Ng and Carley *EPJ Data Science* (2023) 12:63
https://doi.org/10.1140/epjds/s13688-023-00440-3

EPJ Data Science
a SpringerOpen Journal

REGULAR ARTICLE Open Access

Deflating the Chinese balloon: types of Twitter bots in US-China balloon incident

Lynnette Hui Xian Ng[1*] and Kathleen M. Carley[1]

*Correspondence:
lynnetteng@cmu.edu
[1]IDeaS Center for Informed Democracy & Social-CyberSecurity, Carnegie Mellon University, Pittsburgh, Pennsylvania, United States

Abstract

As digitalization increases, countries employ digital diplomacy, harnessing digital resources to project their desired image. Digital diplomacy also encompasses the interactivity of digital platforms, providing a trove of public opinion that diplomatic agents can collect. Social media bots actively participate in political events through influencing political communication and purporting coordinated narratives to influence human behavior. This article provides a methodology towards identifying three types of bots: General Bots, News Bots and Bridging Bots, then further identify these classes of bots on Twitter during a diplomatic incident involving the United States and China. In the balloon incident that occurred in early 2023, where a balloon believed to have originated from China is spotted across the US airspace. Both countries have differing opinions on the function and eventual handling of the balloon. Using a series of computational methods, this article examines the impact of bots on the topics disseminated, the influence and the use of information maneuvers of bots within the social communication network. Among others, our results observe that all three types of bots are present across the two countries; bots geotagged to the US are generally concerned with the balloon location while those geotagged to China discussed topics related to escalating tensions; and perform different extent of positive narrative and network information maneuvers. The broader implications of our work towards policy making is the systematic identification of the type of bot users and their properties across country lines, enabling the evaluation of how automated agents are being deployed to disseminate narratives and the nature of narratives propagated, and therefore reflects the image that the country is being projected as on social media; as well as the perception of political issues by social media users.

Keywords: Twitter; Bots; Digital diplomacy; Bridging; News; Social media

1 Introduction

Digital diplomacy can be understood as the use of digital resources by a country to achieve its foreign policy goals and proactively manage its image and reputation [1]. As the world becomes more digital, there is a growing us of social media platforms by countries as tools of communication with the general public, where nations tailor foreign-policy and nation-branding messages to the digital audience [2]. Digitalized public diplomacy also includes the emphasis on the interactivity of digital platforms [3]. Online political participation by

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

individual users can provide an indication on the perception of political discussions. As individual users share their opinions on global affairs, diplomatic agents can systematically collect these information for campaign analysis [4, 5].

Twitter has become a popular platform for political discussions. Its fluid microblogging structure promotes diversity of opinions and provides a digital platform for messaging campaigns to cross geographical boundaries [6]. Within this digital space, social media bots have been observed to be involved in cross-country relations within the digital space. Bots are loosely defined as inauthentic social media users (i.e., fake user profiles) [7], who are sometimes controlled through software automation to post content or interact with other users [8].

Bots are under scrutiny because past studies have observed that they can be used to alter perceptions of political discourse on social media. Bots associated with Russia have been observed to have employed tactics to sow discord and support specific candidates during the 2016 US Presidential elections [9], which may have contributed towards the perception of American citizens towards the candidates. This is especially of concern if the bots participate in diplomacy, which is the art of "influencing the decisions and behavior of foreign governments and peoples through dialogue", according to Encyclopedia Britannica [10]. In the 2022 Russia-Ukraine war, bots were deployed by both countries on Twitter to shape support for the war. Ukrainian bots overwhelmed the conversation in tweet quantity, but Russian bots had more effective communication manufacturing conflict [11, 12]. Russia bots took part in extensive agenda building activities during the 2016 US elections, showcasing how these automated accounts can be used not only to brand messages for domestic audiences but also for foreign audiences [9]. While these accounts are inauthentic, not all these accounts were fully controlled by software: the Russian Internet Research Agency conducted their work with a mixture of bots and real people employed in a St. Petersburg "troll factory" operated by a large group of human operators [13]. China, similarly, maintains many inauthentic accounts through the 50-Cent Party, the Chinese government's campaign to shape global narratives [14]. The commonality of these accounts in general is that they are inauthentic users and generate a large volume of mostly political tweets, flooding the social media information system.

The United States (US) and China are two major powers on the world stage and have been locked in periods of high tensions. One observation of digital diplomacy between the two countries occurred in 2021, where the US released information on the tracing of the origins of COVID-19, Chinese diplomatic Twitter accounts asserted support for scientific tracing and opposed the politicization of the tracing [15]. Anti-Chinese state political views were discovered on microblogging platforms Twitter and Weibo over the 2017 Spring Festival period. These narratives also include pro-Hong Kong and pro-Uyghurs independence themes, suggesting algorithmic manipulation to boost democratic ideals [16].

One cross-country diplomatic incident between the US and China arose in early 2023. In January 2023, a balloon was spotted floating around in American airspace. US officials quickly determined that it was a high-altitude surveillance balloon originating from China. The balloon was estimated to be flying as high as 60,000 feet above ground, which puts it at about ten times closer than the lowest Earth-orbiting satellites [17]. China asserted that the balloon was merely a weather balloon. The US tried to open lines of communication with Chinese President Xi Jinping, and China expressed its dissatisfaction with the accusation of surveillance [18]. Both countries maintained strong stances with regards to the functionality of the balloon. The balloon was eventually shot down by a US F-22 Raptor fighter jet on February 4, 2023. Online, this balloon incident drew much attention which inspired discussions and memes of fear, anger and humor [19].

This study seeks to study the online political participation during the balloon diplomatic incident between US and China. It measures the inauthentic online engagement aspect of digital diplomacy through analyzing the scope of bot activity on social media. It does so by examining three different types of bots: `General Bots` that are identified by generic bot detection algorithms, `News Bots` that play a key role in providing automated updates to news stories; and `Bridging Bots` connect communities with each other. Briefly, users that are identified as bots through a bot detection algorithm are extracted out. `News Bots` are identified through containing the word "news" in their profile, or having 90% of their tweets classified as news headlines through a machine learning classifier. `Bridging Bots` are identified through their position in a all-communication social network, where they are the bots that straddle between two algorithmically determined Louvain clusters. `General Bots` are bots that are not identified as any of the other two bot types.

This analysis of bots provides insights to inauthentic and automated activity during a diplomatic event that may influence political perceptions of human users. While bots used in digital campaigns are not a new phenomenon, the examination of the social roles that bots play online within a diplomatic incident have not been fully studied. In this work we examine the social roles of different types of bots per region in the Chinese balloon diplomatic incident to provide insights towards the country's portrayal and social media sentiment in the US-China relationship.

1.1 Contributions

Through combining social network analysis, topical analysis and sentiment analysis, we form a picture of the position and perspectives of these automated accounts. Specifically, the contributions of our paper are three-fold:

1. We study a subset of digitalized public diplomacy through the analysis of inauthentic online engagement during a diplomatic incident involving two major world powers.
2. We define and develop methodologies to identify three key types of Twitter bots: General Bots, News Bots and Bridging Bots.
3. With these techniques, we analyze the presence of the three types of bots within a discussion of an event that involved two countries, the Balloon incident between US and China. We do so by analyzing the topic, network and information maneuver techniques of the different types of bots, separated by their self-declared geographic locations.

From this investigation of digital diplomacy on Twitter, our results show that the three types of bots (General Bots, News Bots and Bridging Bots) are consistently present throughout the three geographies (US, China, Rest of the World). The communication network formed by users depict that users from the US and China naturally form separate clusters. Bots geotagged to US are generally concerned with the location of the balloon and the possible surveillance functionality, while bots geotagged to China discussed topics on war and escalation. `General Bots` and `News Bots` are dispersed throughout the network, while `Bridging Bots` are rarer and typically connect between users of both countries. `General Bots` and `News Bots` geotagged to China have the highest average eigenvector and centrality values, indicating that they are more well-connected within the social network compared to the US-geotagged bots, thus having a higher amount of influence. In terms of information maneuvers through the BEND framework, we observe that `General Bots` and `Bridging Bots` make use of emotional appeal rather than logical appeal, and `News Bots` often make their news headlines short and catchy to excite readership.

2 Related work

2.1 Digital diplomacy on social media

The US and China have had a prolonged period of diplomatic tensions in both offline and online world. Since 1949, both countries have had periods of cooperation, competition and tensions in issues related to military, technology, trade, climate change and views on governance (e.g., independence of Taiwan, activism within China) [20].

In today's information age, international politics also hinges on how each country presents the dispute in both traditional and digital media, and how the public reacts to their stories. Both the United States and China have used Twitter as a medium to present their agendas during the South China Sea dispute [21]. Strategic narratives were also dispersed on Twitter by the Chinese authorities during the 2020 COVID-19 pandemic to frame the government response to the pandemic as a proof of the country's strength and resilience [22]. Public responses to politics can also be measured through Twitter discourse, for example the examination of emotional tendency of online users towards the presence of US warships in the South China Sea [23].

The balloon incident comes at a critical moment in US-China relations. Representatives from both countries have met in late 2022 to agree to deepen bilateral relations. They had planned to meet again in January 2023, but the meeting was canceled due to the balloon incident [19]. The increased tensions during the balloon incident is not due to the surveillance functionality of the balloon, but rather, is emblematic of the rising tensions between the two countries over time [19]. The presence of surveillance by China indicates her desire to collect information on its geopolitical rival amid the frayed diplomatic relations.

Chinese government messaging has always leaned towards nation-building and regime legitimacy. The Chinese Communist Party (CCP) has employed the use of emotions such as fear, rage and pride to exert an influence on contemporary Chinese politics [24]. Studies have observed that the younger Chinese generation embody a nationalistic sentiment as a result of being surrounded by Chinese nationalism emotions seeded in official Chinese propaganda online [25].

For the United States, information cyber operations encompasses, among others, the art of spreading propaganda and information to change human behavior [26]. Past work have observed that routine US government videos generally revolve around social issues such as of law enforcement, social issues, transportation, economic development and political issues [27]. Recruitment-intended publicity videos identify with professional and fitness careers such as students, doctors and athletes [28]. While Chinese government messaging aims at enhancing the viewer's love for the country, US government messaging aims to address social issues.

In terms of analyzing differences of the discussions users engage in through patterns of online firestorms between the United States Twitter and China Weibo, past work observed that firestorms in both platforms have significant cultural differences. Users from the two regions US and China engage on social media platforms with different communication behaviors. China Weibo tend to target the social responsibility or ethics-related dimensions, while those in US Twitter target reputation and ability [29].

2.2 Social media bots

Social media bots, which are inauthentic or automated-like accounts, have been observed to participate in political discussions. Evidence of social media bots attempting to manipulate political communication dates back to as early as 2010: in the 2010 US midterms elections, bots were employed to support and discredit candidates by injecting thousands of Tweets pointing to websites with fake news [30]. Similarly, in the 2016 US Presidential campaign, there are two faction of bots supporting both presidential candidates, which run both supportive campaigns for the candidate they affiliate with, and smear campaigns for the opposition candidate. These bots are centrally embedded within the social network, giving them a huge amount of influence [30]. During the same elections, bots originating from Russia actively sowed discord in a complex multi-platform disinformation campaign, purchasing advertisements to promote their political ideals and disseminating curated news content [31].

Bots that seek to purport coordinated narratives to influence human behavior are more prevalent in politics rather than other realms like art and sports [32]. Groups of bots working together have been observed to change the stances of human users online [33, 34]. This is an area of note because changes in a person's stance can be detrimental to society if the person has been convinced to do public harm. These have led to increase coverage and research on the impact of social media bots on the political scene.

Social media bots have been observed to perform information maneuvers. Governments like those of Iran and China are using social media automation to disseminate propaganda and provide digital entertainment to their population [35]. Russian bots have been identified to pretend to be English speakers and exhibit hostile attitudes towards political opponents and Western democracies, using persuasive information maneuvers to express skepticism and promote a lack of trust in the existing governments [36].

To identify whether an account is a bot or human, a series of bot detection algorithms have been developed in literature. These algorithms evaluates the features of social media accounts (e.g., user name, account metrics) and returns a likelihood between 0 and 1 representing whether the account is likely to be a bot or human [37]. Bot detection algorithms are generally machine learning algorithms that train on manually annotated datasets that indicate bot/human labels for data points. These algorithms range from random forests classifiers [38] to neural network formulations [39] to deep learning architectures [40].

The training datasets of these bot detection algorithms consists of a wide variety of bot types from different countries. These algorithms are constructed as generic algorithms that can be trained and applied across multiple datasets with reasonable accuracy. For example, a random forest classification model has had an average performance of 0.72% accuracy of across 11 datasets [41], and neural network-based models constructed on a large proportion of Twitter datasets can also be applied on Reddit datasets with 69.77% accuracy [39]. Therefore, in this paper, we make use of a pre-trained Twitter bot detection algorithm, BotHunter [42], that should be generalizable across the training dataset and the political discourse of our dataset.

3 Data

3.1 Data collection from Twitter

We tracked the political discourse of the Chinese balloon on Twitter. Using a Python script, we collected tweets using the Twitter V1 Streaming API. We streamed tweets containing the search terms #chineseballoon and #weatherballoon from 31 Jan 2023 to 22 Feb 2023. From our streamed tweets, we filtered for tweets only in the English language. In total, we collected 1,192,445 tweets from 121,048 unique users.

3.2 Geographic location identification

We aim to separate the accounts into the two major powers involved in this incident: United States (US) and China, by using information disclosed by the user account. We do this through geographic location identification techniques.

Mapping the geographic location of Twitter users have been a studied topic. Since late 2009, Twitter allowed users to include geographic location as metadata to their profile. This metadata can be included in terms of latitude/longitude coordinates or by place name (georeferenced tweets). The problem with georeferenced location, which are location expressed in text form like "New York City", is that it is prone to duplicates and ambiguity. Geocoding algorithms thus identify location from the surrounding texts (e.g. "Chinatown, New York City" identifies a specific Chinatown through the city name), disambiguates it and converts it to its approximate map coordinates [43]. The disambiguation step involves methods such as text mapping to the Wikipedia gazetteer or a global city gazetteer [43]; or estimation of a user's location based on the content of their tweets, a method that assumes users in similar regions will tweet similar trending topics [44].

For each user account, we assign a geolocation based on their disclosed location. To do so, we extract the "country" field from the account's meta-data and perform a reverse geolocation search using Nominatim API 4.2.1.[1] We input location information from the account's metadata (i.e., latitude/ longitude, location string) to the API call. The API returns a JSON object containing location information, such as state and city, and we extract the country term from this information output. For example, if the account declared its location as "San Francisco, California", and the Nominatim search result returns "United States", we indicate the account to be from the country United States. Similarly, an account with the declared location "Beijing" with the returned Nominatim result "China" will be geotagged as from China. For accounts with locations other than US and China, we classify them into accounts from the "Rest of the World". Accounts where the geolocation is not disclosed or that the Nominatim API does not return a result are disregarded in our subsequent downstream analysis.

Despite the use of geographic location identification, we cannot definitively claim the users originate from these countries. Twitter, as well as other social media sites like Google, Facebook, WhatsApp and YouTube, are banned by China's "Great Firewall". Many users access the application through circumventing the blockage with VPN services [45]. In this study, we do not make a distinction of whether the users are definitely from China or are spoofing their location to be from China. Rather, we focus on the users that participate in the online discourse and present themselves to be from China, and also those that present themselves to be from the US. The external self-presentation of location by

[1] https://nominatim.org.

Twitter users provide an illusion of the activity from the region on the social media space which we use that in our analyses.

4 Methodology

4.1 Overview

In this study, we define and identify three types of bots – `General Bots`, `News Bots` and `Bridging Bots`– in the Twitter discussion surrounding the US-China balloon incident. We use a mixture of machine learning and network analysis methods to segregate these bot accounts from the general pool of accounts. Following the identification of three types of bots, we analyze their activity in terms of their influence in the social network, the narrative themes they put forth and their expressed emotions. We compare these parameters towards Human users, characterizing the differences in the online opinions and discussions between Bots and Humans during this cross-country incident.

For deeper analysis of bot activity within this balloon incident, we used three parameterizations: social network analysis, topical analysis and sentiment analysis.

4.2 Identifying types of bots

In this study, we identify three types of bots:

1. `General Bots`: bot accounts that are identified using generic bot detection algorithms
2. `News Bots`: bot accounts that spread news information, whether through posting original news or by aggregating news accounts
3. `Bridging Bots`: bot accounts that build a communication pathway between two clusters of users

In the following subsections, we describe our methodology for identifying these types of bots in detail. We note that the classification of an agent into a bot is non-exclusive. For example, a bot user can be both a `bridging bot` and a `news bot`. However, for the purposes of this study, if a user is classified as a `news` or `bridging bot`, we do not consider it to be a `general bot`. This construction allows us to perform more segregated analyses towards each bot type. The overview of the identification of the three types of bots are Fig. 1.

4.2.1 General bots

Bot detection algorithms (see Sect. 2.2) are constructed to be generic models and be able to identify a broad range of Twitter bots. As such, we term the bots that are identified through these bot detection algorithms as `General Bots`.

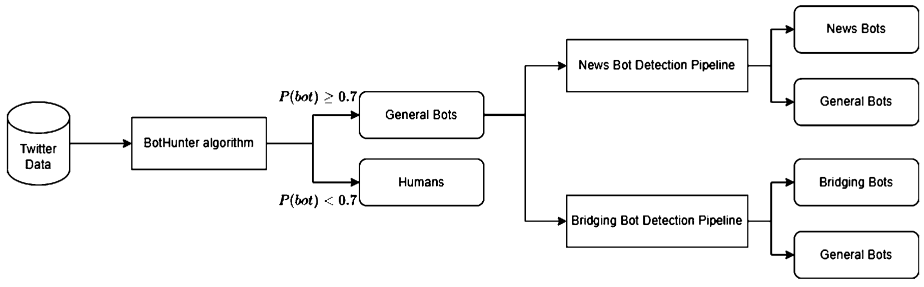

Figure 1 Overview of Methodology for Identifying Types of Bots

In this study, we identified General Bots using the BotHunter algorithm [42]. This algorithm uses a tier-based random forest structure to return the probability of the account being a bot. The algorithm uses an account's tweet text information, temporal patterns of tweeting, and user profile information to determine whether the account is a bot or human. The classifier performed with ∼98% accuracy on the original dataset it was constructed on [42]. This classifier has since been used in studies that studied bots conversations on diplomatic incidents between countries, such as China and Taiwan [46], and Russia and Ukraine [47].

We ran all user data through the BotHunter algorithm, retrieving the bot probability scores for each user. The scores were in the range of 0 and 1. After retrieving the bot likelihood score for each user, one typically sets a threshold value, above which the user is deemed as a bot, while below which it is deemed as a human. In literature, a variety of threshold values have been set, ranging from 0.25 [48] to 0.50 [49] to 0.76 [50]. We adopted the 0.70 value to threshold the likelihood score for marking social media bots to be in consistent with some past work that have used the same algorithm [5, 33]: a user with a score above or equal to 0.70 is deemed as a bot and an account below that value is deemed as a human [37]. We denote the likelihood score as P(bot). The BotHunter algorithm also allows us to process historical data that has already been collected rather than requiring live access. In this article, we also refer to the general bot as a bot.

4.2.2 News bots

News Bots are bots that spread news information. These bots can either be posting original news, from which news originate from; or aggregating news from a series of other original news websites or users. We identify News Bots in two manners: through substring matching and via a machine learning classifier. Figure 2 presents a flowchart of the methodology used to determine if an account is a news bot.

The first manner relies on the explicit expression of a news bot from the user's profile information. From the set of General Bots, we extract the bots that contain the word "news" in their profile (i.e., user name, screen name, description) through regex substring matching in Python. These bots are then reclassified as News Bots.

The second way of identifying news bots deals with the accounts that do not explicitly state the word "news" in their profile but tweet news headlines. To identify these bots, we trained a random forest machine learning classifier. To do so, we obtained 100,000 examples of news headlines used between 1 January 2010 to 31 January 2020 from the News on the Web corpus [51]. We enhanced the news dataset with a non-news dataset

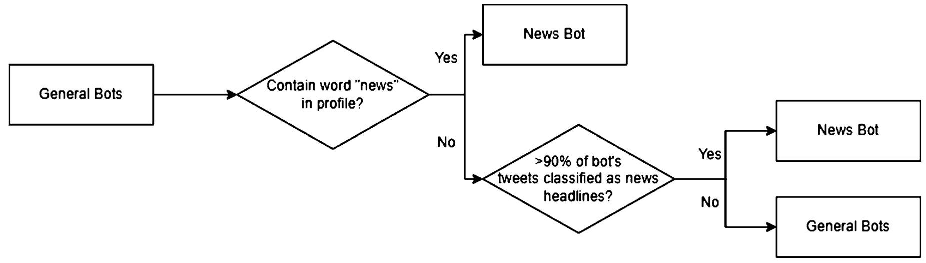
General Bots
Contain word "news" in profile?
Yes
No
News Bot
>90% of bot's tweets classified as news headlines?
Yes
No
News Bot
General Bots

Figure 2 Methodology for identification of News Bots

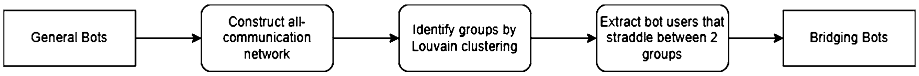
General Bots
Construct all-communication network
Identify groups by Louvain clustering
Extract bot users that straddle between 2 groups
Bridging Bots

Figure 3 Methodology for identification of `Bridging Bots`

of 100,000 tweets from human users obtained from 3298 users that includes ourselves, friends within our social network, politicians and celebrities. This classifier was implemented using the scikit-learn package in Python.[2] This binary classifier takes in a sentence and returns whether the sentence is likely to be a news headline or not. The classifier achieved a 92.3% accuracy. A positive classification of a tweet by this binary classifier indicates that the tweet is likely to be a news headline. By extension, if a majority of a user's tweets are news headlines, the user is likely to be a `news bot`. In this study, we use a 90% threshold: if a classifier reflects that 90% of a user's tweets are similar to news headlines, then we reclassify the user as a `news bot`. We use the threshold 90% to match the accuracy of the classifier. Then, for each bot user that has not been reclassified as a `news bot`, we run their tweets through the classifier and extract the users that are `news bots`.

4.2.3 Bridging bots

`Bridging Bots` build a pathway through two different groups. In this context, the two key groups are: (1) the group of users that are geolocated in the US and (2) the group that are geolocated in China. Figure 3 illustrates the process of identifying `Bridging Bots` in a flowchart.

We identify `Bridging Bots` in the following manner: first, we construct an all-communication social network between all the users in the dataset. In this network, the nodes represent Twitter users. Two nodes are joined together by a link if the two users have a communication relationship; that is, a retweet, @mention, quote tweet or reply tweet. Then, we perform the Louvain clustering algorithm on the constructed network to identify groups of users. From the outcome of the clustering, we identify the bot users that straddle between two clusters, and reclassify these bots from `general bots` to `bridging bots`.

4.3 Analyzing Twitter bot activity

After classifying Twitter users as each type of bot, we analyze the activities that these bot types take part in on social media, and compare them with respect to the human users. Using a combination of computational tools, we measured the influence and emotions of the bots, as well as the themes of the narratives they are disseminating.

In this section, we describe our methodology towards analyzing the political participation of inauthentic accounts on Twitter. The Twitter bot activity is profiled through network, topic and information maneuver analysis. We measure the difference in social network influence between bot types using network centrality measure analysis, visualize the difference and similarities of the texts put forth using topic analysis and quantitatively measure the extent of information maneuver using the BEND framework analysis [52].

[2] https://scikit-learn.org/stable/.

4.3.1 Measuring influence through social network analysis

Social network analysis provides a way to measure the influence of accounts through their positions in an interaction network. This analysis can provide insights to how well-connected and deeply embedded within a social network. Past studies revolving around political discourse on Twitter have observed that as the size of the communities increase, bots become more central in the rebroadcasting network, thus having a higher ability to perform influence activities [30]. Within the discourse surrounding the Russia-Ukraine war, Russian propaganda troll bots are found to actively spread pro-Russian and anti-Ukraine narratives in their Russian tweets, shaping their reasons for the war towards the Russian citizens [47]. The Russian bots were also found to be central to the communication network and thus have influence over the narrative.

Network analysis techniques capture the social dynamics of communities, quantifying the influence of a node through its interactions and analyzing the connection social ties of nodes [53]. These techniques have been used to capture friendship relations, country trade networks and power dynamics between mafias and great families in the Florentine era [54].

To begin, we construct an all-communication network, a network graph of social media users that represent communication between the users. Each users is regarded as a node in the network graph, and a link is drawn between two nodes if they have a communication interaction, i.e., quoted, retweeted, replied-to or @mentioned each other's tweets. The weight of the links represent the number of interactions between the two users. The graph is then pruned to remove node components with less than five nodes and links that have less than ten interactions, so that we can analyze the core structure of the network. With the assumption that similar people form cohesive structures, we use the structure of this all-communication network to identify key groups and measure the influence of the groups within the networks.

We present the results in a network graph visualization using the Gephi software [55], coloring the graphs by different segregations: by country (US, China, Others); by bot class (bot, human), by bot type (news bot, not news bot, bridging bot, not bridging bot).

From the network graphs, we calculated the average of the betweenness, eigenvector and total-degree centrality metrics between each bot class. The betweenness centrality indicates the influence the user has over information flow within the network. The eigenvector centrality indicates how well connected the user is to other highly influential users. The total-degree centrality indicates the extent of the network that can be affected by the user due to their direct connections with the user. These metrics provide quantitative insight towards the degree of influence of the users within the communication network.

4.3.2 Measuring themes through topic analysis

Understanding narrative themes in groups of texts is typically done through topic analysis. Topic analysis is a pivotal way to group the large volume of information being disseminated on social media platforms into common themes. This method has been employed to distill out the degree of support and sympathy shown by other countries towards Palestine on Twitter in the 2016 Palestinian-Israeli conflict [56]. A common method for topic analysis is Latent Dirichlet Allocation, which constructs a probabilistic model of words, sentences and therefore topics. An analysis of the Twitter discourse during the 2014–2015 crisis between Russia and Ukraine where grenades were found in Kyiv, Ukraine, identified that

that deleted accounts (which are most possibly bots) shared topics related to requiring accountability from Ukraine and the accusation of intimidation by Ukraine [57]. A study on the bots in the 2020 Coronavirus pandemic used topic modeling and observed that bots mainly updated news on the pandemic and promoted good hygiene habits [58].

In our topic analysis module, we first preprocess the tweet texts by removing tweet artifacts and stop words. Tweet artifacts are hashtags, URLs and @mentions that users use as part of their interaction towards others within the network. Stop words are common words like "a", "the", "of", and also common event-specific phrases like "united states" and "china". These sets of text are removed from the tweet as they do not contribute to the overall narrative of the tweet and induce noise.

Following which, we used sklearn CountVectorizer function[3] to convert the collection of tweet texts from each region into a matrix of counts that represent the frequency of tokenized words. Then, we construct word clouds to visually aid interpretation of the top 500 words. The larger the size of the word, the more frequent it is used within the text collection. Using the word cloud display, we can interpret the prevailing narratives that are expressed by each group of social media accounts. We opted to use a word cloud built on singular words as after the preprocessing step, the number of words within each tweet are quite little. Tweets are by nature short texts generated through microblogging, and have a maximum of 280 characters. The average text length after the preprocessing step is 6.3 ± 10.6 words.

4.3.3 Measuring information maneuvers through the BEND framework

Information maneuvers on social media are the strategies used in the manipulation of the diffusion of information to steer mass thinking [59]. Several frameworks that have been conceptualized to characterize information maneuvers on social media space. The BEND framework measures narrative and network maneuvers [52], the SCOTCH framework provides a summary of the contribution of social media actions towards the overall campaign [60]; and the ABCD framework describes in detail the Actors, Behaviors, Content and Distribution in an information maneuver [61].

In this study, we make use of the BEND framework. The BEND framework presents online campaigns as sets of narrative and network maneuvers carried out by users engaging in the social network environment, with the intent of influencing the topic-oriented communities [52]. This framework has been applied in understanding the influence of bot users in expressing political opinions regarding the Palestine-Israel conflict [62], and the Russian portrayal of one of its opposition leader [36].

We use this framework because it has a quantitative output for empirical comparison and analysis, thereby giving a repeatable output rather than a subjective classification. We generate probabilities of each type of bot performing the maneuvers using the ORA software.[4] This software takes in a Twitter output file and provides empirical probabilities of the BEND cues through a weighted average of the linguistic cues derived from the text of the tweets for the narrative maneuvers, and the network cues derived from a user's surrounding all-communication network.

[3] https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.CountVectorizer.html.

[4] http://www.casos.cs.cmu.edu/projects/ora/software.php.

Within this study, we focus on the positive maneuvers only, because diplomacy are generally image-enhancing endeavors [63]. Nations typically attempt to portray a good image towards the world [64], or soften their brand name (i.e., Israel's foreign ministry) [2]. Therefore, positive maneuvers are more prominent in the analysis. Positive maneuvers refer to the information maneuvers that are concerned with increasing narrative support and enlarging network groups. This does not necessarily point to good or bad implications of the text in the post, but rather it is a positive maneuver to the user in focus, expanding its reach and information dissemination patterns. In the BEND terminology, the positive maneuvers are the B- and E-maneuvers. The probabilities returned by the positive B- and E-maneuvers are non-negligible while those returned by the negative N- and D-maneuvers are near-zero. In our analysis, we use the mean and standard deviation scores for each maneuver of the bot users and present the result per bot type and country.

The B-maneuvers are four positive maneuvers towards the social network: Back, Build, Boost and Bridge. These maneuvers are concerned with enhancing the connections of the user among the social community. The Back maneuver supports a narrative through increasing the number of likes, shares or @mention/reference. The Build maneuver works towards creating a group by measuring the extensiveness of co-mentioning. The Bridge maneuver introduces members of one group to another through @mentions, or shares hashtags between groups. The Boost maneuver aims to increase the group size through building links between members.

The E-maneuvers are four positive maneuvers towards the narrative: Engage, Explain, Excite and Enhance. These maneuvers are concerned with increasing the attention drawn towards a message within the social network. The Engage maneuver creates a personal affinity through the audience and a message by using lots of first-person pronouns. The Explain maneuver elaborates on a narrative through justification, using lots of function words and connectives. The Excite maneuver elicits positive emotions such as joy, excitement or pride using words affiliated with these emotions, positive emojis/emoticons and exclamation points. The Enhance maneuver expands on a narrative, through replying and quoting a tweet and adding supportive content such as text, images, URLs and so forth.

5 Results

Within our study, we find that there are highest proportion of users geotagged to be from China that are bots, followed by the Rest of the World then the United States. These proportions are illustrated in Fig. 4. In particular, for users that are geotagged as in the United States, 35.24% (N = 26,439) are identified as bots, while 64.76% (N = 48,597) are humans. For users geotagged within China, there are 64.02% (N = 5328) bots and 35.98% (N = 2995) humans. As for the proportions on the Rest of the World, 42.45% (N = 15,998) are bots while 57.55% (N = 21,691) are humans. These numbers are higher than the estimated average percentage of bots on Twitter around the world. Past studies shown that on average, 5-14% of the Twitter users are bot accounts, and in particular, the number of bots geotagged to the US at 14.26% [65].

The distribution of the types of bots within different regions is illustrated in Fig. 4. Table 1 extends this illustration by providing example tweets of each bot type. `General Bots` are the most dominant types of bots from all three regions, then `News Bots`, then `Bridging Bots`. For United States, 38.39% (N = 23,992) are General Bots, followed by 2.79% (N = 2095) of `News Bots` and 0.47% (N = 352) of `Bridging Bots`. For China,

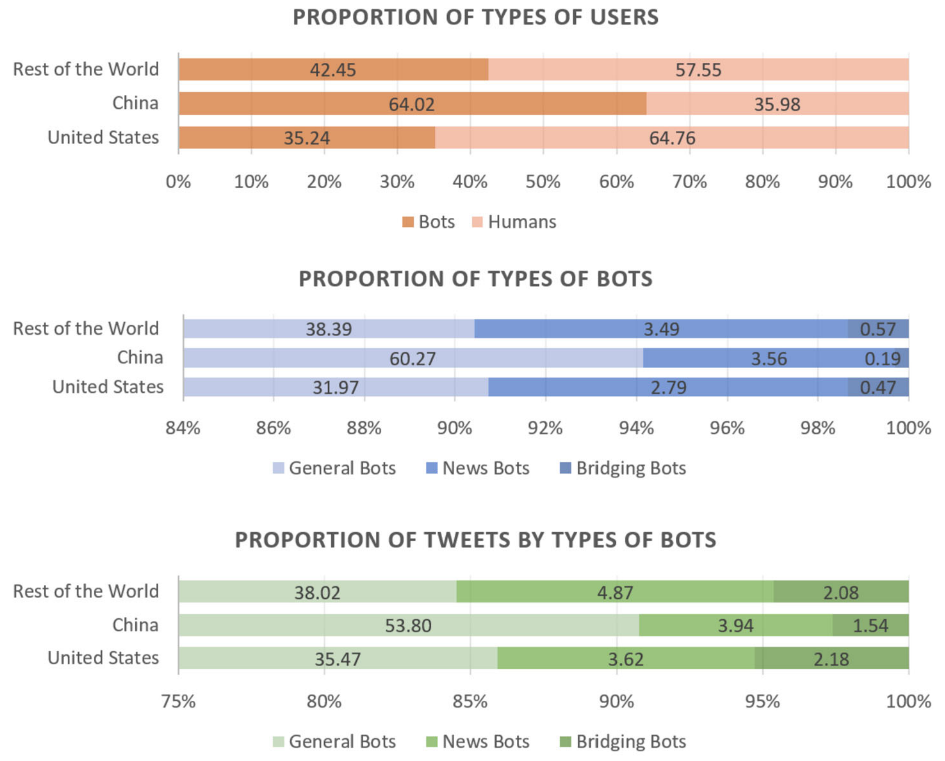

Figure 4 Proportion of User Types

60.27% (N = 5016) are `General Bots`, followed by 3.56% (N = 296) of News Bots and 0.19% (N = 352) of `Bridging Bots`. For the Rest of the World, 31.97% (N = 14,468) are `General Bots`, followed by 3.49% (N = 1316) of `News Bots` and 0.57% (N = 214) of `Bridging Bots`.

The proportion of tweets by types of bots is reflected in the graph in Fig. 4. The number of tweets generated by each type of bot is proportional to the number of the type of bot present. For United States, `General Bots` produced 35.47% (N = 41,750) of the tweets, `News Bots` produced 3.62% (N = 4265), and `Bridging Bots` produced 0.57% (N = 2570) of the tweets. For China, `General Bots` produced 53.80% (N = 5842) tweets, `News Bots` produced 3.95% (N = 428) tweets, and `Bridging Bots` produced 1.54% (N = 2570) tweets. For the Rest of the World, `General Bots` produced 38.02% (N = 20,976) tweets, `News Bots` produced 4.87% (N = 2689) tweets and `Bridging Bots` produced 2.08% (N = 2570) tweets.

Through Fig. 4, we observe that the proportion of bots is the highest in users geotagged to China, providing a glimpse into the larger amount of automation and inauthentic accounts that China-affiliated groups use as compared to US-affiliated or the rest of the world. This might reflect the extent and prolific activity of Chinese affiliated accounts targeting political issues on social media [66, 67]. In addition, `General Bots` make up the largest proportion of bots, indicating that much of these bots do not have a specific information type to disseminate (i.e., news), or do not actively disseminate information to multiple groups (i.e., `Bridging Bots`).

The significant proportion of bot accounts geotagged to the US indicates that the US also establishes portrayals of itself on social media accounts, using their digital diplomacy

Table 1 Examples of Tweets by Bot Types. User names and URLs are removed as these can potentially uniquely identify the users

Bot Type	Example Tweet
Bot	[Rest of the World] I'm bored why can't we have some real life alien invasion #SpyBalloon #ChinaSpyBalloon #AlienInvasion #BBCNews #BBCNewsTen [United States] #ChineseBalloon saga causing political damage already... It's a weather balloon, so #China said [...] (URL) [United States] @(User) I'm not 100% if authentic, but it seems that is a meteorite that came down and may had produced that explosion you heard... Unless is a fake video. But it has nothing to do with the #ChineseBalloon
News Bot	[China] #USA #China #14February [...] One could speculate that the US is using the #ChineseSpyBalloon 'excuse' to escalate tensions with #Beijing.. Recall that US airspace is highly controlled and that there are more accurate satellite technologies for spying (URL) [United States] #USA #China #14February @(NewsUser) - The #Biden administration has blocked the sale of certain US technologies to various Chinese companies - This follows the #ChineseSpyBalloon events - In particular 5 companies allegedly supported programmes for these blimps [...] [Rest of the World] #USA is under attack @(User). Modern wars not fought just using missiles or bombs. #ChineseSpyBalloon #ChinaBalloon #Balloon could be act of Cyber war, #Bioweapon, EMP or surveillance of nuclear installations. The world is watching how president #Biden handle #china firmly on this
Bridging Bot	[United States] @(User): Should have been shot down over Alaska. It's always about the politics. #Biden #ChineseSpyBalloon [Rest of the World] @(User1): Enjoyed joining @(User2) to discuss the #ChineseSpyBalloon [Rest of the World] Balloons have been used in warfare going back 200+ years and you're telling me the most advanced and expensive military the world has ever seen has no way to safely take out a large gently floating bag of air? @(User1) @(User2)

strategies [2]. Digital diplomacy by the two mega-powers is crucial especially in a political event such as this balloon incident for people's perceptions of nations are often shaped by personal encounters, especially on social media channels [2].

Figure 5 depicts the distribution of user types within the all-communication social network. Users of the two key regions - US and China - are generally segregated into different clusters, indicating that they generally interact with users that are of a similar country affiliation. This demonstrates the principle of homophily, where similarity breeds connection [68]. Users within each geographical cluster have an affinity to each other by means of their affiliated geolocation. Network ties of many types – marriage, friendship, work, information transfer, and so forth – have been observed to be homogeneous with regard to sociodemographic characteristics. Community ties that are constructed through homophily in social networks have been a source of interest, and studied for their use in network segregation [69].

`News Bots` are dispersed throughout the network, demonstrating their activity of dispensing news to a variety of user types in social media space. Given that they typically post informative news tweets, many different user types will interact with their tweets, thus they form connections throughout the network.

`Bridging Bots` are rarer throughout the network. The two distinct Louvain communities arising from this network are users from the US and users from China, respectively. Thus, `Bridging Bots` are found straddling connections between the two countries. A total of 592 accounts are identified. Such social media users are rare because they contradict the principle of homophily within the digital space, deliberately forming strong connections between multiple digital communities. The principle of homophily refers to the tendency of similar-minded people interacting with social groups of other similar-minded people and remaining in the community [70]. `Bridging Bots`, however, do

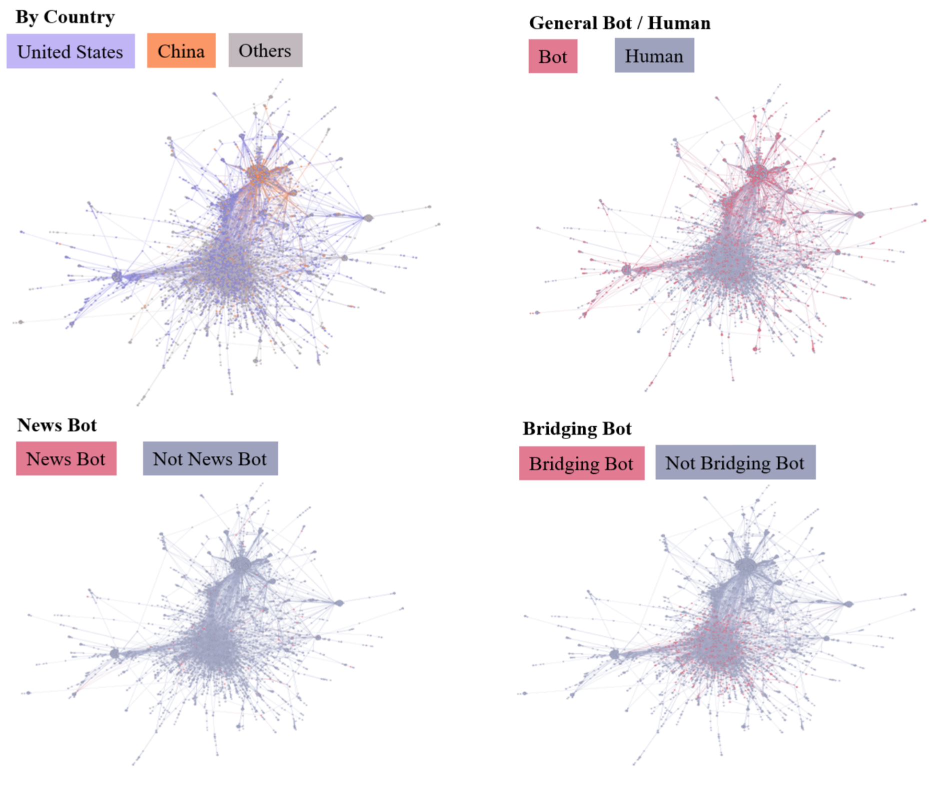

Figure 5 User Type Distribution through Social Network Analysis

Table 2 Average Network Metrics of User Types

	United States	China	Rest of the World
General Bots			
Eigenvector centrality	4.32e–3 ± 9.47e–3	6.84e–3 ± 1.55e–2	3.38e-3 ± 8.05e–3
Betweenness centrality	1.20e–7 ± 2.58e–6	2.31e–9 ± 2.03e–8	1.66e-9 ± 1.98e–8
Total degree centrality	2.45e–6 ± 8.75e–6	2.62e–6 ± 5.25e–6	2.05e-6 ± 4.14e–6
News Bots			
Eigenvector centrality	1.04e–3 ± 2.78e–3	6.63e–3 ± 6.86e–3	8.02e-4 ± 2.63e–3
Betweenness centrality	9.18e–9 ± 4.92e–8	0 ± 0	8.32e-9 ± 3.63e–8
Total degree centrality	4.27e–6 ± 1.24e–5	3.57e–6 ± 3.39e–6	5.47e-6 ± 1.20e–5
Bridging Bots			
Eigenvector centrality	5.99e–5 ± 4.11e–4	5.91e–4 ± 2.03e–3	2.54e-5 ± 6.55e–5
Betweenness centrality	2.80e–9 ± 1.86e–8	6.95e–10 ± 3.55e–9	3.67e-9 ± 2.39e–8
Total degree centrality	2.91e–6 ± 4.84e–6	1.98e–6 ± 1.86e–6	3.00e-6 ± 6.31e–6

not entirely follow this principle since they post tweets that contain users from multiple communities, specifically @mentioning them within the post, suggesting that their choice of user tags is curated. This behavior puts them within more than one set of community, in particular communities that are disparate from each other, as observed from the Louvain clustering algorithm. Nonetheless, these bots do have a key role in the social network to connect communities, in particular, cross-cultural social marketing, bridging communal differences to better disseminate information [71].

Table 2 shows the network metrics measured for each type of user across the three locations of segregation. The metrics are extracted from the same all-communication network, and thus are comparable. In terms of General Bots, Chinese bots have the highest average eigenvector and total-degree centrality values. This indicates that the Chinese bots are the most well-connected within the network and have the highest degree of influence. This means that Chinese bots are better positioned to influence the network of users on the social media platform with their socio-political views and are thus more effective in disseminating their intended information, by means of their connectivity with a large number of users and influential users. For news bots, Chinese bots have the highest eigenvector centrality while US bots have the highest total-degree centrality. Of note is that Chinese news bots have shown an average of 0 for betweenness centrality, or very negligible, which reflects that these bots do not aid in information flow within the network; they are likely existing mainly to push news stories. For bridging bots, Chinese bots have the highest eigenvector centrality, but bots from the reset of the world have the highest betweenness and total-degree centrality. This suggests that bridging bots from both US and China have rather little influence over the network.

Next, we analyze the narrative themes reflects the narrative themes within the text of each type of user, and present the results in Fig. 6. Bots geotagged from the United States are generally concerned with the spatial location of the balloon and the possibility of it being a spy and surveillance balloon. Bridging bots from the United States discuss themes that directly relate political topics to the incident, for example discussion “Trump Administration”, “Republicans”, “Biden”. These terms reflect the perspective that US President Biden hesitated before taking action towards the balloon, and that there were similar bal-

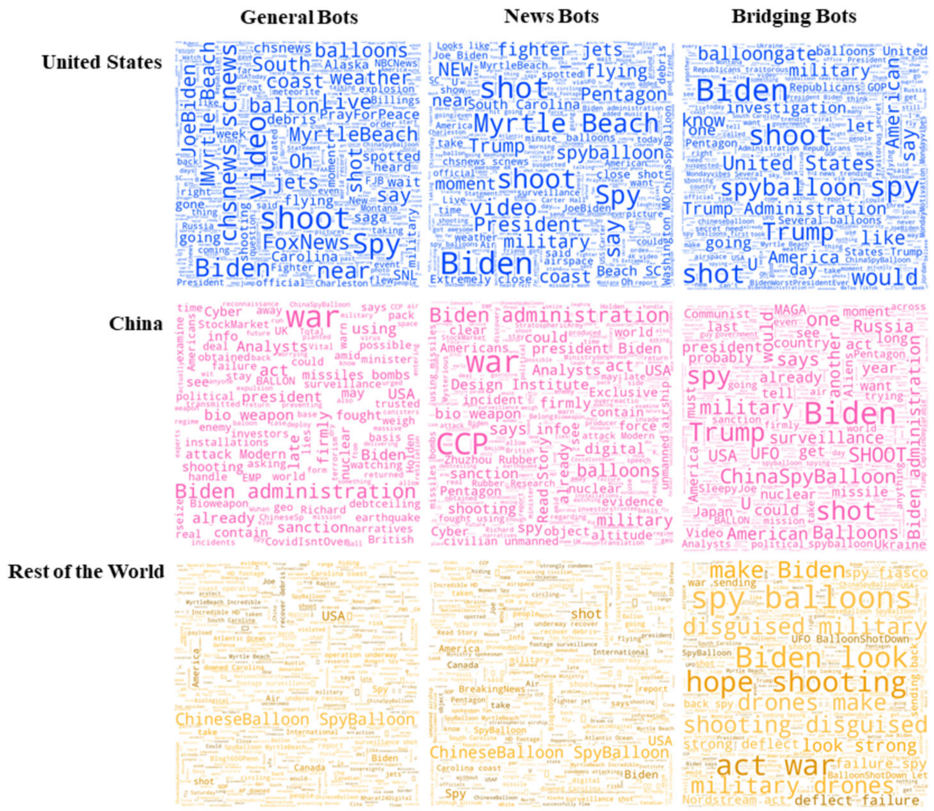

Figure 6 Narrative themes reflected through topic analysis

loons under the Trump Administration that were not discovered [72]. One key phrase that arose is "ballongate", a phrase closely linked to conspiracy narratives generally suffixed with -gate, like Pizzagate and Bridgegate [73]. The term "balloon-gate" has already gained an entry on Urban Dictionary as "a political scandal, usually one with national security implications, in the making" [74]. This definition highlights the importance of this incident on political relations.

Bots geotagged from China discussed topics about war, sanctions, cyber warfare, investment and communism. These topics do not directly describe the balloon incident, but project possibilities of escalated hostility between both countries. It also reflects that Chinese bots view the actions of the US as a sign of aggression.

Bots from the rest of the world discuss a variety of topics, as seen from the generally similar-sized words throughout the word clouds, indicating that there are few extremely predominant topics within the discourse. These topics range from the responses from both countries, the shooting of the balloon, and also partaking in humorous theories such as the possibility of aliens and UFOs.

Figures 7 and 8 and Figures 9 and 10 showcase the differences in the information maneuver tactics used by the different types of bots, measured using the BEND framework. In terms of the B-maneuvers (Figs. 9 and 10), in which the users attempt to manipulate the social network, we find that overall, users perform the Back maneuver the most, followed by the Build, Bridge then Boost maneuver. This indicates that the bots are more concerned with supporting other users through likes and shares, building larger groups through @mentions and hashtags, rather than increasing the linkages between members. `General Bots` performed the most Back maneuvers, `Bridging Bots` performed the most Build maneuvers, `News Bots` performed the most Bridge maneuvers and `General Bots` performed the most Boost maneuvers.

In terms of the E-maneuvers (Figs. 7 and 8), in which users attempt to manipulate narratives, we find that overall, users perform the Engage maneuver the most, followed by the Excite, then Enhance then Explain maneuver. This indicates that much of the narrative manipulation relies more on emotional appeal (Engage, Excite) rather than logical appeal (Explain). `General Bots` performed the most Engage and Explain maneuvers, `Bridging Bots` performed the most Enhance maneuver and `News Bot` performed the most Excite maneuver.

6 Discussion

In this political discussion, we observe that that average proportion of bots is 47.30%. This is higher than the average observed in past studies, which ranged from 5 to 18% [65, 75]. This could be due to a few reasons: the bot percentage in political communities are generally much higher than other communities like entertainment [65], or that this is a diplomatic event that involves two major powers thus gathers more interest, and hence groups of actors are compelled to deploy more bots in an attempt to control the narratives, or that the event is extremely juicy, which can be evidenced by the large number of memes, jokes and taglines that have been constructed online [19]. The differences in the proportion of bots that are geotagged to be from across US, China and the rest of the world indicates that the distribution of Twitter bots are not spatially homogeneous. This provides leads towards the countries that more bots originate from, which could be possible signs of state-sponsored bots, which is especially important in managing the country's image in a political narrative, keeping in line with the intent of diplomacy.

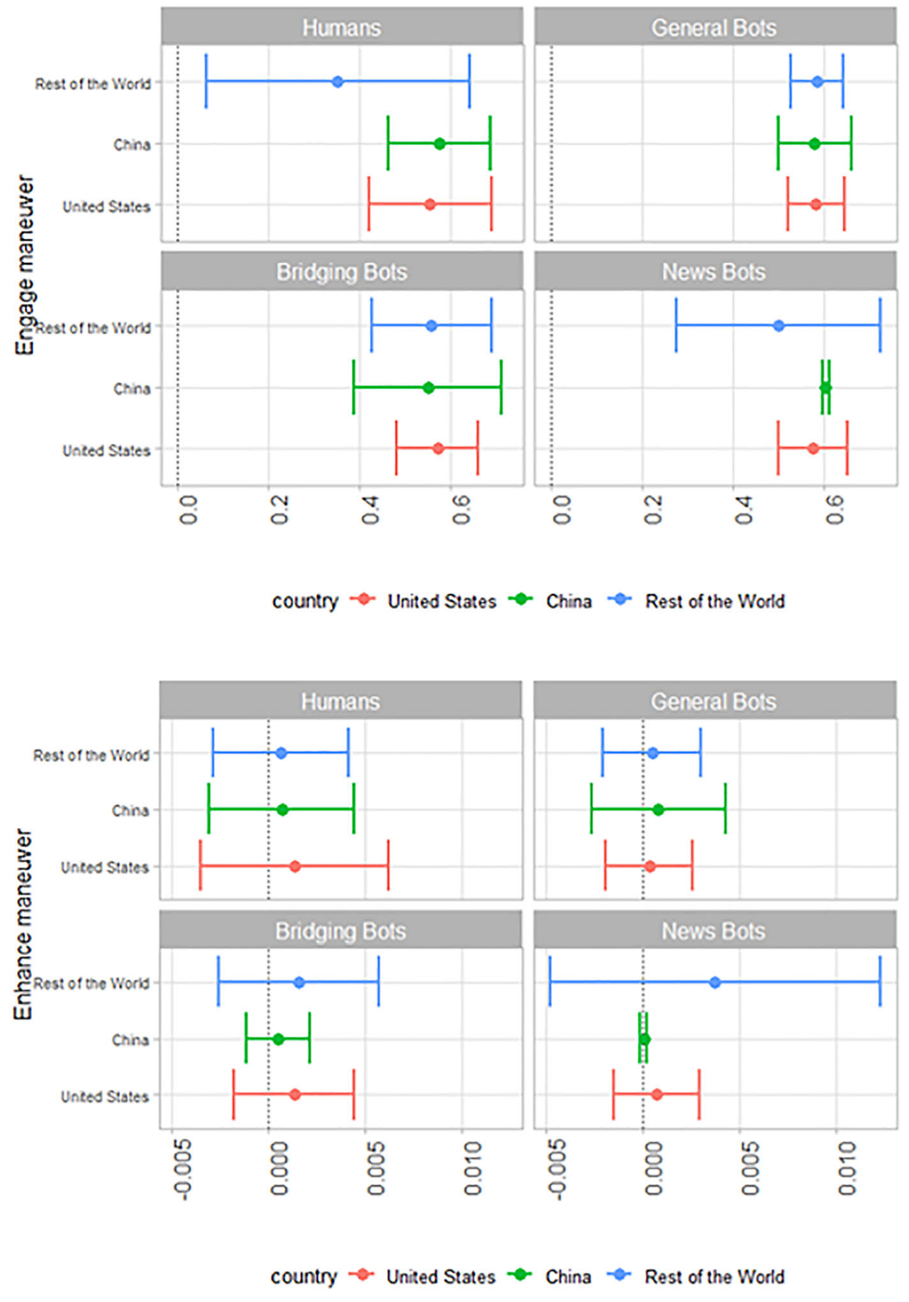

Figure 7 Distribution of the E – Information Maneuver Metrics (1)

One key issue about the distribution of users to note is that while we have segregated users based on their geolocation (US, China, Rest of the World), these users are not necessarily physically originating from the identified geolocated country. Instead, these reflect their association with the country, and by extension our analyses reflect the views of users that affiliated themselves with a particular country. This is important to note because Twitter is banned in China due to the Chinese firewall, yet there are users that reflect a geolocation of China. These users therefore, must be users that are actually geolocated in China, or users that affiliate their geolocation to China. Either way, we unfortunately

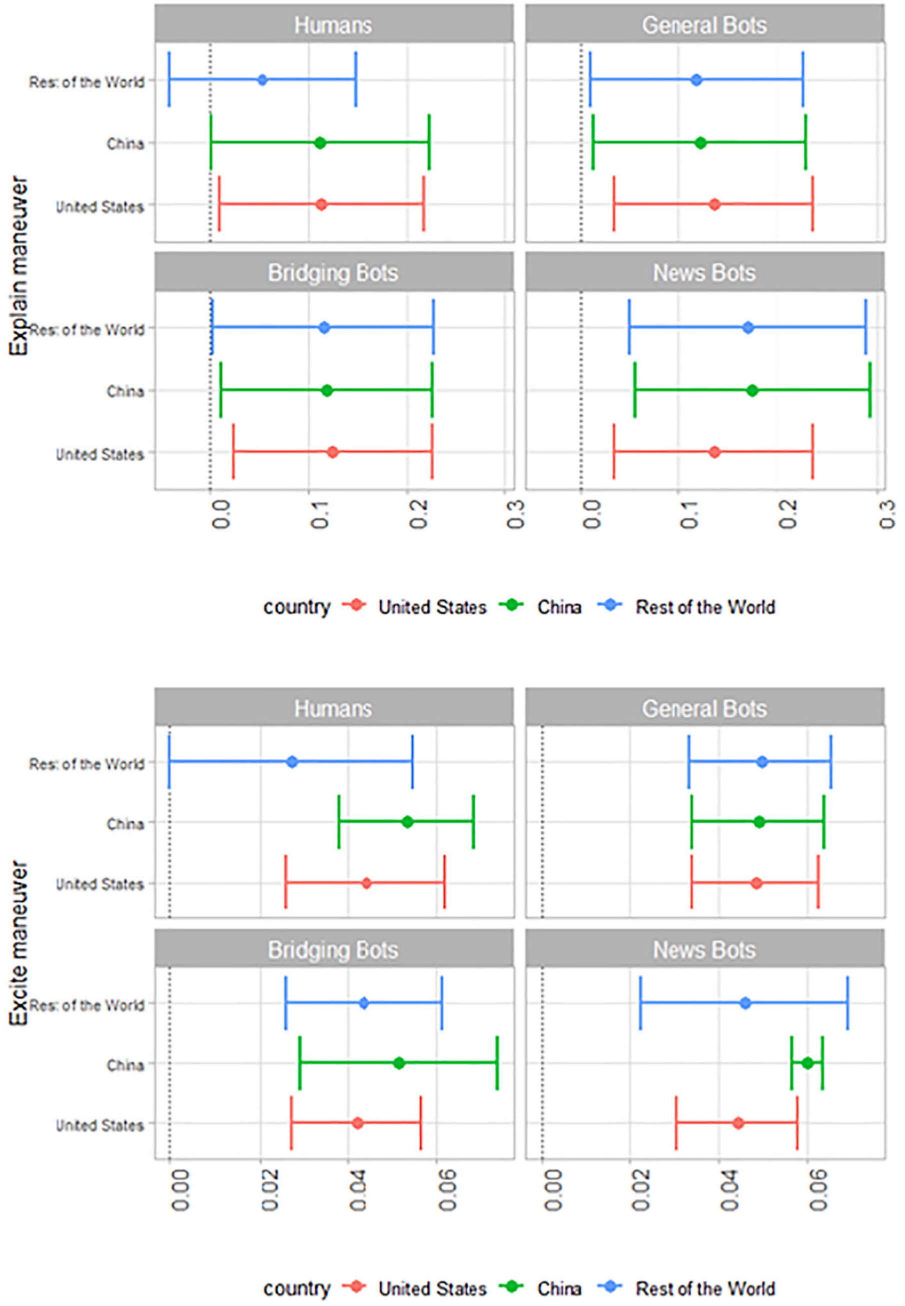

Figure 8 Distribution of the E – Information Maneuver Metrics (2)

are unable to differentiate the truthfulness of the geolocation of Twitter users through the information in the data collected, and therefore rely on the self-presentation of location. Our analysis of only English language tweets also has value to the users that are geo-tagged to China. It reflects the thoughts that users affiliated with China are projecting towards the English-speaking community, showcasing the projection of diplomatic narratives and the projection of soft power.

Across the three main cultural groups (United States, China, Rest of the World), we observe that the same type of social bots exist and play the same roles. The General Bot is the

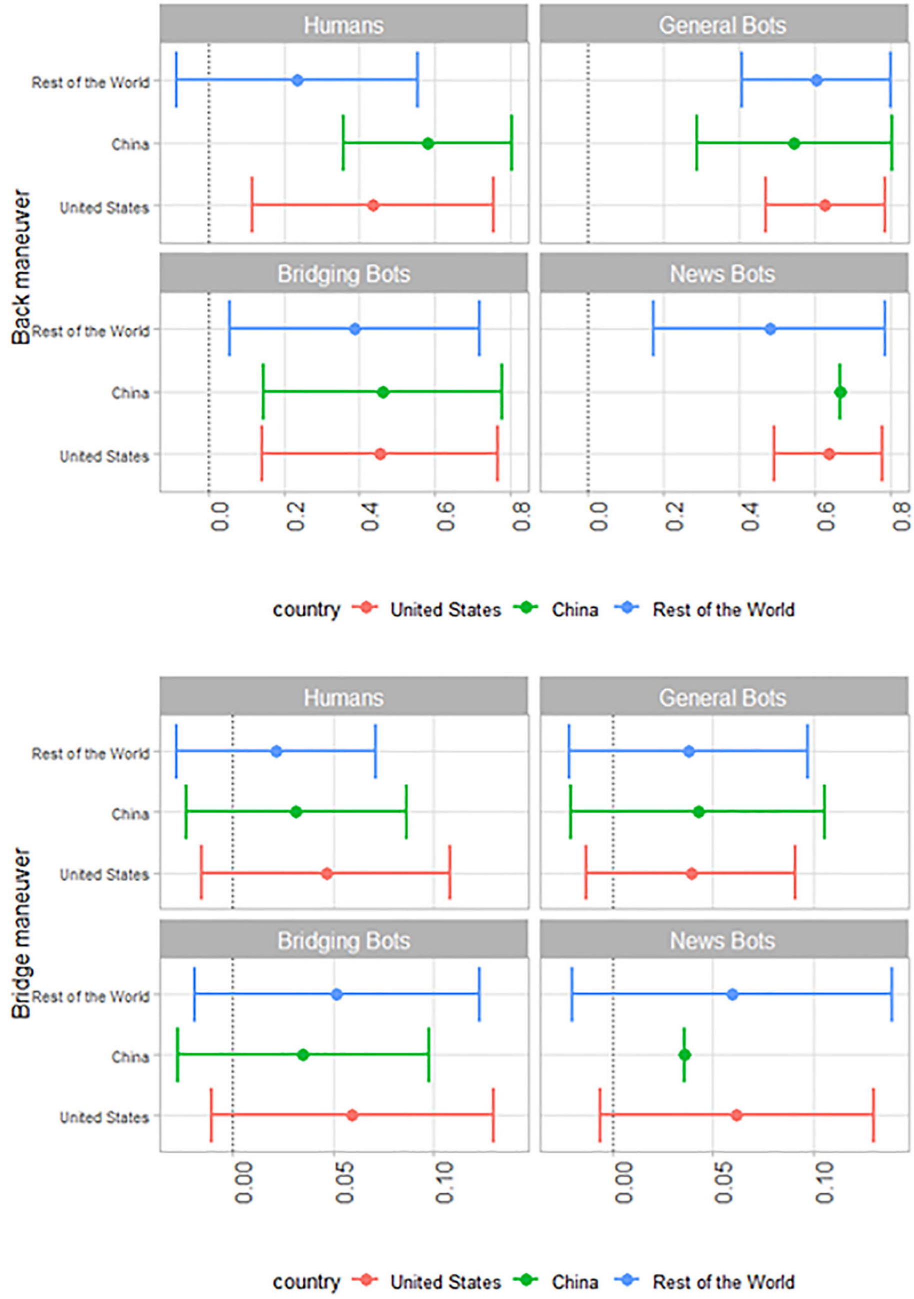

Figure 9 Distribution of the B – Information Maneuver Metrics (1)

most common bot type that is present throughout geotagged bot accounts from all countries, followed by News Bots. The presence and employment of Bridging Bots are generally rare throughout all cultures, possibly because it takes additional effort to program the automated accounts to identify multiple groups of people and link them together.

Within this political event, we identified an average of 3% of the bot users are `News Bots`. This is consistent with previous studies where bots are observed to be used as active news promoters during critical events, such as the 2020 Coronavirus pandemic [58]. The average sentiment of `news bots` is neutral, indicating that the bots do not inject

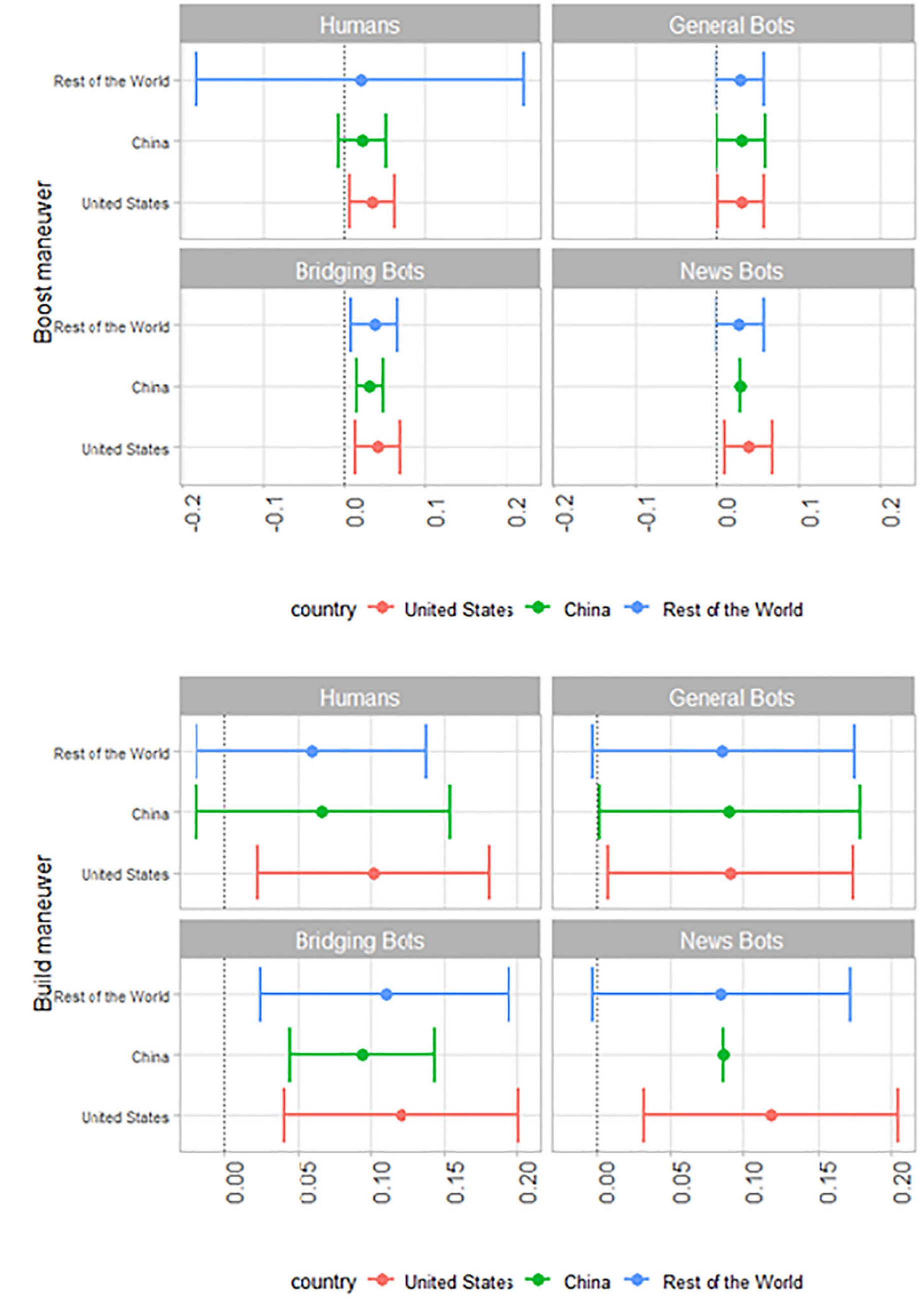

Figure 10 Distribution of the B – Information Maneuver Metrics (2)

much emotion into their posts, and thus do not actively attempt to manipulate opinions. In contrast to the prevailing conception that social media bots are generally malicious bots (80% of Americans who have heard about social media bots view them as malicious [76]), this analysis of `news bots` show that there are bots that are helpful bots: in this case, `news bots` serve to disseminate news.

The proportion of `bridging bots` are extremely rare, with `bridging bots` that originate from all three regions being less than 1%. Despite their small presence within the social media space, these bots play an important role. They enable information flow across boundaries, be it geographical, language or ideological, allowing users from one community to receive information and opinions from the other community. This pattern has also been observed on Twitter during the Arab Spring revolution in Egypt in 2011, where `bridging bots` enabled information flow between Arabic and English language spheres [77]. In our study, bridging bots enabled information flow between China and US bots, promoting the exchange of topics and emotions.

However, the employment of these bots across the cultures differ. Bots from different countries are used to present different narrative themes and frames. This most often aligns with the country's diplomatic perspective of the event. For example, News Bots from the United States focused on the surveillance aspect of the balloon, while those from China focused on the comments from the Biden administration.

Bots within this diplomatic incident mainly use positive information maneuvers, in line with image-enhancing projection techniques in diplomacy [63]. To expand the reach of their message through the network, bots mostly use the Back and Build maneuvers. These maneuvers make use of actions like @mentions, likes and retweets, which can easily be automated through the Twitter API. These observations are similar to previous studies where bots are observed to heavily use the positive B-maneuvers to support their stance towards/against the Palestine-Israel crisis [62]. To increase readership of their message, `General Bots` and `Bridging Bots` make use of emotional appeal using the Engage and Excite maneuvers, rather than logical appeal. This technique has been observed in past studies where bots target emotionally appealing topics and are extremely effective with using emotions as part of their persuasive dialogue in both political topics [78] and general discourse [79]. `News Bots` attempt to make their short news headlines catchy, as evidenced by their high Excite maneuver.

While we have segregated users by geography, we did not investigate evidence of state manipulation, and therefore are unable to comment on whether the users are state-manipulated actors. There is, however, a possibility that a good amount of bot accounts are state-sponsored accounts, be it originating from the US, China or the rest of the world, with intentions to put forth certain narratives that are in line with the diplomatic concerns of the state.

Further, we do not suggest that our typology of bots in this article is exhaustive. There are other types of bots that we have not explored within this discourse that exists in social media. Such bots include amplifier bots which have been shown to intensify opinions in political discussions [80, 81]. Another is spam bots which have been observed to spread phishing links on Twitter [82] and overwhelm Twitter users with messages spreading their own ideology [83].

Our study has broader implications towards policymakers as well. Based on the geolocated discourse, we can understand the narratives for projection of political images used by automated agents affiliated with region. The interactivity on digital platforms provides deeper understanding into the portrayal of a country on social media, and the perception of political issues by discussants on online social media. With these information, those in policy and governance can systematically identify public sentiment, which can be useful in devising communication strategies to address these sentiments. Those involved in studying foreign affairs can better identify a country's projected national image and stance towards the political event, and analyze and anticipate possible political responses.

6.1 Limitations and future work

We highlight a few limitations of our work. Naturally, our discussion is not exhaustive and a few limitations nuance the discussions of the work.

One key limitation of this study is the data source: data collected from the Twitter API only presents 1% of the discourse in the social media space, and thus we make the assumption that our collected data represents the social media discussions. Our study is limited to the discussion on Twitter which is less popular in China because it is a restricted platform [84]. Users with more extreme opinions are typically more vocal on social media, thus we suggest caution in extrapolating the findings, and be cautious of the silent majority/ vocal minority effect [33]. For these reasons, the study does not reveal the full scope of the inauthentic bot activity stemming from both countries during this event. Research of wider breadth is needed to map out the bot campaign and reach of both US and Chinese bot accounts.

Additionally, geolocation identification of user accounts relies on self-presentation of the accounts, and Twitter users can erronously reflect their location. Some do so for humor, like specifying itself from China and having a profile picture of a balloon along with a description "just floating around in cyberspace before being shot down"; others do so to deliberately avoid association with specific countries; and yet others do not provide any location information.

Our bot detection algorithm relies on a supervised machine learning algorithm that is trained on a manually labeled dataset. It extracts bot-like features such as extremely frequent retweeting behavior and temporal periodicity of posting. These general-purpose bot detection algorithms have been found to be prone to error [85], which can therefore affect the observations. In particular, some users identified are the highly engaged user, the user that tweets and retweets extremely often such that the behavior comes across as bot-like to the algorithm. Also, in our determination of whether the user is a bot or not, we used the 0.70 threshold value, based on past systematic large-scale analyses on threshold values [37]. However, further work should be done to measure the impact of different thresholds on the results and on the efficiency of extracting different types of bots.

And lastly, our analysis includes only English language tweets. While this showcases what the English speaking community in both the US and China are discussing about, this precludes the opinions of the Chinese speaking community, a community that is native to the country China.

Following from the limitations, we suggest directions for future work. To cope with the geolocation issue, some researchers have attempted to infer a user's geolocation from the places mentioned within tweets or the style and language of the tweets [86]. Other methods make use of the social network of the user, inferring the user's geolocation via their friends [87]. These methods can be employed to enhance the identification of a user's geolocation via their declared location, and result in a larger number of users that are available for analysis.

We also suggest in-depth investigations of other types of bots that are used for digital diplomacy on social media, expanding the scope of analysis of automated agents that are employed in the realm of cross-country diplomacy. An example of a type of bot that warrants investigation is the propaganda bots, which have been observed during the Gulf crisis to spread propaganda and fake news [88].

Downstream work looks towards performing cross-lingual analysis within a diplomatic event that spans more than one country. This is especially important in understanding the bot activity in social media communities other than English. Particularly, in this event it relates to the Chinese speaking community on Twitter: Chinese language bot activity has increased over the years, and bot accounts are observed to be bombarding searches for Chinese cities with tweets related to pornography and gambling [45]. Analysis of bot-like users within a diplomatic event also includes in-depth investigation into the background intent of these users: sets of inauthentic accounts created and operated by political actors working to influence social discourse, sets of programmed inauthentic accounts that aggresively amplify and disseminate information and the sets of highly engaged and active users that possibly monetize their content or linked content from tweet. Finally, further work can be done to analyze the temporal changes in the usage of information maneuvers, extending our work from a wrinkle in time towards a cinematic replay of the variants of maneuver strategies deployed through time.

7 Conclusion

The topic of automation and online politics have become a major area of investigation in computational social science because the spread of inauthentic bot accounts on social media can pose a problem.

This article is the first to develop methodologies to pick out certain types of bots that are used during a diplomatic incident. These methodologies are not restricted to the incident in the study, nor are they restricted to diplomatic events; they are generic methodologies that can be applied to identifying bots across a variety of events in the social media space. Following which, this article provides the first academic insights into the nature of three types of bots during a diplomatic incident, identifying the differences in the topics and interactions between each type of bot in relation to the country it likely originates from.

We find that all three types of bots examined within this article – General Bots, News Bots and Bridging Bots – are present in our regions of study, namely the United States and China. With regards to the balloon incident which is a diplomatic situation between the two world powers, the bots tweet on different topics. US bots are more interested in the location of the balloon and the eventual shooting down of the balloon, while Chinese bots view the actions by the US as aggression.

All three types of bots engage in the positive narrative and network information maneuvers, but bots from different countries perform different degrees of each maneuver. The most performed narrative maneuver is the Back maneuver as bots prop each other's messages up, while the most performed narrative maneuver is the Engage maneuver as bots actively engage each other through network communication interactions.

As bots become more prevalent in the digital space, they can be used to communicate with the general public (e.g., `news bots`). They should also be monitored to understand the general public, as `general bots` and `bridging bots` can potentially alter the public opinion. Overall, this article analyzed the political participation by automated users. Through analysis of the narratives and the network influence of social media bots affiliated with two major powers, we contribute to the literature on soft power and online diplomacy, and present an understanding of the image that users affiliated with each country are projecting on social media. We hope that the article will set forth discussions surrounding the use of bots in digital diplomacy.

Acknowledgements
We thank our colleagues at the IDeaS lab at Carnegie Mellon University for their initial feedback on the ideas of this work. We also sincerely thank the reviewers for providing great comments that made this piece a much better one.

Funding
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, Office of Naval Research (Bothunter, N000141812108), Scalable Technologies for Social Cybersecurity/ARMY (W911NF20D0002), Air Force Research Laboratory/CyberFit (FA86502126244). The content of the information does not necessarily reflect the position or the policy of the government and no official endorsement should be inferred.

Abbreviations
JSON, JavaScript Object Notation; US, United States; UFO, Unidentified Flying Object; URL, Unified Resource Locator.

Data availability
The original set of data collected for this article can be obtained from https://drive.google.com/drive/folders/1RDH7l2CYsr-DbnW1Si1LGZPX_KcYUE9Z?usp=drive_link. Further data used in this article can be obtained from the corresponding author in accordance to Twitter's Terms and Conditions.

Declarations

Ethics approval and consent to participate
There are several ethical points to consider in our work.

In this study, we only extracted publicly available data using the Twitter API, and no attempt was made to retrieve protected tweets. Within this article, we do not process the usernames or unique personal identifiers of the social media accounts during our analysis. During our analysis, we use only the aggregate trends and do not investigate the profile and activity of individual users. We do not mention specific user names within our report because many of these accounts are still active online.

The conclusions that we obtained through applying our methodology are based of the observations of the Twitter accounts and their posts. This represents but a slice of the discussion online and do not necessarily represent the entire population. Therefore, one must be cautious in using our insights to inform behavior or policy.

Competing interests
The authors declare that they have no competing interests.

Author contributions
LHXN: Conceptualization, methodology, analysis, writing. KMC: Review and editing. All authors have read and agreed to the published version of the manuscript.

Received: 16 August 2023 Accepted: 7 December 2023 Published online: 19 December 2023

References

1. Adesina OS (2017) Foreign policy in an era of digital diplomacy. Cogent Social Sciences 3(1):1297175
2. Manor I, Segev E (2015) America's selfie: how the us portrays itself on its social media accounts. In: Digital diplomacy. Routledge, London, pp 89–108
3. Huang QE (2020) Facebook not statebook: defining sns diplomacy with four modes of online diplomatic participation. Int J Commun 14:18
4. Theocharis Y, Van Deth JW (2018) The continuous expansion of citizen participation: a new taxonomy. Eur Polit Sci Rev 10(1):139–163
5. Ng LHX, Carley KM (2023) A combined synchronization index for evaluating collective action social media. Appl Netw Sci 8(1):1
6. Benney J (2011) Twitter and legal activism in China. Communication, Politics & Culture 44(1):5–20
7. Boshmaf Y, Muslukhov I, Beznosov K, Ripeanu M (2011) The socialbot network: when bots socialize for fame and money. In: Proceedings of the 27th annual computer security applications conference, pp 93–102
8. Gorwa R, Guilbeault D (2020) Unpacking the social media bot: a typology to guide research and policy. Policy Internet 12(2):225–248
9. Linvill DL, Boatwright BC, Grant WJ, Warren PL (2019) "The Russians are hacking my brain!" investigating Russia's Internet research agency Twitter tactics during the 2016 United States presidential campaign. Comput Hum Behav 99:292–300
10. Britannica: Diplomacy | Definition, Meaning, Types, & Examples — britannica.com. https://www.britannica.com/topic/diplomacy. [Accessed 24-Jul-2023] (2023)
11. Shen F, Zhang E, Zhang H, Ren W, Jia Q, He Y (2023) Examining the differences between human and bot social media accounts: A case study of the Russia-Ukraine war. First Monday
12. Zhao B, Ren W, Zhu Y, Zhang H (2023) Manufacturing conflict or advocating peace? A study of social bots agenda building in the Twitter discussion of the Russia-Ukraine war. J Inf Technol Polit 1–19
13. Dawson A, Innes M (2019) How Russia's Internet research agency built its disinformation campaign. Polit Q 90(2):245–256
14. DiResta R, Miller C, Molter V, Pomfret J, Tiffert G (2020) Telling China's story: the Chinese communist party's campaign to shape global narratives. Stanford Internet Observatory, Stanford
15. Repnikova M, Chen KA (2023) Asymmetrical discursive competition: China–United States digital diplomacy in Africa. Int Commun Gaz 85(1):15–31

16. Bolsover G, Howard P (2019) Chinese computational propaganda: automation, algorithms and the manipulation of information about Chinese politics on Twitter and Weibo. Inf Commun Soc 22(14):2063–2080
17. Barnes JE, Wong E, Cooper H, Buckley C (2023) China's balloons spy on countries around the world, US officials say. The New York Times 12
18. Chen Q US urged to reflect on China-US relations, correct wrongdoings over balloon incident - Global Times (2023). https://www.globaltimes.cn/page/202302/1285614.shtml [Accessed 24-Jul-2023]
19. Kutllovci L (2023) That's no moon... It's a balloon! European View 22(1):140–142
20. on Foreign Relations, C. (2023) Timeline: U.S.-China Relations — cfr.org. https://www.cfr.org/timeline/us-china-relations. [Accessed 30-07-2023]
21. Guo L, Mays K, Wang J (2019) Whose story wins on Twitter? Visualizing the South China Sea dispute. Journalism Studies 20(4):563–584
22. Moral P, Marco G (2023) Assembling stories tweet by tweet: strategic narratives from chinese authorities on Twitter during the covid-19 pandemic. Communication Research and Practice 1–25
23. Xiaomeng Z, Chong Z, Zipei Y (2020) Emotional tendency analysis of Twitter texts based on cnns model. In: 2020 International Conference on Big Data and Informatization Education (ICBDIE). IEEE, pp 379–382
24. Zhang C, Wang Z (2023) Despicable 'other' and innocent 'US': emotion politics in the time of the pandemic. Humanit Soc Sci Commun 10(1):1–11
25. Guo Y (2004) Cultural nationalism in contemporary China. Routledge, London
26. Aleroud A, Bani Melhem A, Alhussien N Albert CD (2023). span-prop: combatting contextualized social media state-linked propaganda in the middle east
27. Kavanaugh A, Fox EA, Sheetz S, Yang S, Li LT, Whalen T, Shoemaker D, Natsev P, Xie L (2011) Social media use by government: from the routine to the critical. In: Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times. dg.o '11. Association for Computing Machinery, New York, pp 121–130. https://doi.org/10.1145/2037556.2037574
28. Ng LHX, Cruickshank IJ (2023) Recruitment promotion via Twitter: a network-centric approach of analyzing community engagement using social identity. Digit Gov: Res Pract. https://doi.org/10.1145/3617127 4(4):22
29. Kim S, Sung KH, Ji Y, Xing C, Qu JG (2021) Online firestorms in social media: comparative research between China Weibo and USA Twitter. Public Relat Rev 47(1):102010
30. Bessi A, Ferrara E (2016) Social bots distort the 2016 us presidential election online discussion. First monday 21(11–7)
31. Ng LH, Taeihagh A (2021) How does fake news spread? Understanding pathways of disinformation spread through apis. Policy Internet 13(4):560–585
32. Stieglitz S, Brachten F, Ross B, Jung A-K (2017) Do social bots dream of electric sheep? A categorisation of social media bot accounts. arXiv preprint. arXiv:1710.04044
33. Ng LHX, Carley KM (2022) Pro or anti? A social influence model of online stance flipping. IEEE Trans Netw Sci Eng 10(1):3–19
34. Gionis A, Terzi E, Tsaparas P (2013) Opinion maximization in social networks. In: Proceedings of the 2013 SIAM international conference on data mining. SIAM, Philadelphia, pp 387–395
35. Aleroud A, Alhussien N, Albert C (2022) From theory to practice: towards an osint framework to mitigate Arabic social cyber attacks. In: 2022 international conference on Intelligent Data Science Technologies and Applications (IDSTA). IEEE, pp 146–151
36. Alieva I, Moffitt J, Carley KM (2022) How disinformation operations against Russian opposition leader Alexei Navalny influence the international audience on Twitter. Soc Netw Anal Min 12(1):80
37. Ng LHX, Robertson DC, Carley KM (2022) Stabilizing a supervised bot detection algorithm: how much data is needed for consistent predictions? Online Soc Netw Media 28:100198
38. Schnebly J, Sengupta S (2019) Random forest Twitter bot classifier. In: 2019 IEEE 9th annual Computing and Communication Workshop and Conference (CCWC). IEEE, pp 0506–0512
39. Ng LHX, Carley KM (2023) Botbuster: multi-platform bot detection using a mixture of experts. In: Proceedings of the international AAAI conference on web and social media, vol 17, pp 686–697
40. Martín-Gutiérrez D, Hernández-Peñaloza G, Hernández AB, Lozano-Diez A, Álvarez F (2021) A deep learning approach for robust detection of bots in Twitter using transformers. IEEE Access 9:54591–54601
41. Yang K-C, Varol O, Hui P-M, Menczer F (2020) Scalable and generalizable social bot detection through data selection. In: Proceedings of the AAAI conference on artificial intelligence, vol 34, pp 1096–1103
42. Beskow DM, Carley KM (2018) Bot-hunter: a tiered approach to detecting & characterizing automated activity on Twitter. In: Conference paper. SBP-BRiMS: international conference on social computing, behavioral-cultural modeling and prediction and behavior representation in modeling and simulation, vol 3
43. Leetaru K, Wang S, Cao G, Padmanabhan A, Shook E (2013) Mapping the global Twitter heartbeat: The geography of Twitter. First Monday
44. Cheng Z, Caverlee J, Lee K (2010) You are where you tweet: a content-based approach to geo-locating Twitter users. In: Proceedings of the 19th ACM international conference on information and knowledge management, pp 759–768
45. Liao R (2022) Despite ban, Twitter downloads surge in China amid COVID protests |. TechCrunch — techcrunch.com. https://techcrunch.com/2022/11/28/despite-ban-twitter-downloads-surge-in-china-amid-covid-protests/. [Accessed 23-Jul-2023]
46. Jacobs CS, Carley KM (2022) Taiwan: China's gray zone doctrine in action. Small Wars J 3:1–2
47. Alieva I, Ng LHX, Carley KM (2022) Investigating the spread of Russian disinformation about biolabs in Ukraine on Twitter using social network analysis. In: 2022 IEEE international conference on big data (big data). IEEE, pp 1770–1775
48. Zhang Y, Shah D, Foley J, Abhishek A, Lukito J, Suk J, Kim SJ, Sun Z, Pevehouse J, Garlough C (2019) Whose lives matter? Mass shootings and social media discourses of sympathy and policy, 2012–2014. J Comput-Mediat Commun 24(4):182–202
49. Varol O, Ferrara E, Davis C, Menczer F, Flammini A (2017) Online human-bot interactions: detection, estimation, and characterization. In: Proceedings of the international AAAI conference on web and social media, vol 11, pp 280–289
50. Rauchfleisch A, Kaiser J (2020) The false positive problem of automatic bot detection in social science research. PLoS ONE 15(10):0241045

51. NOW: News on the Web Corpora. https://www.english-corpora.org/now/
52. Carley KM (2020) Social cybersecurity: an emerging science. Comput Math Organ Theory 26(4):365–381. https://doi.org/10.1007/s10588-020-09322-9
53. Tang J, Sun J, Wang C, Yang Z (2009) Social influence analysis in large-scale networks. In: Proceedings of the 15th ACM SIGKDD international conference on knowledge discovery and data mining, pp 807–816
54. Wasserman S, Faust K (1994) Social network analysis: methods and applications
55. Bastian M, Heymann S, Jacomy M (2009) Gephi: an open source software for exploring and manipulating networks. In: Proceedings of the international AAAI conference on web and social media, vol 3, pp 361–362
56. Al-Agha I, Abu-Dahrooj O (2019) Multi-level analysis of political sentiments using Twitter data: A case study of the Palestinian-Israeli conflict. Jordanian Journal of Computers and Information Technology 5(3)
57. Volkova S, Bell E (2016) Account deletion prediction on runet: a case study of suspicious Twitter accounts active during the Russian-Ukrainian crisis. In: Proceedings of the second workshop on computational approaches to deception detection, pp 1–6
58. Al-Rawi A, Shukla V (2020) Bots as active news promoters: a digital analysis of Covid-19 tweets. Information 11(10):461
59. Al-Khateeb S, Agarwal N (2016) Understanding strategic information manoeuvres in network media to advance cyber operations: a case study analysing pro-Russian separatists' cyber information operations in crimean water crisis. Journal on Baltic Security 2(1)
60. Blazek S (2021) SSCOTCH: A framework for rapidly assessing influence operations. https://www.atlanticcouncil.org/blogs/geotech-cues/scotch-a-framework-for-rapidly-assessing-influence-operations/
61. Alaphilippe A (2020) Adding a 'D' to the ABC disinformation framework. Brookings. https://www.brookings.edu/techstream/adding-a-d-to-the-abc-disinformation-framework/
62. Danaditya A, Ng LHX, Carley KM (2022) From curious hashtags to polarized effect: profiling coordinated actions in Indonesian Twitter discourse. Soc Netw Anal Min 12(1):105
63. Sterling DP (2018) A new era in cultural diplomacy: promoting the image of China's "belt and road" initiative in Asia. Open Journal of Social Sciences 6(2):102–116
64. Surmacz B (2016) New technologies in diplomacy. New Technologies as a Factor of International Relations, 71–90
65. Tan Z, Feng S, Sclar M, Wan H, Luo M, Choi Y, Tsvetkov Y (2023) Botpercent: estimating Twitter bot populations from groups to crowds. arXiv preprint. arXiv:2302.00381
66. Molter V, DiResta R (2020) Pandemics & propaganda: how Chinese state media creates and propagates ccp coronavirus narratives. Harvard Kennedy School Misinformation Review 1(3)
67. Jacobs CS, Ng LHX, Carley KM (2023) Tracking China's cross-strait bot networks against Taiwan. In: International conference on social computing, behavioral-cultural modeling and prediction and behavior representation in modeling and simulation. Springer, Berlin, pp 115–125
68. McPherson M, Smith-Lovin L, Cook JM (2001) Birds of a feather: homophily in social networks. Annu Rev Sociol 27(1):415–444
69. Bisgin H, Agarwal N, Xu X (2010) Investigating homophily in online social networks. In: 2010 IEEE/WIC/ACM international conference on web intelligence and intelligent agent technology, vol 1. IEEE, pp 533–536
70. Khanam KZ, Srivastava G, Mago V (2023) The homophily principle in social network analysis: a survey. Multimed Tools Appl 82(6):8811–8854
71. Moriuchi E (2021) References. Cross-cultural social media marketing: bridging across cultural differences Emerald Publishing Limited, pp 123–134. https://doi.org/10.1108/978-1-83867-175-420211012
72. Bertrand N (2023) Chinese spy balloons under Trump not discovered until after Biden took office |. CNN Politics — cnn.com. https://www.cnn.com/2023/02/05/politics/chinese-spy-balloons-trump-administration/index.html [Accessed 27-07-2023]
73. Tangherlini TR, Shahsavari S, Shahbazi B, Ebrahimzadeh E, Roychowdhury V (2020) An automated pipeline for the discovery of conspiracy and conspiracy theory narrative frameworks: bridgegate, pizzagate and storytelling on the web. PLoS ONE 15(6):0233879
74. Dictionary U (ed). Balloon-gate. https://www.urbandictionary.com/define.php?term=Balloon-gate
75. Fukuda M, Nakajima K, Shudo K (2022) Estimating the bot population on Twitter via random walk based sampling. IEEE Access 10:17201–17211
76. Stocking G, Sumida N (2018) Most Americans have heard about social media bots; many think they are malicious and hard to identify. https://www.pewresearch.org/journalism/2018/10/15/most-americans-have-heard-about-social-media-bots-many-think-they-are-malicious-and-hard-to-identify/. [Accessed 26-07-2023]
77. Bruns A, Highfield T, Burgess J (2013) The Arab Spring and social media audiences: English and Arabic Twitter users and their networks. Am Behav Sci 57(7):871–898
78. Nonnecke B, Perez de Acha G, Choi A, Crittenden C, Gutierrez Cortes FI, Martin Del Campo A, Miranda-Villanueva OM (2022) Harass, mislead, & polarize: an analysis of Twitter political bots' tactics in targeting the immigration debate before the 2018 us midterm election. J Inf Technol Polit 19(4):423–434
79. Paavola J, Helo T, Jalonen H, Sartonen M, Huhtinen A-M (2016) Understanding the trolling phenomenon: the automated detection of bots and cyborgs in the social media. Journal of Information Warfare 15(4):100–111
80. McKelvey F, Dubois E (2017) Computational propaganda in Canada: the use of political bots
81. Yoon N, Hemsley J, Smith A, Simpson E, Eakins J (2022) Super-amplifiers! The role of Twitter extended party networks in political elections. Policy Internet 14(3):711–730
82. Chu Z, Gianvecchio S, Wang H, Jajodia S (2010) Who is tweeting on Twitter: human, bot, or cyborg? In: Proceedings of the 26th annual computer security applications conference, pp 21–30
83. Jamison AM, Broniatowski DA, Quinn SC (2019) Malicious actors on Twitter: a guide for public health researchers. Am J Publ Health 109(5):688–692
84. Sullivan J (2012) A tale of two microblogs in China. Media Cult Soc 34(6):773–783
85. Hays C, Schutzman Z, Raghavan M, Walk E, Zimmer P (2023) Simplistic collection and labeling practices limit the utility of benchmark datasets for Twitter bot detection. In: Proceedings of the ACM web conference 2023, pp 3660–3669

86. Han B, Cook P, Baldwin T (2014) Text-based Twitter user geolocation prediction. J Artif Intell Res 49:451–500

87. Jurgens D, Finethy T, McCorriston J, Xu Y, Ruths D (2015) Geolocation prediction in Twitter using social networks: a critical analysis and review of current practice. In: Proceedings of the international AAAI conference on web and social media, vol 9, pp 188–197

88. Jones MO (2019) The gulf information war| propaganda, fake news, and fake trends: the weaponization of Twitter bots in the gulf crisis. Int J Commun 13:27

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com