Multiplatform Social Cybersecurity Analysis of the Information Environment during the 2022 Russian Invasion of Ukraine

Ian Kloo, Rebecca Marigliano, and Kathleen M. Carley

February 08, 2024
CMU-S3D-24-100

Software and Societal Systems Department
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work supported by the U.S. Army Research Office and the U.S. Army Futures Command under Contract No. W519TC-23-F-0055. The content of the information does not necessarily reflect the position or the policy of the government and no official endorsement should be inferred.

Center for the Computational Analysis of Social and Organizational Systems
CASOS technical report.

Keywords: Social Cybersecurity, Disinformation, Ukraine, Russia, Telegram, Twitter, BEND, Dynamic Network Analysis, ORA, Stance Detection, Bot Detection

Abstract

Russia's 2022 invasion of Ukraine was accompanied by maneuvers in information space meant to shape the social media conversation surrounding the war. BEND provides a useful frame for these maneuvers that can be applied to multiple social media platforms, informing a robust social cybersecurity analysis. Using a toolkit including ORA, Netmapper, and Botbuster, we identified and characterized information space maneuvers on Twitter and Telegram. On both platforms, we found that pro-Russian bots employed sophisticated maneuvers. We also found evidence of authentic (non-bot) pro-Russian users employing a unique combination of BEND maneuvers when compared to other user types on Telegram. Ultimately, this report serves as a case study and capability demonstration to inform broader social cybersecurity analyses.

Table of Contents

1 Introduction

This document presents a case study demonstrating the analytic capabilities of ORA for processing multiplatform data during the early days of the 2022 Russian invasion of Ukraine. In this study, we examine the dynamics of this conflict through the emerging lens of social cybersecurity, contrasting discussions of "Nazi-hood" on platforms like X (formerly Twitter) and Telegram, based on social media data. This is not meant to be a comprehensive analysis of the events surrounding the war. Instead, we seek to show specific results that demonstrate some of the core capabilities of ORA. The associated PowerPoint document includes detailed instructions for running the ORA reports used in this analysis, while this document seeks to provide a more in-depth, long-form analysis.

Social cybersecurity, a pivotal area of computational social science, aims to characterize, understand, and forecast cyber-mediated changes in human behavior and social, cultural, and political outcomes [1]. By leveraging AI and network science, it identifies, counters, and measures the impact of communication objectives [2], highlighting the importance to individuals, communities, and nations [3].

Understanding how social media platforms differ is key to social cybersecurity for several reasons:

- Different User Behaviors dictate that users interact differently across social media platforms, influencing the types of information shared and susceptibility to cyber threats [4].
- Varied Security Features mean each platform has unique security and privacy features, critical for mitigating risks and protecting user data [5].
- Unique Threat Landscapes indicate that different platforms may be targeted by unique cyber threats, making some threats common on one platform but rate on another [6].
- Influence Operations show that social media platforms are often used for spreading disinformation to disrupt civil discourse [1].

Understanding the difference among social media platforms is critical for effective social cybersecurity, enabling the development of tailored strategies and tools to protect against platform-specific threats and support open safe discourse.

Telegram and Twitter, as distinct social media platforms, play significant roles in the Ukrainian conflict for several reasons:

- Real-Time Information provided by these platforms is crucial for citizens making important decisions [7].
- Communication Channels like these has been utilized by both Ukrainian and Russian governments, as well ordinary citizens, for disseminating vital information. For instance, Ukrainian President Volodymyr Zelensky has used them to rally global support, disseminate air raid warnings, and share maps of local bomb shelters [8].

- Documentation of Events, particularly through Telegram, has offered live footage of the war of bombings from residents' phones and security cameras, potentially serving as evidence of war crimes [8].
- Dissemination of Propaganda and Disinformation through these platforms has created a digital battlefield where messages can either take hold without fact-checking or get thoroughly debunked and rebutted [9,10].
- Recruitment and Organization efforts have also been facilitated through social media [7].
- Bridge to the Western World, where Telegrams provides unique insights into the conflict by acting as the last social media bridge from the Western world to the Russian world [8].

Ultimately, we find key differences between the activity on two prominent social media platforms, Telegram and Twitter, that are critical to a comprehensive understanding of the total information space. Our results highlight the importance of employing analytic tools that can process data from different platforms and sources, and a deep understanding of these differences is critical for crafting effective social cybersecurity strategies.

2 Background

This section will provide some background on the Russian invasion of Ukraine to better contextualize our data and analysis. Additionally, we will describe Twitter and Telegram with a focus on the differences between the two platforms.

2.1 Russia and Ukraine

As part of their invasion of Ukraine in 2022, Russia engaged in various disinformation campaigns on multiple social media platforms [11] [12]. For example, a prominent campaign saw the introduction of the idea that Ukraine was controlled by or otherwise collaborated with Nazis. This idea was central to Putin's public comments justifying his country's military action [13]. The narrative spread through Western news media and was regularly repeated on social media platforms.

In addition to disinformation campaigns, both pro-Ukraine and pro-Russia actors engaged in general information operations meant to promote their causes and degrade the opposition. These operations included significant bot activity with varied maneuver strategies, and they took place on multiple social media platforms [14].

2.2 Telegram and Twitter

While many social media platforms were host to information maneuvers during the Russian invasion of Ukraine, Twitter and Telegram were especially significant due to their user bases and global reach. Twitter is popular in the US and other English-speaking countries but has users around the world. Given the importance of US funding

of the Ukrainian defense, Twitter was an important battleground in the information war surrounding the Russian invasion.

Telegram has a more global reach and is especially popular in both Russia and Ukraine [15]. The platform was developed by a Russian citizen, Pavel Durov, and though the Russian government has intermittently attempted to block access to Telegram, it is still one of the most popular social media platforms in the country. Telegram is also popular in the US for groups that fear real or perceived censorship on platforms like Twitter [17].

Both Twitter and Telegram are microblogging platforms based on short-text posts. Twitter relies on explicit connections between users via replies, retweets, and mentions. Users on Twitter discover new content by scrolling through an algorithmically determined news feed.

Telegram does not present users with new content, instead requiring that users seek out and subscribe to channels. Channels resemble a traditional blog and are run by individuals, or small groups of individuals focused on a specific topic. Most channels also contain an associated "chat," which is an area where subscribers can interact. There is also a direct messaging component of Telegram, but this paper will focus on the social interactions that happen on public channels and groups.

Another key difference between Twitter and Telegram is the use of hashtags. Twitter uses hashtags to tag a post as relevant to a certain topic or concept. These hashtags are globally searchable and a keyway for users to discover new content relevant to a specific topic. Telegram also allows users to post hashtags, but these tags are only searchable within a specific channel. Users can search for hashtags across all their channel subscriptions at the same time, but they cannot use hashtags to search for content outside of the channels they are already subscribed to.

3 Data

There are key differences in the APIs available to access data on Twitter and Telegram, and this section will begin with a description of the data collection methodology used to compensate for and take advantage of these differences. We will conclude the section with an overview of the data from each platform.

3.1 Collection Methodology

At the time of data collection, Twitter data was readily accessible to researchers using the platform's API. We used keywords related to Russia and Ukraine to create a Twitter dataset relevant to this topic. Telegram also allows for API access, but there is no keyword search capability. Instead, the Telegram API allows users to access any public channel by name. Without a robust search feature, building lists of Telegram channels relevant to a topic is an extremely difficult task. To address this issue, we developed the methodology shown in Figure 1.

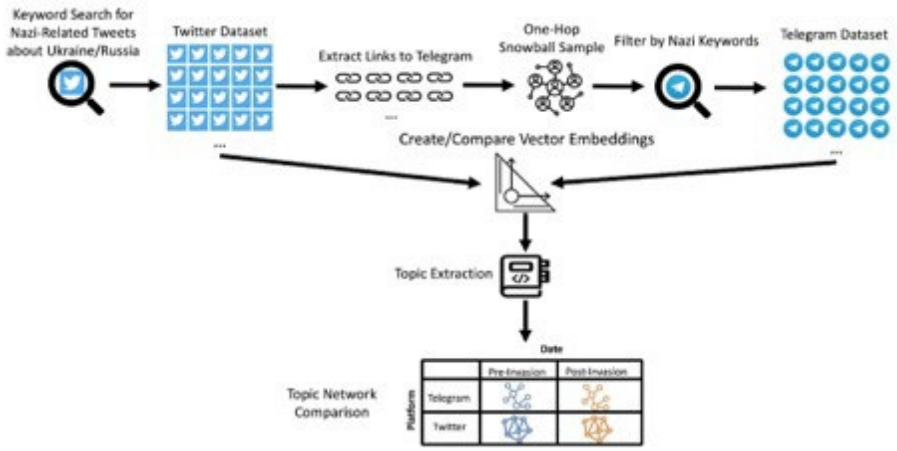


Figure 1: Data collection methodology for Telegram.

We start by using Twitter's keyword search capabilities to extract Tweets relevant to a certain topic. We then extract links to Telegram from the Twitter messages, which results in a relatively small number of Telegram channels of interest. To ensure that we are capturing a relevant sample of Telegram data, we use snowball sampling to find channels that are mentioned by our initial channel set. This results in a much larger list of Telegram channels that we can mine for relevant keywords. While the Telegram collection methodology creates the possibility for bias (in that we may not collect all relevant channels), we are unaware of alternative methods that solve this problem.

3.2 Data Overview

The Twitter data is from February 8th, 2022, to March 15th, 2022, and contains Tweets that mention a keyword related to Russia or Ukraine. To subset the data to a usable size, we truncated our data to only include bots and the users they interacted with. See Table 1 for the number of specific features in the data.

The Telegram was much denser than the Twitter data, so we subsetted it to a single day: March 1st, 2022. Bot activity is much less understood on Telegram, so we were not comfortable subsetting to only bot accounts and instead opted to include all bot and non-bot activity. See Table 1 for the number of specific features in the data.

Table 1: Data Set Feature Sizes

	Messages/Tweets	**Channels**	**Users**	**Hashtags**	**Urls**
Twitter	640,681	NA	213,968	23,873	108,463
Telegram	246,272	1,254	66,555	66,419	12,695

4 Analysis/Results

In this section, we will apply stance detection, bot detection, and BEND analysis to extract insights from both the Twitter and Telegram datasets. More details on running each method using ORA, Netmapper and Botbuster are provided in the accompanying PowerPoint document.

4.1 Stance Detection

ORA's stance detection report uses a weakly supervised network propagation approach to generate stance labels for a dataset using a small set of user-supplied labels [18]. For example, users can label several hashtags or URLs and propagate those results to label users, messages, and channels (in Telegram).

Figure 2 shows the results of running the stance report for Telegram channels. We observe three main channel communities that are divided by language. The Ukrainian-language community is almost exclusively anti-Russian, while the Russian-language community is nearly all pro-Russian. The English community is more contested but is primarily pro-Russian.

There are many "barbell" formations in the channel network, and most of these represent the connection between a channel and its associated discussion group. In some cases, the stances of the channel and group are different, which suggests there are users with opposing stances participating in these communities.

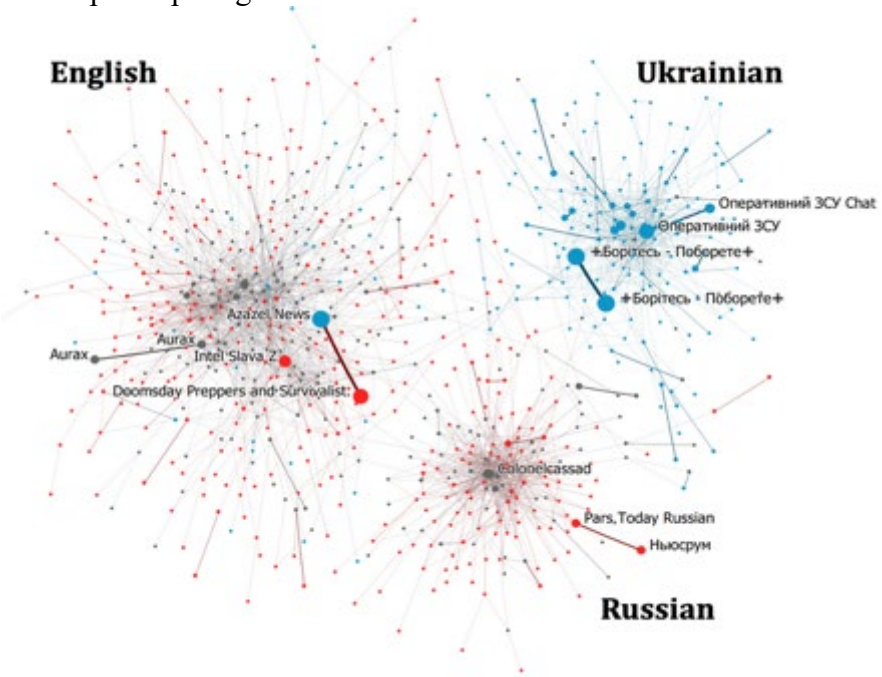


Figure 2: A network of Telegram channel stances. Nodes represent Telegram channels and edges denote that a channel forwarded content from another channel. Node color codes for stance where red nodes are pro-Russian, blue are anti-Russian, and gray are neutral. Node size corresponds to subscriber count.

Applying the stance methodology to Twitter, we find both pro-Russian and anti-Russian content, but there is more apparent coordination in the anti-Russian content. Figure 3 shows an example ego network for an anti-Russian hashtag along with a similar network for a pro-Russian hashtag. We can see that the anti-Russian hashtag is surrounded by a more densely connected set of additional anti-Russian hashtags. Given that this data contains only bot accounts, we can infer that the pro-Russian bots are using a strategy that results in a less cohesive network of linked topics when compared to the anti-Russian bots.

A) An ego network for a pro-Ukrainian hashtag. Red nodes are anti-Russian, blue nodes are pro-Ukrainian, and green are neutral.

B) An ego network for a pro-Russian hashtag. Red nodes are anti-Ukrainian, blue nodes are pro-Russian, and green are neutral.

Figure 3: Twitter hashtag ego networks.

4.2 Bot Detection

Botbuster uses a machine learning approach that employs a mixture of experts' methodology to label bots, leveraging both textual and network features [19]. Botbuster's capabilities on Twitter are well-documented, but it has recently been adapted to work with Telegram data as well.

The Twitter data used in this analysis is already subsetted to only include bot activity. Overall, there are more pro-Ukrainian bots in the Twitter data, but these bots mostly interacted with other pro-Ukrainian users. Conversely, the pro-Russian bots interacted more with neutral-stance users. Figure 4 shows a prominent pro-Ukraine bot along with a prominent pro-Russian bot demonstrating this dichotomy.

The Telegram data contains both bots and authentic users. 2.5% (667) of the users in the dataset were identified as bots. As shown in Table 2, we found that both authentic users and bots tended to interact more with authentic users with a compatible stance. For example, both pro-Ukrainian bots and authentic users interacted most with authentic, pro-Ukrainian users. This suggests that the bot communities did not leverage on-platform communication to promote other bot accounts.

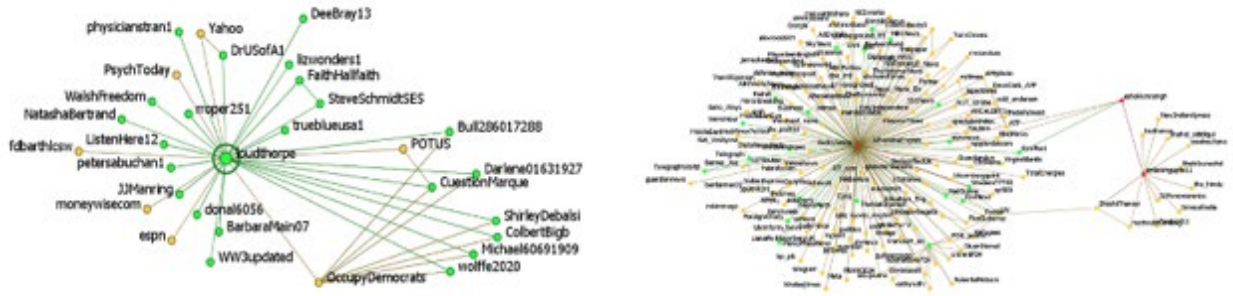


Figure 4: Twitter bot ego networks. Green nodes are pro-Ukraine, red nodes are pro-Russian, and orange nodes are neutral. We can see that pro-Ukraine bot mainly interacted with other pro-Ukraine accounts while the pro-Russian bot interacted with more neutral accounts.

While both sets of bots interacted regularly with authentic users, we found that pro-Russian bots used twice as many hashtags and URLs when compared to pro-Ukrainian bots (and authentic users of any stance). The increase in posted URLs indicates that the pro-Russian bots used a strategy that sought to drive users to external sights.

Table 2: Telegram Interactions Between Bots and Authentic Users, by Stance

	pro_authentic	**anti_authentic**	**pro_bot**	**anti_bot**
pro_authentic	52,250	989	16,474	430
anti_authentic	983	51,680	249	15,844
pro_bot	16,394	249	5,161	196
anti_bot	334	16,735	112	5,293

4.3 BEND Analysis

BEND is a framework for describing and characterizing social cybersecurity maneuvers using social (network) and linguistic cues [20]. The text-based cues are extracted from the text data (Tweets or messages) using an associated natural language processing tool, Netmapper. Combining these linguistic cues with network features allows ORA to detect BEND maneuvers in both Twitter and Telegram data.

Figure 5 shows that there was a fairly even distribution of BEND maneuvers present in the Twitter dataset. The pro-Ukrainian bots focused on positive community-building maneuvers, which aimed to boost the visibility and significance of pro-Ukrainian messaging. Conversely, the pro-Russian bots focused on negative maneuvers, which aimed to counter the pro-Ukrainian strategy.

Figure 5: BEND results for pro-Ukraine (stance = 1) and pro-Russian (stance = -1) bots on Twitter.

On Telegram, we found that the Neglect maneuver was much more common than any of the other BEND maneuvers (Figure 6). This maneuver is meant to decrease the size of an existing group, and we found that both pro- and anti-Russian users regularly authored comments that were identity attacks meant to belittle the opposing group.

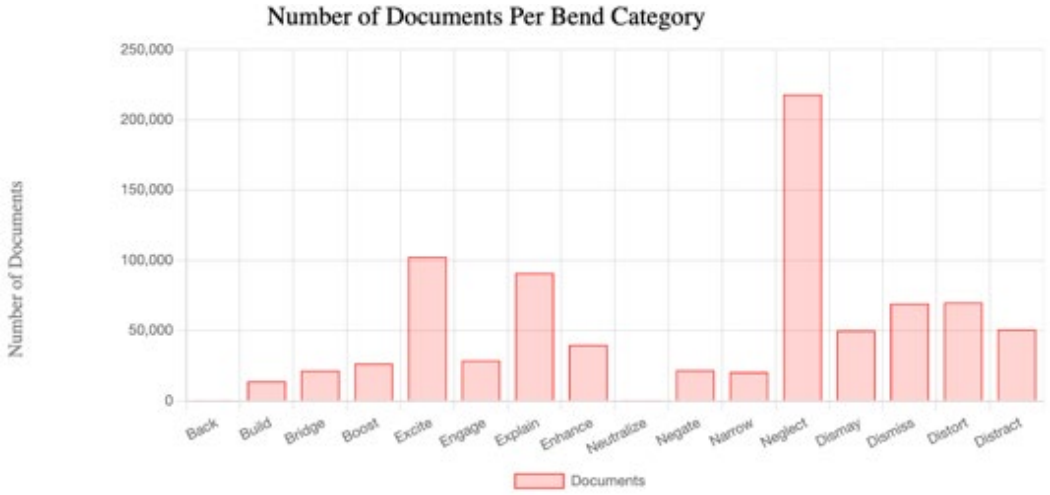


Figure 6: BEND results for all Telegram users.

As Figure 7 shows, we found that pro- and anti-Russian bots and authentic users employed the BEND maneuvers to a proportionally similar degree; however, we found that only pro-Russian authentic users employed Neutralize and Back maneuvers. Even though this is a relatively small number of users (~30), they were conducting notably different information maneuvers when compared to the other groups, which suggests a specific strategy was being employed. In this case, both are narrative maneuvers, so it is possible that there was a concerted effort by pro-Russian users to try to increase the profile of accounts they support while degrading their opposition.

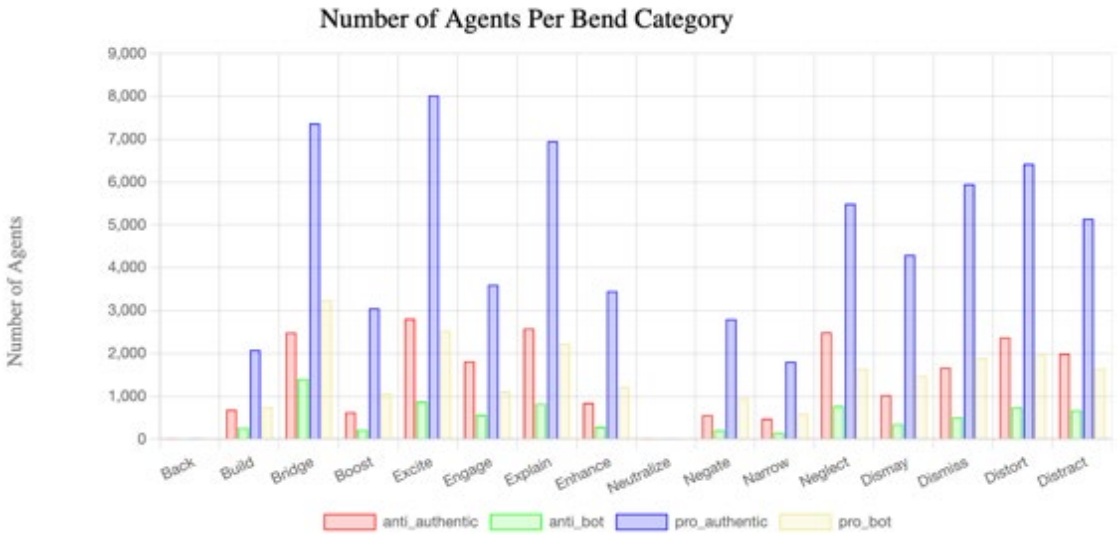


Figure 6: BEND results for pro- and anti-Russian bots and authentic users on Telegram.

5 Discussion

Throughout this analysis, we found important insights on Twitter and Telegram that were unique to each platform. Twitter appears to be much more pro-Ukrainian by volume, but the pro-Russian bots on the platform employed a more sophisticated strategy by targeting neutral users. Conversely, the pro-Russian bots relied on a less dense network of hashtags, suggesting they did not prioritize the use of hashtags on Twitter.

Telegram is much more balanced between pro- and anti-Russian users, both authentic and bots; however, the pro-Russian accounts also appeared to employ a more sophisticated strategy when compared to the anti-Russian accounts. Specifically, we observed that pro-Russian bots tended to use more URLs than their anti-Russian counterparts. Also, we found that the only agents employing Build and Neutralize maneuvers were pro-Russian, authentic users.

Overall, we found that while different tactics were employed on the different platforms, the Twitter and Telegram analyses largely validate the idea that Russia was conducting more sophisticated information operations during the early days of the invasion. We also demonstrated that Twitter was specifically targeted by a proportionally large number of pro-Ukrainian bots, which we did not observe on Telegram.

6 Conclusion

The analysis presented in this document showed some key insights into information operations in the early days of the Russian invasion of Ukraine. We found evidence of more sophisticated Russian operations that used a combination of bot and authentic accounts, as well as many pro-Ukrainian maneuvers on Twitter relative to Telegram. Ultimately, our analysis shows the importance of analyzing multiple platforms to build a more comprehensive understanding of the information space. Using tools like ORA that

support multiple platforms in their analytic pipelines is critical to this style of analysis, and the potential utility reaches far beyond what was shown in this small case study.

7 References

[1] Kathleen M. Carley, 2020, "Social Cybersecurity: An Emerging Science," *Computational and Mathematical Organization Theory*, 26(4): 365-381.

[2] National Academies of Sciences, Engineering, and Medicine, 2019, A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis. Ch. 6. Washington, DC: The National Academies Press. DOI: https://doi.org/10.17226/25335

[3] David M. Beskow and Kathleen M. Carley, 2019, "Army Must Regain Initiative in Social Media," *Association of the United States Army*, July 18, 2019, Available at: https://www.ausa.org/articles/army-must-regain-initiative-social-cyberwar

[4] Department of Homeland Security. (2019). *Social Media Cybersecurity,* Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf

[5] Canadian Centre for Cyber Security. (2022, January). Security considerations when using social media in your organization ITSM.10.066. https://www.cyber.gc.ca/en/guidance/security-considerations-when-using-social-media-your-organization-itsm10066

[6] Albladi, S.M., Weir, G.R.S. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecur* 3, 7 (2020). https://doi.org/10.1186/s42400-020-00047-5

[7] Engelhaupt, E. (2022, March 23). How social media like TikTok is shaping Russia's war in Ukraine. Science News. https://www.sciencenews.org/article/ukraine-russia-war-social-media-tiktok-telegram.

[8] Bergengruen, V. (2022, March 21). Telegram becomes a digital battlefield in Russia-Ukraine war. TIME. https://time.com/6158437/telegram-russia-ukraine-information-war/

[9] Kraus, R. (2022, March 2). In the Russia-Ukraine conflict, encrypted messaging apps can both amplify misinformation and fight it. Mashable.

[10] Loucaides, D. (2022, March 10). Telegram: The digital battlefront between Russia and Ukraine. POLITICO. https://www.politico.eu/article/telegram-the-digital-battlefront-between-russia-and-ukraine/

[11] V. Tolz and S. Hutchings, "Truth with a Z: disinformation, war in Ukraine, and Russia's contradictory discourse of imperial identity," *Post-Soviet Affairs*, 39:5, 347-365, April 2023.

[12] F. Bryjka, "Russian Disinformation Regarding the Attack on Ukraine," *The Polish Institute of International Affairs: Spotlight*, February 2022.

[13] Al Jazeera Staff. "'No other option': Excerpts of Putin's speech declaring war," *Al Jazeera,* February 2022. [Online]. Available: https://www.aljazeera.com/news/2022/ 2/24/putins-speech-declaring-war-on-ukraine-translated-excerpts. [Accessed January 12, 2024].

[14] D. Geissler, D. Bär, N. Pröllochs and S. Feuerriegel, "Russian propaganda on social media during the 2022 invasion of Ukraine," *EPJ Data Science*, 12(1), 35. December 2023.

[15] We Are Social and Meltwater. "Digital 2023 Global Overview Report," June 2023. [Online]. Available: https://datareportal.com/reports/digital-2023-global-overview-report. [Accessed January 12, 2024].

[16] Statista. "Share of online population using Telegram each month worldwide," *Statista*. [Online]. Available: https://www.statista.com/statistics/1336855/telegram-downloads-by-country. [Accessed January 12, 2024].

[17] J. Liedke and G. Stocking. "Key facts about Telegram. Pew Research Center," December 2022. [Online]. Available: https://www.pewresearch.org/short-reads/2022/12/16/key-facts-about-telegram/. [Accessed January 12, 2024].

[18] S. Kumar, "Social Media Analytics for Stance Mining A Multi-Modal Approach with Weak Supervision," *Carnegie Mellon University*. 2020.

[19] L. Ng and K. Carley, "Botbuster: Multi-platform bot detection using a mixture of experts," *In Proceedings of the International AAAI Conference on Web and Social Media*, 17, 686-697. June 2023.

[20] J. Blane, "Social-Cyber Maneuvers for Analyzing Online Influence Operations," *Carnegie Mellon University*. May 2023.

8 Appendix: Slide Tutorial

This appendix includes a slide tutorial demonstrating how to manipulate the data and generate the reports used for the analysis in this paper. The slides serve as a stand-alone document but contain less detailed analyses than the report.

Multiplatform Social Cybersecurity Analysis of the Information Environment during the 2022 Russian Invasion of Ukraine

Ian Kloo, Reba Marigliano, and Kathleen M. Carley

January 2023

Carnegie Mellon University

1

Introduction

- This document serves as:
  - 1) a case study of the information environments on two social media platforms and
  - 2) a tutorial demonstrating an analytic pipeline in ORA, including:
    - Exploratory analysis, Stance Detection, Bot Detection, and BEND analysis
- Please also see the associated long-form report for more detailed descriptions and analysis

2 Carnegie Mellon University

Background: Russian Invasion of Ukraine

- Russia invaded Ukraine on 24 February 2022 using the (fictitious) justification that Ukraine was being run by, or was otherwise harboring, Nazis.
- Russia promoted the Nazis in Ukraine narrative using official channels (e.g., Putin's speeches) and media platforms leading up to and during the invasion.
- The Nazis in Ukraine narrative, along with additional pro-Russian narratives and anti-Russian responses, flooded the information space.
- Comparing the resulting communications on two popular platforms (Twitter and Telegram) serves to enhance the understanding of the full information environment.

3

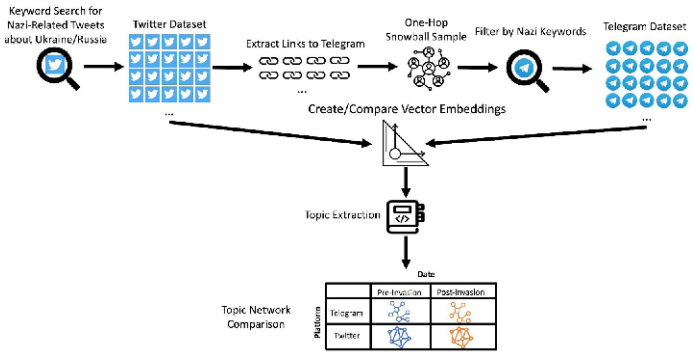
Background: Twitter and Telegram

- Twitter and Telegram are popular microblogging (short-text) social media platforms
- Twitter is primarily popular in the United States, but is used globally as well.
- Telegram is popular in Russia and Ukraine, and it has more global reach than Twitter. Telegram use in the United States is limited and is most commonly associated with those avoiding (real or perceived) censorship on other platforms.
- Twitter users interact directly with each other, while Telegram users subscribe to channels where they interact.
- Twitter uses an algorithmic news feed to help users discover new information, while users on Telegram must find channels of interest using outside sources, search engines, or by following forwarded content on channels they already subscribe to.

4

Data Collection

- Date range of interest = February - March 2022
- Twitter data was collected using keywords:
  - Contains a variation of "Nazi" AND a variation of "Ukraine"
- Telegram cannot be collected with keywords (API limitation), so we found links to Telegram in the Twitter data and snowball sampled to find related channels.



Carnegie Mellon University

Data Description - Twitter

- Twitter dataset that focused on English-language content featuring specific keywords: "Russian invasion," "Russian military," "military buildup," and "invasion of Ukraine" from 01JAN-20NOV 2022.
- For ease of demonstration and analysis, we will subset to Twitter activity related to the Russian-Ukraine War during the initial period of the Russian invasion from 08FEB - 15MAR 2022.

Tweets	640,681
Agents	213,968
Url	108,463
Hashtags*	23,873

- Note: This dataset is only bot related activity

Carnegie Mellon University

Data Description - Telegram

- There are over 6 million Telegram messages captured from the snowball sampling method described on the Data Collection slide.
- For ease of demonstration and analysis, we will subset to a single day during the early invasion of Ukraine: March 1, 2022.
- The data contains the following:

Messages	246,272
Channels	1,254
Users	66,555
Url	66,419
Hashtags*	12,695

- *Note: hashtags are used on Telegram, but differently than they are on Twitter. Telegram hashtags are not globally searchable, but are searchable inside specific channels. Additionally, users can search all of their subscriptions for specific hashtags or create alerts.

CASOS IDeaS Carnegie Mellon University

Data Exploration on ORA Overview

- ORA's toolkit supports easy data exploration with statistical and network visualizations
- Graph-based analysis and visualization:
  - ORA employs graph-based techniques to delineate relationships between entities in a network and visualize those networks
- Case-based Learning for Practical Application:
  - ORA provides a structured layout to conduct step-by-step approach for understanding complex networks

CASOS IDeaS Carnegie Mellon University

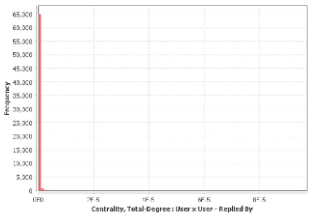
Data Exploration on ORA: Twitter

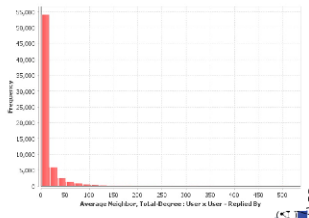
- **Dominant Themes**: "Ukraine," "Russia," Russian Invasion."
- **Key Players**: Names such as Putin, Zelensky, and Kremlin, suggest a focus on the leadership of Russian and Ukraine.
- **Public Sentiment**: Strong public sentiment against the invasion and a call for support for Ukraine.

Carnegie Mellon University

Data Exploration on ORA: Telegram

- Users interacted with an average of 3.7 other users, but most users had few interactions:
  - 43% of users had only 1 interaction
  - Only 7.6% of users had 10 or more interactions with other users
  - The maximum number of interactions was 161.
- Users regularly interacted with other users with few interactions of their own (i.e., interactions were not disproportionately between super users)

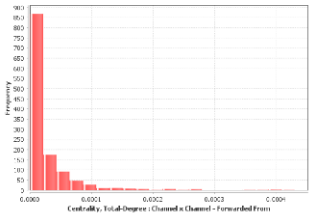


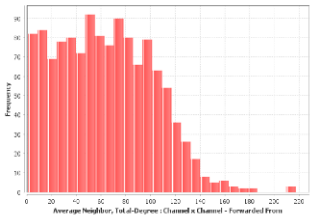


Carnegie Mellon University

Data Exploration on ORA: Telegram

- Channels interacted with an average of 20 other channels, and they interacted much more than the users (on average):
  - 11% of channels had only 1 interaction
  - Only 49.6% of channels had more than 10 interactions with other channels
  - The maximum number of interactions was 217.
- Unlike users, channels tended to interact with other channels with higher degrees (i.e., channels tend to forward content from popular channels.





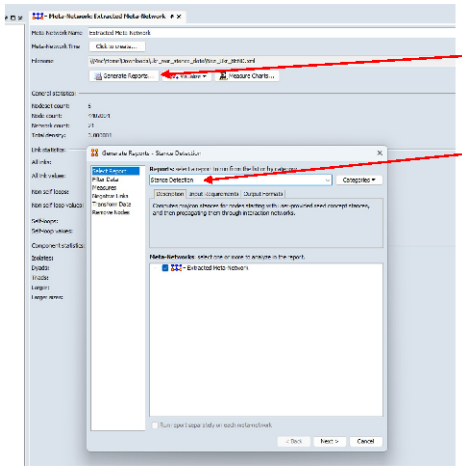
Carnegie Mellon University

Stance Report Overview

- The stance report uses a semi-supervised network-propagation approach to label nodes according to their stance on a particular issue.
  - Users are asked to label nodes with known stance, for example URLs, Users, Channels, or Hashtags that clearly represent a given stance.
  - Network relationships between these tagged nodes are used to propagate labels to the full nodeset(s)
- The results of the Stance Report are useful in downstream analyses that benefit from dividing the data by stance.
  - Ex) Determining if bots tend to be pro- or anti-Russian
  - Stance results are especially useful for BEND analysis.

Carnegie Mellon University

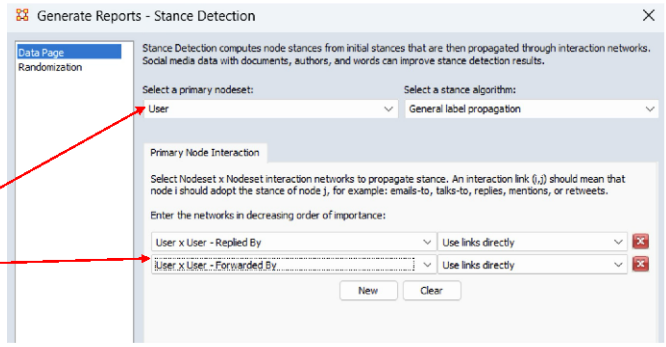
Stance Report Process



- Initiate report using “Generate Reports”
- Select “Stance Detection” and your meta network.

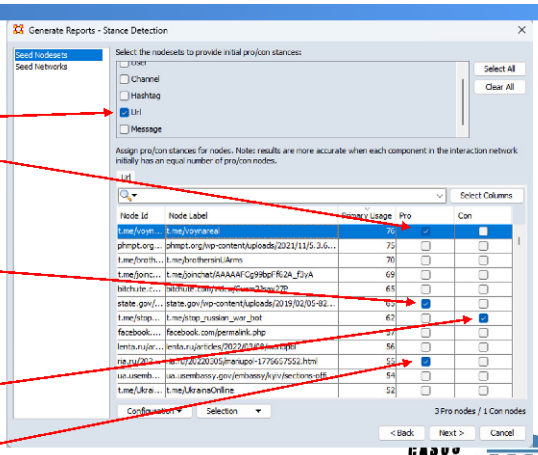
Stance Report Process

- Select the primary nodes that have an interaction that you want to use to propagate stance.
- For Twitter, this is usually “User” and for Telegram either “User” or “Channel”.



Stance Report Process

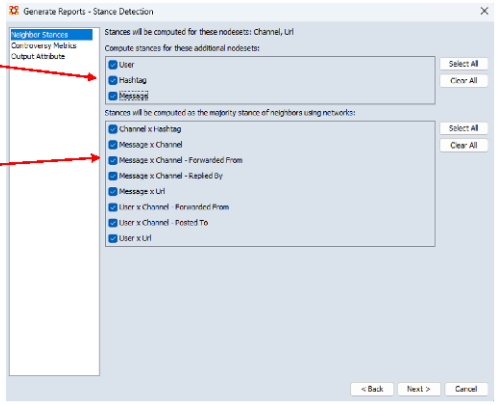
- Pick the attributes you will use to tag stances. For Twitter, we use URLs or Hashtags. For Telegram, we use URLs.
- Tag some URLs with known stances (you may have to do some research to determine these.
- State.gov link is to a document pointing to a weapons agreemement between US and UKR. People claim it as evidence of a chemical weapons program (pro-Russian talking point)
- Stop_Russian_War_Bot is a channel that is against Russia's invasion.
- RIA is a Russian state-sponsored media organization that posts pro-Russian content.



Carnegie Mellon University

Stance Report Process

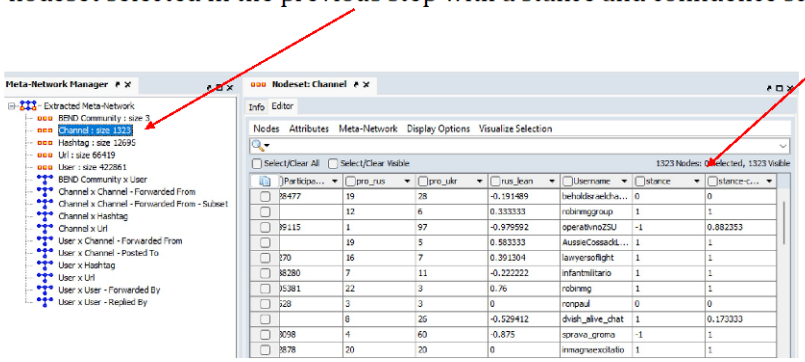
- Select what nodesets you want to get stances for.
- The selected interaction networks will be used to perform the network propagation.



Carnegie Mellon University

Stance Report Process

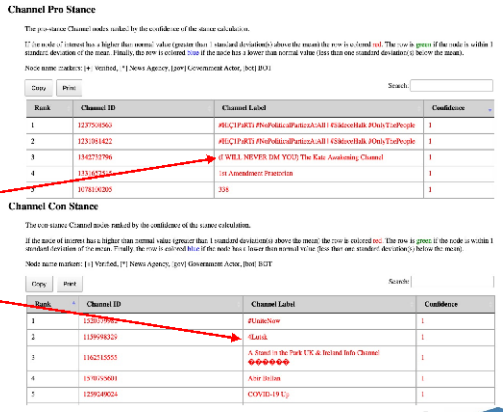
- ORA will generate a report (shown in next slide) as well as two columns in each nodeset selected in the previous step with a stance and confidence score.



Carnegie Mellon University

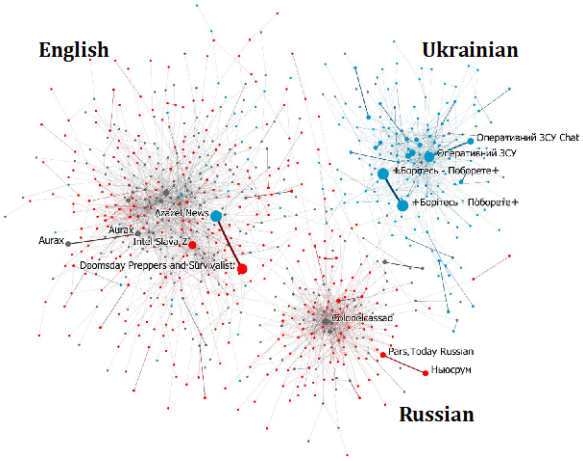
Stance Report Results: Telegram

- We can validate the Stance output by spot checking a few of the labeled channels:
  - Kate Awakening Channel is verified a far-right US commenter who is anti-Ukraine.
  - 4Lutsk is verified as a pro-Ukrainian channel



Carnegie Mellon University

Stance Report Results: Telegram



- Network Description:
  - Nodes = Channels
  - Edges/Size = number of forwards between channels
  - Node Color = Russia Stance (red = pro-, blue = anti-, gray = neutral)
  - Node Size = subscriber count
- "Barbell" channels that are heavily linked are channels and their associated chats
- Some channels and chats have different stances (e.g., Azazel and Doomsday).
- Three separate groups are language-specific - blue is Ukrainian language, red is Russian, mixed is English

Carnegie Mellon University

Stance Report Results: Twitter

- There are far more significant pro-Ukraine stance hashtags than pro-Russian stance hashtags.
- The pro-Ukraine stance was mostly in support of Ukraine and condemning Russia, while the pro-Russian stance was mostly

Hashtag Stance Summary

Stances were computed from the Pro, Con, and Neutral stances of neighboring nodes defined by network: Agent x Hashtag (transposed)

If the fraction of its Pro or Con neighbor nodes is greater than 0.50, then the node is assigned that stance.

Confidence equals the product of (1) the fraction of neighbor nodes that defined its stance, and (2) the average confidence of these neighbor stances.

	Number of nodes	Mean node confidence
Pro Nodes	11,805	0.843
Con Nodes	688	0.165
Not Assigned	11,380	

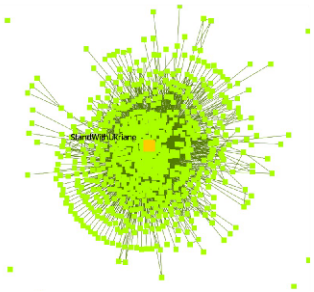
Nodeset	Node	Stance
Hashtag	StandWithUkraine	pro
Hashtag	PutinsPuppets	pro
Hashtag	istandwithukraine	pro
Hashtag	PutinPuppet	pro
Hashtag	RussianWarCrimes	pro
Hashtag	FUCKPUTIN	pro
Hashtag	NatoAllies	pro

Nodeset	Node	Stance
Hashtag	denazify	con
Hashtag	istandwithrussia	con
Hashtag	#nekUN	con
Hashtag	ISStandWithPutin	con
Hashtag	ISUPPORTRUSSIA	con
Hashtag	Natodefensemeasures	con
Hashtag	NatoLovesNazi	con

Carnegie Mellon University

Stance Report Results: Twitter

- Pro-Ukraine Stance (#StandWithUkraine)
  - The multiple blue nodes surrounding the ego, highlights the strong positive sentiment and support for Ukraine, while the red nodes showcase the condemnation of Russia
  - The interconnectedness of these nodes shows a cohesive community within Twitter bots who are programmed to align with pro-Ukraine stance

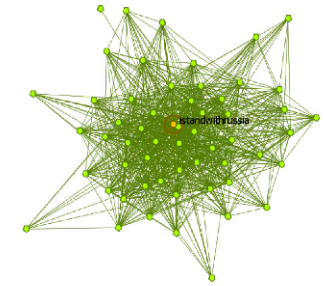


- Note: Orange node is the ego, red is anti-Russian sentiment, blue is pro-Ukraine sentiment, green is neutral

Carnegie Mellon University

Stance Report Results: Twitter

- Pro-Russian Stance (#istandwithrussia)
  - The lack of nodes surrounding the ego highlights that pro-Russian stance has less dense clustering of hashtags, implying a less cohesive or smaller group of Twitter bots that share pro-Russian sentiment



- Note: Orange node is the ego, red is anti-Ukrainian sentiment, blue is pro-Russian sentiment, green is neutral

Carnegie Mellon University

Botbuster Process

- Botbuster labels users as bots using a mixture of experts machine learning methodology
- More details on the Botbuster can be found here: https://doi.org/10.1609/icwsm.v17i1.22179 .
- Botbuster has been extensively tested on Twitter, and it also works well on Telegram. A paper demonstrating performance on Telegram is currently in revision.
- Botbuster is currently not available via a GUI, as it is run via command-line tools. For access to Botbuster, please contact CASOS.

23

Carnegie Mellon University

Botbuster Results: Telegram

- 677 (2.5%) of users were identified as bots
- Bots had more interactions with other users when compared to authentic users (average of 4.76 vs. 3.71)
- Bots (regardless of stance) have much higher E/I than authentic users, suggesting bots interact with authentic users more than each other
- Bots and non-bots had similar hashtag and URL usage (proportionate to their total messages) with the exception of pro-Russian bots, which used proportionally double the hashtags and URLs when compared to all other groups.

Community	Degree Centralization	Density	E/I Index	Echo Chamberness	Extreme Cohesiveness	Reciprocity	Specialty Concepts	Total Hashtag	Total Message	Total Url	Total User
anti_authentic	9.290e-04	6.616e-04	-0.032	0.519	0.046	0.143	RuSSiaKills, Zelensky, ЗСУ, напишут, Чернігів	146	26,904	374	4,731
anti_bot	0.001	6.490e-04	0.756	0.287	0.047	0.160	StopWar, WarOnFarms, вам_пишуть, Unity, общество	51	7,804	100	1,506
No Value	5.297e-05	4.801e-06	0.294	0	0.007	0.077	FlannelFriday, потерывает, draintheswamp, transhumanism, Petition	285	75,918	258	44,839
pro_authentic	3.475e-04	1.961e-04	0.037	0.096	0.030	0.143	ANTIWEF, HumanRights, together, Ukraina, StopTheTreaty	266	40,603	430	11,848
pro_bot	5.056e-04	1.993e-04	0.776	0.098	0.031	0.149	WEF, украина, MarchMADNESS, USA, Mariupol	136	12,855	263	3,631

24

Carnegie Mellon University

Botbuster Results: Telegram

Cross-Community Agent Interaction

This shows the amount of agent interaction between the communities. Values are the total sum of link weights from one community to another across all agent interaction networks.

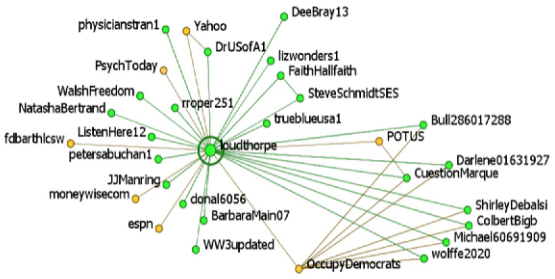
	pro_authentic	anti_authentic	pro_bot	anti_bot
pro_authentic	52,250	989	16,474	430
anti_authentic	983	51,680	249	15,844
pro_bot	16,394	249	5,161	196
anti_bot	334	16,735	112	5,293

- Bots interacted with authentic users more than they did with other bots.
- Both bot and authentic users tended to interact with users with a matching stance.

Carnegie Mellon University

Botbuster Results: Twitter

- Visualization of ego-network of "LoudThorpe" bot user (pro-Ukraine stance)
  - Pro-Ukraine stance bots create echo chambers when non-bot (human probable) users are removed from the analysis own stances, indicating a lack of cross-communication between Pro-Ukrainian and Pro-Russian positions
  - Loudthorpe has over 1200 tweets with over 4000 followers, indicating that this bot had significant influence.

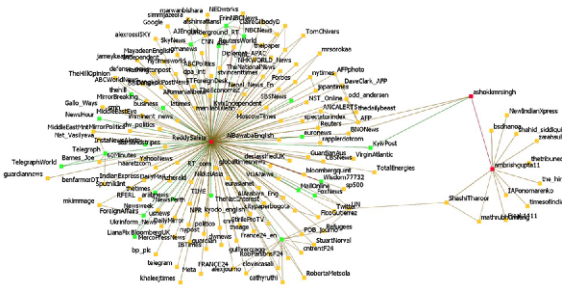


Note: Green is Pro-Ukraine stance, Red is pro-Russian stance, and Orange is neutral

Carnegie Mellon University

Botbuster Results: Twitter

- Visualization of ego-network of "ambrishgupta11" bot user (pro-Russian stance)
  - There are less pro-Russian stances bot users
  - The pro-Russian bots interact more with neutral stance bot users, trying to engage with the opposing view and potentially trying to influence the neutral and positive users towards a pro-Russian viewpoint.



Note: Green is Pro-Ukraine stance, Red is pro-Russian stance, and Orange is neutral

Carnegie Mellon University

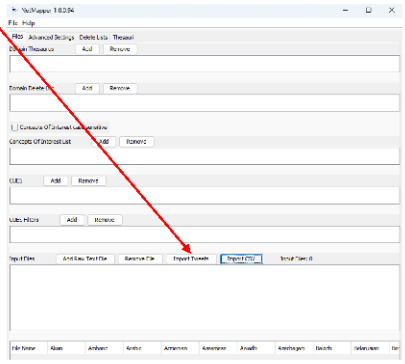
BEND Report Overview

- BEND is a framework to describe social cybersecurity maneuvers using social and linguistic cues.
- ORA provides BEND-detection capability through the BEND report.
- Outputs of the report are useful for locating and characterizing information space maneuvers.
- BEND is especially powerful if used comparatively - for example, comparing information space maneuvers between pro- and anti-Russian networks.

Carnegie Mellon University

BEND Report Process

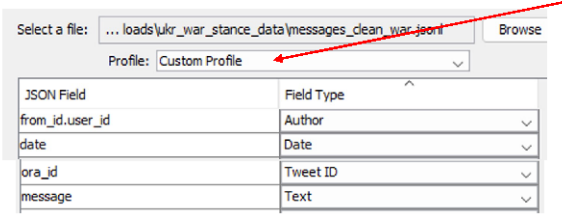
- BEND relies on the CUES generated by Netmapper.
- For Twitter, select Import Tweets and accept the defaults.



Carnegie Mellon University

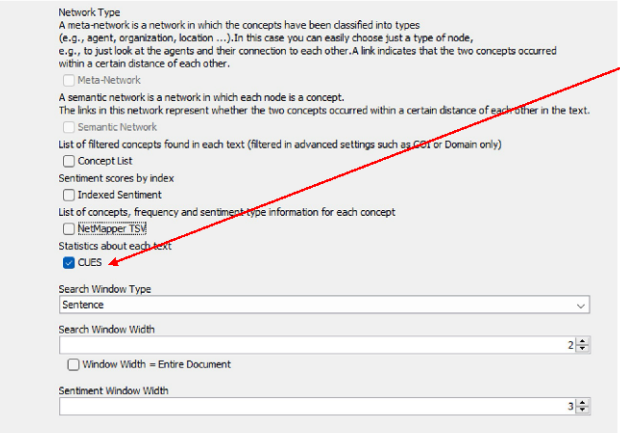
BEND Report Process

- BEND relies on the CUES generated by Netmapper.
- For Telegram, also select Import Tweets, but then select "Custom Profile" and modify the field types:



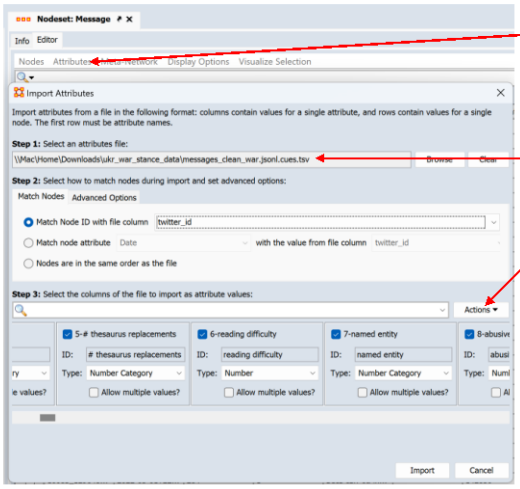
Carnegie Mellon University

BEND Report Process



- Make sure CUES is checked, and accept the remaining defaults.

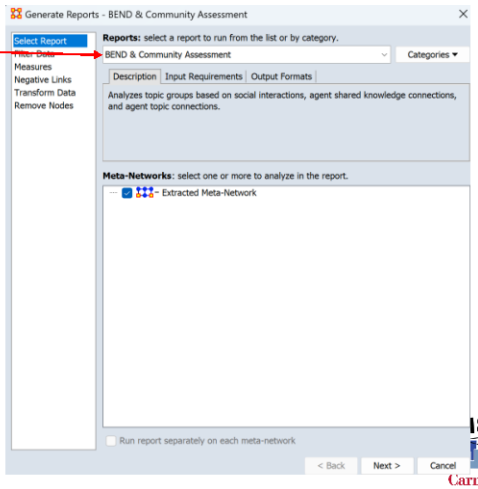
BEND Report Process



- To import the Netmapper CUES into the ORA Message nodeset, select “Import Attributes”
- Find your ORA output file
- Select all columns for import

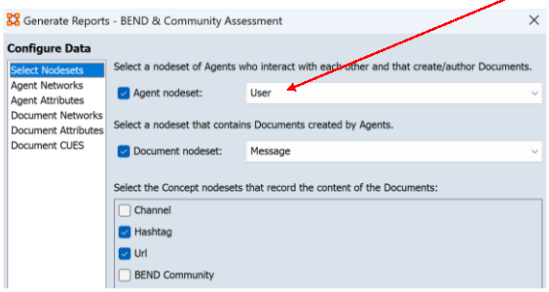
BEND Report Process

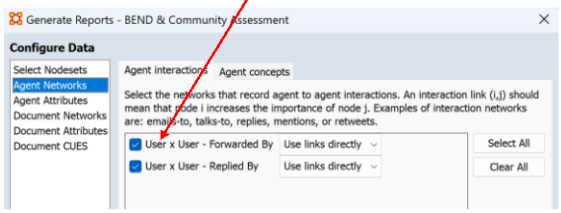
- Starting BEND report:



BEND Report Process

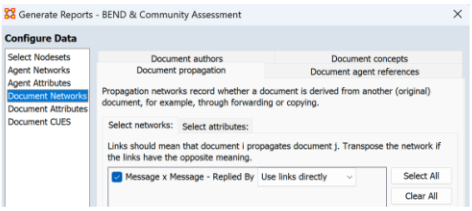
- It can be useful to run the BEND report for both Channels and Users for Telegram.
- For Twitter, Users should be the agent nodeset.

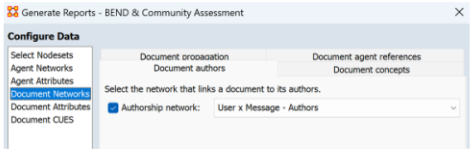


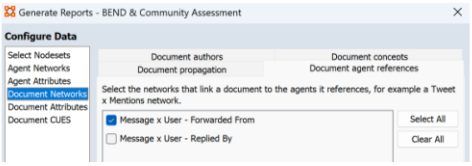


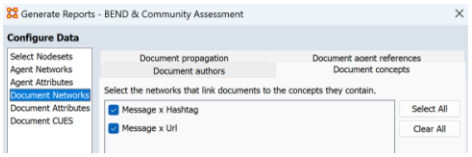
BEND Report Process

- Make the following selections for Document Networks:







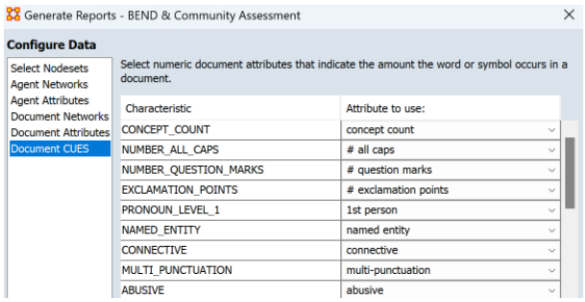


35

Carnegie Mellon University

BEND Report Process

- Netmapper CUES will automatically populate if they are imported into your Message nodeset. See earlier slide for importing instructions.

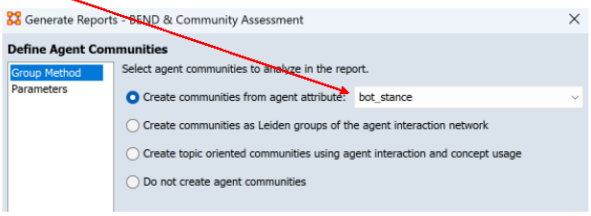


36

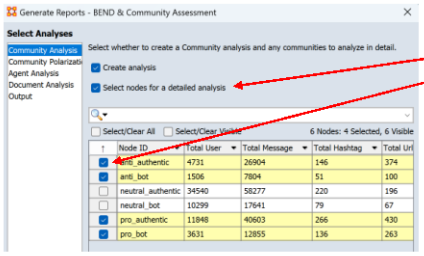
Carnegie Mellon University

BEND Report Process

- Select stance to compare BEND maneuvers by stance group.

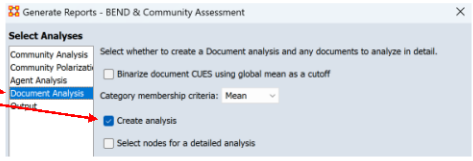


BEND Report Process



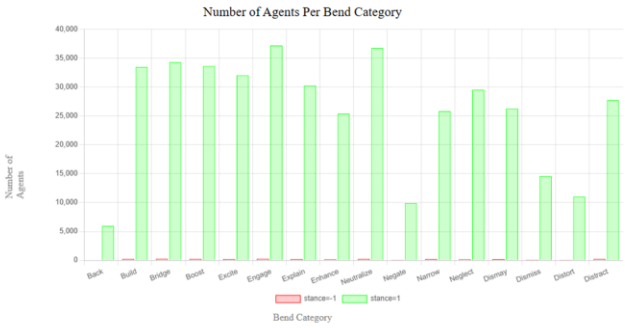
- Select the groups you want to analyze in detail.

- Select "Create analysis" to run document-level analytics



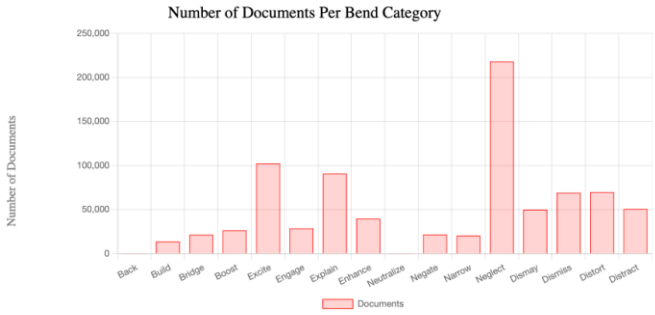
BEND Report Results: Twitter

- Pro-Ukraine bots focus on positive community building, aiming to boost the visibility and significance of pro-Ukraine voices and narratives.
- Pro-Russian bots focus on negative sentiment maneuvers, aiming to undermine pro-Ukraine narratives and evoke negative emotions regarding the conflict.



Carnegie Mellon University

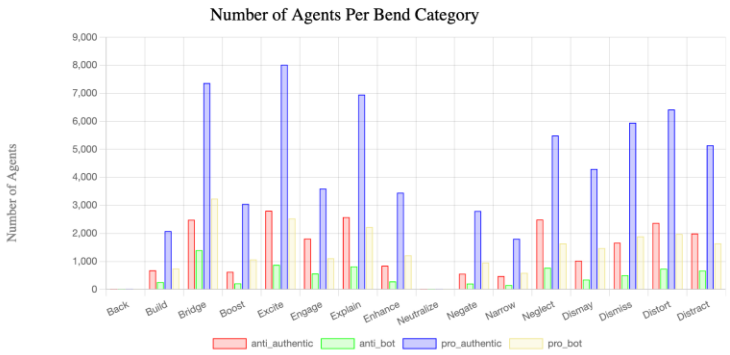
BEND Report Results: Telegram



- Neglect was the most-used maneuver
- The Neglect maneuver is meant to decrease the size of an existing group (it is a community maneuver)
- The next most prevalent maneuvers are all narrative maneuvers

Carnegie Mellon University

BEND Report Results: Telegram



- The proportion of maneuvers in each category is fairly consistent by stance and bot designation
- Pro-Russian authentic users are the only agents conducting Back and Neutralize maneuvers in the data.

Carnegie Mellon University

Discussion: Twitter vs. Telegram

- Stance:
  - Both platforms host varied stances, but Twitter has much more pro-Ukraine content.
  - Telegram hosts more varied stance on the war, and there is considerable interaction between channels with different stances.
- Botbuster:
  - Twitter bots tended to be pro-Ukrainian. The pro-Ukrainian bots interact primarily with other pro-Ukrainian users while the pro-Russian bots tend to interact with more neutral users.
  - Telegram bots were balanced between pro- and anti-Russian stance. Bots tend to interact with authentic users who hold similar stance on Russia as the bot account.
  - Twitter bots interacted with each other regularly, while Telegram bots typically interacted with authentic users.

Carnegie Mellon University

Discussion: Twitter vs. Telegram

- BEND:
  - Twitter:
    - Pro-Ukraine stance focused more on eliciting positive emotions to boost morale and support for Ukraine, whilst condemning Russian actions.
    - Pro-Russian stance focused more on evoking negative emotions to manipulate public sentiment in how Ukraine and NATO are corrupt.
  - Telegram:
    - Users of all categories employed the Neglect maneuver, aimed at decreasing the size of the opposing stance community.
    - A small group of pro-Russian authentic users were the only users to attempt Back and Neutralize community maneuvers

Discussion: Types of Tasks this Analytic Process can Help with

- Identifying and analyzing key actors and influencers:
  - ORA can detect central figures within a network, assess their level of influence, and understand the structure of their connections to other actors
- Evaluating community structures and dynamics:
  - ORA can uncover patterns and interactions of communities on social media platforms, able to detect echo chambers, polarized groups, bot networks, and more.
- Targeted actor analysis:
  - ORA's data management tools enable isolation and in-depth analysis of specific network segments or particular actors, allowing for detailed examination of their role within networks

Conclusions

- The Nazis and Ukraine narrative was widespread on both Twitter and Telegram.
- Both pro- and anti-Russian authentic users and bots conducted information maneuvers.
- Tactics on Telegram and Twitter were distinct:
  - Pro-Russian bots on Twitter had a more sophisticated approach, targeting neutral users. Anti-Russian Twitter bots and all Telegram bots primarily communicated with users holding the same stance.
  - BEND maneuver usage was more balanced on Twitter, while Telegram users tended to use Neglect maneuvers.
- Future analysis should seek to identify if these platform-specific differences are consistent across different domains and topics.

Acknowledgement

This material is based upon work supported by the U.S. Army Research Office and the U.S. Army Futures Command under Contract No. W911NF-20-D-0002. The content of the information does not necessarily reflect the position or the policy of the government and no official endorsement should be inferred.

For More Information

- Ian Kloo- iankloo@cmu.edu
- Reba Marigliano - rmarigli@andrew.cmu.edu
- Director, Kathleen M. Carley - kathleen.carley@cs.cmu.edu
- IDeaS website - https://www.cmu.edu/ideas-social-cybersecurity/
- CASOS website – http://www.casos.cs.cmu.edu/
- Facebook: @IDeasCMU
- Twitter: @IDeaSCMU
- YouTube: IDeaS Center

47