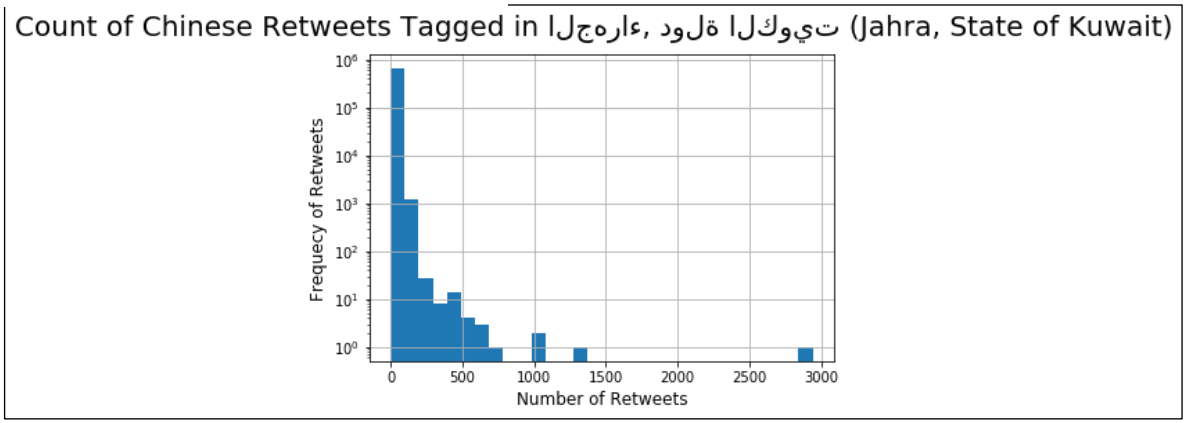
Appendix D.4



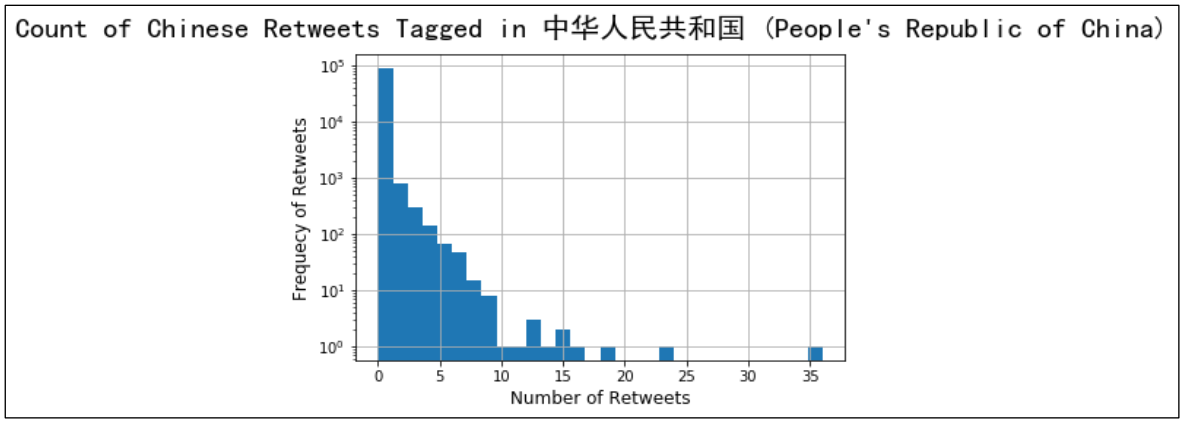
Appendix D.5



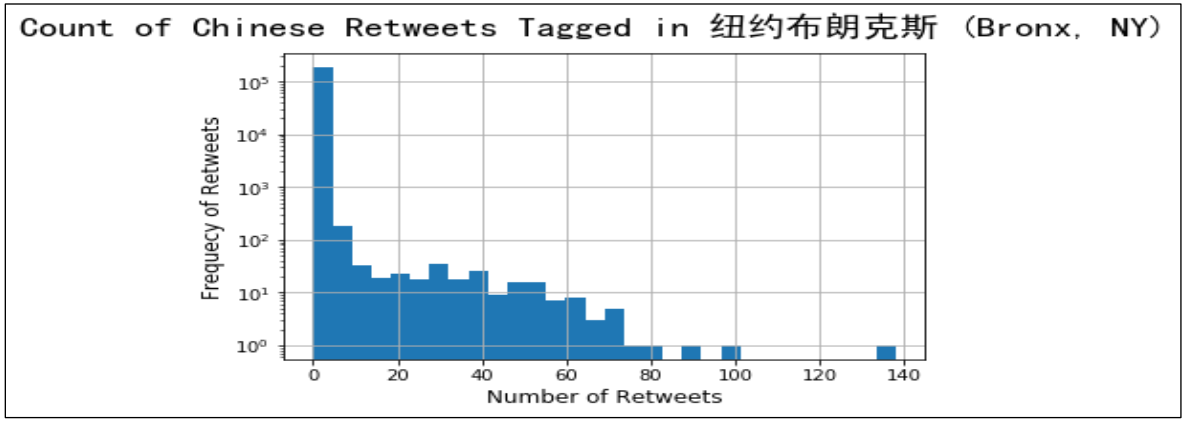
Appendix D.6



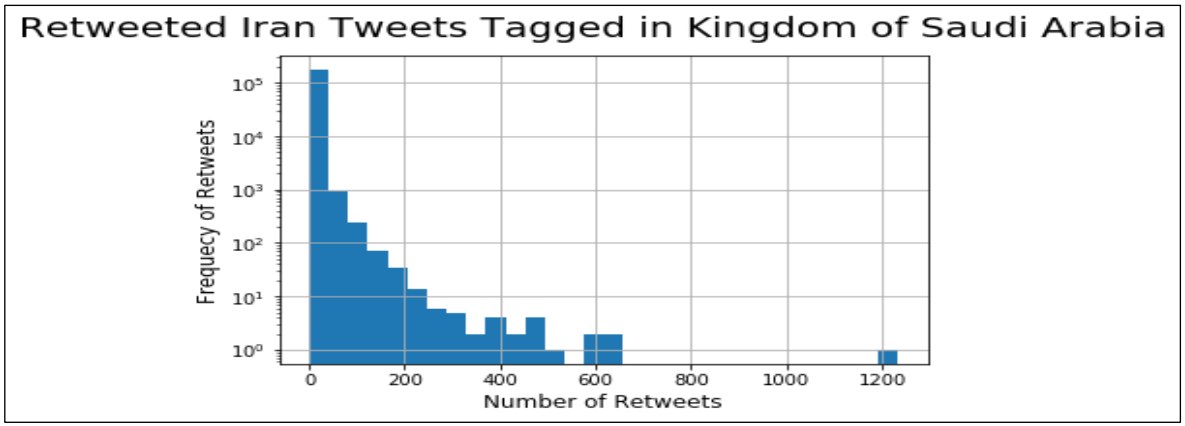
Appendix D.7



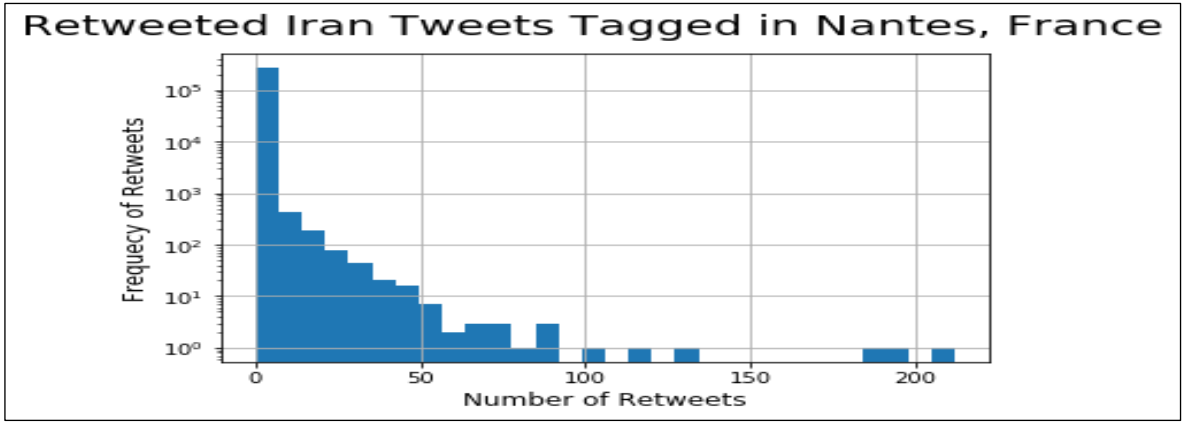
Appendix D.8



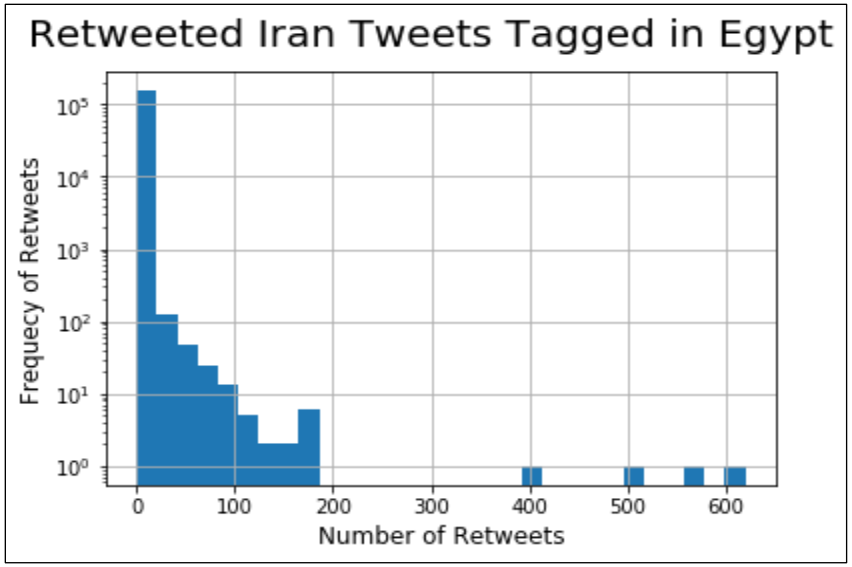
Appendix D.9



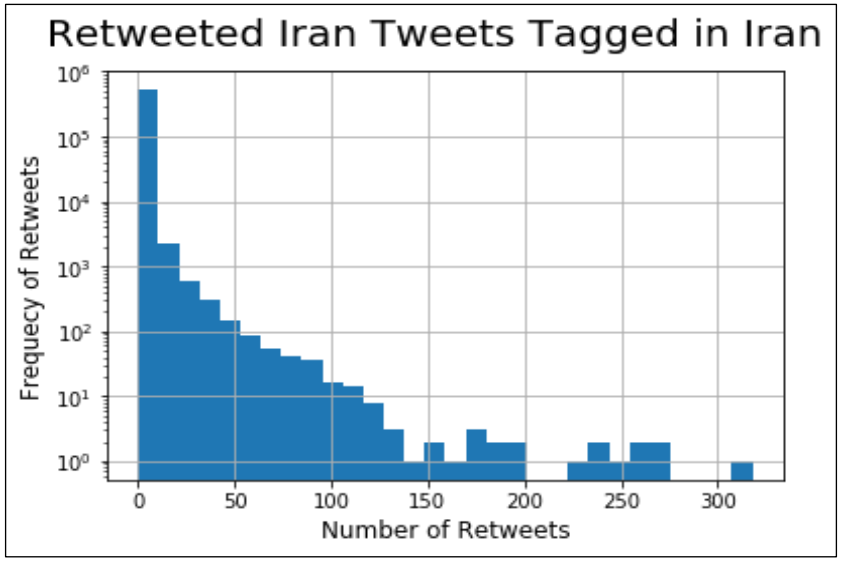
Appendix D.10



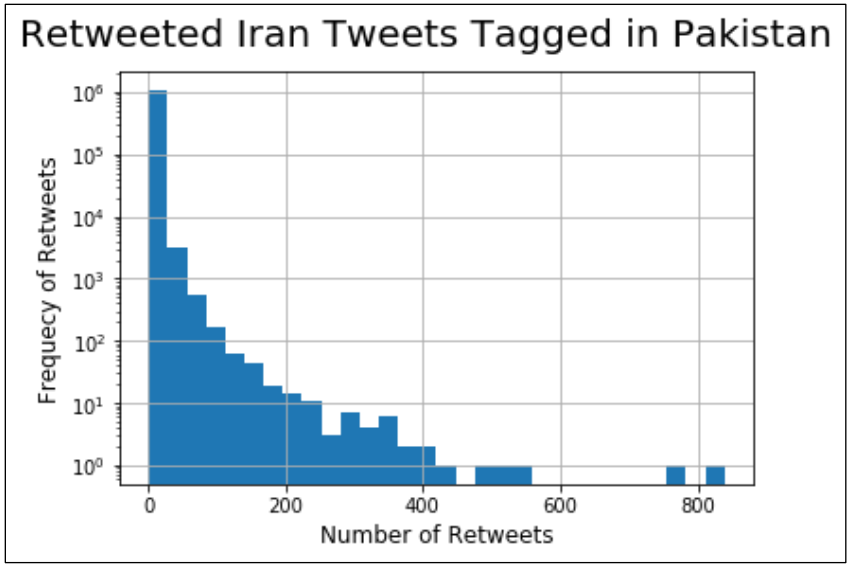
Appendix D.11



Appendix D.12



Appendix D.13



Appendix D.14