ISSN 2007-9737

# Characterizing Arabic Computational Propaganda on Twitter

Bodor Moheel Almotairy*, Manal Abdullah, Dimah Alahmadi

King Abdulaziz University,
Department of Information systems,
Faculty of Computing and Information Technology,
Saudi Arabia

bateekalmutairi@stu.kau.edu.sa, {maaabdullah, dalahmadi}@kau.edu.sa

**Abstract.** Background: The rise of social media has nourished the "computational propaganda" phenomenon. Propagandists rely on advanced artificial intelligence methods to change their writing style with every new campaign, allowing them to evade detection methods easily. Detecting computational propaganda in Arab countries has become a trending topic in social media research. Most of the proposed methods have been focused on detecting propaganda based on the writing style. Unfortunately, these approaches were marred with significant limitations because propagandists' traits and behaviours must be considered. Objectives: This study aims to demonstrate the value of characterizing Arab computational propaganda on Twitter to close the research gap. It follows a data-driven approach to investigate the main characteristics that can distinguish Arab computational propaganda on Twitter. Method: It follows a scientific approach to obtain and combine data from reliable and propagandistic users who discuss the same topics. Then, it provides a deep analysis of two communities that discussed different topics. It characterizes the key features that can be used to differentiate between them. Finding: The findings show that around 70 per cent of propagandists rely on artificial amplification by retweeting to produce an echo chamber supporting their viewpoints. The propagandists' following-to-follower ratio is between 0.8 and 1, indicating they are a coherent army that supports each other. 98 per cen of the propagandists' users participate in diverse topic discussions, indicating that topic diversity and publishing volume are very important features for detecting propaganda on Twitter. Publishing periods can strongly help in detecting propagandists. Novelty: The study offers early evidence on social media regarding the behaviour of propagandists' users and messages. This study enlightens future research by identifying the important features needed to propose anti-propaganda detectors.

**Keywords.** Computation propaganda, online propaganda, disinformation, social media, propagandists' characteristics.

## 1 Introduction

Social media networks have made communication easier by offering a variety of capabilities for transmitting data from one to another. They have revolutionized information distribution and become a prime reference for information and news. Amy Watson's 2022 survey found that more than 50 percent of adults in different Western countries heavily rely on social media as their main resource for information and news.

At the same time, 61 percent of Arab youth use social media as a news source, and 82 percent use social networks despite thinking they are unreliable [1]. Social media posts can range from being ostensibly impartial to being blatantly biased. Rather, the case went beyond that; social media became a fertile ground for spreading misleading content while ensuring it reached the largest segment of users regardless of geographical location. The 2016 US presidential election is a good example of the undeniable change from a "post-trust" to a "post-truth" society [2].

The long-standing argument about how the media and the public good are related has been reinvigorated. Some concerns have raised scholars' and social media administrators' worries about social media's effect on destroying democracy's integrity [3]. Propaganda is the main method of distributing misinformation and

disinformation [4]. The propagandists employ logical fallacies to appeal to the audience's emotions and convince them that the content transmitted is trustworthy and real. Additionally, to avoid the idea of "lies" in the propaganda, they use facts that appeal to the audience's emotions. In the social media era, computational propaganda phenomena have appeared.

It can strongly affect several different domains in different ways. Computational propaganda employs automation, AI algorithms, and human curation to produce and disseminate false content. Many platforms' anonymity features have encouraged the growth of automated and phoney accounts, which may be exploited to spread false information or suppress opposition [5].

Online computational propaganda has affected Different domains of interest. Over 81 different nations have been manipulated over social media [6]. Research by Twitter and Facebook showed that discovering propagandists' account characteristics significantly halts propaganda campaigns [7]. Most of the work has focused on propaganda detection, or, in other words, identifying whether the information is propaganda based on writing style and network structure.

Unfortunately, early approaches were marred with significant limitations due to propagandists' traits and behaviour not being made clear enough [8]. Although Arab countries are among the countries affected by computational propaganda, studies on Arab computational propaganda are rare and must be highlighted deeply. Advanced artificial intelligence (AI) systems can sort through large volumes of social media content, such as videos, photos, and text, more quickly than humans.

This scalability is crucial for studying social media material's vast and ever-changing world. Sentiment analysis, topic modelling, and network analysis are AI-enabled activities critical to identifying and classifying propaganda. Automatically completing these procedures allows researchers to identify propaganda narratives and patterns of dissemination quickly.

This research attempts to answer the following question:

(i) Are these the inevitable results of the presence of groups with similar ideas, traits, and the coordinated operations of "propaganda agents," or do we still need to understand something?

(ii) How do group cohesion and coordination dynamics among "propaganda agents" influence the dissemination and effectiveness of propaganda campaigns?

(iii) What role do technological affordances and algorithmic amplification play in shaping the reach and impact of propaganda content propagated by ideologically aligned groups?

To answer this question, the present paper takes a data-driven approach. It demonstrates the value of characterizing Arab computational propaganda on Twitter to close the research gap. The findings are extracted from high-quality data, as propagandists' data was shared via Twitter. Plus, it follows a scientific approach to gathering data from reliable users with the same interests as the propagandists.

Then, it conducts a deep analysis of a mixture of the two groups. The insights are gained by two classification approaches: (i) using the content of tweets and (ii) identifying users who actively participate in disseminating propaganda. The data covered two topics: sports issues and banking issues. The investigation was conducted on two topics to highlight the propagandists' characteristics, whatever their agenda.

Throughout this paper, we refer to the social media platform formerly known as Twitter as 'X,' reflecting its recent name change.

The rest of the paper is structured as follows: Section two discusses the computational propaganda behaviour resulting from the previous research results. Section 3 explains the research methodology. Section 4 shows the exploratory data analysis at the user level in 4.1 and the tweet level in 4.2. The results and the future work are discussed in Section 5. Finally, the research is concluded in Section 6.

## 2 Computational Propaganda Characteristics

Previous studies depend on two major elements to distinguish computational propaganda

characteristics: post-content characteristics and network structure characteristics. The next subsections discuss these characteristics.

### 2.1 Propagandist Post Characteristics

Regarding tweeting behaviour, the posts distributed by propagandists are usually identical and repetitive in that different users may have posted the same post. At the same time, they are usually high frequency, whereby a huge number of posts are made within a short period in a way that is not humanly possible [9,10]. These posts mostly contain links that lead users to the same article on a specific external website.

They are usually bracketed within hashtags, whereby a hashtag is used before and after a tweet, but these hashtags are not necessarily related to the specific post. Complex and longer sentences are another technique of propagandist posts [11], and it may occupy half of the sentence [12]. However, research findings contradict this observation [13, 14]; slogans are the best example of these techniques [15].

As for the characteristics of the contents, the propagandist content tends to use self-reference [16], personal pronoun and repetitive and irrelevant words [14,17]. These include words meant to exaggerate, employing subjective, superlatives, hedging words and modal adverbs. On the other hand, truthful posts contain words meant to give users concrete figures, such as money and numbers and use comparatives.

The posts by propagandists can be identified as satire and not real news, while non-propagandists may contain elements such as humour and assertive words. Propagandists utilize emotional language;for example, ironic and negative words that evoke their desired emotions are the most utilized. Exaggerated punctuation is another common element of propagandist posts. Such is the copious use of capital letters and exclamation marks unnecessarily [18].

The titles the propagandists use are usually different because they are longer, with fewer stop words and nouns, but with more proper nouns. The propagandist posts are mostly related to a prominent topic that headlines the mainstream media. A similar hashtag is used in a propagandist community, leading to an easier exploration of propagandist topics.

Each automated malicious account possesses a characteristic vocabulary. Such accounts may differ regarding the sophistication of their languages and the topics addressed. Some may lack the diversity of vocabulary and topics, so their persuasiveness may be lower and easy to detect.

On the other hand, others may employ more sophisticated language with more diversity in topics, meaning they are more likely to pass as human accounts. Name-calling and loaded language are the most common propaganda techniques used.

### 2.2 Propagandist Network Structures Characteristics

In the network, a conceptual connection of users represents the topological organization, while the clusters of the network are highly polarized compared to clusters represented in the entire network. In other words, the cluster of propagandists has the structure of a partisan community and a similar cluster of users with the same user identity. Unfortunately, the structure has a dynamic propagandist's user clusters [19].

This means that the partisanship of the users and the polarization of the users in a certain issue do not match. As such, the community structure used for interaction in the network is highly affected by the discussed topic, altering the users' perceived affiliation. Moreover, malicious accounts with similar stances do not necessarily belong to the same group but may even belong to opposing groups from different countries [20].

Different promoting strategies, such as complicated news websites and sharing similar content in one group, are used in organized groups, where different accounts share similar news from many websites. Content duplication and automatic retweets ensure that accounts work in a coordinated network to promote an account or story. There is a higher likelihood of internally mentioning or retweeting in a large community of propagandists.

Other research found that a propaganda network takes posts created by various users covering different propaganda items, and those

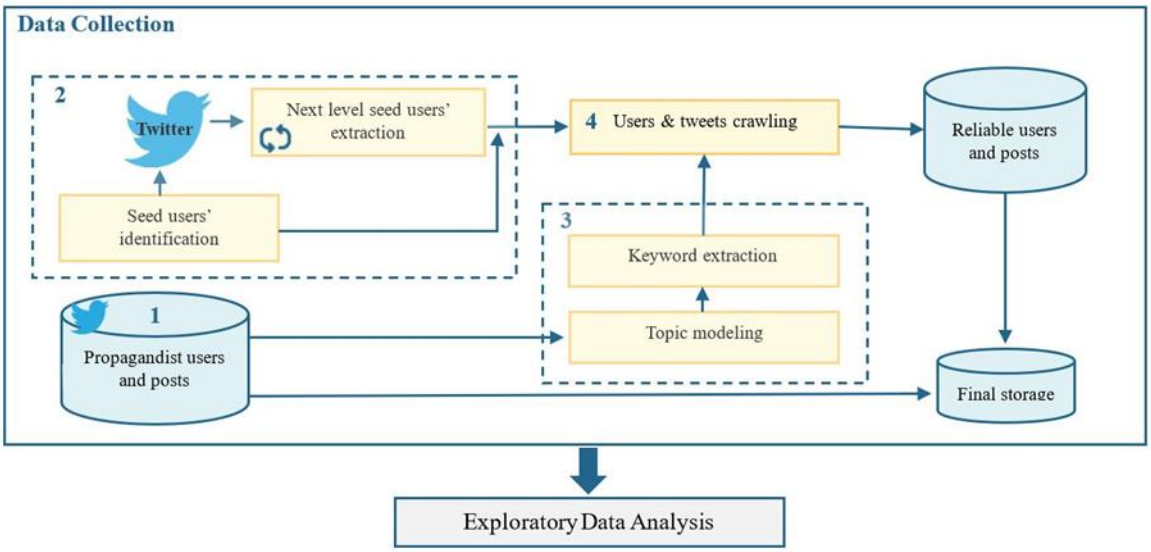


**Fig. 1.** Data collection framework

who share the items are consistent regardless of cluster polarization.

In some scenarios, the position of the posts' seeders is clear in the network. It can be in the communication strategy, as a broker, or at the centre, while in other cases, it is hard to identify the position of the seeders. If the position cannot be determined, information is broadcast from a few coordinated accounts that are not influential but significantly affect propaganda sharing.

Previous research has focused on understanding writing style and network structure to detect computational propaganda. At the same time, they agree that propagandists mimic non-propagandists in their writing styles. Plus, they change their strategies when launching a new campaign [21]. What this study is trying to explore differs from previous research. It searches for behaviours and characteristics that characterize propagandists, which can later be used in developing anti-propaganda models.

## 3 Methodology

Investigating propagandist behaviour on Twitter requires data about their profiles, tweets, and activities. To better understand their features, comparing them with non-propagandist features is important. Therefore, the non-propagandist tweets must cover the same topics that were covered by the propagandist tweets. As shown in Figure 1, the process started by determining the accounts of Saudi official news ecosystem stakeholders on Twitter and crawling their profile data. In parallel, the propagandist data, which includes propagandists' users and their tweets, was requested from Twitter.

Then, the main topics and keywords were extracted from the propagandists' tweets. The corresponding tweets of the official news ecosystem stakeholders crawled. Finally, a deep analysis was conducted to discover the main features distinguishing propaganda and non-propaganda users and contents. The next subsections describe the data collection procedures in detail.

### 3.1 Propagandist Data Requesting

Twitter provides publicly available archives of tweets through the Twitter Election Integrity Hub, which includes timely disclosure of information regarding organizations attempting to use Twitter to manipulate public opinion. The selected propagandist dataset was published in 2019- 2020. It contains 5929 Saudi accounts and 50 M tweets on general topics. The dataset was published in

**Table 1.** Total of official accounts

| Individual Account | | | | New Agencies | | | Government Sectors | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Author | Journalist | Important People | Formal Speaker | News Papers | TV News Channels | News Agencies | Ministries | Organization | Region's Administrators | Others | Universities |
| 345 | 401 | 34 | 11 | 25 | 3 | 26 | 25 | 42 | 14 | 136 | 395 |

two files: one includes the users' fields, while the other includes the tweets' fields.

The users' fields file includes 10 features about the users' metadata: user ID, display name, screen name, location, profile description, follower counts, following counts, account creation date, and account language.

The tweet field file includes twenty features in addition to all the features mentioned in the user's file: tweet ID, tweet language, tweet text, tweeting time, tweet client name, latitude and longitude of geo location if available, the list of hashtags that were used in this tweet, the list of URLs that were utilized in the tweet, the list of usernames that were mentioned in the tweet, and the total number of tweets that mention, reply, like, and retweet this tweet.

The other six features are about the tweet's originality. They are a bool variable to indicate if this tweet is a retweet, the user ID of the original user to whom this tweet is a reply or retweet, and finally, the ID of the original tweet to which this tweet is a reply, quote, or retweet.

### 3.2 Reliable Seed Users Identification

To create a reliable dataset, we must first identify credible news sources. Then, we can observe how those reliable users discussed the propagandists' topics. Identifying such sources will be worth considering the "news ecosystem". The term "news ecosystem" was first used in 2001 and is credited to renowned academic Henry Jenkins [22]. Like any other, a news ecosystem comprises linked networks.

Morgan Fionahas sought to determine the stakeholders in the news ecosystem. He suggests that it comprises government organizations, libraries, universities, newsrooms, media training, people, platforms, and informal and formal information. However, these new ecosystems' limits are inconsistent and understood [23].

Because the propagandist dataset is from Saudi Arabia, reliable users were selected from the same country. Based on Morgan Fiona's classification, the stakeholders of the Saudi news ecosystem are divided into four categories: individual accounts, news agencies, government sectors, and universities. Each category has subcategories. Table1 shows the subcategories in each category.

We selected the Saudi news ecosystem stakeholders list from Wikipedia articles, including government sectors, news agencies, and universities. Regarding the individual account, we have searched for famous and reliable Saudi journalists. Once those reliable sources were identified, we manually looked up their Twitter accounts, which acted as the seed users. This procedure resulted in 86 official accounts. The "snowball sampling" technique expanded the users' lists.

On Twitter, lists can be used for the "snowball sampling" technique [24], as they contain other Twitter users' accounts with the same interest. Finally, we obtained a total of six Twitter lists named "government accounts," "newspapers," "Saudi government bodies," "official sources," and "universities," with a total of 1,457 official accounts, as shown in Table1.

When selecting accounts, the following criteria were considered: First, the account must be active and verified, and the account is considered active if it publishes at least one tweet daily. Second, the journalists and authors must belong to official

magazines, newspapers, news agencies, or universities. Third, important people include ministers, organization managers, and executive directors.

### 3.3 Keyword Extraction Processes

Extracting keywords can be defined as identifying the linguistic units that best describe the document. Recently, supervised and unsupervised approaches have been used to retrieve keywords. The supervised model is trained to classify whether a given term is a keyword. This approach requires a human-annotated dataset as a training set. However, getting a trustworthy and exhaustive training dataset is difficult [25].

So, to avoid this difficulty, many unsupervised approaches have been adopted, considering keyword extraction as a ranking problem. Deep learning algorithms excel at keyword extraction problems [26].

According to Twitter, the propagandist's dataset used in this study is general. So, to extract the keywords, we probably must consider two points: First, good keywords must be related to the main document topics. Typically, words are rated highly when tightly connected to other terms, but this does not imply that they reflect the document's key topics. Second, the extracted keywords should cover all the main topics.

So, it is necessary to add a topic modelling step to the keyword extraction processes to address this issue. In this study, the keyword extraction method is decomposed into two methods. The first method is to model the topics, and the second is to find keywords under each topic. Only keywords related to the document are extracted, ensuring good coverage of all topics.

The size of the propagandist dataset reaches 50 million tweets. This data is huge, so the authors focused only on the tweets published by the most active propagandists. The activity of the users was measured based on their number of tweets. This resulted in 2,237,447 tweets published by the most active 1000 users. The next subsection discusses the processes in detail.

#### 3.3.1 Topic Modeling

Several methods for inferring latent topics have been presented in machine learning, known as latent topic models. One of the famous efforts in topic modelling is using the FastText unsupervised model to represent the language's hidden information in the text as vectors and then implement K-means clustering to group texts into topics [27]. FastText is a free, open-source package that Facebook AI Research (FAIR) developed to learn character-level word embedding.

Huge amounts of digitized text were used to train word embedding models, which then used the data to learn word co-occurrence statistics. It enables the development of supervised and unsupervised learning algorithms for generating word vector representations. Furthermore, it guarantees that even rare words will have the proper vector embeddings.

On the other hand, K-means clustering is a popular unsupervised machine-learning approach. It is used to group relevant data points. It helps to discover data patterns and organize written content into themes [28]. Applying FastText and K-means clustering consecutively helps to identify patterns in the data and group similar text documents together.

**Data Cleaning Step**

All the null values, non-Arabic texts, URLs, punctuation marks, whitespace, and new lines were removed. Cleansing the Arabic language is vital as Arabic is an inflectional language.

The Farasa Library (Arabic segmentation) is used in this research for lemmatization Normalization is applied to standardize the shape of Arabic words and letters so that they may be expressed in one form without compromising the sense of the phrase [29]. The dataset is normalized using Python's Tashaphyne module. It is an Arabic light stemmer that primarily supports light stemming (removing prefixes and suffixes) and offers all conceivable segmentations.

**Text Vectorizing Step**

Skip-gram [30] model was used to represent the text vectors. The Skip-gram model is a particular kind of neural network to produce word embeddings. It predicts the words in the context given a target word, Enriching Word Vectors with Subword Information. The Skip-gram model has the advantage of being able to produce high-

**Table 2.** The Top 10 refined keywords

| Topic | Top 10 frequent keywords | The Top 10 refined keywords (Arabic) | Keyword translation |
|---|---|---|---|
| Saudi sport | بطولات – دوري ابطال– هدف الاهلي – بطول – السد القطري – الهلال و السد – الهلال جمورك – التعاون يعيد -مبار النصر- فوز | دوري -دوري ابطال اسيا - دوري أبطال آسيا نهائي أبطال -دوري ابطال آسيا - أبطال اسيا – نهائي أبطال آسيا-نهائي ابطال آسيا-آسيا فوز-هدف--مباريات - بطولة – بطولات -النصر-الأهلي-جمهور-جمهورك-الهلال السد- التعاون | AFC Champions League - Asian Champions final- championships - championship - matches-victory-goal-audience-"your audience - Al Hilal club - Al Ahly club – AL Cooperation club -Al Sadd club |
| Banking issues | سدادقرضة – ايقاف الخدمات – تسديد قروض – متعثرات – اسلامية – بنك الراجح – تمويل بنك – الاهلي – اسقاط قروض – سداد متعثرات | سداد قرض – ايقاف الخدمات – تسديد قروض – متعثرات – قروض اسلامية – بنك الراجحي – تمويل بنكي –بنك الاهلي – اسقاط القروض – سداد المتعثرات | Repayment of a loan - suspension of services - overdue - Islamic loans - Al-Rajhi Bank - bank financing - Al-Ahly Bank - dropping loans - paying overdue loans |

**Table 3.** Dataset size

| Category | Topic | Tweet | Users |
|---|---|---|---|
| Propaganda | Sport | 514613 | 487 |
| | Banking | 246,119 | 478 |
| Non-propaganda | Sport | 2012 | 306 |
| | Banking | 51703 | 669 |

quality word embeddings that can represent the semantic and syntactic links between words.In our experiment, we used the default values of the parameters.

### Clustering Step

Mini-Batch K-Means was used because the dataset is huge. Mini-Batch K-Means is a K-Means clustering algorithm version that uses smaller random batches rather than the complete dataset for each iteration.

As a result, it outperforms the traditional K-Means method in speed and scalability [31]. In this experiment, the batch size was 216. An elbow approach was utilized to identify the ideal number of clusters, K [32].

In the elbow approach, the value of k is continually iterated from k = 2 to k=n (n was set to 20) and calculated Inertia for each K. Inertia is a K-Means algorithm performance metric. It is calculated by measuring the distance between each data point and its centroid, squaring these distances, and adding these squares for each cluster.

### Main Topics

With the help of a volunteer journalist, the main topics of the clusters were identified as follows: One political cluster includes tweets about countries' issues and some political figures. Two sports clusters include tweets about clubs and players in Saudi football. Two social issue clusters include tweets about Saudi bank issues and strong objections to bank loans.

Four clusters include tweets containing supplications. Three clusters include tweets containing poems. One cluster includes tweets containing different ads. One cluster includes tweets that contain only a few words that do not present any meaning.

### 3.3.2 Keyword Detection

Recent developments in deep learning have qualified researchers to enhance traditional keyword extraction techniques, which rely solely on statistical or graph measurements [33]. KepBert is an open-source deep learning keyword extraction method that uses pre-trained word embedding models (BERT) to extract keywords'

semantic similarity relationships between words, increasing the efficiency of the retrieved keywords. BERT, which stands for Bidirectional Encoder Representations from Transformers, is the model proposed by Google researchers to improve NLP tasks [34].

The keyword extraction processes start with KeyBERT tunning and then evaluation of the KeyBERT results. KeyBERT with the maxsum method was used to extract the keywords. It was configured to generate n-grams varying in size from one to three. The five top terms are retrieved and evaluated against the manually provided terms. The model was controlled with diversity = 0.7, method = 'maxsum', top_n = 5, and ngram_range = (1, 3).

The evaluation process includes two steps. The first step is human-based annotation, while the second measures the overlap between the keywords extracted by the human being and KeyBERT.

Three volunteer annotators (journalists) used an in-house labelling approach to label 1000 tweets on sports and banking topics. The first two annotators give keywords to tweets individually, set to 3 in this research.

In which the first two annotators disagree, the third annotator separately labelled the Tweet. The degree of agreement between the two annotators was measured using Cohen's kappa [35]. Cohen's Kappa demonstrated 'good' agreement with a kappa=0.633, indicating 85 per cent agreement.

To evaluate KeyBERT results, we applied the evaluation method proposed by Rousseau et al. [36] called Partial Match Framework. The reasoning for this architecture is that while keyword extraction methods frequently provide the right terms, the tests frequently produce poor results when evaluated under precise matching.

The partial F1 score (pF1) is the harmonic mean of the partial recall and precision. pF1 is the number of retrieved keywords that correspond partially to those labelled by annotators, which is set to 3 in this research. The evaluation result as the following with Partial Precision=0.682, Partial Recall= 0.719, and pF1 = 0.7

### 3.3.3 Keywords Refining

Based on the keywords' keyness property, the semantic features are not equally important in all applications, documents, and domains [25]. Moreover, the proper number of keywords is not strictly limited. Thus, a suitable trade-off must be identified between extracted keywords' quantity and quality.

They must be minimized regularly, as must the exhaustivity of the document description provided by them. Similarly, a keyword should be neither too particular nor too broad. At the same time, clarity is essential. For the sake of efficiency, some of these principles, such as well-formedness, may be ignored. Ill-formed terms can be useful in increasing keyword matching.

Table 2. Shows in the first column the top ten extracted keywords by KeyBERT. The next column in the tables shows the extracted keywords after refinement by experts to satisfy the keyness properties, while the final column includes the translation of the keywords.

To refine the keywords, the truncated keywords that are ill-formed were corrected, such as (مبار) is replaced by (مباراة) (match). Contiguous words have been rewritten correctly by adding spaces between them, such as (سدادقرضة) by سدادقروض) ) or (سدادقرض). All letterforms were considered; this is because some Arabic letters can be written in several forms according to Arabic linguistic rules, such as (أ) could be written (ا)(إ)(آ), but social media users do not adhere to such rules.

The phrase (أبطالآسيا) (Asian champions) could be written as (ابطالاسيا) or (أبطالاسيا) or (ابطالآسيا). The experts added the general words to each other to form more specific keywords, such as the word (الراجحي), which is a bank's name, added to the word (قرض), which means loan.

Some words were added to the keyword even though they did not appear in the keywords list; adding them makes the keyword more particular. For example, the words (آسيا) (Asia) were added to the phrase (دوريابطال) (Asian champions).

### 3.3.4 Non-propagandist Data Crawling

Tweet crawling is the process of gathering tweets. Academic Research license was used to crawl reliable data. It lets researchers search the full history of public Tweets. An R Package called 'academictwitteR' was used to query the Twitter Academic Research Product Track, enabling full-archive search and additional v2 API endpoints.

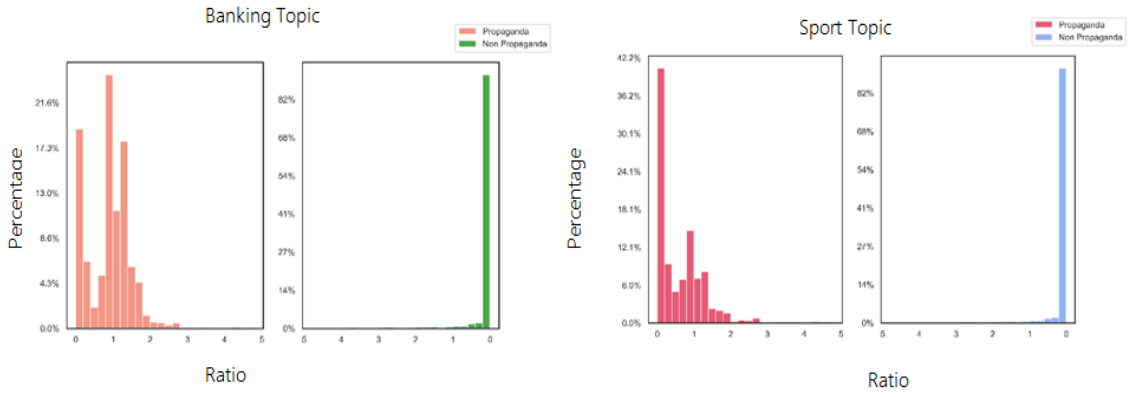


**Fig. 2.** Following to followers ratio

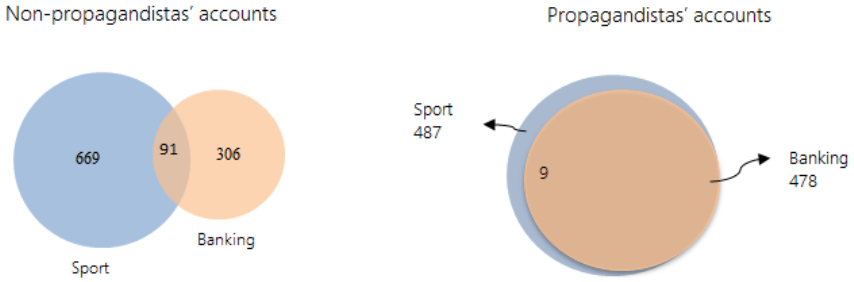


**Fig. 3.** Accounts overlapping

The data was crawled from January 1, 2019, to December 31, 20202, based on pre-identified keywords in Section 3.3.3 and pre-identified reliable accounts defined in Section 3.2. We chose this timeframe to capture the same topics and events discussed by the propagandists.

As a result, we crawled 53715 tweets from 975 accounts, as shown in Table 3. The table also shows the propagandist tweets and users on banking and sports topics. Although the numbers of propagandists' and non-propagandist users are almost equal, there is a large discrepancy between tweets, especially regarding banking issues.

## 4 Exploratory Data Analysis

An exploratory data analysis (EDA) is conducted to discover the behaviours and features distinguishing between computational and non-computational propaganda. The analysis was applied at the user level to discover the features that distinguish propagandist accounts and the tweet level to discover the features that distinguish the propagandist's tweets.

### 4.1 User Level Analysis

The users' level aims to investigate the differences between propagandist users and non-propagandist users from different perspectives: popularity perspective, account age perspective, profile description perspective, and accounts overlapping perspective. The following subsections describe each perspective in detail.

#### 4.1.1 Popularity Perspective

When a user follows an account on Twitter, his stream will include tweets from that account, and his account will appear publicly in the list of that

account's followers. Following someone indicates the user is interested in the account's topic or a fan of the account's owner.

At the same time, the following person will evaluate the account that is following him. If he is interested, he will return the following. Thus, the number of followers can be increased from the number of followers. The number of followers a user accumulates depends on his fame and activity level. The influence of a user can be associated with the number of followers because their tweets reach a wide audience [9].

The following-to-follower ratio of the account refers to how many accounts it follows compared to how many followers the account has on social media platforms. It is believed that people can quickly determine how "credit" an account is based on the user's follow ratio.

This is because popular accounts often have much larger followers than followers, and vice versa [36]. Figure 2 shows the following-to-follower ratio of propagandists and non-propagandists in banking and sports topics based on equation 1:

$$Ratio = Following / Followers. \quad (1)$$

The ratio will equal zero when the Followers equal 0, and the ratio will be equal to 1 if the Followers equal Following. If the ratio is greater than 1, the Twitter user is following more users than they are following back, and vice versa. A ratio that is nearer zero increases the user's influence. According to research that analyzed a sample of data from roughly 10K profiles worldwide, 70 per cent have a following-to-followers ratio of less than 5 [36].

As shown in Figure 2, the pattern of banking and sports topics is similar. More than 85 per cent of the non-propagandist accounts have a ratio between 0 and 0.2. Almost all the rest are between 0.2 and 0.5, indicating that they follow the normal pattern. It is quite different regarding propagandist users.

We found that the peak of the ratio was between 0.8 and 1 in banking. In the sports topic, most of the users have a ratio between 0 and 0.2. The reason may be that social media users interact more with sports accounts [37, 38]. At the same time, we found that about 50 per cent of the users have a ratio of more than 1.

This finding confirms our suggestion in the previous section, which indicated that the propagandists' users are an army that is coherent and interacts with each other. They are trying to immerse themself in Twitter communities and seek to increase their followers by increasing the number of people following them.

### 4.1.2 Accounts Overlapping Perspective

Propagandists rely on the artificial amplification of Twitter interactions, including establishing several or overlapping accounts [39]. Figure 3 depicts the intersections between propagandist users in banking and sports topics. It illustrates that the propagandists' users are completely overlapped.

Only nine propagandist users participated in the computational propaganda sports campaign and did not participate in the banking campaign. That means the propagandist accounts used to manipulate public opinion on the banking topic were the same ones used to manipulate public opinion on the sports topics.

Regarding the non-propagandists' users, figure 3 shows that the users who post on both topics are only 91 accounts. So, this finding assures that to evaluate the account's reliability, it is important to understand the topicsthe author addresses and his stance [40].

### 4.1.3 Accounts Overlapping Perspective

The account creation date was not widely investigated in respect of propaganda detection. This research assumes that the age of the Twitter account is an indicator that may be considered when detecting propagandists' accounts [41].

The reason is that, based on previous studies, propaganda campaigns are carried out by an electronic army created for this purpose. Thus, the army will most likely be established in the same year the propaganda campaign is launched. The question may arise whether using the same army more than once is possible.

The sure answer is that we can use it technically, but Twitter makes a great effort to detect and close these accounts. Many of the accounts of former armies may have been eliminated. Figure 4 proves our assumption. It illustrates the account creation years of the propagandists' and non-propagandists' users.

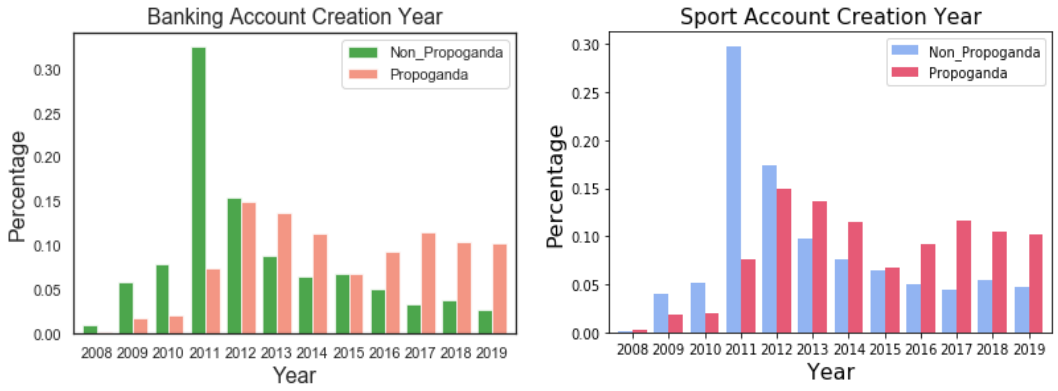


**Fig. 4.** The accounts creation years of propagandist and non-propagandist users

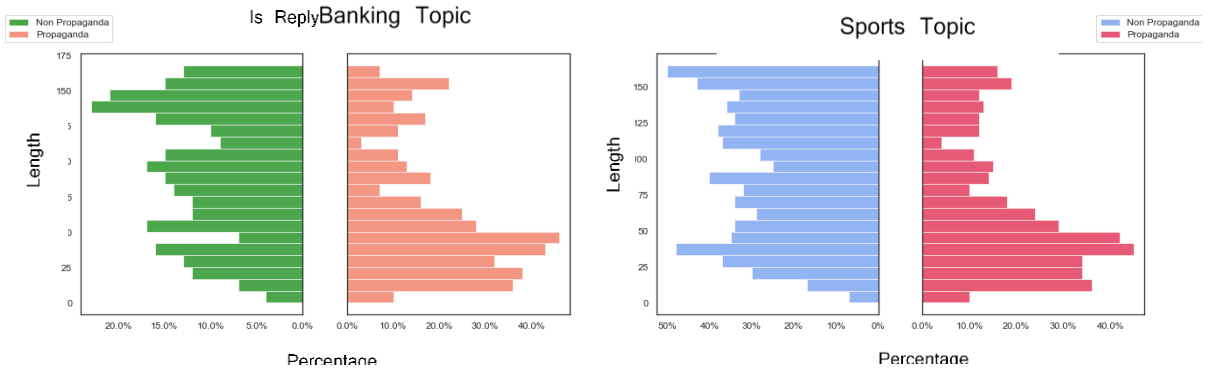


**Fig. 5.** Distributions of bio length of the propagandist and non-propagandist users in banking and sports topic

As shown in the figure, the propagandists' accounts are considered newer than non-propagandist accounts; about 40 percent were established in the last four years before the campaign.

### 4.1.4 Profile Description Perspective

The Twitter account profile description was analyzed as a feature often ignored in relevant works [42]. At this stage of the analysis, the content of the description in terms of the number of characters, the occurrence of hashtags, and the occurrence of URLs were considered. Figure 5 illustrate the differences in bio length between propagandist and non-propagandist users.

As shown in the figure, 10 per cent of the propagandist users do not provide any description in their profile for banking and sports topics. On the other hand, only about 3 per cent of banking non-propagandists and 4 per cent of sport non-propagandists do not describe themselves in their profiles.

In general, non-propagandists tend to describe themselves in long sentences more than propagandists

## 4.2 Tweet Level

To understand the pattern of computational propaganda, the EDA has been conducted at the tweet level. The analysis included several perspectives: first, it explored the tweets' originality by determining whether the propagandists' tweets were original or interactive. Second, it compared

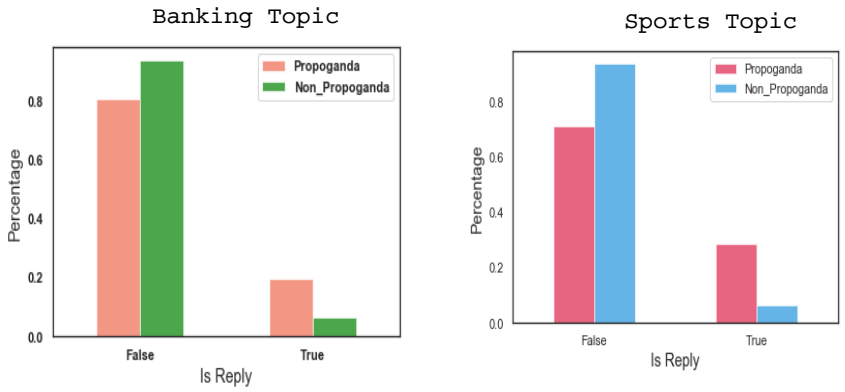


**Fig. 6.** Percentage of replies to tweets

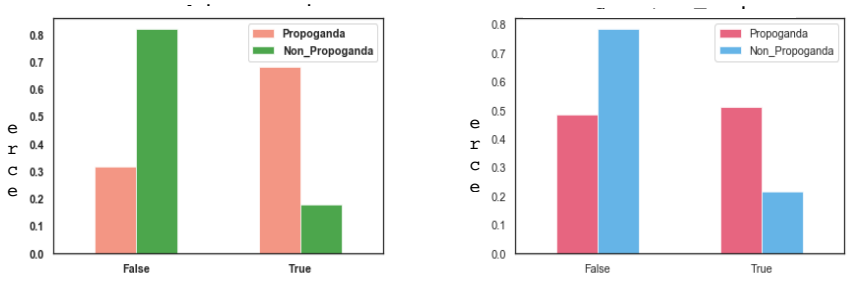


**Fig. 7.** Percentage of retweeted tweets

propagandists' tweets with non-propagandists' tweets regarding their ability to ignite interaction with the other users.

Third, it discovers their behaviour of embedding URLs and hashtags in tweets. Finally, it compares the daily publishing rates of propagandists and non-propagandists.

### 4.3 Tweet Originality Perspective

This analysis aims to explore the tweets' originality. Such analysis provides insights into whether to agree or refuse an existing approach. It assumes that postings from propagandists' accounts are almost identical since the supporters frequently pre-write the material [9, 10].

Figures 6 and 7 compare propagandist and non-propagandist patterns of originality in tweets on sports and banking topics. In general, we found that the pattern is similar in both topics. The propagandists' users tend to retweet the propagandists' tweets more than reply to them.

According to Figure 6, 20 percent of propagandists' banking tweets and 29 percent of propagandists sport tweets are replies, implying that some propagandist users try to engage in discussions by replying to each other. Based on the finding of Pacheco et al. [19], this behaviour increases the dynamicity of the propagandist's user clusters. As such, the community structure used for interaction in the network is highly affected by the discussed topic, altering the users' perceived affiliation.

However, we do not find many propagandists' tweets replying to other propagandists' tweets because the automated propagandist's accounts are just looking for a tale based on a narrative (or are expressly directed to a tweet or story). Moreover, they do not reply since they are unlikely to have NLP-Generation capabilities.

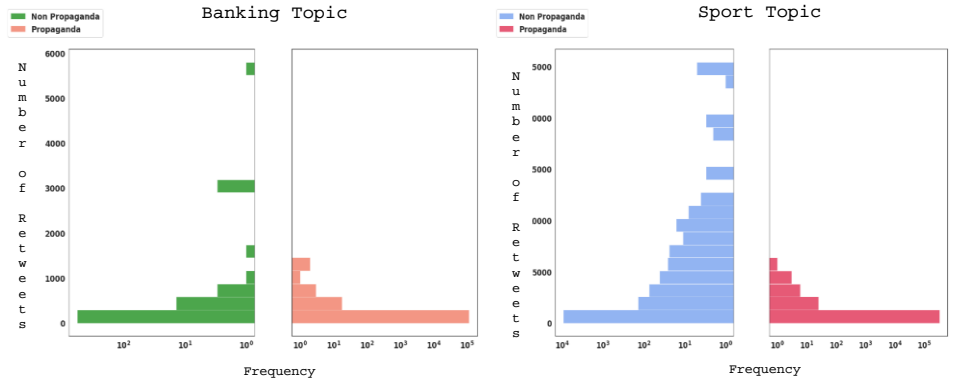


**Fig. 8.** Distributions of retweets interactions

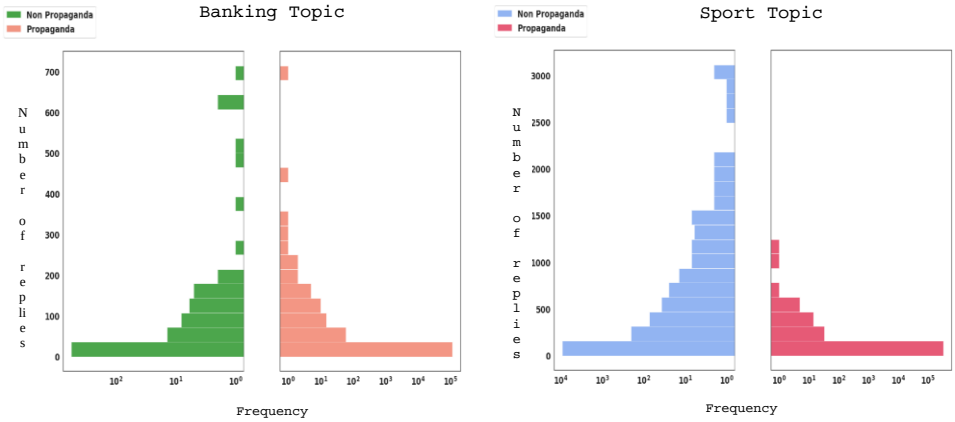


**Fig. 9.** Distributions of replies to interactions

Figure 7 shows that retweeting is a clear feature of propagandists' users: 68 percent of banking propagandists' tweets and 51 percent of sports propagandists' tweets are retweets.

This insight supports the finding of Pacheco et al. [19] that propagandists' tweets tend to duplicate and retweet content automatically to ensure that accounts work in a coordinated network to promote an account or story. Eventually, 81 percent and 78 percent of the non-propagandists' tweets on banking and sports topics are original, and they interact with each other in a normal pattern.

### 4.4 Engagement Rate Perspective

This aspect of the EDA attempts to compare the patterns of interactions ignited by both propagandists' and non-propagandists' tweets. It tracks how many retweets and replies each tweet receives in both topics. This will provide valuable insight as it determines the strength of a tweet's impact. As is customary, people click on links they believe will interest them.

They favour posts that they think are particularly noteworthy. However, they retweet anything that they believe would be of interest to their followers [5, 41]. Figure 8 shows the distribution of the gained retweets. The retweet amount of the sports non-propagandists' tweets is high, proving the finding of Tristan Handy [38], who found that 21 of 50 retweet accounts were sports-focused on social activity.

Furthermore, the figure shows that non-propagandists' tweets were continuously

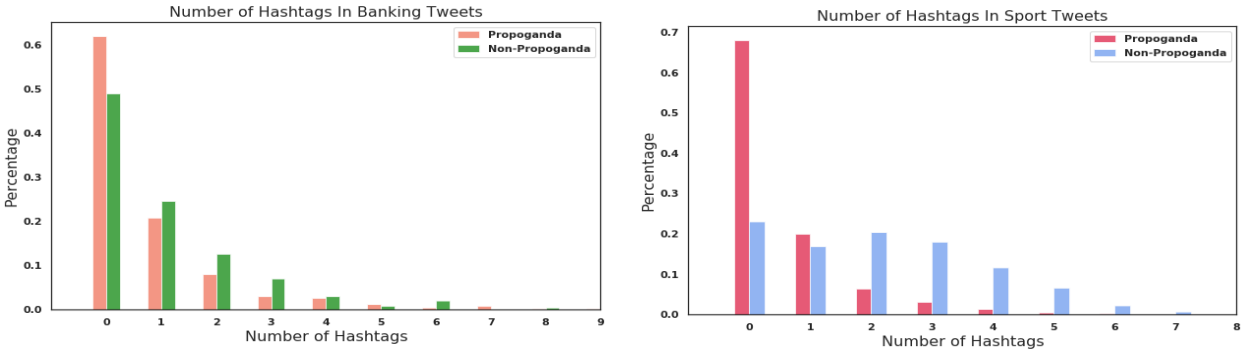


**Fig. 10.** Distributions of Hashtags embedded in tweets

retweeted on both topics, whereas propagandists' tweets were not frequently retweeted. The reason may be that the propagandists' tweets were originally retweets, as we mentioned above, and these retweets were not retweeted again. These notes reinforce the broker communication strategy discussed by Agarwal et al. [9]. Weber and Neumman [39] concluded there is a higher likelihood of mentioning or retweeting propaganda in a large community of propagandists internally.

Thus, we can assume that the propagandist army retweeted the tweets of their broker. As a result, a conceptual connection of users represents the topological organization, while the network clusters are highly polarized compared to clusters represented in the entire network [2]. In other words, the cluster of propagandists has the structure of a partisan community and a similar cluster of users with the same user identity.

Regarding participating in discussions, most of the replies on Twitter were related to sports topics. As shown in Figure 9, the non-propagandists' tweets ignited more replies on sports topics, although the number of propagandists' tweets is much higher than the propagandists' tweets in the dataset. Note that the replies do not have to be from non-propagandist users, as this is the goal of propaganda campaigns: to engage people in discussions to manipulate their opinions.

On the other hand, replies may be one of their strategies to influence the dynamics of the community structure [19], altering the users' perceived affiliation. So, we cannot consider the amount of replies as a distinguishing feature between propagandists' and non-propagandists' users.

### 4.4.1 Text Content Perspective

A hashtag is created on Twitter by adding a "#" to the beginning of an unbroken word or phrase. When a hashtag is included in a tweet, it links to all the other tweets that use it. Figure 10 illustrates the distribution of the hashtags used in propagandists' and non-propagandists' tweets on sports and banking topics.

The figure shows that non-propagandists users tend to embed hashtags in their tweets more than propagandist users. This can be attributed to the fact that including a hashtag in a tweet provides an explanation and helps users readily track subjects of interest.

As shown in Figure 10, 62 percent and 67 percent of the propagandists' tweets did not include hashtags in the banking and sports topics, respectively. On the other hand, 49 percent and 23 percent of the propagandists' tweets did not include hashtags in the banking and sports topics, respectively.The similarity of this behaviour between propagandists in both topics reflects the following behaviour.

However, these findings contradict Agarwal et al. [9],who found that propagandist posts are usually bracketed within hashtags. However, these findings prove that the propagandists change their strategies every time they deploy a new campaign [5]. Usually, a link is placed in the tweet when we want to direct users to a site outside of Twitter.

Figure 11 illustrates the distribution of URLs used in propagandists' and non-propogandists'

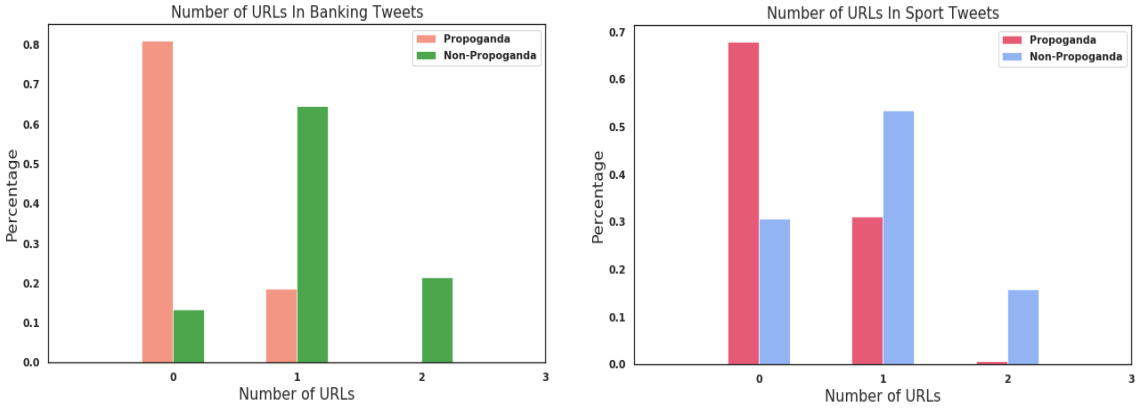


**Fig. 11.** Distributions of URLs embedded in tweets.4.2.4. Publishing time perspective

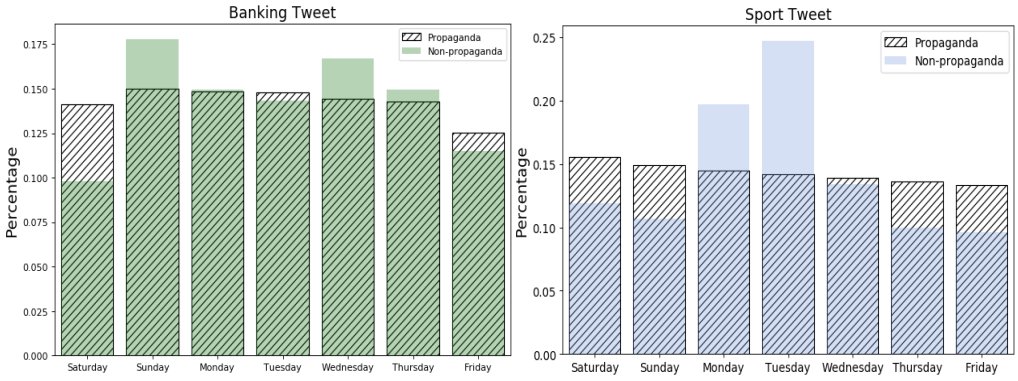


**Fig. 12.** Distributions of publishing days

tweets on sports and banking topics. It seems that non-propogandists' tweets include URLs more than propogandists' tweets.

Approximately 81 percent of propagandists' tweets on banking topics and 67 percent on sports topics did not include URLs. Almost all of the remaining propagandist tweets contain just one URL. There are very few tweets on the sports topic that include two URLs. On the contrary, URLs appear in 87 percent of non-propagandist tweets in banking topics and 69 percent in sports topics.

According to Agarwal et al. [9], the propagandists' tweets mostly contain links that lead users to the same article on a specific external website.

This finding contradicts ours, demonstrating no clear understanding of computational propaganda strategies because propagandist users change their strategy to manipulate public opinion at each campaign deployment [5].

### 4.4.2 Publishing Time Perspective

People log in to Twitter at various times based on their schedules and time zones. To reach a broad portion of the audience, it is necessary to determine what time of day the audience likes to view tweets so that they may be published properly. Choosing the right timing is certainly one of the strategies of the propagandists' users.

The time was analyzed for publishing days and periods to discover the propagandists' behaviours. Figure 12 investigates the publishing days. In both topics, propagandists' users do not differentiate between the days of the week; they post throughout the week almost equally as if they have a task to accomplish.

This behaviour is completely different from that of non-propagandists' users, as shown in the figure. Therefore, the number of tweets circulated on a suspicious topic throughout the day is an important indicator for detecting propaganda. The posting period was examined to obtain the most accurate results.

The posting timespan in the dataset has been modified to match the timing of the Kingdom of Saudi Arabia, which was targeted in this propaganda campaign. Figures 13 and 16 show the distribution of the posting timespan.

The result was very strange. The posting timespan pattern for banking andsports topics varied to match the posting timespan of non-propagandists' users interested in the same topic. We can conclude that the timing of propaganda campaigns is analyzed carefully to target the segment interested in the topic.

Therefore, the timespan is an important indicator for detecting propaganda while considering the topic.

#### 4.4.3 Publication Frequency Perspective

While excellent content is unquestionably the most crucial aspect of constantly increasing users' presence on social media, understanding how frequently to publish is critical to ensuring that users reach their target audience [43]. It is typically advised to publish no more than 1-2 times per day and no more than 3-5 times per day. Data reveals that engagement drops dramatically after the third tweet of the day [44]. Figure 14 depicts the distribution of daily posting times in both topics between propagandists and non-propagandists.

According to the figures, the number of daily tweets by non-propagandist users on both topics did not exceed 8 posts and 43 posts per day on the banking and sports topics, respectively [45].

Most of them publish only one tweet per day. As previously stated, Twitter users are typically active in sports topics due to their competitive nature. Therefore, we find that the number of daily tweets on sports topics exceeds those on banking topics.

Regarding propagandist users, daily posts reach 121 posts on the banking topic and 308 on the sports topic. Less than 50and 30 per cent publish one daily tweet on banking and sports topics, respectively.

That means propagandists rely on the artificial amplification of Twitter postings. These findings agree with those of Weber et al. [10] and Agarwal et al. [9] found that propagandist posts are usually made at high frequency, whereby many posts are made within a short period in a way that is not humanly possible.

## 5 Discussion, Result and Future Works

This research aims to reveal the characteristics of propagandist users and their posts on Twitter. It goes over the dataset collection and exploration process. The data-gathering procedure collects tweets from Twitter to create ground truth. Detecting propagandists on Twitter necessitates information on their accounts, tweets, and activity.

The propagandist dataset, which includes the propagandists' user-profiles and tweets, was requested from Twitter. However, to properly grasp their features and behaviours, they must be compared to reliable accounts' features. This entails determining Saudi official news ecosystem stakeholders' accounts.

Then, they gather their tweets on the same topics the propagandists' users discussed. An unsupervised technique was utilized to extract the primary topics discussed by propagandists. Eventually, two topics were selected to be investigated: sports and banking, since they represent the largest percentages of the dataset.

The related keywords were then extracted from these topics using the BERT approach. The final keywords were then refined concerning their keyness properties. Finally, the resulting keywords were used to crawl official users' tweets that discussed the same topics as propagandists' users in the same timeframe.

Exploratory Data Analysis (EDA) was conducted to analyze and discover propagandist users' main characteristics and tweets. It helps to discover data patterns, spot anomalies, and make assumptions. The analysis revealed that propagandists were primarily amplifying content beneficial to their clients, mostly through inauthentic engagement strategies such as retweeting and duplicating content.

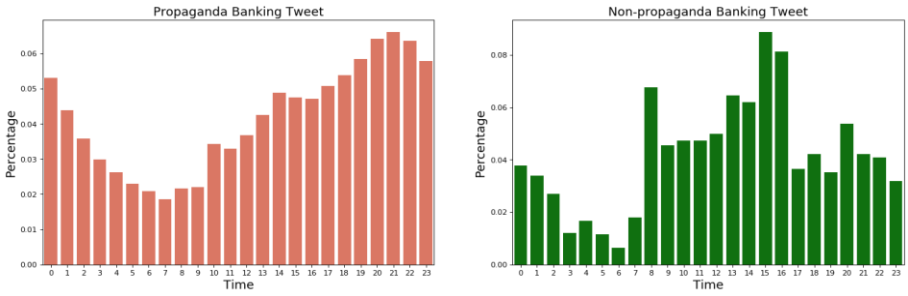


**Fig. 13.** Distributions of posting timespan in banking topic

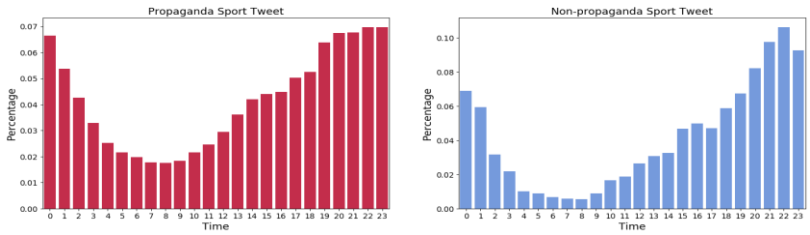


**Fig. 14.** Distributions of posting timespan in sport topic.

This insight supports Pacheco et al.'s [19] finding that propagandists' tweets tend to duplicate and retweet content automatically to ensure that accounts work in a coordinated network to promote an account or story. Since ancient times, repetition has been considered one of the techniques used to spread propaganda, but in the social media era, it is the most widely adopted technique [4].

What made matters worse was engaging many of the automated propagandist accounts to publish a mix of propagandist and non-propagandist content in enormous quantities. Usually, propagandists publish a mix of propaganda and non-propaganda tweets to hide their identities [4]. Using automation to tweet useful content does not violate Twitter's rules.

However, this behaviour was used carefully to conceal the larger platform manipulation perpetrated. This approach makes identifying propagandist tweets in the timelines of accounts that largely share automated, non-propagandist content more challenging.

The analysis was conducted on the user profile and tweet levels for a more in-depth investigation. In general, the analysis revealed some features of propagandist users discovered that are surprisingly different from those reported in other research.

For example, Agarwal et al. [9] found that propagandist posts are usually bracketed within hashtags, which contradicts the results of the analysis of this research. However, these findings prove that the propagandists change their writing style whenever they deploy a new campaign [5]. The analysis at the user level revealed important points. First, propagandists' users are greatly seeking to increase their popularity.

This point has not been investigated widely in previous literature [9]. The analysis revealed that propagandists implant themselves in Twitter communities by following a large segment of Twitter users because those following are expected to return the favour.

Thus, the number of followers can be increased by increasing the number of followers. In the social media era, the influence of a user can be associated with the number of their followers because their tweets reach a wide audience [9].

Second, the age of the account can be considered a feature that may help detect propagandists' users, although it was not widely investigated regarding propaganda detection.

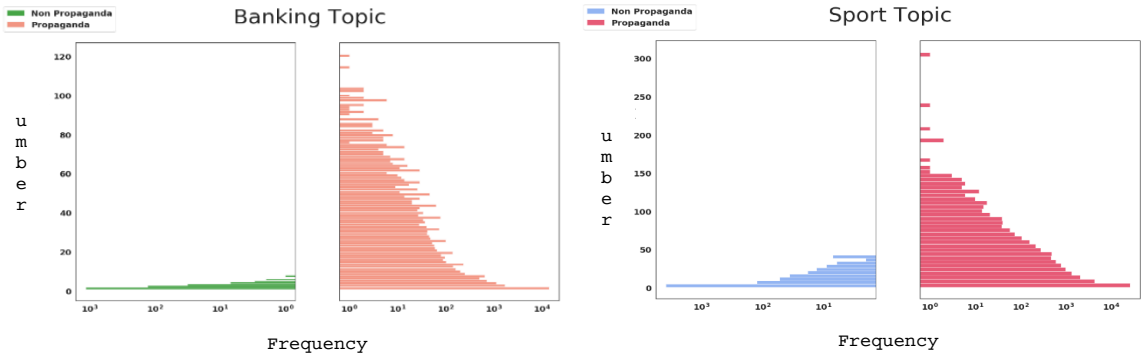


**Fig. 15.** Distributions of posting frequencies

Approximately 40 per cent were created four years before the campaign. Third, unlike propagandists, non-propagandists tend to describe themselves in their profiles with long sentences. Although the results show differences in profile length, we cannot consider him a propagandist user because he describes himself in a short sentence.

Many non-propagandists describe themselves in short sentences. To my knowledge, this feature has not been investigated widely [4]. Fourth, propagandists rely on the artificial amplification of Twitter interactions, including establishing several or overlapping accounts [39].

Regarding the analysis results related to the tweet level, we found thatmost propagandists' tweets are not original compared to non-propagandists' users. Propagandists' users tend to duplicate and retweet content automatically to ensure that accounts work in a coordinated network to promote a story, as stated by Agarwal et al. [9]. Second, propagandists rely on artificial amplification through widespread retweeting while posting little original content.

This result agrees with Guarino et al. [2], who found that the tweets of propagandists are retweets of their brokers. Third, propagandists tend to send a high volume of tweets in a short amount of time. Fourth, contradicting Agarwal et al. [9], the propagandists' users did not bracket their tweets with hashtags like the non-propagandists' users. They also did not embed URLs like the non-propagandist users.

Finally, the timespan is an important indicator for detecting propaganda if the campaign's topic has been considered.

Despite all the efforts, there is still no clear and definitive definition of what a malicious account looks like, which has created conflicting definitions. Unfortunately, research has shown that current technological weapons are used by malicious accounts just like their hunters, which increases their ability to escape detectors. Plus, a lack of real-ground truth allows for further investigation. We know that the data released by Twitter relates to propagandists.

However, at the level of their tweets, they are not classified; they mix propaganda and non-propaganda tweets to hide their identities. It would be very useful for the scientific community to classify propagandists' tweets to close the gap. The severity of this problem calls for special consideration from societies and research communities for a solution to be attained.

## 6 Conclusion

This research is motivated by the scarcity of research on Arab computational propaganda despite the significant increase in Arab social media users. Furthermore, the initial results motivate this research to enhance the previously cited efforts by discovering the features that can help detect Arab computer propaganda. It conducted a deep analysis to determine the propagandists' behavior and characteristics, regardless of their goals and writing style.

The results offer early evidence on social media regarding the propagandists' users and messages. Popularity, originality, topic diversity, publishing volume, and profile age metrics proved to be very informative features for detecting propaganda on Twitter. The oncoming research can combine these features with writing style features to develop a robust hybrid model.

## References

1. **Gil-de-Zúñiga, H., Jung, N., Valenzuela, S., (2012).** Social media use for news and individuals' social capital, civic engagement and political participation. Journal of Computer-Mediated Communication, Vol. 17, No. 3, pp. 319–336. DOI: 10.1111/j.1083-6101.2012.01574.x.
2. **Guarino, S., Trino, N., Celestini, A., Chessa, A., Riotta, G. (2020).** Characterizing networks of propaganda on Twitter: a case study. Applied Network Science, Vol. 5, No. 1, pp. 1–22. DOI: 10.1007/s41109-020-00286-y.
3. **Murphy, B. (2023**). Disinformation and democracy. Foreign Disinformation in America and the US Government's Ethical Obligations to Respond, pp. 25–35. DOI: 10.1007/978-3-031-29904-9_3.
4. **Howard, P., Lin, F., Tuzov, V. (2023).** Computational propaganda: Concepts, methods, and challenges. Communication and the Public, Vol. 8, No. 2, pp. 47–53. DOI: 10.1177/20570473231185996.
5. **Martino, G. D. S., Cresci, S., Barron-Cedeno, A., Yu, S., Di-Pietro, R., Nakov, P. (2020).** A survey on computational propaganda detection. IJCAI International Joint Conference on Artificial Intelligence, pp. 4826–32. DOI: 10.48550/arXiv.2007.08024b.
6. **Ferrara, E., Chang, H., Chen, E., Muric, G. Patel, J., (2020).** Characterizing social media manipulation in the 2020 US presidential election. First Monday, Vol. 25, No. 11. DOI: 10.5210/fm.v25i11.11431.
7. **Alvari, H., Sarkar, S., Shakarian, P. (2019).** Detection of violent extremists in social media. 2019 2nd international conference on data intelligence and security (ICDIS), IEEE, pp. 43–47. DOI: 10.1109/ICDIS.2019.00014.
8. **Chaudhari, D. D., Pawar, A. V. (2022**). A systematic comparison of machine learning and NLP techniques to unveil propaganda in social media. Journal of Information Technology Research (JITR), Vol. 15, No. 1, pp. 1–14. DOI: 10.4018/JITR.299384.
9. **Agarwal, N., Al-khateeb, S., Galeano, R., Goolsby, R. (2017).** A systematic comparison of machine learning and NLP techniques to unveil propaganda in social media. Defence Strategic Communications, Vol. 2, No. 2, pp. 87–112. DOI: 10.30966/2018.riga.2.4.
10. **Weber, D., Neumann, F. (2020).** Who's in the gang' revealing coordinating communities in social media. Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 89–93. DOI: 10.1109/ASONAM49781.2020.9381418.
11. **Khanday, A. M., Khan, Q. R., Rabani, S. T. (2021).** Identifying propaganda from online social networks during COVID-19 using machine learning techniques. International Journal of Information Technology, Vol. 13, No. 1, pp. 115–22. DOI: 10.1007/s41870-020-00550-5.
12. **Da-San-Martino, G., Yu, S., Barrón-Cedeño, A., Petrov, R., Nakov, P. (2019).** Fine-grained analysis of propaganda in news article. Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, pp. 5635–5645. DOI: 10.18653/v1/D19-1565v.
13. **Kumar, S., Cheng, J., Leskovec, J., Subrahmanian, V. S. (2017).** An army of me: sockpuppets in online discussion communities. Proceedings of the 26th International Conference on World Wide Web, pp. 857–866. DOI: 10.1145/3038912.3052677.
14. **Horne, B. D., Adalı, S. (2017).** This just in: fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news. Proceedings of the International AAAI Conference on Web and

Social Media DOI: 10.1609/icwsm.v11 i1.14976.

15. **Abdullah, M., Altiti, O., Obiedat, R. (2022).** Detecting propaganda techniques in english news articles using pre-trained transformers. 13th International Conference on Information and Communication Systems, pp. 301–308. DOI: 10.1109/ICICS55353.2022.9811117.
16. **Rashkin, H., Choi, E., Jang, J. Y., Volkova, S., Choi, Y., Allen, P. G. (2017).** Truth of varying shades: Analyzing language in fake news and political Fact-Checking. 2017 conference on empirical methods in natural language processing. pp. 2931–2937. DOI: 10.18653/v1/D17-1317.
17. **Horne, B. D., Adali, S. (2017)**. This just in: Fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news. Vol. 11, No. 1, pp. 759–766. DOI: 10.18653/v1/D17-1317.
18. **Nerino, V. (2021).** Tricked into supporting: A study on computational propaganda persuasion strategies. Italian Sociological Review, Vol. 11, No. 3. DOI: 10.13136/isr.v11 i4S.438.
19. **Pacheco, D., Flammini, A., Menczer, F. (2020).** Unveiling coordinated groups behind white helmets disinformation. The Web Conference 2020, Companion of the World Wide Web Conference, pp. 611–616. DOI: 10.1145/3366424.3385775.
20. **Darwish, K., Alexandrov, D., Nakov, P., Mejova, Y. (2017).** Seminar users in the arabic twitter sphere. Lecture Notes in Computer Science [Internet], Springer, pp. 91–108. DOI: 10.1007/978-3-319-67217-5_7.
21. **Howard, P., Lin, F., Tuzov, V., (2023).** Computational propaganda: Concepts, methods, and challenges. Communication and the Public, Vol. 8, No. 2, pp. 47–53. DOI: 10.1007/978-3-319-67217-5_7.
22. **Wiard, V. (2019).** News ecology and news ecosystems. Oxford Research Encyclopedia of Communication, DOI: 10.1093/acrefore/978 0190228613.013.847.
23. **Barbas, Á., Trere, E. (2023).** The rise of a new media ecosystem: exploring 15M's educommunicative legacy for radical democracy. Social Movement Studies, Vol. 22, No. 3, pp. 381–401. DOI: 10.1080/14742837. 2022.2070738.
24. **Jarwar, M. A., Abbasi, R. A., Mushtaq, M., Maqbool, O., Aljohani, N. R., Daud, A., Chong, I. (2017).** CommuniMents: A framework for detecting community based sentiments for events. International Journal on Semantic Web and Information Systems, Vol. 13, No. 2, pp. 87–108. DOI: 10.4018/IJSWIS. 2017040106.
25. **Firoozeh, N., Nazarenko, A., Alizon, F., Daille, B. (2020).** Keyword extraction: Issues and methods. Natural Language Engineering [Internet], Vol. 26, No. 3, pp. 259–291. DOI: 10.1017/S1351324919000457.
26. **Giarelis, N., Kanakaris, N., Karacapilidis, N. (2021).** A Comparative assessment of state-of-the-art methods for multilingual unsupervised keyphrase extraction. IFIP Advances in Information and Communication Technology, Springer International Publishing, pp. 635–645. DOI: 10.1017/S1351324919000457.
27. **Vargas-Calderón, V., Dominguez, M. S., Parra-A, N., Vinck-Posada, H., Camargo, J. E. (2020).** Using machine learning techniques for discovering latent topics in twitter colombian news. Communications in Computer and Information Science, pp. 132–141. DOI: 10.1080/10810730.2018.1423648.
28. **Mannor, S., Jin, X., Han, J., Jin, X. (2011).** K-means clustering. Encyclopedia of Machine Learning, pp. 563–564. DOI: 10.1007/978-0-387-30164-8_425.
29. **Lulu, L., Elnagar, A. (2018).** Automatic arabic dialect classification using deep learning models. Procedia Computer Science, Vol. 142, pp. 262–269. DOI: 10.1016/j.procs.2018. 10.489.
30. **Bojanowski, P., Grave, E., Joulin, A., Mikolov, T. (2017).** Enriching word vectors with subword information. Transactions of the Association for Computational Linguistics, Vol. 5, pp. 135–146. DOI: 10.1162/tacl_a_00051.
31. **Newling, J., Fleuret, F. (2016**). Nested mini-batch K-Means. Advances in Neural Information Processing Systems, pp. 1360–1368. DOI: 10.5555/3157096.

**32. Wang, S., Li, H. (2020).** Adaptive K-valued K-means clustering algorithm. Proceedings 2020 5th International Conference on Mechanical, Control and Computer Engineering, pp. 1442–1445. DOI: 10.1109/ICMCCE51767.2020.00316.

**33. Pazos-Rangel, R. A., Florencia-Juarez, R., Paredes-Valverde, M. A., Rivera, G. (2020).** Handbook of research on natural language processing and smart service systems. IGI Global. DOI: 10.4018/978-1-7998-4730-4.

**34. Devlin, J. (2018).** Bert: Pre-training of deep bidirectional transformers for language understanding. DOI: 10.18653/v1/n19-1423.

**35. Pontius, R. G., Millones, M. (2011**). Death to Kappa: birth of quantity disagreement and allocation disagreement for accuracy assessment. International Journal of Remote Sensing, Vol. 32, No. 15, pp. 4407–4429. DOI: 10.1080/01431161.2011.552923.

**36. Rousseau, F., Vazirgiannis, M. (2015).** Main core retention on graph-of-words for single-document keyword extraction. Advances in Information Retrieval, Springer, pp. 382–393. DOI: 10.1007/978-3-319-16354-3_42.

**37. Al-Zoubi, A. M., Alqatawna, J., Faris, H. (2017).** Spam profile detection in social networks based on public features. 2017 8th International Conference on Information and Communication Systems, pp. 130–135. DOI: 10.1109/IACS.2017.7921959.

**38. Pancer, E., Poole, M., (2016).** The popularity and virality of political social media: Hashtags, mentions, and links predict likes and retweets of 2016 US presidential nominees' tweets. Social Influence, Vol. 11, No. 4, pp. 259–270. DOI: 10.1080/15534510.2016.1265582.

**39. Weber, D., Neumann, F. (2021).** Amplifying influence through coordinated behavior in social networks. Social Network Analysis and Mining, Vol. 11, No. 1, pp. 1–42. DOI: 10.1007/s13278-021-00815-2.

**40. Hardalov, M., Arora, A., Nakov, P., Augenstein, I. (2021).** A Survey on stance detection for mis and disinformation identification. Findings of the Association for Computational Linguistics, pp. 1259–1277. DOI: 10.48550/arXiv.2103.00242.

**41. Ilias, L., Roussaki, I. (2021).** Detecting malicious activity in Twitter using deep learning techniques. Applied Soft Computing, Vol. 107, p. 107360. DOI:10.1016/J.ASOC.2021.107360.

**42. Hardalov, M., Arora, A., Nakov, P., Augenstein, I. (2021).** A survey on stance detection for mis- and disinformation identification. Findings of the Association for Computational Linguistics: NAACL 2022 Findings, pp. 1259–1277. DOI: 10.48550/arXiv.2103.00242.

**43. Hayawi, K., Mathew, S., Venugopal, N., Masud, M. M., Ho, P. H. (2022).** DeeProBot: a hybrid deep neural network model for social bot detection based on user profile data. Social Network Analysis and Mining, Vol. 12, No. 1, pp. 1–19. DOI: 10.1007/s13278-022-00869-w.

**44. Farivar, S., Wang, F., Turel, O. (2022).** Followers' problematic engagement with influencers on social media: An attachment theory perspective. Computers in Human Behavior, Vol. 133, p. 107288. DOI: 10.1016/j.chb.2022.107288.

**45. Valencia-Segura, K. M., Escalante, H. J., Villasenor-Pineda, L. (2023).** Automatic depression detection in social networks using multiple user characterizations. Computación y Sistemas, Vol. 27, No. 1, pp. 283–294. DOI: 10.13053/cys-27-1-4540.

*Article received on 25/02/2024; accepted on 15/05/2024.*
**Corresponding author is Bodor Moheel Almotairy.*