# Bots on Twitter: An Exploratory Analysis Approach on The Content they Share

Term Paper for the Seminar "Web & Society: A Computational Social Science Perspective"

submitted by Trinidad Bosch [deleted]

Gina-Maria Unger [deleted]

at the



Faculty of Law, Economics and Politics

Department of Politics and Public Administration

Examiner: Professor Doctor Juhi Kulshrestha

Konstanz, 2022

Abstract: Bots are nowadays all-over social media, sometimes even the expression "social bot pandemic" is used to describe this circumstance. Mostly the doing of these bots is associated with malicious practices and hence its consequences are viewed as a threat to the basis of society. Given this background, we want to investigate how much of these concerns are justified. Thus, this work concentrates on answering the questions: About what topics bots communicate, how they connotate these topics, and if any malicious intentions can be sensed in this topic connotation. Our main findings suggest that bots reflect the hot topics valid users stick to and concentrate primarily on current events. Moreover, the bot connotation of topics primarily depends on the areas studied, for example, the topic "stock markets" topic has a quite neutral significance for bots.

# **Table of Content**

List	of Figures	5
List	of Tables	5
1.	Introduction	6
2.	State of the Art	7
3.	Theory	9
4.	Data and Methods	10
5.	Results	14
6.	Discussion	20
7.	Limitations	21
9.	Statement of Contributions	24
10.	Appendix	25

# **List of Figures**

- Figure 1: Bot and valid user data shapes after reduction via UMAP to 2-dimensions. P12
- Figure 2: Silhouette Coefficient analysis for k-Means clustering for bots. P13
- Figure 3: Silhouette Coefficient analysis for k-Means clustering for valid users. P13
- Figure 4: DBCV score for minimum cluster sizes in bots. P13
- Figure 5: DBCV score for minimum cluster sizes in valid users. P13
- Figure 6: Racism and Crime cluster wordcloud for bot users. P16
- Figure 7: Racism and Crime cluster wordcloud for valid users. P16
- Figure 8: Tweet sentiment per type of user. P18
- Figure 9: Tweet sentiment in bots per topic. P18
- Figure 10: Tweet sentiment in valid users per topic. P19

### **List of Tables**

- Table 1: Dataset frequency for users per country. P11
- Table 2: Cluster topics for bot users, showing the top 20 words that construct them. P15
- Table 3: Cluster topics for valid users, showing the top 20 words that construct them. P16
- Table 4: Random tweets of the Racism and Crime cluster per type of user. P17
- **Table 5:** Random tweets of the Covid-19 cluster per type of user. P17
- **Table 6:** Tweet Sentiment distribution per user type in % (total column). P17
- **Table 7:** Sentiment Analysis per important topic in bot users in % (total column). P18
- Table 8: Sentiment Analysis per important topic in valid users in % (total column). P18
- Table 9: Inter-Rater Reliability Score for bots. P19
- Table 10: Rater-Model Reliability Score for bots. P19
- Table 11: Inter-Rater Reliability Score for valid users. P19
- Table 12: Rater-Model Reliability Score for valid users. P19
- Table 13: Rater-Cluster Reliability % Score for bots per topic. P20
- Table 14: Rater-Cluster Reliability % Score for valid users per topic. P20

#### 1. Introduction

"Social bots coexist with humans since the early days of online social networks."

When Cresci (2020) states this, he is not just in the right but also refers to an inherent issue of social networks. The question is how big of an issue is this often so-called "social bot pandemic"? For instance, in 2021 Twitter was among the 20 most populated social networks (Jay, 2022) which makes it a "big global network player". Besides this fact, in 2017 the average presence of bots on Twitter was estimated to be around 15% (Varol et al., 2017), which could make it a medium for social bots and a "big global threat".

Giving some background, the interactive microblogging social platform Twitter allows its community to publish text-based posts, known as "tweets". Hereby the community has the chance to connect themselves, where each user can be a friend and follower of another user. Practically users can be anyone, your fellow research college, a local store, a company, or even an automated account or so-called "social bot". In the early days of social media creating such a bot account was difficult as a skilled programmer was needed to understand the platform's documentation and to build an automated account able to act in a human-like manner. Today, reading better tech blogs or searching online for source code is often enough (Ferrara, 2020). For example, Gilani et al. (2017) set up a bot account on Twitter and found that even if bots are smaller in number than valid users, they have a great impact on content popularity and activity.

Presently these social bot accounts are mainly associated with malicious intentions, transmitted via online misbehavior and the spread of misinformation. Consequently, they are viewed as a threat to the basis of society. This view is also present in the juridical and political world, thus in 2017, the representatives of Twitter were summoned to testify before Congress in the light of investigations about enabling foreign bot manipulation during the 2016 U.S. Presidential election (Grootendorst, 2020). Furthermore, the dominant literature streams in social bot research mainly concentrate on their negative effects. Given that framing we want to investigate how much of these concerns and the hysteria about the "social bot pandemic", is justified. Thus, this work concentrates on answering the research questions: About what topics social bots communicate, how they connotate these topics, and if any malicious intentions can be sensed in this topic connotation. Our main findings suggest that the bot's hot topics reflect the big events happing due the time of the data collection, July to September 2020, same goes for valid users. In addition, the connotation of these topics depends on the area, for example, the topic "stock markets" was found to be quite neutral connotated by social bots.

Therefore, in the following, we will first review the state-of-the-art bot research. Here we discuss the term "bot" itself and point out the three major streams in the research literature – researching legitimate bots, illegitimate bots, and bot detection methods. The preceding section presents the research questions that guide our explanatory approach. After that we described the used data basis, the 'TwitBot-20' dataset (Feng et al., 2021), and research methods, which include the embedding of tweets with a sentence transformer, the clustering algorithm HDBSCAN, topic modeling based on a class-based TF-IDF variant, and sentiment analysis. The next section describes the research results, finishing with a summary. Lastly, we discuss implications for further research and the limitations our research approach underlies.

#### 2. State of the Art

In the following section, the literature considering bots will be sketched and sorted into one of its three dominant streams. This is done so that readers can grasp an overview of the literature's status quo. Before proceeding with this plan, first, the meaning of the term "bot" should be debated to establish a common ground about the concept.

In its simplest form, the term "bot" means "robot" (Gorwa and Guilbeault, 2020), though this meaning is mostly not the intended one when we talk about bots. Accordingly, the question "What is its intended meaning?" arrives. Unfortunately, this question has no simple answer, as the word itself is ambiguous, it underlies multiple meanings and timely changes. In the early days of personal computing, the term referred to a variety of different software systems such as daemons and scripts (Leonard, 1998). In the 2000s that meaning changed due to its usage in the network and information security literature and applied to compromised computers (Yang et al. 2014). With the emergence of online social networking and microblogging tools, its meaning shifted again, now applying to the automated accounts active on these platforms.

Shedding the term in a more technical light, it is used nowadays for full or partial automated programs based on algorithms and AI, that were built with the intention of assistance or malicious plans (Chu et al. 2010; Cresci 2020). From these intentions the second is the more dominant one in bots (Ferrara et al. 2016; Stieglitz et al. 2017). Narrowing down the technical terms, bots can be grouped into bots, bot-assisted humans, and human-assisted bots. Hereby, bot-assisted humans and human-assisted bots – often called cyborgs – are mixed creatures between a bot and a human, and simultaneously driven by algorithms and human intervention (Chu et al. 2010; Cresci 2020).

Besides this comparably technical perspective, there are also other bot-related terms, which unfortunately do not underly a clear typology and are too many to write them down. Most of these terms are either strongly related to the field they are used in or based on the specific behavior the exemplary bots exhibit. Gorwa and Guilbeault (2020) developed a broadish nonexclusive overview, which delivers a good basis for getting a grip of the most used bot terms. The authors make separation into six categories, which are (1) crawlers and scrapers, (2) chatbots, (3) spambots, (4) social bots, (5) sockpuppets, and (6) hybrid accounts. Beginning with crawlers and scrapers, these terms refer to automated scripts that try to download and index websites in bulk. Further, chatbots are human-computer dialog systems that mimic the natural human language to enable automated online guidance and support. They use primarily Natural Language Processing and Machine Learning to emulate natural language (Caldarini et al. 2022). The term spambots refer to computers or other networked devices compromised by malware and controlled by a third party. Moreover, social bots are various forms of computer algorithms specifically operating on social media platforms. These bots tend to produce content and interact with users about specific topics. More often than less, their dominant behavior is malicious, including misleading, exploiting, and manipulating the social media discourse (Ferrara et al. 2016). The term sockpuppet describes an often politically motivated fake identity on a social network used to interact with ordinary users. Lastly, hybrid accounts are identical to the earlier described cyborgs.

Not surprisingly as the research community did not establish clear and exhaustive definitions of the concept bot, also the literature going beyond simple definitions is comparably unsorted.

This might also be attributable to the fact that studies on "the characterization, detection, and impact estimation of bots are published at an impressive rate" (Cresci 2020). Cresci (2020) estimated that if this publishing trend continues, by 2021 there will be more than one new paper published per day. Given that framing, the following sorting of the bot's literature might be one possible approach out of many. Specifically, we divide the literature into three major streams: (1) The research about legitimated bots, their effects, and limitations. (2) The research about illegitimate bots, especially malicious social bots, the topics they communicate on, and their effects. (3) The research on benchmark creation and detection of malicious bots.

Diving into the first stream, it can be said that it is mostly dominated by research about chatbots. This might be because these programs often get implemented in a variety of fields, for instance, "e-commerce education", encompassing healthcare and entertainment" (Caldarini et al. 2022), to provide virtual assistance to customers. Hence their evaluation might be of interest due to educational and financial considerations. For instance, Abd-Alrazaq et al. (2019) reviewed 53 studies about chatbots used in therapy, training, and screening of mental disorders, and found that chatbots are useful tools for individuals with mental disorders. Moreover, Jenneboer et al. (2022) found a connection between chatbots and customer loyalty. Nonetheless, chatbots are not perfect, some areas for improvement are contextual and emotional understanding and gender biases. Often chatbots tend to take on traditionally feminine roles and features, thereby displaying stereotypical behavior and gender biases (Caldarini et al. 2022).

Contrary to the first rather positive connotated stream stays the research on illegitimate bots and their effects. Hereby the concentration typically lies on malicious social bots, as their possible influence on society might be harmful. One well-researched field in which social bots are active in politics, especially during election times. Not seldom do social bots increase their online presence when political interests are at stake (Cresci 2020) and try to manipulate the situation. For example, Stukal et al. (2017) found when concentrating on the tensest time of the Russo-Ukrainian War, that the proportion of Tweets produced by bots during that time exceeds 50%. Further, Ferrara (2020b) found that social bots played an important role in promoting the disinformation campaign MacronLeaks in the run-up to the 2017 French Presidential election. In addition, Ratkiewicz et al. (2021) argues that in astroturf political campaigns politically motivated individuals and organizations create multiple centrally controlled Twitter accounts to fabricate the appearance of widespread support for a candidate or opinion. Observing instead of politics the field of economy, Cresci et al. (2019a) estimates that in 2019 71% of Twitter users mentioning trending U.S. stocks, were most likely bots. He detects that coordinated groups of bots aim at promoting low-value stocks by exploiting the popularity of high-value ones. Nearly the same mechanism is practiced by social bots in cryptocurrency discussions too (Nizzoli et al. 2020). When it comes to the field of climate change Marlow et al. (2020) estimated that during a short time before and after Ex-President Donald Trump's announced the United States' withdrawal from the 2015 Paris Climate Agreement, around 17% of the tweets were created by social bots, which also more likely include links sharing denialist research. Glancing further at the online traffic related to the Covid-19 pandemic, it seems to be the case that social bots played a major part in its "infodemics" (Gallotti et al. 2020). Further, Ferrara (2020a, 2020c) found evidence that bots use COVID-19 to promote the visibility of ideological alt-right hashtags in the United States.

The last remaining stream considers literature about the detection of malicious bots. Not seldom are respective works accompanied by a self-created dataset serving as a new benchmark to evaluate developed detection procedures. Hereby the literature on bot detection can be split into three paradigms, namely individual, group, and adversarial approaches (Cresci 2020). The first work relating to bot detection was published in 2010 (Yardi et al. 2010). This and the preceding works attributable to the first paradigm have in common that they are based on supervised machine learning techniques and analyze individual accounts. Further exemplary works of this paradigm are Cresci et al. (2015) and Yang et al. (2019), while the earlier reported in addition to other techniques to support vector. Unfortunately, with the advances in the methods of detecting automated accounts, social bots advanced too. Consequently, the detectors had to adjust their methods, thus works of the 2012 upcoming second paradigm prefer systems targeting groups of accounts and unsupervised learning. One possible example of this paradigm would be Cresci et al. (2017a), in this work the authors create a Social Fingerprinting technique for modeling the behaviours of social network users. The last and most recent paradigm of the bot detection literature is still not very advance. It is based on adversarial learning, which is, as "all tasks related to the detection of online deception, manipulation and automation are intrinsically adversarial" (Cresci 2020), very promising. These adversarial learning methods could be used for example to create synthetic bots as in the work of Cresci et al. (2019b), hence enabling the creation of better training data and detection systems proactively.

# 3. Theory

Given that a common ground about the understanding of the term bot and its variations was established, as well as the three major streams in the bot literature were characterized, the purpose of the underlying section is to build on this foundation to outline the research interest of the underlying work and their scientific relevance.

As one could read the literature about bots is quite broad and comparably hard to narrow down. Most research works seem to concern just very specific aspects of bot behavior, bot characteristics, effects of bots, and bot detection. Moreover, they are often limited to particular fields like politics or economy. More general research approaches considering multiple of these subjects in one work seem to be barely existent. Not to forget to mention the circumstance, that the first two research streams seem to be biased towards the study of either rather positive or negative effects and are mainly limited to the observance of chatbots and social bots.

Thus, we attempt the extend the literature, precisely its second stream considering illegitimate bots, by resorting to a more general and less one-sided approach. By relying on the Twibot-20 data set, which indicates valid users and social bots on the free social media and microblogging platform Twitter, we want to draw a more diverse picture of what topics bots are communicating on Twitter, and if the main fields they are interested in overlap with the ones of valid users. Further, we would like to study how social bots communicate on these topics, do they tend to frame their subjects more positively or negatively? Retrieving such an overview of their topic framing would allow reasonings about their intentions and possible effects in fields prone to their influence, and consequently, also highlight areas for further research. To put it simply, we ask ourselves can we confirm the theory about malicious social bots? Given that framework, the underlying work tries to answer the following explorative research questions:

- I. What are the major "hot topics" that social bots and valid users communicate on, on Twitter?
- II. How do social bots connote the "hot topics" they communicate on, on Twitter?
- III. Can the preferred connotations of "hot topics" of social bots on Twitter be attributed to malicious intentions?

Obviously by glancing at these questions one might figure out that research question III. is not only of scientific and public interest but also relatively difficult to answer. In this case, we can just be answered approximately.

#### 4. Data and Methods

#### 4.1) Data

In the following subsection the data basis of the underlying work and to it applied preprocessing steps get explained. Particularly the used data basis is the 'TwitBot-20' (Feng et al., 2020), which was built with the purpose of being the main benchmark for bots detection in the Twittersphere at the time of 2020¹. The data collection strategy of 'TwitBot-20' made use of breadth-first search algorithm starting with different root nodes, namely seed users, trying to represent the platform's diversity. To achieve this goal, the design of the search took the subjects 'politics', 'business', 'entertainment' and 'sports' as domains, which greatly overlap over the Twitter users, and unlike previous datasets not only focus on specific subjects. A total of 40 'seed users', equally distributed, came from these domains. The extraction period was between July and September 2020, so we expect to see this context in our results.

The TwitBot-20 dataset contains information on 229.573 users, 33.488.192 tweets, 8.723.736 user property items and 455.958 follow relationships. In terms of user information, the last 200 tweets were extracted to capture semantic information. Further, the property information provided by the Twitter API and neighbourhood information (followers and followings) was extracted. In the aftermath of the data retrieval the dataset was manually annotated under 5 'bots' characteristics: "lack of pertinence and originality in tweets, highly automated activity and API usage, tweets containing external link promoting phishing or commercials, repeated tweets with identical content and tweets containing irrelevant URLs" (Feng, et.al, 2020. p.3).

In total the dataset is subdivided in 4 different files: training, dev, test, and support where users in training, dev and test are labelled as bots (1) and valid users (0). Since the goal of our research is to explore the content shared by bots, which is out of the scope of bot detection, only files with labelled data were used. Further, the scope of this study is on English speaking countries, specific the US and UK, and on English tweets. After the application of this filtering the final dataset contained a total of 4.862 users (bots and valid users) and 95.314 tweets.

The preprocessing techniques applied afterwards over the reduced dataset consist in removal of hashtags, retweets ("RT"), mentions, emojis, smiles, links, audiovisuals and the strip of punctuation. As tweets are small sequences of 280 words, stopword removal and lemmatization were not applied, as they could have generated changes in the meaning of the tweets what would be inappropriate considering the later applied methodological procedure.

<sup>&</sup>lt;sup>1</sup> The data set owners Feng et al (2020) are currently also in the building of a 2022 version of the 'TwitBot-20' - the TwitBot-22' (Feng et al., 2022).

Table 1: Dataset frequency for users per country

	Bots	Valid Users	US	UK
User	2022 2809		3989	842
Total Users	4831		4831	
Tweets	34026	46514	66688	13852
Total Tweets	80540		805	540

#### 4.2) Method

Since what must be answered is already outlined, how it should be answered must be discussed. In consequence, the following subsection presents the methodological basis, which is used to tackle the three presented research questions.

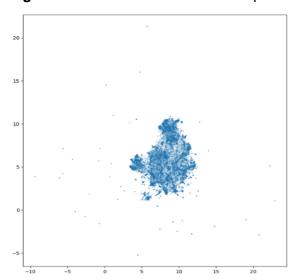
Starting with a glance at the tweet text data at hand and thinking about what is necessary to approach the stated research questions, the first step should be to map each tweet in a vector space to allow the later application of a clustering algorithm to the data. Accordingly, this vectorization process should be done in such a way, that semantically more similar tweets are closer to each other. This vectorization gets implemented by using a general-purpose sentence transformer model<sup>2</sup>, which is under the hood a modified high-performance version of the pretrained BERT network adjusted to sentence structures by using siamese and triplet network structures (Reimers & Gurevych, 2019). Therefore, the model enabled us to retrieve semantically meaningful embeddings for the tweet text data.

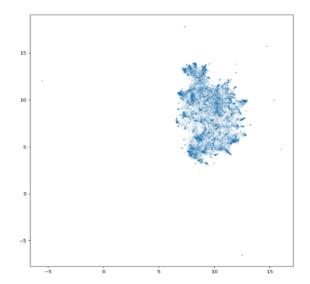
Before proceeding with the clustering of the tweet vector data, the vectors should be reduced in dimensionality, as the computing time of clustering algorithms scales with the dimensionality of to be clustered data. Since each tweet is after the embedding procedure represented by a vector of 768 dimensions, this reduction seems reasonable. The dimension reduction technique of choice is UMAP3, which is a manifold learning technique for dimension reduction developed from a theoretical framework based on Riemannian geometry and algebraic topology. UMAP's advocates, which led to its selection to solve the dimension reduction task, are that it is a well scalable algorithm, that enables good visualizations, which has no computational restrictions on the number of embedding dimensions, and it preserves global structures well (McInnes et al., 2018). With the help of UMAP, we reduced the vector data to a dimensionality of 5 and could apply on top of these results a selected clustering algorithm. Inevitably the question must be asked, which algorithm should be used. To stick to an educated selection practice, we choose to first visualize the embeddings before applying any clustering algorithm to it, that way we can scan the shape of our data and make a suitable algorithm choice. The scatterplots of the to two dimensions reduced tweet vectors for social bots and valid users look thusly:

<sup>&</sup>lt;sup>2</sup> We used the "all-mpnet-base-v2" model of the python library "sentence\_transformers" (Reimers & Gurevych, 2019).

<sup>&</sup>lt;sup>3</sup> We implemented the UMAP algorithm by using the function "UMAP" of the python library "umap-learn", which is based on the mathematics of the work from McInnes et al. (2018).

Figure 1: Bot and valid user data shapes after reduction via UMAP to 2-dimensions

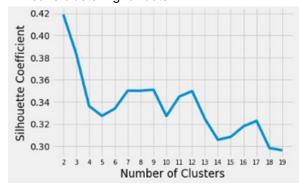




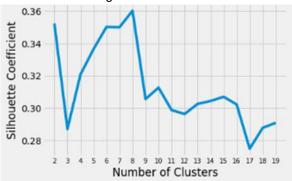
While inspecting these visualisations more closely, we came to the resolution that a density-based clustering method would be the best choice to stick with, as: (1) The clustering structure does not seem to be spherical. (2) There are regions of higher dimensionality, separated by regions of lower dimensionality. (3) Outliers seem to be existed. (4) A purely hierarchical clustering does not seem to be appropriate for answering the outlined research questions.

In addition, to reassure our choice in favour of a density-based clustering method, we choose to calculate the average silhouette coefficient for multiple k-Means<sup>4</sup> clusterings. The coefficients development for bots and valid user, for a k ranging from 2 to 20, look as follows:

**Figure 2:** Silhouette Coefficient analysis for k-Means clustering for bots



**Figure 3:** Silhouette Coefficient analysis for k-Means clustering for valid users



Having in mind that the silhouette coefficient varies from -1 to 1, while values near 1 indicate that the clusters are well-separated, these visualisations seem to underline the density-based clustering choice too. Being more precise, bot graphs have a local peak for low k's of 2 and do not follow a smooth continuous downwards curve which would be typical for an "elbow plot", hence this might indicate that the underlying clustering structure could be nested. Furthermore, for those interested beyond that we visualised the respective word clouds for a k-Means clustering where k is set to 2, which can be found in the appendix.

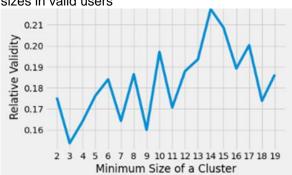
<sup>&</sup>lt;sup>4</sup> For retrieving the average silhouette coefficient and implementing the k-Means algorithm we used the functions "silhouette\_score" and "KMeans" of the respective modules "sklearn.metrics" and "sklearn.cluster" from the python library "scikit-learn" (Pedregosa et al., 2011).

As a next step, we planned to apply the HDBSCAN<sup>5</sup> clustering algorithm to the 5-dimenisonal tweet vector data. HDBSCAN is an algorithmic improvement over OPTICS that performs DBSCAN over varying epsilon values and selects the clustering resulting in the best stability over epsilon. Being less technical, the algorithm generates a complete density-based clustering hierarchy from which a simplified hierarchy composed only of the most significant clusters gets extracted. The algorithms needs only one input parameter, namely a lower bound for the minimum size a final cluster can have (Campello et al., 2013). Furthermore, besides these advantages we relied on HDBSCAN as it works quite well with chosen dimension reduction technique UMAP. Nonetheless, the factor that HDBSCAN relies on just one parameter can also be a disadvantage, if the respective parameter does not get selected appropriately. Therefore, we choose to calculate the relative validity<sup>6</sup>, an approximation of the DBCV score, for different minimum cluster size values to evaluate which value should be preferred for the parameter (Moulavi et al., 2014). The graphical display for the DBCV scores for social bots and valid users, for minimum cluster sizes ranging between 2 and 20, looks as follows:

Figure 4: DBCV score for minimum cluster sizes in bots



**Figure 5:** DBCV score for minimum cluster sizes in valid users



Since the DBCV is like the silhouette coefficient a relative validity criterion, ranging from -1 to +1, it can be interpreted in the same manner. Implying greater values of the measure indicating better clustering solutions. The important difference to the silhouette coefficient is that it is applicable to the results of density-based clustering methods, as it takes density and shape properties of clusters into account and deals with (Moulavi et al., 2014). Hence, given the displayed results we choose to select for the HDBSCAN algorithm a minimum cluster size of 15 for the social bot and of 14 for the valid user data. For those eagerly interested, we visualised the respective HDBSCAN clustering for 2 dimensions in the appendix.

After gaining the clustering results, we aimed to know what lead to its specific structure. This means we want to know in which way do the clusters differ between each other based on their content? Answering this query would allow to answer the first research question. Therefore, we decide to extract the topics of the retrieved clustering by treating each cluster as one topic and use a class-based variant of TF-IDF<sup>7</sup>. Precisely, we apply TF-IDF to the clusters, while treating each cluster as one complete document, thus the resulting TF-IDF score would demonstrate the important words

<sup>&</sup>lt;sup>5</sup> We relied on the function "HDBSCAN" of the python library "hdbscan" to implement the HDBSCAN algorithm (Campello et al., 2013).

<sup>&</sup>lt;sup>6</sup> The relative validity is a retrievable object attribute of a HDBSCAN clustering constructed through the function "HDBSCAN" of the python library "hdbscan". It just approximates the DBCV and is computed using the mutual- reachability minimum spanning tree, instead of the all-points minimum spanning tree. The resulting values are no objective measure of the goodness of clustering but can be used to compare results relying on different hyper-parameters.

<sup>&</sup>lt;sup>7</sup> The term frequency-inverse document frequency is a statistic that reflects how important a word is to a document in a corpus. An explanation of how to derive a class-based version of it is done by Grootendorst (2020, October 5).

in a document, and since we the words document and topic can be used in this case interchangeably, we retrieve the words primarily defining a topic. Due the massive number of topics for both, social bots and valid user, we decide to just concentrate on the 5 most important per group.

Remembering that we do not wish to just extract the topical structure of the clustering but also grab a sense of how the topics a connotated and if this connotation could be attributed to malicious intends of the social bots, we carried out a sentiment analysis<sup>8</sup> on the individual tweet level. Hereby the tweets get labelled with two polarities – positive and negative. By doing so we can extract the pre-dominant sentiment per topic.

Finally, although we already validated the parameter selection of the clustering algorithm by calculating the DBCV score, we intended further to validate the clustering itself. Therefore, we randomly sample 300 tweets of the social bot and valid user data, and manually label them by hand for the 5 biggest topics. For this task we did not rely on a precisely developed coding schema, but rather on our impression what the five biggest topics for social bots and valid users are and labelled the tweets respectively. After each author of the underlying work labelled the in total 600 tweets individually the Inter-rater Reliability gets calculated, in the given case the percent agreement for two raters, to get an idea on how the encoding is. Finally, this procedure was replicated under those 'agreed' cases for both raters and were compared with the clustering method, getting a validation over the general dataset and each topic in specific, to view if the derived results of the topic extraction can be justified.

#### 5. Results

In this section, we analyse the results obtained after the application of the outlined methodological procedure, meaning after the clustering process with HDBSCAN, the sentiment analysis, and topic extraction. Hereby we are comparing bots and valid users under the scope of the US and UK. This section will finish with a short summary of the major findings.

#### 1) HDBSCAN Topic Modeling Results

The following analysis is focused on the five largest clusters for both, bots and valid users. This selection is mainly due the vast number of extracted topics, which cannot be discussed completely due the scope of this work. Respectively, after we applied the HDBSCAN clustering algorithm and extracted the topics, we retrieved a total of 198 clusters for bots and 290 for valid users. In both cases the -1 cluster, called the "outlier" cluster, appears, which refers to all documents that did not have any topic. Is important to note that when extracting topics this cluster not always appears. In both cases, the outlier topic represents 52% of the total tweets, what are 17857 tweets for bots and 24078 for valid users.

<sup>&</sup>lt;sup>8</sup> For implementing the sentiment analysis we relied on the sentiment classifier "TextClassifier" and the function "Sentence", creating an appropriate sentence object for the classifier, of the modules "flair.models" and "flair.data" from the python library "flair" (Akbik et al., 2018).

**Table 2:** Cluster topics for bot users, showing the top 20 words that construct them.

Topic	Size	% Total tweets	Top 20 words	Cluster name
138	1487	3.1	police, black, white, people, portland, shot, blm, antifa, man, cops, lives, amp, officers, killed, gun, matter, portland, racist, shooting, racism, protesters	Racism and Crime
204	939	2.0	chicken, cream, coffee, food, dinner, cheese, eat, recipe, ice, good, just, amp, pizza, drink, lunch, time, dinner, fish, favorite, day, best	Food and Entertainment
271	898	1.9	covid, coronavirus, virus, cases, pandemic, deaths, vaccine, new, testing, trump, cdc, people, number, just, positive, test, pandemic, tested, died, daily, health	Covid- 19
200	854	1.8	league, club, season, goal, liverpool, united, premier, fans, champions, player, players, team, messi, city, southampton, football, liverpool, goals, manchester, just, transfer	Football
286	687	1.5	market, stocks, trading, stock, fed, dow, bitcoin, amp, inflation, markets, nasdaq, week, day, just, price, tsla, fed, financial, trade, finance, rates	Stock markets

**Table 3:** Cluster topics for valid users, showing the top 20 words that construct them.

Topic number	Size	% Total tweets	Top 20 words	Cluster name
65	1281	3.8	police, black, people, white, women, officers, shot, shooting, man, amp, protests, racism, law, cops, lives, killed, women, protesters, officer, federal, violence	
137	659	1.9	covid, coronavirus, pandemic, virus, cases, deaths, people, test, positive, testing, spread, tested, trump, new, health, rate, cases, tests, quarantine, reported, amp	Covid-19
151	619	1.8	song, album, music, new, listen, video, playlist, songs, playing, love, single, live, remix, ft, just, track, listen, spotify, amp, like, feat	
169	547	1.6	life, god, dont, know, things, jesus, just, people, don, way, love, self, want, think, bitch, person, things, energy, friends, im, need	
108	447	1.3	dm, hi, help, send, sorry, email, contact, thanks, team, com, hear, experience, look, let, support, account, sorry, number, able, thank, contacting	Customer Service

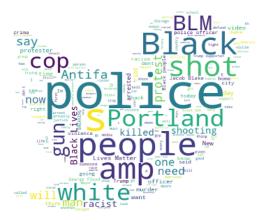
Coming back to the first exploratory research question "What are the major "hot topics" that social bots and valid users communicate on, on Twitter?", our models retrieved some shared topics and others more specific for each type of user. To begin, in both cases the larger cluster can be interpreted as "Racism and Crime" were the words with higher weight in both cases are "police", "black", "people" and "white". This clearly reflects the context of 2020, where after the death of Georg Floyd on May 25<sup>9</sup>, a series of protests took place all over the US. To get a

15

<sup>&</sup>lt;sup>9</sup> A timeline of Racial protests after the death of Georg Floyd Protest can be found in the article by Bryson(2021, November 5).

better understanding of the semantic meaning of this cluster, we selected 3 random tweets for both types of users and created word clouds. In both cases, there is not much difference in the semantic composition of the messages shared by both, bots and valid users, rather there is a difference in length between them, but this feature cannot be generalized at the moment. Thus, a more detailed analysis would be needed to deliver more insights.

**Figure 6:** Racism and Crime cluster wordcloud for bot users



**Figure 7:** Racism and Crime cluster wordcloud for valid users



Table 4: Random tweets of the Racism and Crime cluster per type of user

User	Tweet (clean)				
	"NYC is taking after Portland - a trans femme protestor was pulled into an unmarked van at the Abolition Park protest – t"				
Bot	"Yall not hating white women stealing from our culture enough for me"				
	"David and Ezra went back to the arena today, doing a follow-up story. We were on a sidewalk on public property, doing accountability journalism in the public interest. But then police pulled up and ordered them to stop, and to leave via"				
	"Be careful right now about making yourself feel better by calling people racist. This is hard work amp it won't get done in bursts of self-righteousness.I reread this story regularly to remind myself. Thank you"				
Valid User	"Protest but do it peacefully. Youre not helping the cause if youre being violent and looting.  Stay focused on what this is really about."				
	"Bloomberg went with Black and White as of last week or so. Many of us, of all races, feel a little weird about White. But there are arguments for it from across the spectrum. NABJ recommends it, for one."				

Furthermore, both type of users also shares a "Covid-19" cluster which is a consequence of the data collection period of TwitBot-20. During the collection time, the world was passing through the first waves of the virus and the clustering shows how different types of users on Twitter were sharing information about it. The following table shows some randomly sampled tweets to grab a better understanding of what was shared related to Covid-19 by bots and valid users.

Table 5: Random tweets of the Covid-19 cluster per type of user

User	Tweet (clean)				
	"Coronavirus closures could lead to a radical revolution in conservation"				
Bot	"It is important to understand that we can mitigate the spread. We are in this together! Keep your distance, wash your hands, and avoid going to social gatherings."				
	"Yesterday saw the first four positive Coronavirus cases recorded in Derry and Strabane for over a month.The Public Health Agency said this is to be expected with lockdown restrictions easing which is why the Test, Trace and Protect programme is in place."				
	"PLEASE keep our incredible doctors and nurses well and safe. It would be terrifying going to work daily under these conditions. We MUST protect them."				
Valid User	"For the average American the best way to tell if you have covid- is to cough in a rich persons face and wait for their test"				
	"Turkey confirms new coronavirus cases in the country which is the highest daily amount since June"				

Furthermore, the 3 remaining clusters for bots seem to be about "Food and Entertainment", "Football" and "Stock Markets". They do not intersect with the three remaining topics of the valid users. One can see that the words that compound the "Food and Entertainment" topic are related to types of food, for instance, chicken, cheese, and ice cream, and also the moment and feeling the food itself provides, like with words such as "lunch" and "favorite". In addition, the topic "Football" consists of words that refer to the Champions League, which took place between August 2020 and May 2021. Also, it is very interesting that the clustering algorithm resulted in a "Stock markets" topic, which is in line with what Cresci et al (2019a) and Nizzoli et al (2020) mentioned in their works. Both estimate a high volume of bot users sharing information about this financially volatile area on Twitter.

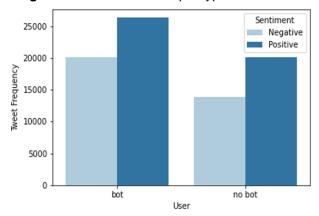
To finish this first part of the result presentation and answer the first research question, it should be mentioned that the last 3 topics shared by valid users can be sorted into the categories "Music", "Religion" and "Customer Service". This grouping of tweets could be interpreted in the way, that labor considering these areas is still being done by humans and automated accounts found no interest in them until now. Part of the top 20 words that compose the "Customer Service" cluster are "email", "contact", "support" and "team", hence we expect a stronger negative connotation for it, as relations with customers via these communication channels are often triggered due to complaints about products or bad experiences over the service provided.

#### 2) Sentiment Analysis

**Table 6:** Tweet Sentiment distribution per user type in % (total column)

%	Bots	Valid User
POSITIVE	56,7	59,1
NEGATIVE	43,3	40,9
Total	100,0	100,0

Figure 8: Tweet sentiment per type of user



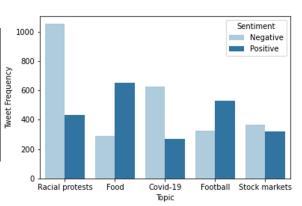
After the extraction of the topics using HDBSCAN, we applied sentiment analysis to the tweets of the preprocessed dataset to get an idea of the sentiment polarity that users give to what they share. In both, the bot and valid user sub-datasets, tweets are more positive than negative connotated, almost resembling a 60:40 distribution. We assumed a detailed analysis of the 5 most important topics per user type would bring more clarity about the results of the general sentiment, and hence proceeded likewise. This might be especially the case as the application of the tweet sentiment analysis was made over the whole data set, also including those tweets that built the -1 'outlier' topic.

#### a. Sentiment Analysis per Topic

**Table 7:** Sentiment Analysis per important topic in bot users % (total column)

%	Racism and Crime	Food	Covid -19	Footbal I	Stock markets	Total
Positive	29,1	69,2	30,3	62,1	46,9	45,3
Negative	70,9	30,8	69,7	37,9	53,1	54,7
Total	100	100	100	100	100	100

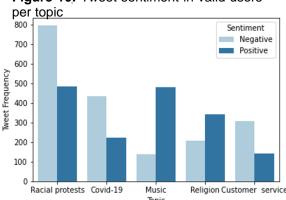
Figure 9: Tweet sentiment in bots per topic.



**Table 8:** Sentiment Analysis per important topic in valid users in % (total column)

%	Racism and Crime	Covid- 19	Music	Religi on	Custo mer service	Total
Positive	37,9	33,8	77,7	62,3	31,5	47,0
Negative	62,1	66,2	22,3	37,7	68,5	53,0
Total	100	100	100	100	100	100

Figure 10: Tweet sentiment in valid users



On a topic level, both "Racism and Crime" and "Covid-19" clusters have a negative association for bots and no bots users, whereas in no bots users this weight is higher than for bots. The same phenomena happen for the "Covid-19" cluster. These findings show somehow some insights into this expected "malicious" content social shared by bots on these platforms, but still, to properly answer our exploratory question Can the preferred connotations of "hot topics" of social bots on Twitter be attributed to malicious intents? this analysis should be fine graned which cannot be done in this research due to time limitations (which will be discussed later on). On the other hand, the tone for "Food" and "Football" topics in bots users is positive. Both subjects are related to hobbies or entertainment, therefore is not surprising that this is the given connotation. In the Football case, the share of positive meaning is lower than for Food, probably due to the passion that fans can share over social media which can lead to fights. It is interesting to note that the tone in the "Stock markets" topic is more neutral, which can also be an insight related to our last research question, where this type of user is being used with informative purposes than with a malicious intention. A random tweet was selected to zoom in a get a better feeling of what can be a bot sharing about stock markets:

"Stock Market hits new Record High. Confidence and enthusiasm abound. More great numbers coming out!"(ID: 824981224443826177, Sentiment: Positive).

Moving to no bots users, from all the topics "Customer Service" has the strongest negative meaning (67%), and as we can see words like "help" and "sorry" are part of the most important when building this cluster. Is highly possible that the negative connotation of this cluster is reflecting responses to customer complaints. Again, a random tweet was selected to get a better feeling of this:

"Hi there, we want to apologize for the frustration this has caused. Please send us a DM with your Oscar ID number so that we may escalate this issue to our team." (ID: 1603882129, Sentiment: Negative)

Wrapping up this whole analysis is interesting to check how bots and valid users share some topics and show us what was happening during the period that TwitBot-20 was built. Is important to note that both "Racism and Crime" and "Covid-19" clusters are part of the most frequent and are connotated as negative. Therefore, one main conclusion is that occurrences that are perceived as negative to the population generate an effect on what people share on their social media, these 'hot topics' are influenced by how much they affect people's lives and shows that Twitter, as a microblogging platform, allows the population to share their disconfirm towards them.

Along with these findings, the fact that a "stock markets" cluster exists in bots users with a more neutral connotation, works somehow as a validation of the assumption made by Cresci et al. (2019a) and Nizzoli et. al (2020) about bots accounts in Twitter. A more fined-grained analysis over this discovery is one of the many possible edges for the study of bots in social media.

#### 4. 3) Cluster Validation

To end with the analysis and as was stated in the method section, the clustering process needs to be validated to check how accurate the process of grouping together tweets for both types of users are and classifying them into different topics. To achieve this, the validation process consisted first of a hand-labeling of the different topics where an 'others-99' label was added when it was considered necessary. After an Inter-Rater Reliability analysis was applied by getting a percentage of agreement between the rater (both researchers in this case) and after getting this score we proceeded to calculate the same percentage but compared only those 'agree' cases with what was the output of the model. The results can be found in the following tables.

**Table 9:** Inter-Rater Reliability Score for bots

IRRS	Count	%
Agree	270	90
Disagree	30	10
Total	300	100

**Table 11:** Inter-Rater Reliability Score for valid users

IRRS	Count	%			
Agree	249	83			
Disagree	51	17			
Total	300	100			

**Table 10:** Rater-Model Reliability Score for bots

IRMRS	Count	%
Agree	260	96
Disagree	10	4
Total	270	100

**Table 12:** Rater-Model Reliability Score for valid users

RMRS	Count	%
Agree	237	95
Disagree	12	5
Total	249	100

To have a solid baseline when comparing the results of the model with the hand-labeled topics, we decided to contrast the 'agree' cases, therefore, 270 cases for bots users and 249 for valid users. For both cases, the Rater-Cluster Reliability Score was above 95% which means that the clustering method used for this research was able to capture with good accuracy different topics for both bots and valid users.

**Table 13:** Rater-Cluster Reliability % Score for bots per topic

Topic	%
Racism and Crime	93
Football	95
Covid-19	98
Food/Entertainment	98
Stock markets	100

**Table 14:** Rater-Cluster Reliability % Score for valid users per topic

Topic	%
Religion/Personal	85
Racism and Crime	95
Music	96
Covid-19	96
Customer service	100

#### 6. Discussion

In this study, we examined in an exploratory way what is the content that bots share on Twitter. The intention in picking this topic was to extend the literature about illegitimated bots by resorting to a more general and less one-sided approach. Acknowledging that this study could have gone deeper, as we specified later on in the limitations section, this work provides a description over an intended neutral scope from our part over these accounts.

By trying to keep a neutral approach over bot accounts on Twitter, a short summary of the findings of our research questions is presented in the following:

# - What are the major "hot topics" that social bots and valid users communicate on, on Twitter?

The understanding of a "hot topic" is highly associated with the time frame our used data was collected, therefore the context is an important variable while analysing the data. After applying the described methods, the clustering and topic extraction procedure enabled us to identify the hot topics of mid 2020 in the US and UK. Moreover, after the validation analysis we can state that this clustering process works well. Precisely the 5 "hottest topics" of bots could be identified as "Racism and Crime", "Food and Entertainment", "Covid-19", "Football", and "Stock markets". Future work to continue proving this diagnosis would be interesting to enable comparisons in derivations.

- How do social bots connote the "hot topics" they communicate on, on Twitter? Both positive and negative sentiment were found over the clustered topics. Nonetheless, it is very interesting that the 'hottest topics' in both, bots and valid users, are presumed as negative. So here the intention between the connotation is not clear, are bots sharing this negative content because valid users do it first? Are the negative opinions of valid users boosted by bots? Moreover, some topics like "Stock markets" get a more neutral connotation, and "Food and Entertainment" and "Football" are more positively framed.

# - Can the preferred connotations of "hot topics" of social bots on Twitter be attributed towards malicious intents?

Last but not least, it has to be stated that this research question requires a more detailed analysis and could be the start of a whole new research project. To answer this question well a precise operationalization of the term 'malicious' would be first needed and a proper analysis under the scope of this process done on tweets that are shared by bots. As we saw with the second research question, the main hot topics do get connotated more negatively by bots, but the intentions behind the framing of these messages cannot be clearly stated. A glimpse of neutrality can be found with the "Stock market" cluster, where the messages are probably more informative than contain much emotion. Nonetheless, the fact that the "Food and Entertainment", "Football", and "Stock markets" area are either connotated neutral or positive and that all three can be associated with bigger cash flows, could also be seen as evidence that bots might be stronger attracted to profitable fields and indeed serve some – moneyoriented – malicious intentions.

#### 7. Limitations

Our work faced many limitations which can also pave future edges on the study on bots tweet content. The main limitation was time, as this research is part of a seminar course, the period constraint limited the research on a specific timeframe. This limitation affected in different ways, first the deepen level this research can go. Also, it is not possible to study on detail the composition of this clusters, making comparisons in terms of type of words, length, etc that composes the same cluster by type of users. In addition to that, also due to time limitations we can not observe changes in the extracted topics over the time and finally, it was not possible to do a comparison between TwitBot-20 and the new release TwitBot-22 because the newest version comes in a different structure and due time, we could not work on it.

Along with this, another set of limitations are related to the TwitBot-20 dataset, in first place this dataset is manually labeled and we did not have the time to validate the accuracy of the label process. Also, the dataset came in 4 files were only 3 are labeled, so it was not possible to work with the entire data. Finally, the country information of users was nos given and it has to be extracted from the coordinates in those users that had that feature available.

Another important limitation to take into account is the validation strategy, as only a team of 2 person constructed this research and hand labeled a random selection of tweets to validate the clustering method, this hand-made approach can lead to bias for instance the knowledge on the specific topics that each one of us has.

Finally, as this research focuses on english speaking cuntries (more specific the US and UK), is limited on external validation and is not possible to compare what do bots share on Twitter with other languages. An extension over this aspect can lead to interesting research.

# 8. Bibliography

- Abd-Alrazaq, A. A., Alajlani, M., Alalwan, A. A., Bewick, B. M., Gardner, P., & Househ, M. (2019). An overview of the features of chatbots in mental health: A scoping review. *International Journal of Medical Informatics*, *132*, 103978. https://doi.org/10.1016/j.ijmedinf.2019.103978
- Akbik, A., Blythe, D., & Vollgraf, R. (2018). Contextual string embeddings for sequence labeling. In *COLING 2018, 27th International Conference on Computational Linguistics*.
- Bryson (2021, November 5). Georg Floyd Protests: A Timeline. *The New York Times*. https://www.nytimes.com/article/george-floyd-protests-timeline.html
- Caldarini, G., Jaf, S., & McGarry, K. (2022). A literature survey of recent advances in chatbots. *Information*, *13*(1), 41. https://doi.org/10.3390/info13010041
- Campello, R. J. G. B., Moulavi, D., & Sander, J. (2013). Density-based clustering based on hierarchical density Estimates. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, J. Pei, V. S. Tseng, L. Cao, H. Motoda, & G. Xu (Eds.), Lecture Notes in Computer Science. Advances in Knowledge Discovery and Data Mining (Vol. 7819, pp. 160–172). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-37456-2\_14
- Chu, Z., Gianvecchio, S., Wang, H. [Haining], & Jajodia, S. (2010). Who is tweeting on Twitter. In C. Gates, M. Franz, & J. McDermott (Eds.), *Proceedings of the 26th Annual Computer Security Applications Conference on ACSAC '10* (p. 21). ACM Press. https://doi.org/10.1145/1920261.1920265
- Cresci, S. (2020). A decade of social bot detection. *Communications of the ACM*, 63(10), 72–83. https://doi.org/10.1145/3409116
- Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2015). Fame for sale: Efficient detection of fake Twitter followers. *Decision Support Systems*, *80*, 56–71. https://doi.org/10.1016/j.dss.2015.09.003
- Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017). Social fingerprinting: detection of spambot groups through DNA-inspired behavioral modeling. *IEEE Transactions on Dependable and Secure Computing*, 1. https://doi.org/10.1109/TDSC.2017.2681672
- Cresci, S., Lillo, F., Regoli, D., Tardelli, S., & Tesconi, M. (2019). Cashtag piggybacking. *ACM Transactions on the Web*, *13*(2), 1–27. https://doi.org/10.1145/3313184
- Cresci, S., Petrocchi, M., Spognardi, A., & Tognazzi, S. (2019). Better safe than sorry. In P. Boldi, B. F. Welles, K. Kinder-Kurlanda, C. Wilson, I. Peters, & W. Meira (Eds.), *Proceedings of the 10th ACM Conference on Web Science* (pp. 47–56). ACM. https://doi.org/10.1145/3292522.3326030
- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, É. (2011). Scikit-learn: Machine learning in python. *Journal of Machine Learning Research*, *12*(85), 2825–2830. http://jmlr.org/papers/v12/pedregosa11a.html
- Feng, S., Tan, Z., Wan, H., Wang, N., Chen, Z., Zhang, B., ... & Luo, M. (2022). TwiBot-22: Towards Graph-Based Twitter Bot Detection. *arXiv preprint arXiv:2206.04564*.
- Feng, S., Wan, H., Wang, N., Li, J., & Luo, M. (2021). TwiBot-20: A comprehensive Twitter bot detection benchmark. In G. Demartini, G. Zuccon, J. S. Culpepper, Z. Huang, &

- H. Tong (Eds.), *Proceedings of the 30th ACM International Conference on Information & Knowledge Management* (pp. 4485–4494). ACM. https://doi.org/10.1145/3459637.3482019
- Ferrara, E. (2020). # covid-19 on twitter: Bots, conspiracies, and social media activism. *ArXiv Preprint ArXiv:* 2004.09531.
- Ferrara, E. (2020). Bots, elections, and social media: A brief overview. In K. Shu, S. Wang, D. Lee, & H. Liu (Eds.), *Lecture Notes in Social Networks. Disinformation, Misinformation, and Fake News in Social Media* (pp. 95–114). Springer International Publishing. https://doi.org/10.1007/978-3-030-42699-6\_6
- Ferrara, E. (2020). What types of COVID-19 conspiracies are populated by Twitter bots? *First Monday.* Advance online publication. https://doi.org/10.5210/fm.v25i6.10633
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96–104. https://doi.org/10.1145/2818717
- Gallotti, R., Valle, F., Castaldo, N., Sacco, P., & Domenico, M. de (2020). Assessing the risks of 'infodemics' in response to COVID-19 epidemics. *Nature Human Behaviour*, *4*(12), 1285–1293. https://doi.org/10.1038/s41562-020-00994-6
- Gilani, Z., Farahbakhsh, R., & Crowcroft, J. (2017). Do bots impact Twitter activity? In R. Barrett, R. Cummings, E. Agichtein, & E. Gabrilovich (Eds.), *Proceedings of the 26th International Conference on World Wide Web Companion WWW '17 Companion* (pp. 781–782). ACM Press. https://doi.org/10.1145/3041021.3054255
- Gorwa, R., & Guilbeault, D. (2020). Unpacking the social media bot: A typology to guide research and policy. *Policy & Internet*, *12*(2), 225–248. https://doi.org/10.1002/poi3.184
- Grootendorst (2020, October 5). Topic Modeling with BERT. Leveraging BERT and TF-IDF to create easily interpretable topic. *Towardsdatascience*. https://towardsdatascience.com/topic-modeling-with-bert-779f7db187e6
- Jay (2022, August) Number of Twitter Users 2022/2023: Demographics, Breakdowns & Predictions. *Finances Online*.
- Jenneboer, L., Herrando, C., & Constantinides, E. (2022). The impact of chatbots on customer loyalty: A systematic literature review. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(1), 212–229. https://doi.org/10.3390/jtaer17010011
- Leonard, A. (1998). Bots: The origin of new species. Penguin Books.
- Marlow, T., Miller, S., & Roberts, J. T. (2020). *Twitter discourses on climate change:*Exploring topics and the presence of bots. https://doi.org/10.31235/osf.io/h6ktm
- McInnes, L., Healy, J., & Melville, J. (2018). UMAP: Uniform manifold approximation and projection for dimension reduction. *arXiv preprint arXiv:1802.03426*.
- Moulavi, D., Jaskowiak, P. A., Campello, R. J. G. B., Zimek, A., & Sander, J. (2014). Density-Based Clustering Validation. In M. Zaki, Z. Obradovic, P. N. Tan, A. Banerjee, C. Kamath, & S. Parthasarathy (Eds.), *Proceedings of the 2014 SIAM International Conference on Data Mining* (pp. 839–847). Society for Industrial and Applied Mathematics. https://doi.org/10.1137/1.9781611973440.96
- Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., & Ferrara, E. (2020). Charting the landscape of online cryptocurrency manipulation. *IEEE Access*, *8*, 113230–113245. https://doi.org/10.1109/ACCESS.2020.3003370
- Ratkiewicz, J., Conover, M., Meiss, M., Goncalves, B., Flammini, A., & Menczer, F. (2021). Detecting and tracking political abuse in social media. *Proceedings of the International AAAI Conference on Web and Social Media*, *5*(1), 297–304. https://ojs.aaai.org/index.php/ICWSM/article/view/14127

- Reimers, N., & Gurevych, I. (2019). *Sentence-BERT: Sentence embeddings using Siamese BERT-networks*. https://doi.org/10.48550/ARXIV.1908.10084
- Smialek (2018, May 21). Twitter Bots May Have Boosted Donald Trump's Votes by 3.23%, Researchers Say. *Time*. https://time.com/5286013/twitter-bots-donald-trump-votes/
- Stieglitz, S., Brachten, F., Ross, B., & Jung, A.-K. (2017). Do social bots dream of electric Sheep? A categorisation of social media bot accounts. https://doi.org/10.48550/ARXIV.1710.04044
- Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2017). Detecting bots on Russian political Twitter. *Big Data*, *5*(4), 310–324. https://doi.org/10.1089/big.2017.0038
- Varol, O., Ferrara, E., Davis, C., Menczer, F., & Flammini, A. (2017). Online human-bot interactions: Detection, estimation, and characterization. *Proceedings of the International AAAI Conference on Web and Social Media*, 11(1), 280–289. https://ojs.aaai.org/index.php/ICWSM/article/view/14871

#### 9. Statement of Contributions

The authors confirm their contribution to the paper and writing of its underlying script as follows:

#### **Trinidad Bosch:**

- Code: Data Preprocessing, K-Means Clustering, HDBSCAN Clustering, Sentiment Analysis, Visualisations, Validation
- Introduction
- State-of-the-art
- Data
- Analysis
- Validation
- Discussion
- Limitations

#### **Gina-Maria Unger:**

- Code: Data Scraping, Data Preprocessing, Embedding Extraction (sentence-transformer, UMAP), Silhouette coefficient, DBCV, Topic extraction, Visualisations
- Abstract
- Introduction
- State-of-the-art
- Theory
- Methods
- Analysis

# 10. Appendix

Word clouds for k-Means clustering for social bots (left) and valid users (right) for k=2:









2-dimensional visualisation of the HDBSCAN clustering for social bots (left) and valid users (right) given respective minimum cluster sizes of 15 and 14:

