We Didn't Start the Tweets

An Analysis of Disinformation Networks on Twitter

Ronald E. Thompson III*

Department of Computer Science
Tufts University

December 18, 2020

With social media being ubiquitous in our everyday lives, it presents a new and highly exploitable threat vector for malicious actors and intelligence services. Nation states, such as Russia and Iran, have sanctioned groups to spread disinformation, while not revealing their identities, on platforms such as Twitter. Twitter has attempted to flag and remove these accounts through its Information Operations Center. This paper investigates some of the characteristics that these flagged accounts have displayed, such as forming of issue communities, centralized accounts that generate most of the content, and the languages/issues being targeted. Additionally, this research raises some questions about the accuracy of the methodology Twitter is using to flag these accounts. This research contributes to the emerging field of Disinformation Studies as well as International Security and Public Policy.

1 Introduction

When social media was first gaining traction, it was heralded as a game-changing technology. From organizing protests of the Colombian dissident group, the Revolutionary Armed Forces of Colombia,[1] to "several millions of tweets containing the hashtags libya or egypt" being generated during the Arab Spring [6], social media platforms have materialized as a way to topple authoritarian regimes. As these events have occurred, nation-states have watched and taken note. In particular, the Russian Federation and Islamic Republic of Iran have monitored activists. As we move into a world where cyber operations become the dominant mechanism of warfare, we'll see a decline in "hot" conflicts, where actual shots are fired, and more focus on operations that do not lead to kinetic engagements. One of the ways in which this will be done is using information warfare, and a tool that is being called disinformation.

The Internet Research Agency (IRA), a Russian-backed organization, most famously used these techniques in the 2016 US election, with both individual accounts creating US personas and bot-nets that amplified these messages.[11] Additional research by Twitter and others has shown that countries such as Venezuela and Iran have deployed similar techniques.[13] Iran is a particularly interesting example as previous reports have shown Russian-backed hackers have disguised themselves as Iranians when attacking other nation-states.[9] Proper attribution will be an imperative as nation states develop policy prescriptions around disinformation.

As disinformation and computational propaganda becomes a more studied phenomenon in political science, psychology, and computer science departments it is vital that we distinguish between individuals and groups that hide their identity on behalf of a nation state compared to others. The former are groups that can and should be prosecuted under 52 USC § 30121 for foreign interference in US elections and other tools available to the Department of Defense and Intelligence Community. Domestic groups spreading disinformation, not acting on behalf of nation-states, are equally worrisome, but the legitimacy or illegitimacy, for the United States, is less clear as is the legal framework for which this type of action can be prosecuted.

[*] Email: ronald.thompson@tufts.edu

1.1 Literature Review

A rather prescient paper was published in 2010 in the *Journal of Information Warfare* by an Australian researcher, P Chamberlain[8]. Chamberlain discusses how Twitter even in 2008/9 was used to spread false rumors and disinformation. He warned that Twitter is "especially suitable for use in disinformation operations due to the casual nature of communication and the asymmetrical structure of Twitter networks."[8]

Current research into disinformation operations generally can be bucketed into two groups. The first focuses on the work done by the IRA in 2016 and the other generally is more centered on how disinformation spreads on social media. The former group are using the same data that this paper analyzes, although in many cases the set is smaller as additional accounts have been released in the past few months. Numerous papers deal with the more general problem of disinformation spread on social media networks, but these serve mainly to identify false information rather than to characterize the actual network or to look at the problem of attribution.

The papers that we wish to highlight are those that look specifically at the IRA accounts. Xia et al[14] dove into the specifics of one account that has been attributed to the IRA, "Jenna Abrams". Their analysis focused more qualitatively on how the IRA built up the persona and the content that was being generated. Badaway et al[3] performed a larger study on the network of IRA accounts identified by Twitter. Overall their analysis was examining at the network. However, one part of their analysis worth noting is their use of k-core decomposition as a way to find the accounts that were most central to spreading disinformation, although they don't discuss if they tried other methods to compare the effectiveness. Linvill and Warren focused more specifically on the types of content being generated by the network instead of the structure of the network itself. In their work they distinguished some interesting labels in which to group these accounts, something that could be expanded on as the network structure is investigated more. We also wish to spotlight a paper that specifically focused on the IRA compares and contrasts the IRA's network to the network Twitter has attributed to the People's Republic of China from Beskow and Carley.[4] They hope to expand the binary classification of bot or not to include additional characteristics of the networks and accounts.

One additional paper worth noting is *Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web* by Zannettou et al[16]. We are highlighting this paper for two reasons: the first is most of the above papers are the product of social scientists, and this one was developed by cybersecurity academics. Given the goal of this paper is to further develop an attribution model, we believe there should be more literature in the cybersecurity space looking at this issue and leveraging the current research being used to identify Advanced Persistent Threats (a term first coined by Air Force analysts in 2006). Also, the analysis by Zannettou et al is interesting as they compared many aspects of the IRA network to random networks pulled from the larger Twitter network.[16]

2 Data

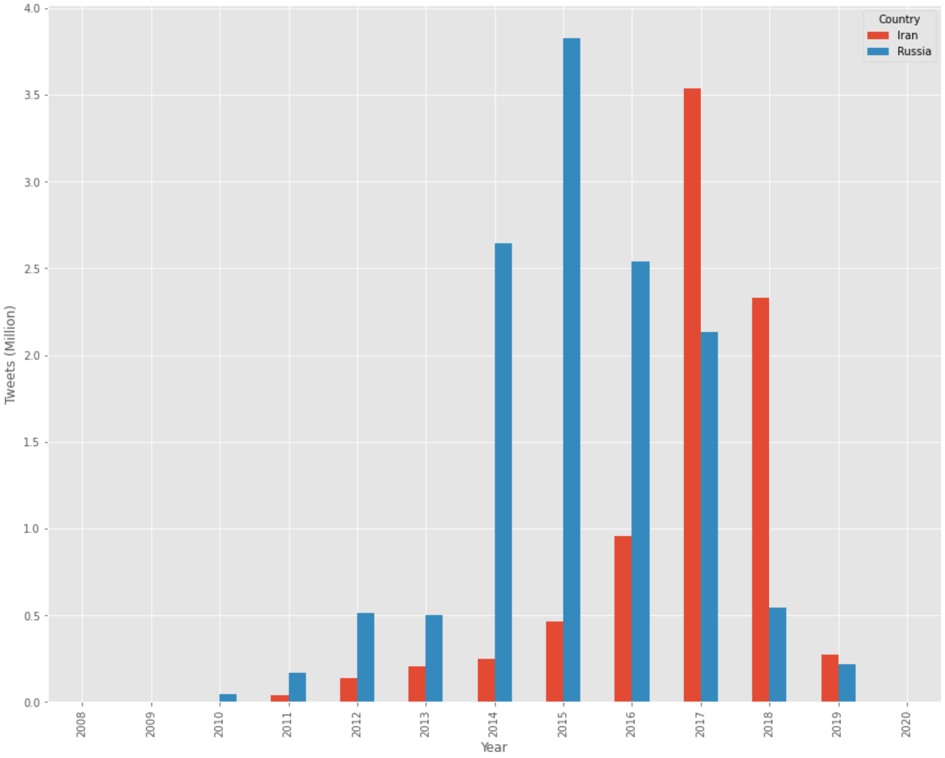
In October 2018, Twitter released the first of several data dumps pertaining to accounts that they believed to have "resulted from state-backed information operations on our service."[2] Subsequently, they have dumped nine additional data sets segmented by country. Each of these dumps contains files with a list of users, associated tweets and media content. Initially, Twitter labelled the data associated with the Internet Research Agency as separate from Russia, but they have since used the labels interchangeably. Additionally, Twitter has not provided guidance on how these accounts or tweets were identified, something a number of the papers mentioned above have flagged as a problem. From this point forward, we will refer to Russian-backed accounts simply as Russian and Iranian-backed accounts as Iranian in this paper.

The data was in csv format and retrieved from Twitter's Information Operations webpage [1]. Each of the separate files containing users and tweets were combined generating two data sets, users and tweets. These formed the basis of all the analysis presented.

The user data contained information pertaining to the accounts that had been flagged by Twitter as state-backed accounts. Using the file source we attributed each account to Russia or Iran. For each user, we were given an UserID that could be looked up on Twitter's API, approximately 11,332 (94.6% of users) had

[1] https://transparency.twitter.com/en/reports/information-operations.html

Figure 1: Number of Tweets Flagged by Twitter



their IDs hashed because of the size of the account and to protect user privacy. In this paper we did not attempt to look up any of these users on the API. The data also contained information about the account, such as the follower count, following count, and account language. There are a total of 11,973 users and 94.6% of these accounts have their UserID hashed to protect the identity of the user in case they have been misidentified. The tweet data contains 21,319,900 tweets that span from 2008-04-30 to 2020-08-21. Each tweet has information about when it was posted, how many interactions it had, if it was a retweet or mentioned another user, the tweet content, and the language it was written in. There are a total of 10,579 accounts that tweeted, 97.4% were in the flagged users files, the other accounts that tweets are listed for are most likely ones that had some disinformation content associated with state-backed operations in the specific tweets, but not enough to warrant the account being flagged. This is another question that is something we would like Twitter to address. The breakout of the users can be found in Table 1.

Table 1: User Breakout

Country	Origination	Users
Iran	Interacted with Flagged Tweet	406,993
	Flagged Users	6,788
	Tweeted, but not Flagged	275
Russia	Interacted with Flagged Tweet	1,153,164
	Flagged Users	5,185
	Tweeted, but not Flagged	2

Using this data we generated two graphs, G_{Total} and G_{Core}, which is a subgraph of G_{Total}. Almost all of the analysis done is focused on G_{Core} as this was a more manageable network in terms of size and it also had less noise in terms of the nodes listed should be those that are disinformation accounts.

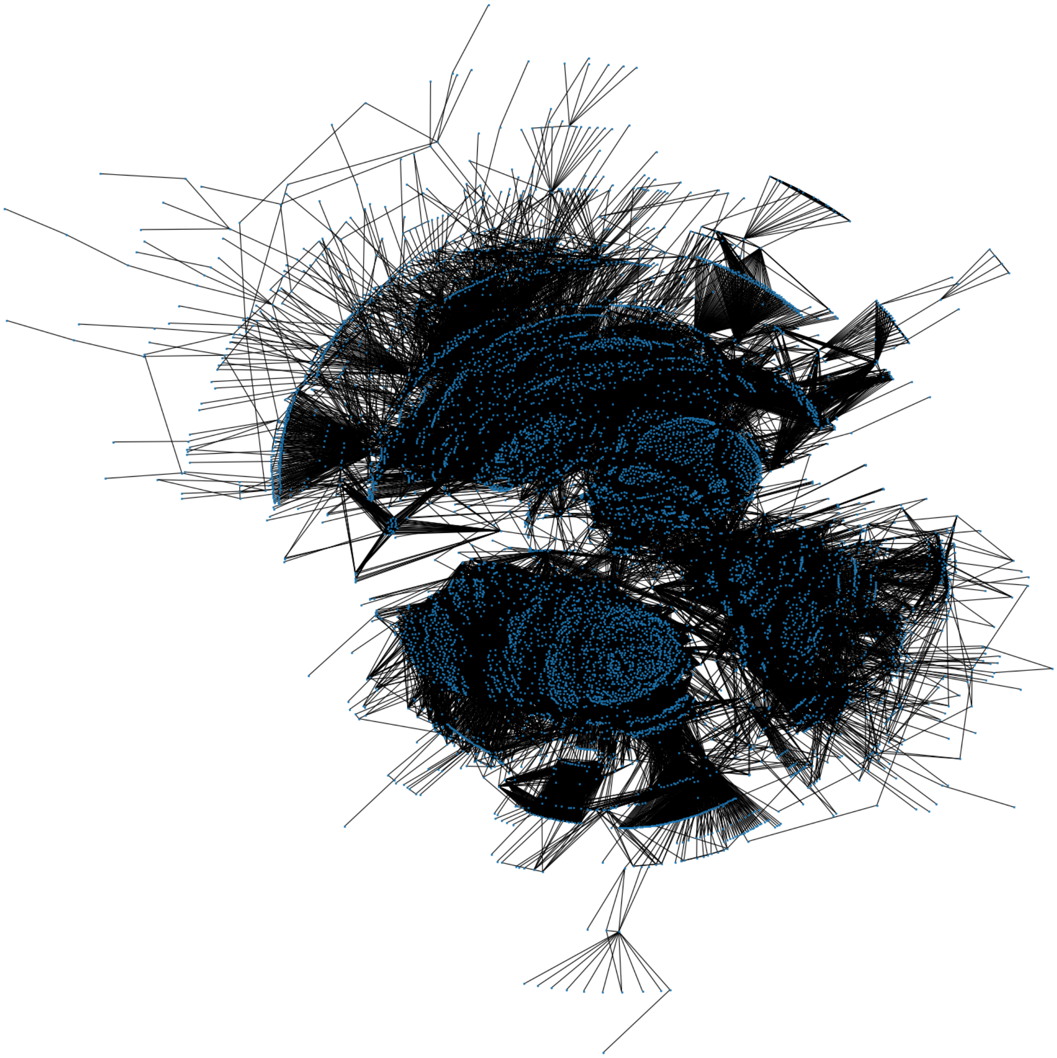
Each account represents a node and an edge is created if there is an interaction between two accounts. An interaction is defined by a retweet, reply, or mention. To turn this into a directional graph, direction is from

Table 2: Network Information for Tweets

	Russian		Iranian		Total	
	G_{Core}	G_{Total}	G_{Core}	G_{Total}	G_{Core}	G_{Total}
Nodes	5,185	1,158,351	6,788	414,056	11,973	1,537,292
Edges	170,598	2,450,582	2,3687	1,324,605	194,644	3,765,821

one person interacting with another. For example if User A replies to a tweet from User B then the edge goes $A \rightarrow B$. The weight of the edge is the total number of interactions between those two nodes. G_{Total} contains all the accounts and tweets that have been flagged; of all the edges created in G_{Total}, 2.15% of the edges are between nodes that have not been flagged specifically as state-backed disinformation accounts, again this was not explained by Twitter. G_{Core} contains just the accounts that Twitter flagged as state-backed accounts.

Figure 2: Network of G_{Core}



3 Analysis

As we stated earlier, the focus of the analysis was on G_{Core}. The goal of the analysis was to answer three main research questions.

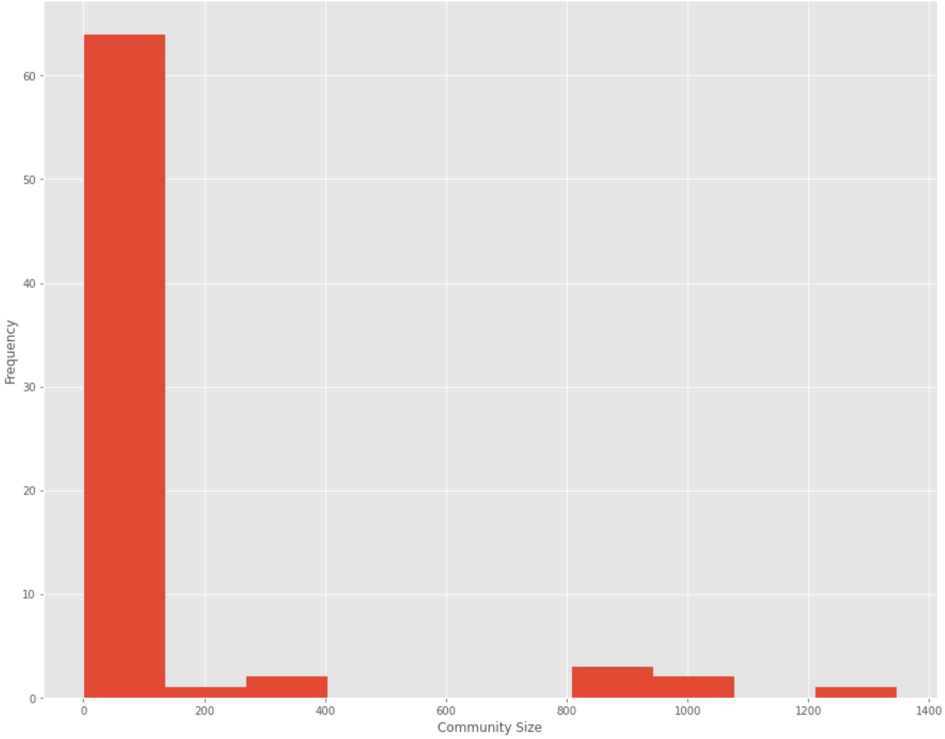
- **RQ1:** Do distinct groups exist among the nation state groups? Are there specific characteristics that we can pull out from these groups?
- **RQ2:** Was the dominant focus of these accounts on the US or the West in general? Were accounts dual purpose in looking at both domestic issues and foreign ones?
- **RQ3:** Are there specific accounts that serve as command and control?

3.1 RQ1: Groupings of Accounts

As we can see in Fig 2, some distinct communities might exist. To understand if distinct groups exist, we took a few different approaches to identify what they might be. When segmenting by nation, a clear definition starts to shape up. The top half of Fig 2 were Iranian accounts and the bottom half were Russian. We also observed that the Iranian accounts were more ”fanned” out while the Russians formed two more distinct groups. Pujol et al showed that the Louvain Community Detection Method[5] is effective for splitting Twitter networks for analysis and maintaining important characteristics.[12]

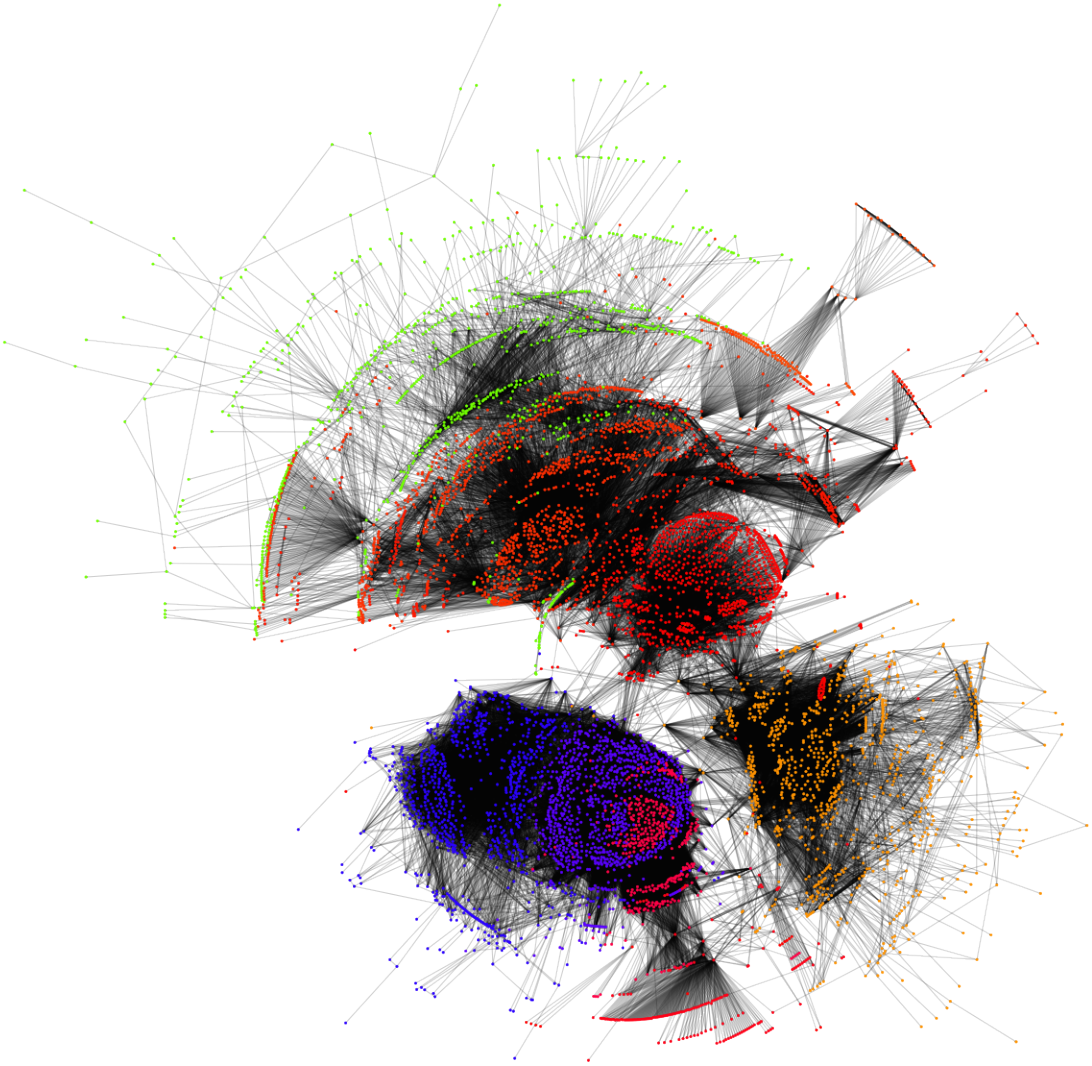
To investigate potential groupings, we used G_{Core} and removed any nodes that had only self-loops. Using the Louvain implementation in NetworkX[10], we ran it until it reached an equilibrium, where the modularity of the graph remained constant. We found a total of 73 groups using the Louvain method. 85% of the communities had less than 50 nodes, which suggests that there were some core groups that were driving the messaging campaigns. It also suggests that some of these smaller communities could be made up of accounts that may not be part of the actual effort, but instead were caught up in the net that Twitter used.

Figure 3: Distribution of Community Size



60% of the communities were a majority Iranian, and when you look at the ten largest communities the split was even. The distribution of the percentage Iranian/Russian was bimodal, greater than 95% and less than 5%. This suggests that the groupings were quite distinct from each other. Due to the small groupings potentially being noise, we focused specifically on the groups that had more than 100 nodes in them. This subset can be seen in Fig 4. When looking at commonalities that existed between these larger groups one of the distinct characteristics was the primary language that these accounts tweeted in, which ties into **RQ2**.

Figure 4: Network of Core Node Communities



We removed the smaller communities, that had less than 100 nodes as those bear characteristics more similar to what you would expect of normal groups rather than an concerted misinformation campaign.

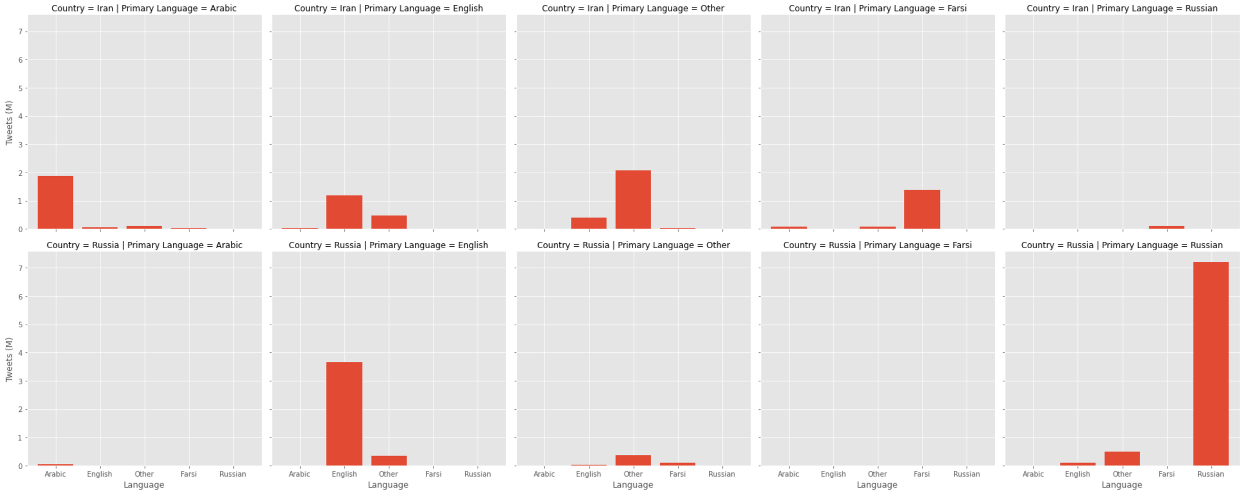
3.2 RQ2: Foreign or Domestic Focus

There are a number of different proxies to figure out the focus of these accounts, from more simplistic measures using the language of the account/tweets to more complex Natural Language Processing (NLP) of the tweet content. Our approach was more on the simple end, but in future work we would love to expand to a deeper dive into the content of the tweets. We focused on the language of the tweets as well as some initial exploration of the hashtags being used as a way to understand if these accounts were focused on domestic issues or foreign ones, and in particular election interference.

3.2.1 Language of Tweets

Segmenting G_{Core} into subgraphs for the Russian and Iranian networks some interesting differences emerge. The Iranian accounts mainly tweeted in languages other than Farsi. Most were in languages other than Arabic and English. However, both Russian and Iranian accounts were quite diverse in the languages that they used, ranging from Cherokee to Tamil to Swedish. Because the focus was to see how much these accounts were tweeting in their own language compared to English and others, we only looked at Arabic, English, Farsi, and Russian and we bucketed the other languages into an other category.

Figure 5: Number of Tweets by Language Bucket by Country of Origin and Primary Language of Account



Russian was the most common language overall for G_{Total}, 7.4M tweets, followed by English (5.4M), and other (3.95M). Both Russians and Iranians seemed not to focus on one another. Less than .001% of Russian-backed accounts were in Farsi, and 1.45% of Iranian-backed tweets were in Russian. 60% of Russian-backed tweets were in Russian, and the accounts that predominantly tweeted in Russian used languages other than English if they tweeted in more than one language.

Looking at the network representation in Fig 4, the communities that we can distinguish are some of the groups by primary language of tweets. For instance the Purple/Pink groups in the bottom left represent Russian-backed accounts that primarily tweeted in Russian, and the light orange in the bottom right and red in the middle both are English language accounts. This does suggest that these groupings do have some common characteristics and mission sets. Nodes that are on the periphery generally were other language accounts, or while the primary language was Russian or Farsi, they were less concentrated on that language and more spread out in their targets.

3.2.2 Hashtags

In the exploration of hashtags, we found that Russian-backed accounts preferred to use common hashtags when tweeting in English, but they were much more diverse in the hashtags for Russian language tweets. The main hashtags utilized by the Iranians were concentrated on other countries rather than their own, in particular Bahrain. Here we examined the entire dataset and pulled out the information on the number of tweets by user and language with the hashtags being used.

The Russian-backed accounts used hashtags that suggested they were sharing important information that was credible news. In particular, they favored news and новости (which means news in Russian) as well as targeting more specific local issues as a means to build credibility. In their English language accounts they favored hashtags like local or Chicago, which might have served as an attempt to make them seem more

Table 3: Top 10 Hashtags Across all Tweets

Hashtag	Country	Tweets
news	Russia	249,504
sports	Russia	99,525
новости	Russia	84,024
politics	Russia	78,184
البحرين[2]	Iran	75,587
СПб	Russia	65,340
Bahrain	Iran	64,047
MAGA	Russia	61,097
local	Russia	54,977
GroupPalestine	Iran	48,844

connected to a local community. They also used this same tactic when looking inwards with hashtags like СПб or Уфа targeted specific areas, in this case St. Petersburg and Ufa both cities in Russia.

Iranian accounts were more focused on other countries; Bahrain, Palestine, and Pakistan particularly were a focus of their hashtags. Most of these hashtags were in Arabic, which suggests that while a majority of Iranian accounts were focused on content in Farsi, they limited the use of consistent hashtags. Only 6 of the top 50 hashtags used by the Iranian accounts were in Farsi. Potentially this is a cultural difference or something different with their approach focused on Iran. Generally, the Iranians used less hashtags than the Russians, but they were more consistently used when targeting other countries.

3.3 RQ3: Command and Control

Command and Control (C2) is a term to refer to processes, organizational hierarchy, and other aspects of military operations in order to achieve mission success. In this context, we were interested in understanding if there is an organizational hierarchy within these networks. Through **RQ1** and **RQ2** we have seen that an organizational structure does exist, but the hierarchical structure is not clear. Fig 6, shows the positive skewness of the number of tweets per account. This is especially the case in the Russian accounts tweeting in English, where most accounts had less than 50 tweets. The English language accounts show a big difference in tactics between the Iranian and Russian groups that is interesting to note. The effectiveness difference is not known, but something that might be explored in further research.

Figure 6: Distribution of Accounts with less than 1,500 Tweets (80% of Accounts)

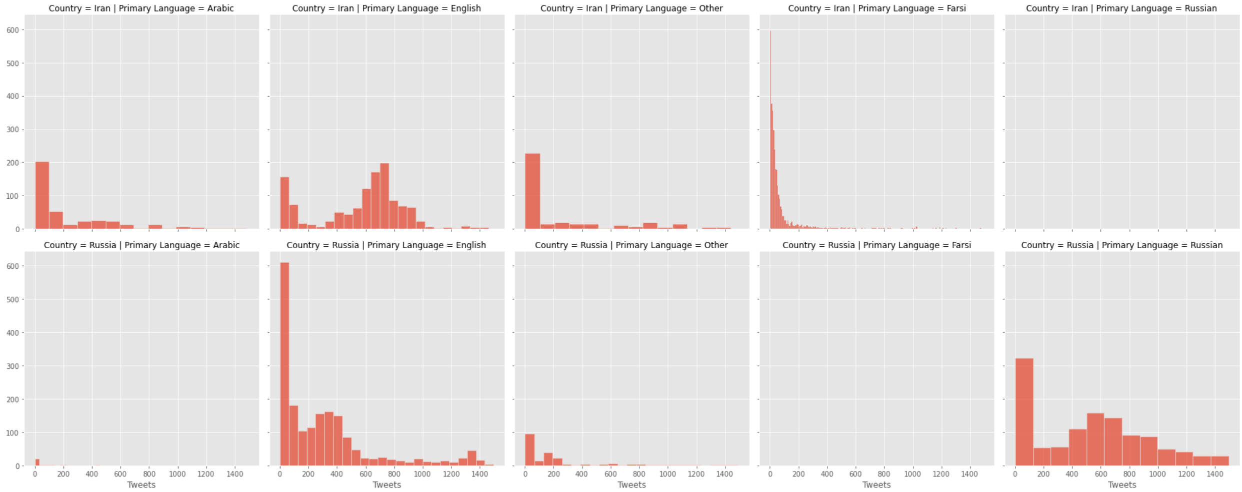
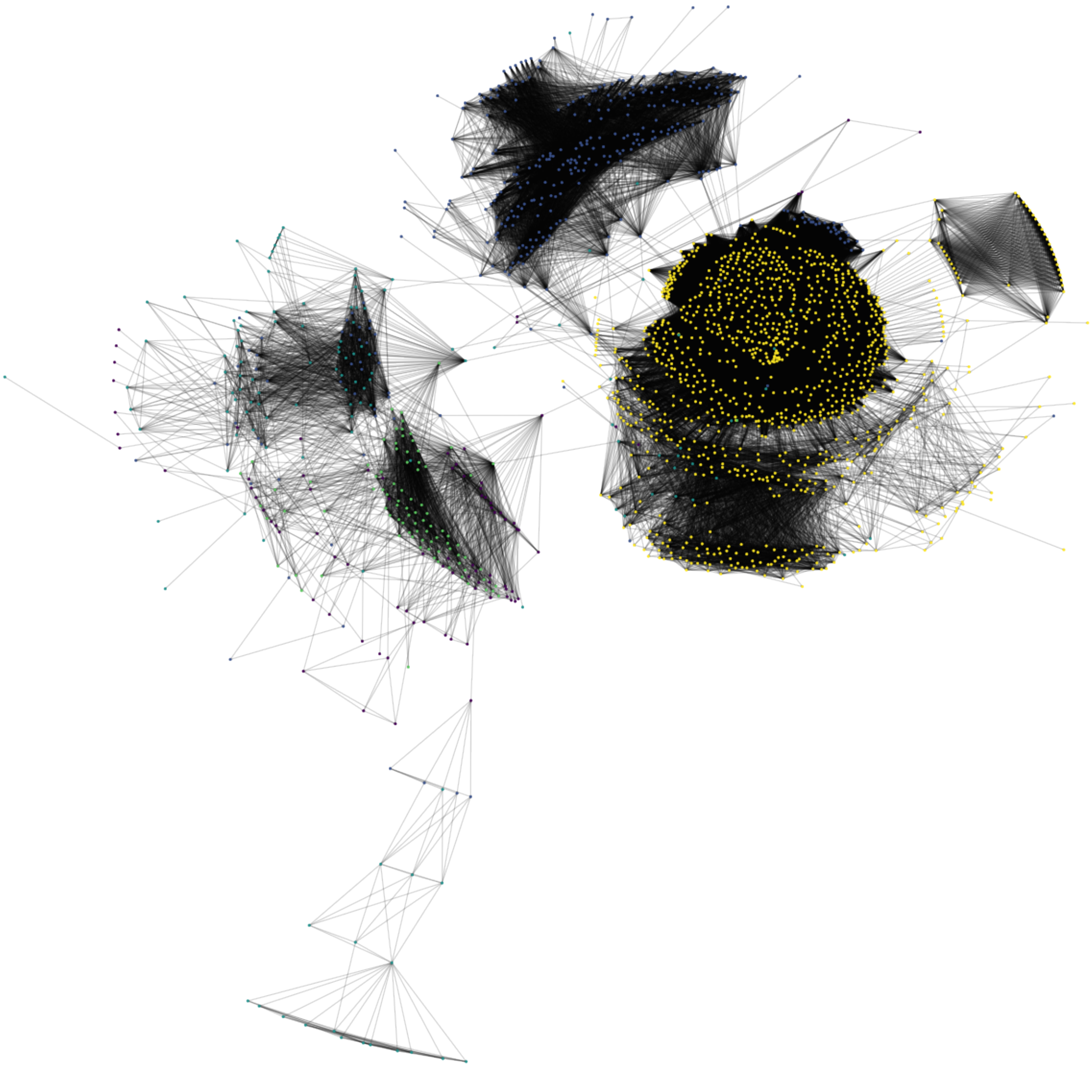


Fig 6 looks only at the accounts that had less than 1,500 tweets as we found there were a number of outlier accounts that obscured any potential pattern. Those 20% of accounts that had more than 1,500 tweets were mainly Russian-backed accounts (approx 80%), of those 75% were Russian language accounts. This suggests that Russian-backed accounts tweeting in Russian had a large control network, while they changed their tactics for English language accounts to have a smaller number of control accounts. This could be a function of focus or a tactic difference depending on the audience. Our hypothesis is that Russian-backed accounts were more focused on domestic issues as it is a higher priority for Russian security services to maintain power at home, but this is something that should be investigated more.

Figure 7: Network of High Tweeting Nodes Segmented by Primary Language



Russian language nodes are colored yellow, English nodes are blue, Persian nodes are green, Arabic nodes are purple, and Other nodes are turquoise

Visualizing this network in Fig 7, the structure that has been observed throughout this paper can still be observed. The Russian language, yellow nodes, are particularly interesting as you have a strong dense core with some sparser groups on the periphery. This potentially are accounts focused on narrow issues or geographic region as we saw in **RQ2** with some of the hashtags they utilized.

3.4 Other Analysis

In addition to **RQ1**, **RQ2**, and **RQ3**, we did additional work understanding the density of the subgraphs for Russian-backed and Iranian-backed accounts as well as other cuts by language etc. Our hope was also to present analysis using similarity measures such as Personalized PageRank[15] and Diffusion State Distance[7], but because of the size of the networks (even when using G_{Core}) and our implementation (most likely the driver of issues) these methods so slow that it was not feasible to experiment on the network. Future research that we plan on doing will also look to use MapReduce implementations to help increase the speed in which these algorithms run.

4 Discussion

The biggest takeaway from this analysis was the distinct approaches used by the Russian-backed and Iranian-backed accounts. It has been well-documented in both the news and Congressional hearings that Russian security services have demonstrated much more sophistication and historical use of disinformation operations. This analysis made this clear with the reach of the Russian accounts, and the experimentation in methods by the IRA that we saw. The Iranian accounts take similar approaches to the IRA in that they focus more on domestic content and regional groups, followed by the US and rest of the world.

The fact that both of these groups were focused more on domestic issues demonstrates that this is most likely the area that should be investigated further to understand the methods that they might be testing on their own population before using on other countries. This approach of using domestic groups, followed by regional players, to trial methods before going global is again something that has been an observed tactic of Russian security services.

Further research should examine this analysis and similar ones to create a classification framework to link accounts to various groups, whether the IRA or others. It will also be important to investigate the C2 structure of these organizations and understand how accounts are split based on issue, language or some other focus. Additionally, this analysis would benefit from determining how this evolved temporally to understand how tactics changed and how much experimentation was being done.

4.1 Limitations

There were two large limitations of this analysis, were made more inhibitory by the time frame in which this work was completed. The first was a function of computational power. Consistently there were problems with the size of the data set and the memory requirements to analyze the entire network. A number of experiments were done in order to make the problem more manageable, such as random sampling and focusing on the core network. Interestingly, there does not appear to be much in the way of implementation of graph theory or network science algorithms in the open-source PySpark libraries. This lack of tooling for PySpark is something that we hope to rectify and contribute to in the future.

The other limitation was that there is no literature about how the accounts/tweets have been identified by Twitter. Despite their commitment to providing this data to researchers, they did not respond to all the attempts to communicate with them. It is unclear if all the accounts that have been identified by Twitter are actually state-backed disinformation accounts or even accounts that are purposefully spreading disinformation. Much in the same way that security researchers publish extensively about the attribution methodology that they have used, it is important that Twitter do the same. In any follow-on work, we plan on using a method similar to Zannettou et al in pulling random samples of Twitter users to compare to.

5 Conclusion

Overall, this analysis has expanded the research that has been done about the Russian and other state-backed disinformation networks with some different methodological approaches. We found that there was more sophistication in how the Russians employed disinformation accounts compared to the Iranians, including the use of centrally placed nodes to spread information, accounts that served to amplify only a few messages, and the use of more narrowly focused geographic hashtags. We did not find evidence of Russians manipulating the Iranian accounts, both by the lack of interaction between the groups and by the difference in tactics used.

The field of computational propaganda and disinformation will continue to flourish in the coming years. It is important to make sure that this research addresses the differences between domestic actors spreading disinformation and state-backed groups. The latter is more readily subject to international norms and law, while the former needs to be regulated on a nation level. It is also important that as this type of analysis does not provide a framework of how to be more effective at running disinformation campaigns, this area alone could be its own body of research and should be in the back of all researchers' minds as they study this topic.

References

[1] Facebook Used to Mobilize Against FARC, . URL https://www.npr.org/templates/story/story.php?storyId=18689653.

[2] Information Operations - Twitter Transparency Center, . URL https://transparency.twitter.com/en/reports/information-operations.html.

[3] A. Badawy, A. Addawood, K. Lerman, and E. Ferrara. Characterizing the 2016 Russian IRA influence campaign. *Social Network Analysis and Mining*, 9(1):31, July 2019. ISSN 1869-5469. doi: 10.1007/s13278-019-0578-6. URL https://doi.org/10.1007/s13278-019-0578-6.

[4] D. M. Beskow and K. M. Carley. Characterization and Comparison of Russian and Chinese Disinformation Campaigns. In K. Shu, S. Wang, D. Lee, and H. Liu, editors, *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*, Lecture Notes in Social Networks, pages 63–81. Springer International Publishing, Cham, 2020. ISBN 978-3-030-42699-6. doi: 10.1007/978-3-030-42699-6_4. URL https://doi.org/10.1007/978-3-030-42699-6_4.

[5] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre. Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2008(10):P10008, Oct. 2008. ISSN 1742-5468. doi: 10.1088/1742-5468/2008/10/P10008. URL http://arxiv.org/abs/0803.0476. arXiv: 0803.0476.

[6] A. Bruns, T. Highfield, and J. Burgess. The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their Networks. *American Behavioral Scientist*, 57(7):871–898, July 2013. ISSN 0002-7642. doi: 10.1177/0002764213479374. URL https://doi.org/10.1177/0002764213479374. Publisher: SAGE Publications Inc.

[7] M. Cao, C. M. Pietras, X. Feng, K. J. Doroschak, T. Schaffner, J. Park, H. Zhang, L. J. Cowen, and B. J. Hescott. New directions for diffusion-based network prediction of protein function: incorporating pathways with confidence. *Bioinformatics*, 30(12):i219–i227, June 2014. ISSN 1460-2059, 1367-4803. doi: 10.1093/bioinformatics/btu263. URL https://academic.oup.com/bioinformatics/article-lookup/doi/10.1093/bioinformatics/btu263.

[8] P. R. Chamberlain. Twitter as a Vector for Disinformation. *Journal of Information Warfare*, 9(1):11–17, 2010. ISSN 1445-3312. URL http://www.jstor.org/stable/26480487. Publisher: Peregrine Technical Solutions.

[9] J. Cook. Russian hackers disguised cyber attacks using Iranian spying gang. *The Telegraph*, Oct. 2019. ISSN 0307-1235. URL https://www.telegraph.co.uk/technology/2019/10/21/russian-hackers-disguised-cyber-attacks-using-iranian-spying/.

[10] A. A. Hagberg, D. A. Schult, and P. J. Swart. Exploring network structure, dynamics, and function using networkx. In G. Varoquaux, T. Vaught, and J. Millman, editors, *Proceedings of the 7th Python in Science Conference*, pages 11 – 15, Pasadena, CA USA, 2008.

[11] R. S. Mueller III. Report on the Investigation into Russian Interference in the 2016 Presidential Election. *Department of Justice*, 1:448, Mar. 2019.

[12] J. M. Pujol, V. Erramilli, and P. Rodriguez. Divide and Conquer: Partitioning Online Social Networks. *arXiv:0905.4918 [cs]*, May 2009. URL `http://arxiv.org/abs/0905.4918`. arXiv: 0905.4918 version: 1.

[13] T. Romm. Twitter removed some accounts originating in Iran, Russia and Venezuela that targeted U.S. midterm election. *Washington Post*. ISSN 0190-8286. URL `https://www.washingtonpost.com/technology/2019/01/31/twitter-removed-some-accounts-originating-iran-russia-venezuela-that-targeted-us-midterms/`.

[14] Y. Xia, J. Lukito, Y. Zhang, C. Wells, S. J. Kim, and C. Tong. Disinformation, performed: self-presentation of a Russian IRA account on Twitter. *Information, Communication & Society*, 22(11): 1646–1664, Sept. 2019. ISSN 1369-118X, 1468-4462. doi: 10.1080/1369118X.2019.1621921. URL `https://www.tandfonline.com/doi/full/10.1080/1369118X.2019.1621921`.

[15] W. Xie, D. Bindel, A. Demers, and J. Gehrke. Edge-Weighted Personalized PageRank: Breaking A Decade-Old Performance Barrier. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '15*, pages 1325–1334, Sydney, NSW, Australia, 2015. ACM Press. ISBN 978-1-4503-3664-2. doi: 10.1145/2783258.2783278. URL `http://dl.acm.org/citation.cfm?doid=2783258.2783278`.

[16] S. Zannettou, T. Caulfield, E. De Cristofaro, M. Sirivianos, G. Stringhini, and J. Blackburn. Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web. In *Companion Proceedings of The 2019 World Wide Web Conference*, pages 218–226, San Francisco USA, May 2019. ACM. ISBN 978-1-4503-6675-5. doi: 10.1145/3308560.3316495. URL `https://dl.acm.org/doi/10.1145/3308560.3316495`.