Güv. Str. Derg. 2024, 20:47, 99-122

Arastırma Makalesi DOI: 10.17752/guvenlikstrtj.1396705 Research Article

Social Media as an Agent of Influence: Twitter Bots in Russia - Ukraine War

Bir Etki Ajanı Olarak Twitter: Rusya-Ukrayna Savaşında Twitter Botları

Muhammed Hayati TABAN*

İsmail GÜR**

Asst Prof Turkish National Defence University. Alparslan Defence Sciences and National Security Institute, Intelligence Studies Department, Ankara, Türkiye, ORCID:0000-0003-1785-9965, e-mail: mhtaban@kho.msu.edu.tr

** Ph.D Student, Hacettepe University, Actuarial Sciences Ankara, Türkiye, ORCID: 0000-0001-7014-4606 e-mail: igur44@gmail.com

Geliş Tarihi / Submitted: 27.11.2023

Kabul Tarihi / Accepted: 31.01.2024

Abstract

The world has been witnessing a war in Ukraine since Russia started its attacks on 24 February 2022. At this point, Russia has not only deployed its troops but also put its Twitter bots to work. The war has both covered conventional spaces and unconventional spaces like social media. In this regard, our study aims to understand to what extent bots were used by Russia during the first eight days of the war. To this end, we collect data between the 24th of February and the 4th of March. On data collection, we carry out a bot prediction for collected tweets. Findings suggest that Twitter reacted to bots quite quickly and that Russia could not manage to exploit the Russian Twitter sphere as much as it did before. Therefore, Russia chose to block Twitter.

Keywords: Twitter, Bots, Russia, Ukraine, Social Media Intelligence

Rusya'nın 24 Şubat 2022'de başlattığı saldırıdan bu yana dünya Ukrayna'da bir savaşa tanıklık ediyor. Bu sayasta Rusya'nın sadece askerlerini konuslandırmakla kalmadığını, aynı zamanda Twitter botlarını da devreye soktuğuna tanıklık etmekteyiz. Rusya-Ukrayna savaşı bu açıdan hem geleneksel hem de sosyal medya gibi geleneksel olmayan alanlarda süregelmektedir. Bu bağlamda, çalışmamız savaşın ilk 8 gününde botların Rusya tarafından ne ölçüde kullanıldığını anlamayı amaçlamaktadır. Bu amaçla 24 Subat ile 4 Mart tarihleri arasında Twitter'dan veri toplanmıştır. Veriler toplandıktan sonra, elde edilen tweetler için bir bot tahmini gerçekleştirilmiştir. Bulgular, Twitter'ın botlara oldukça hızlı tepki verdiğini ve Rusya'nın Rus Twitter atmosferini eskisi kadar istismar edemediğini göstermektedir. Bu acıdan düsünüldüğünde Rusya'nın Twitter'ı neden engellemeyi sectiği daha iyi anlaşılmaktadır.

Anahtar Kelimeler: Twitter, Botlar, Rusya, Ukrayna, Sosyal Medya İstihbaratı



Introduction

Since Russia first attacked Ukraine on 24 February 2022, we have been witnessing one of the most important armed conflicts in Europe after World War II. As of October 2023, the Office of the United Nations High Commissioner for Human Rights (OHCHR) recorded 27.768 civilian casualties in the country: 9.806 killed and 17.962 injured. And there is another casualty: "truth". Especially in difficult times like crises, conflicts and wars, truth is among the first values we lose. Today, it is lost within the limitless boundaries of social media with the help of new developments.

It is undeniable that social media has been a part of our everyday lives for a while. It has almost replaced the traditional media tools. Every day more and more people give up buying newspapers and start getting the news from social media. According to October 2023 statistics, 4,95 billion people use social media worldwide.² As a result, people are exposed to propaganda and disinformation through social media more than ever.³ This exposure paves the way for malicious purposes. More specifically, those, who need manipulation, resort to social media immediately, as social media is the easiest and fastest way to achieve it.⁴ To put it simply, social media platforms can turn into a warfare zone (for information wars) and parties of a conflict put their effort into winning this war too. At times of conflict, it is believed that the more you lie, the less you need to use real weapons, therefore you will not even need to shoot a bullet if you can prove the success of your propaganda.⁵

The power of social media is doubled with the introduction of automated programs like bots. Due to being easy, cost-effective and prevalent, social media is exploited with automated programs especially at times of crises at both local and global scale. During the said times, accuracy and truth are replaced with confusion and distortion of truth by entities who need public manipulation. At this point, political actors, governments, and parties in a conflict employ social media tools to shape public opinion. Especially during conflicts, social media plays a significant role in influencing domestic opinion, shaping international opinion, and winning hearts and minds within conflict zones. Therefore the impact of social media has reached to a point in which it has becomes a weapon that is available for anyone to use and bots are useful power amplifiers of this weapon.

100 Vol: 20 Issue: 47,

¹ Office of The High Commissioner for Human Rights, "Ukraine: Emergency-UNHCR Data Portal," October 2023, https://data.unhcr.org/en/documents/download/104244, accessed 11.11.2023

² Statista, "Number of Social Media Users Worldwide as of October 2023", https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=Of%20this%20total%2C%204.95%20billion,population%2C%20were%20social%20media%20users, accessed 28.12.2023

³ Kai Shu et al., "Fake News Detection on Social Media: A Data Mining Perspective," *ACM SIGKDD Explorations Newsletter* 19:1, 2017, p. 12.

⁴ Caroline Jack, "Lexicon of Lies: Terms for Problematic Information" (Data & Society Research Institute, 2017),

^{3,} https://datasociety.net/wp-content/uploads/2017/08/DataAndSociety_LexiconofLies.pdf, accessed 11.11.2023.

⁵ Andrei Aliaksandrau, "Brave New War: The Information War between Russia and Ukraine", *Index on Censorship* 43:4, 2014, p. 57.

⁶ Samuel C. Woolley and Philip N. Howard, "Social Media, Revolution, and the Rise of Political Bot", Piers Robinson, Philip M. Seib & Romy Fröhlich (eds.), *Routledge Handbook of Media, Conflict and Security*, New York, NY, 2017, p. 287.

⁷ David Miller, Piers Robinson and Vian Bakir, "Propaganda and Persuasion in Contemporary Conflict", Piers Robinson, Philip M. Seib & Romy Fröhlich (eds.), *Routledge Handbook of Media, Conflict and Security*, Routledge, New York, NY, 2017, p. 309.

⁸ Mariam Orabi et al., "Detection of Bots in Social Media: A Systematic Review", *Information Processing & Management* 57:4, 2020, p. 1.

As far as Twitter⁹ is concerned, it has a different place for disinformation campaigns than all other social media platforms. Most importantly, its features allow for easier exploitation especially by automated programs (bots) as long as they do not violate the Terms of Service. Hence, anyone or any group can use Twitter to manipulate Twitter users.¹⁰ As it gets so common to use bots on Twitter, it becomes easy to share (fake) news, distort reality, and facilitate global engagement.¹¹

To fight against this threat, the Twitter company started a deep investigation, after the 2016 United States (US) presidential elections and disclosed 3.814 Russian state-sponsored accounts on demand by US authorities. ¹² Furthermore, Twitter updated its policies and analysis about bots, launched an Information Quality initiative, and hardened its stance against the bots. ¹³ As we see in detail in the following sections and mentioned in Twitter's statement about the 2016 US presidential elections, Russia is among those who exploit Twitter many times for disinformation purposes. After the Russian attacks on Ukraine, Twitter took quick measures and even limited content from more than 300 official Russian government accounts, including that of Russian President Vladimir Putin. ¹⁴ As a reaction to these developments, Russia chose to block access to Twitter. ¹⁵

This study aims to understand how social media, Twitter in our case, was employed by Russia in the Russian Twitter-sphere (Russian-speaking Twitter users) during the first eight days of its attacks on Ukraine and why Twitter was blocked. To this end, we use Russian tweets by specific keywords collected through Twitter API and we focus on the eight days between 24 February 2022 (the start of the attacks by Russia) and 4 March 2022 (the Twitter ban by Russia) to understand the first wave of disinformation by bots together with attacks on the field. The use of bots is the focus point of the study because the literature on Russian disinformation suggests that the use of bots is one of the main tactics of Russian disinformation campaigns. Therefore, we will try to uncover to what extent Russia used bots during the first days of the conflict by using a bot detector, Tweetbotornot2.

In the following sections, we first explain disinformation on social media and the usage of bots within this context. We visit literature and try to put forth how social media is studied in the context of disinformation and propaganda. Then, we try to explain the understanding of bots' usage in social media. In the second part, we seek to describe Russian disinformation on social media and its strategies during critical moments. This brings us to build our research hypothesis. Then, we offer our data, methodology, and the findings of our research. In the end, we present a summary, the limitations of this study, and suggestions for future studies.

⁹ Twitter was renamed as "X" after being acquired by X Corporation by Elon Musk in 2022. However, the study was conducted while its official name was Twitter, so "Twitter" was chosen for the rest of the study. After the acquisition, the Twitter authentication protocol was terminated for academic uses, through which 10 million Tweets per month were allowed to be obtained.

¹⁰ Samuel C. Woolley and Philip Howard, "Computational Propaganda Worldwide: Executive Summary", *The Computational Propaganda Project*, 2017, p. 6.

¹¹ Yevgeniy Golovchenko, Mareike Hartmann, and Rebecca Adler-Nissen, "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation," *International Affairs*, 94:5, 2018, p. 977.

¹² US. Department of Justice, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," 2019, https://www.justice.gov/archives/sco/file/1373816/download, accessed 03.05.2022.

¹³ Twitter, "Update on Twitter's Review of the 2016 US Election", January 19, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html, accessed 03.05.2022.

¹⁴ James Clayton, "Twitter Moves to Limit Russian Government Accounts", April 5, 2022, https://www.bbc.com/news/technology-60992373, accessed 03.05.2022.

¹⁵ Luke Harding, "Russia Blocks Access to Facebook and Twitter", March 4, 2022, https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter, accessed 03.05.2022.

1. Disinformation on Social Media and Bots

In addition to bot analysis, Twitter is a rich source for many different kinds of studies. For example, Tasdelen examines the online reflections of hate speech against immigrants on Twitter to determine how hate speech against refugees is carried out online. She collects 1545 tweets related to the hashtag on Twitter and analyse them through content analysis. 16 Atabek analyses Tweets of local political figures to understand the difference between two different political communication styles.¹⁷ Agralı, Sökün and Karaaslan focus on Tweets about the İzmir Earthquake that took place in October 2020. They try to understand if such analysis can be used to make social inferences on time. They use data mining and natural language processing (NLP) methods. 18 Mehmetcik, Koluk and Yüksel aim to understand the perception of Turkey among US Members of Congress. To this end, they analyse Twitter data from 2009 to 2021 by using statistical methodologies, network analysis, computational text analysis, and topic modelling tools. 19 Yılmaz, Elmas and Eröz investigates how language is used to produce online discourses in tweets about refugees in the aftermath of a major social triggering event in Türkiye. They use critical discourse analysis of a randomly selected subset of 100 tweets for this purpose. ²⁰ Kortunay analyses the usage of Twitter by universities in Turkey from a marketing perspective. She focuses on the Official Twitter accounts of 40 universities (20 of which are state universities, 20 of which are foundation universities) and uses Nvivo 11 for the study.²¹ Cam, Cam, Demirel and Ahmed conduct a sentiment analysis combining the lexicon-based and machine learning (ML)-based approaches in Turkish to investigate the public mood for the prediction of stock market behaviour in BIST30, Borsa Istanbul.22

The focal point of this study is disinformation analysis. Disinformation is not a new term, but it is best to start by clarifying this term. Though disinformation, misinformation, and propaganda can be used interchangeably, they are essentially different. From the general to the specific terms, we can say that propaganda is the umbrella concept including strategies and methods to manipulate people about a topic. In this sense, disinformation is the deliberate act of spreading misleading or false information to deceive people. On the other hand, misinformation carries also deceitful and false messages, but the intent of the spreader is not deliberate.²³ Here, we can say that disinformation is deliberately created to achieve a distortion of realities and facts.²⁴

¹⁶ Birgül Taşdelen, "Twitter'da Suriyeli Mültecilere Karşı Çevrimiçi Nefret Söylemi: #suriyelileriistemiyoruz", Gümüşhane Üniversitesi Sosyal Bilimler Enstitüsü Elektronik Dergisi, 11:2, 2020, pp. 562-575.

¹⁷ Ümit Atabek, "Twitterda Yerel Siyasal İletişim: Türkiye'de İki Farklı Tarz", *Galatasaray Üniversitesi İletişim Dergisi*, 2020, p. 33.

¹⁸ Özgür Agralı, Hakan Sökün and Enis Karaaslan, "Twitter Data Analysis: Izmir Earthquake Case", *Journal of Emerging Computer Technologies*, 2:2, 2022, pp. 36-41.

¹⁹ Hakan Mehmetcik, Melih Koluk and Galip Yüksel, "Perceptions of Turkey in the US Congress: A Twitter Data Analysis", *Uluslararası İlişkiler Dergisi*, 19:76, 2023, p. 69-89.

²⁰ Fahri Yılmaz, Tugay Elmas and Betil Eröz, "Twitter-Based Analysis of Anti-Refugee Discourses in Türkiye", *Discourse & Communication*, 17:3, 2023, pp. 298-318.

²¹ Nevin Kortunay, "Turkish Universities' Use of Twitter: A Content Analysis", *Pamukkale Social Sciences Institute Journal*, 56, 2023, pp. 267-279.

²² Handan Cam et al., "Sentiment Analysis of Financial Twitter Posts on Twitter with the Machine Learning Classifiers", *Heliyon* 10:1, 2024.

²³ European Commission, "Joint Communication To The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions", 2018, https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf; accessed 20.11.2022, Andrew M. Guess and Benjamin A. Lyons, "Misinformation, Disinformation, and Online Propaganda", Nathaniel Persily & Joshua A. Tucker (eds.), Social Media and Democracy: The State of the Field, Prospects for Reform, 1st ed, 2020, p. 10-11, Jack, "Lexicon of Lies," pp. 2-3.

²⁴ Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking", Council of Europe Strasbourg, 2017, p. 20.

As mentioned earlier, social media is one of the means by which disinformation is commonly used to manipulate public opinion in recent years. The past decade has seen the rapid development of studies which indicate that social media has a significant role in spreading manipulative disinformation campaigns during elections, political scandals, and national security crises.²⁵ Furthermore, disinformation in social media has become a public loss that strong institutions even felt the necessity to take steps. To this end, the European Commission prepared its action plan against disinformation in 2018.²⁶

Automation is a common tool for disinformation, such that automated content is beyond our predictions. Twitter bots are among these kinds of automation. They perform simple, repetitive, and robotic tasks. This way they can both create their own content and interact with other users. Bots are also difficult to track because they can be deployed anywhere, including cloud computing environments, digital devices, and appliances. Therefore, bots are effective tools aiming at strengthening online propaganda and manipulation.²⁷ They can also mimic human accounts to amplify or choke certain messages distributed on social media.²⁸ They can hide their bot identity by mimicry and they can seem to be interesting to normal users by doing window dressing.²⁹ To illustrate, bots don't tweet or retweet about a specific agenda all the time, they sometimes post tweets about ordinary topics.³⁰ They can also create a network of bots (botnet) that can accomplish a coordinated social media campaign.³¹ Caldarelli et al. use a different term for coordinated bot accounts and call them "bot squats".³² These campaigns supported by automated programs are even called with a new term "computational propaganda".³³

There is a consensus among studies that bots are common on Twitter for different purposes. The number of bots and the percentage may vary depending on time and topic. A study carried out in 2016 claims that about 8.5% of all Twitter users are bots.³⁴ Varol et al. go

²⁵ Emilio Ferrara et al., "The Rise of Social Bots," *Communications of the ACM*, 59: 7, 2016, p. 96,; Timothy Graham et al., "Like a Virus: The Coordinated Spread of Coronavirus Disinformation", *The Australia Institute*,2020, https://eprints.qut.edu.au/202960/1/P904_Like_a_virus_COVID19_disinformation_Web_.pdf, accessed 18.10.2022; Tobias R. Keller and Ulrike Klinger, "Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications," *Political Communication*, 36:1, 2019, pp. 171-189; Shu et al., "Fake News Detection on Social Media"; Onur Varol and Ismail Uluturk, "Journalists on Twitter: Self-Branding, Audiences, and Involvement of Bots," *Journal of Computational Social Science*, 3:1, 2020, pp. 83-101; Samuel C. Woolley and Philip N. Howard, "Introduction", Samuel C. Woolley & Philip N. Howard (eds.), *Computational Propaganda Political Parties, Politicians, And Political Manipulation On Social Media*, Oxford University Press, UK, 2019, pp. 3-18.

²⁶ European Commission, "Joint Communication to The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions."

²⁷ Chengcheng Shao et al., "The Spread of Low-Credibility Content by Social Bots," *Nature Communications*, 9:1,2018, p. 5; Denis Stukal et al., "Why Botter: How Pro-Government Bots Fight Opposition in Russia," *American Political Science Review*, 2022, p. 3; Woolley and Howard, "Computational Propaganda Worldwide," p. 6.

²⁸ Woolley and Howard, "Computational Propaganda in Russia," pp. 4-6.

²⁹ Simon Hegelich and Dietmar Janetzko, "Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet", 2016, 582, https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13015/12793, accessed 07.10.2023.

³⁰ Sergey Sanovich, "Computational Propaganda in Russia: The Origins of Digital Misinformation", Samuel Woolley & Philip N. Howard (eds.), Computational Propaganda Political Parties, Politicians, And Political Manipulation on Social Media, Oxford University Press, Oxford, 2019, p. 31.

³¹ Kai-Cheng Yang et al., "Arming the Public with Artificial Intelligence to Counter Social Bots," *Human Behavior and Emerging Technologies*, 1:1, 2019, p. 49.

³² Guido Caldarelli et al., "The Role of Bot Squads in the Political Propaganda on Twitter," *Communications Physics*, 3:1, 2020, p. 2.

³³ Woolley and Howard, "Computational Propaganda Worldwide," p. 3-6.

³⁴ Venkatramanan S. Subrahmanian et al., "The DARPA Twitter Bot Challenge", Computer, 49:6, 2016, pp. 38-46.

beyond this number and claim that 9-15% of all accounts on Twitter are bots.³⁵ Another study done by the Pew Research Center in 2018 estimates that 66% of tweeted links to popular news and current events websites are posted by automated bots.³⁶ Similarly, Woolley and Howard indicates that over a third of Twitter's users are bots.³⁷ When it comes to amplifying a specific topic, the number of bots on Twitter may be dramatic. For example, according to Cresci et al., 71% of Twitter users mentioning trending US stocks are likely to be bots.³⁸ Studies agree on the idea that Twitter has a bot problem. For example, Shao et al. discuss the bot problem from the perspective of spreading low-credibility sources. They prove that bots (they call them "social bots") have a great role in spreading articles from low-credibility sources by analysing 14 million tweets.³⁹ Furthermore, bots sometimes tweet news stories without links to the source of the news as a part of their strategies to promote specific news stories.⁴⁰ Pierri and Ceri also suggest that false news spreads faster than the truth on social media, especially by bots and echo chambers.⁴¹ Likewise, Caldarelli et al. point out that bots have the power to spread significant content on Twitter.⁴²

The number and impact of Twitter bots rose so rapidly that the Defence Advanced Research Projects Agency (a body under the United States Department of Defence) started a competition to find state-of-the-art bot detection methods on Twitter. Due to being cost-effective, fast and easy, all parties (political parties, states, other groups), who want to manipulate the public (through disinformation or fake news etc.), to suppress online opposition or to amplify official messages at home and abroad, resort to social media, Twitter in our case, using bots. 44

Collectively, studies show us that bots are employed at critical moments. A longitudinal study by Broniatowski et al. reports how bots can influence social media discussions by examining 1,793,690 tweets between 2014 and 2017.⁴⁵ In a well-known study by Bessi and Ferrara, it is proven that about 19 million bot accounts tweeted to distort online discussions regarding the 2016 US presidential election.⁴⁶ In the same vein, Badawy et al. analyse the 2016 US elections on Twitter and, after examining 13 million tweets, point out that about 5% and 11% of liberal and conservative users are bots. According to their results, these

³⁵ Onur Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization", in *Proceedings of the International AAAI Conference on Web and Social Media*, 11, 2017, p. 280-289, https://ojs.aaai.org/index.php/ICWSM/article/view/14871, accessed 11.12.2023.

³⁶ Stefan Wojcik et al., "Bots in the Twittersphere," 2018, 8, https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/, accessed 11.12.2023.

³⁷ Woolley and Howard, "Computational Propaganda in Russia," p.7.

³⁸ Stefano Cresci vd., "Cashtag Piggybacking: Uncovering Spam and Bot Activity in Stock Microblogs on Twitter", ACM Transactions on the Web, 13:2, 2019, pp. 1-27.

³⁹ Shao et al., "The Spread of Low-Credibility Content by Social Bots."

⁴⁰ Denis Stukal et al., "Detecting Bots on Russian Political Twitter", Big Data, 5:4, 2017, p. 319.

⁴¹ Francesco Pierri and Stefano Ceri, "False News On Social Media: A Data-Driven Survey", ACM SIGMOD Record, 48:2 2019, p. 9.

⁴² Caldarelli et al., "The Role of Bot Squads in the Political Propaganda on Twitter".

⁴³ Subrahmanian et al., "The DARPA Twitter Bot Challenge", 2016.

⁴⁴ Samantha Bradshaw and Philip N. Howard, "The Global Organization of Social Media Disinformation Campaigns", *Journal of International Affairs*, 71:5, 2018, p. 24; Shu et al., "Fake News Detection on Social Media", p.1; Stukal et al., "Detecting Bots on Russian Political Twitter," p. 310; Woolley and Howard, "Social Media, Revolution, and the Rise of Political Bot", p. 287.

⁴⁵ David A. Broniatowski et al., "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate", *American Journal of Public Health*, 108:10, 2018, pp. 1378-1384.

⁴⁶ Alessandro Bessi and Emilio Ferrara, "Social Bots Distort the 2016 US Presidential Election Online Discussion", *First Monday*, 21:11, 2016.

bots talk about sensitive issues like refugees, terrorism, Islam, school shootings, and the police. ⁴⁷ Howard and Kollanyi and Bastos and Mercea also show how Twitter bots polluted online discussions during the Brexit referendum, especially by amplifying hyper-partisan news. ⁴⁸ Another study by Gorodnichenko, Pham, and Talavera focuses on both the 2016 Brexit Referendum and the 2016 US Presidential Election in terms of bots on Twitter. They suggest that the use of bots can double the political polarization and shape public opinion in such crucial times by utilising the fragmentation in society. ⁴⁹

The studies presented thus far provide evidence that Twitter bots are common tools in disinformation campaigns. In the next section, we will present how Russia specifically exploit social media and use bots in its disinformation campaigns. Hence, we can take another step towards understanding the reasons and strategies behind the use of bots on Twitter by Russia.

2. Russian Disinformation

Russian Federation, as a successor of the Union of Soviet Socialist Republics (USSR), has been using disinformation campaigns in the last decades. There are some studies which date the first Russian disinformation campaign back to the 2008 Georgia conflict.⁵⁰ However, in terms of social media, the annexation of Crimea in 2014 can be seen as the starting point of these campaigns. It is widely accepted by international media outlets such as Forbes that Russia started an effective social media campaign, especially after the Crimea conflict.⁵¹ Since then, Russian disinformation campaigns have become a threat especially to the West so much that the European Parliament agreed on a Resolution condemning it on 23 November 2016. The Resolution clearly defines the Russian threat and highlights the role of social media as an instrument for Russian disinformation purposes.⁵²

From the Russian perspective, Twitter is a tool for Western disinformation purposes. The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) of the Russian Federation claims that Twitter keeps spreading banned content. Russian government offices keep accusing Twitter of spreading disinformation.⁵³ Moreover, the Russian Federation started to criminalize Russian citizens who have a role in the dissemination of fake news about Russian armed forces.⁵⁴

⁴⁷ Adam Badawy et al., "Characterizing the 2016 Russian IRA Influence Campaign", Social Network Analysis and Mining, 9:1, 2019, p. 3.

⁴⁸ Marco T. Bastos and Dan Mercea, "The Brexit Botnet and User-Generated Hyperpartisan News", *Social Science Computer Review*, 37:1, 2017, pp. 38-54; Philip N. Howard and Bence Kollanyi, "Bots,# StrongerIn, And# Brexit: Computational Propaganda during the UK-EU Referendum", *SSRN Electronic Journal*, 2016.

⁴⁹ Yuriy Gorodnichenko, Tho Pham and Oleksandr Talavera, "Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection," *European Economic Review*, 136, 2021, p. 103772.

 $^{50\} Christopher\ Paul\ and\ Miriam\ Matthews,\ "The\ Russian\ 'Firehose\ of\ Falsehood'\ Propaganda\ Model'',\ RAND\ Corportation,\ 2016,\ p.1,\ https://www.rand.org/pubs/perspectives/PE198.html,\ accessed\ 11.12.2023.$

⁵¹ Paul Roderick Gregory, "Inside Putin's Campaign of Social Media Trolling And Faked Ukrainian Crimes Paul Roderick Gregory," Forbes, May 11, 2014, https://www.forbes.com/sites/paulroderickgregory/2014/05/11/inside-putins-campaign-of-social-media-trolling-and-faked-ukrainian-crimes/?sh=15dbee407140, accessed 11.12.2023.

⁵² European Parliament, "European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against It by Third Parties," November 23, 2016, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441 EN.html?redirect, accessed 11.12.2023.

^{53 &}quot;No Reason to Lift Russian Ban on Twitter - Roskomnadzor," April 10, 2023, https://interfax.com/newsroom/top-stories/89467/, accessed 11.12.2023.

⁵⁴ Fred Weir, "In Russia, Critiquing the Ukraine War Could Land You in Prison," The Christian Science Monitor, December 5, 2022, https://www.csmonitor.com/World/Europe/2022/1205/In-Russia-critiquing-the-Ukraine-war-could-land-you-in-prison, accessed 11.12.2023.; "Russia Criminalizes Independent War Reporting, Anti-War Protests," March 7, 2022, https://www.hrw.org/news/2022/03/07/russia-criminalizes-independent-war-reporting-anti-war-protests, accessed 11.12.2023.

The reason why Russia is doing it now is not within the scope of this study. Here, we try to put forth how Russia employs social media and bots in its disinformation campaign. Before explaining the use of social media and bots by Russia, we should first look into Russia's disinformation strategy briefly.

As noted above, the Crimea conflict in 2014 was such a turning point for information warfare that some researchers like Thornton even claim that Crimea was "won" with the success of the information campaign.55 Likewise, General Philip Breedlove, NATO's Supreme Allied Commander Europe admitted after the crisis that "Russia was waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."56 Before the Russian annexation of Crimea in 2014, some studies pointed out the Russian leaders' ongoing threat perception from abroad and within. This perception can be seen as one of the fundamental reasons why Russian leaders see disinformation as a part of information warfare.⁵⁷ Vladimir Kvachkov, a former GRU (Russia's military intelligence service) officer, explains this clearly: "A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare -information warfare."58 Valeriy Gerasimov, Chief of the General Staff of the Russian Armed Forces, also highlights the importance of information side of conflicts his own words: "The emphasis on the methods of fighting moves toward the complex application of political, economic, information, and other non-military means, carried out with the support of military force. 59 Studies on Russian bots present evidence by revealing the existence of bots on Twitter amid the Ukrainian presidential crisis in 2014⁶⁰ and after the downing of Malaysian Flight 17.61 We can say that disinformation campaigns are embraced by Russia as a tool to back up their policies.

To contribute to our understanding of how Russia uses social media, Yin et al. clearly explain the role of bots in Russian disinformation strategy. They suggest that Russian bots use three different tactics: First, they spread junk news, especially at critical times. Second, they make use of local media outlets to seem trustworthy. Third, they spread polarizing news or content to amplify polarization in the target society. Similarly, Aleksejeva et al. summarize the Russian strategy as "divide, discredit, and distract" in their thorough analysis of Russian disinformation operations. Russian disinformation operations.

⁵⁵ Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *The RUSI Journal*, 160:4, 2015, p. 40.

⁵⁶ Peter Pomerantsev, "Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare", The Atlantic, 2014, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/, accessed 15.12.2023.

⁵⁷ Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency", *American Foreign Policy Interests*, 35:1, 2013, p. 42.

⁵⁸ Keir Giles, Handbook of Russian Information Warfare, Rome: NATO Defense College, 2016, p. 3, https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20Warfare.pdf, accessed 15.12.2023.

⁵⁹ Giles, p. 3.

⁶⁰ Hegelich and Janetzko, "Are Social Bots on Twitter Political Actors?", p. 579.

⁶¹ Alexander Spangher et al., "Analysis of Strategy and Spread of Russia-Sponsored Content in the US in 2017," ArXiv Preprint ArXiv:1810.10033, 2018, p. 14.

⁶² Leon Yin et al., "Your Friendly Neighborhood Troll: The Internet Research Agency's Use of Local and Fake News in the 2016 US Presidential Campaign", SMaPP Data Report, 2018, https://csmapnyu.org/assets/publications/2018 01 IRA Presidential Campaign.pdf, accessed 15.12.2023.

⁶³ Nika Aleksejeva et al., "Operation Secondary Infektion", *Digital Forensic Research Lab: The Atlantic Council*, June 22, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/operation-secondary-infektion/, accessed 15.12.2023.

Russia does not only disseminate its views but also pollutes and blurs social media by exploiting divisions and fragmentations in the target society by using text, video, and audio with the support of thousands of fake accounts, so it can manipulate public opinion at the international level and make great gains (such as Crimea).⁶⁴ Using bots on social media at different times and for different purposes is an important part of the Russian strategy of disinformation.

To sum up, Russia uses bots in social media for various purposes to serve its goals. These bots are orchestrated by one center in a way to strengthen Russia's position during times of crisis. Furthermore, Russia does not only meddle with issues directly related to its interests but also interferes with issues of other countries. For these reasons, it was surprising that Russia banned Twitter. Based on the literature, we formulate the following hypothesis:

RH: Russia chooses to block Twitter when it realizes that it cannot manipulate the platform.

3. Data and Methods

As bots have been a part of Twitter, researchers have developed bot detection tools by using different features and techniques. There has been a significant rise in the studies that have tried to automate bot detection in the last decade. When analyzed thoroughly it can be seen that machine learning methods dominate bot detection literature.

There has been a great interest in developing bot detection tools based on supervised machine learning. Wang is one of the pioneers who use a supervised machine learning approach using graph-based features to detect bots on Twitter.⁶⁵ Likewise, Chu et al. define a classification system using supervised machine learning to understand whether a Twitter account is a human, bot or cyborg.⁶⁶ In the same vein, both Yang, Harkreader, and Gu and Guo and Chen use a combined technique in which they use graph-based features with other features like neighbour-based features in their supervised machine learning approach.⁶⁷ Dickerson, Kagan, and Subrahmanian put the sentiment into practice and build a bot detection tool using a supervised approach (SentiBot).⁶⁸

Cresci et al. use 49 distinct features and eight different supervised machine learning classifiers to understand the best way of bot detection on Twitter. They conclude that social ties between an account and its neighbours are more effective than any other information in detecting bots. Similarly, in DARPA's 2016 challenge, six teams competed. They all started with supervised learning but, in the end, it was concluded that semi-supervised methods

⁶⁴ Edward Lucas and Peter Pomeranzev, "Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda," 2016, 2, https://cepa.ecms.pl/files/?id_plik=2715, accessed 20.12.2023; Paul and Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," p. 2; Thornton, "The Changing Nature of Modern Warfare", pp. 43-44.

⁶⁵ Alex Hai Wang, "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach", Sara Foresti and Sushil Jajodia (eds.), *Data and Applications Security and Privacy XXIV*, vol. 6166, Lecture Notes in Computer Science, Berlin, Heidelberg, 2010, pp. 335-342.

⁶⁶ Zi Chu et al., "Who Is Tweeting on Twitter: Human, Bot, or Cyborg?", in *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10*, the 26th Annual Computer Security Applications Conference, Austin, Texas: ACM Press, 2010, p. 21.

⁶⁷ Chao Yang, Robert Harkreader and Guofei Gu, "Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers", *IEEE Transactions on Information Forensics and Security*, 8:8, 2013, pp.1280-1293.

⁶⁸ John P. Dickerson, Vadim Kagan and V.S. Subrahmanian, "Using Sentiment to Detect Bots on Twitter: Are Humans More Opinionated than Bots?", in 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, China: IEEE, 2014, pp. 620-627.

⁶⁹ Stefano Cresci et al., "Fame for Sale: Efficient Detection of Fake Twitter Followers", *Decision Support Systems*, 80, 2015, pp. 56-71.

were useful in bot detection, using inconsistency detection and behavioural modelling, text analysis, network analysis, and machine learning together.⁷⁰

Again in 2016, Davis et al. start to develop one of the most common supervised machine learning approaches, which extracts over 1.000 features of Twitter accounts. They developed their bot detection tool, BotOrNot, which gave a classification score called "bot score". The same researchers improved their bot detection tool (version 2) by focusing on users' and friends' meta-data, tweet content and sentiment, network patterns, and activity time series. The team added new features to their tool (version 3) to capture more sophisticated bot behaviours. Recently, Sayyadiharikandeh and his colleagues from the BotOrNot team improved Botometer into version 4 for a better and faster Twitter bot detection tool. In their work, they built a system, which is open to learning through new domains.

Stukal et al. develop their supervised bot detection a bot detection ensemble algorithm using an ensemble of classifiers. Gilani, Kochmar, and Crowcroft also use a supervised machine-learning method to build a classifier for bot detection. Kudugunta and Ferrara develop their supervised approach using a deep neural network approach based on contextual long short-term memory (LSTM) architecture. In their supervised system, Efthimion, Payne, and Proferes focus on three features: profile, account activity, and text mining. Wright and Anise also build their bot detection tool based on a supervised machine-learning approach by using account features, content features and content metadata. Heidari, Jones and Uzunel focus on users' profiles (including age, gender, personality, and education) to build their supervised bot detection tool on Twitter.

There are also studies which prefer unsupervised machine learning for building bot detection tools. Ahmed and Abulaish conduct one of these studies. They make use of graph clustering and statistical features related to URLs, hashtags, mentions, and retweets. Similarly, Miller et al. develop an unsupervised machine-learning system for bot detection. They focus on one-gram features in their system. See Chavoshi, Hamooni, and Mueen focus on

⁷⁰ Subrahmanian et al., "The DARPA Twitter Bot Challenge", 2016.

⁷¹ Clayton Allen Davis et al., "BotOrNot: A System to Evaluate Social Bots", in *Proceedings of the 25th International Conference Companion on World Wide Web - WWW*, '16, 2016, pp. 273-274.

⁷² Varol et al., "Online Human-Bot Interactions".

⁷³ Yang et al., "Arming the Public with Artificial Intelligence to Counter Social Bots".

⁷⁴ Mohsen Sayyadiharikandeh et al., "Detection of Novel Social Bots by Ensembles of Specialized Classifiers", in *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*, 2020, pp. 2725-2732.

⁷⁵ Stukal et al., "Detecting Bots on Russian Political Twitter".

⁷⁶ Zafar Gilani, Ekaterina Kochmar, and Jon Crowcroft, "Classification of Twitter Accounts into Automated Agents and Human Users", in Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney Australia, 2017, pp. 489-496.

⁷⁷ Sneha Kudugunta and Emilio Ferrara, "Deep Neural Networks for Bot Detection", *Information Sciences*, 467, 2018, pp. 312-322.

⁷⁸ Phillip George Efthimion, Scott Payne, and Nicholas Proferes, "Supervised Machine Learning Bot Detection Techniques to Identify Social Twitter Bots", *SMU Data Science Review*, 1:2, 2018, pp. 1-70.

⁷⁹ Jordan Wright and Olabode Anise, "Don't @ Me, Hunting Twitter Bots at Scale", 2018, https://i.blackhat.com/us-18/Wed-August-8/us-18-Anise-Wright-Dont-@-Me-Hunting-Twitter-Bots-at-Scale-wp.pdf, accessed 15.12.2023.

⁸⁰ Maryam Heidari, James H Jones and Ozlem Uzuner, "Deep Contextualized Word Embedding for Text-Based Online User Profiling to Detect Social Bots on Twitter," in *International Conference on Data Mining Workshops (ICDMW)*, Sorrento, Italy, 2020, pp. 480-487.

⁸¹ Faraz Ahmed and Muhammad Abulaish, "A Generic Statistical Approach for Spam Detection in Online Social Networks", *Computer Communications*, 36:10-11, 2013, pp. 1120-1129.

⁸² Zachary Miller et al., "Twitter Spammer Detection Using Data Stream Clustering", *Information Sciences*, 260, 2014, pp. 64-73.

cross-correlating user activities to build their bot detection tool (DeBot) with an unsupervised technique to identify abnormally correlated user accounts on Twitter.⁸³ Minnich et al. develop their unsupervised bot detection tool (BotWalk), which uses metadata, content, temporal, and network-based features.⁸⁴ Cornelissen et al. combine network structure measures and unsupervised machine learning to devise their bot detection tool.⁸⁵

As shown, there are various kinds and techniques for bot detection on Twitter. For this research, we used a supervised machine-learning tool, "tweetbotornot2", an R package for Twitter bot detection. This package considers different types of features for the prediction of authors whether they are bot or not. Tweetbotornot2 is a behaviour-based supervised machine learning bot detection tool that uses users' profiles, metrics, tweets' content, and time between tweets for probability. It gives a probability score between [0, 1] as output. If the probability is close to 0, it means human-like users and if the probability is close to 1, it indicates bot-like users. 86

The reasons why we use this package can be listed as follows: First, this package can examine a large amount of data free of charge while some other bot detection tools like "botometer" require payment. Second, it processes large amounts of data quite quickly (6,000 predictions per hour or 144,000 predictions per day⁸⁷). When we try "botometer" and "botometerlite" packages for comparison, we either get results relatively slowly for a full sample dataset or we exceed the daily usage given by default. Third, tweetbotornot2 gives us an interpretable score instead of a definite binary output. We take the score of 0.5 as a threshold in the study. To put it simply, we mark the accounts whose scores are over 0.5 as bots.

For data collection, we get authentication with Twitter Developer API so that we can obtain access to full-archive search with access tokens, access keys, and bearer key. Thanks to this authorization, researchers can download 10 million tweets per month by using the "academictwitterR" package⁸⁸ with Twitter Academic Research Product Track authentication. This package has been developed for the use of researchers working on tweet analysis.

After setting up the bearer key for integration of the package and Twitter API, we can build queries with keywords and hashtags, and we can also filter tweet languages and locations by both using country name and latitude-longitude box window inputs.

In the first step of data collection, we aim to obtain the tweets that satisfy the status explained in Table 1.

⁸³ Nikan Chavoshi, Hossein Hamooni and Abdullah Mueen, "Identifying Correlated Bots in Twitter", Emma Spiro & Yong-Yeol Ahn (eds.), *Social Informatics*, vol. 10047, Springer International Publishing, Cham, 2016, pp.14-21. 84 Amanda Minnich et al., "BotWalk: Efficient Adaptive Exploration of Twitter Bot Networks", in *Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Sydney Australia, 2017, pp. 467-744.

⁸⁵ Laurenz A. Cornelissen et al., "A Network Topology Approach to Bot Classification", in *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, Port Elizabeth South Africa, 2018, pp. 79-88.

⁸⁶ Tweetbotontot2 was created by Michael W. Kearney, as R package for detecting Twitter bots via machine-learning. It is an open access package which means it is free of charge for all users. https://github.com/mkearney/tweetbotornot2.

⁸⁷ https://github.com/mkearney/tweetbotornot2.

⁸⁸ Christopher Barrie and Justin Ho, "AcademictwitteR: An R Package to Access the Twitter Academic Research Product Track v2 API Endpoint", *Journal of Open Source Software*, 6:62, 2021, p. 3272.

Table 1: Information about Dataset

Dataset Name	Keywords and Hashtags	From	То	Language
Data_Ru	Украина OR Украинец OR	2022-02-	2022-03-	Russian
	Донецк OR Луганск OR	24T00:00:00	04T00:00:00	
	HATO OR война OR операция			
	OR #IStandWithPutin OR			
	#IStandWithRussia			
	(In English: Ukraine OR Donetsk			
	OR Luhansk OR Ukrainian			
	OR Military OR Operation OR			
	NATO OR #IStandWithPutin OR			
	#IStandWithRussia)			
Date of Data Collection: 08-				
04-2022				
Date of Bot Prediction: 12-04-				

With the help of keywords and hashtags listed above, we collect Russian language tweets that contain some critical Ukrainian locations attacked by Russia ("Donetsk" and "Luhansk") and the country-related words ("Ukrainian" and "Ukraine") and some words related to war ("Military", "Operation", "NATO") and popular hashtags appeared then ("#IStandWithPutin", "#IStandWithRussia") from 24 February 2022 to 3 March 2022.

Regarding the selection of the keywords and period, we consider the following conditions:

- The period including the first wave of Russian invasion till the Twitter ban in Russia,
- Critical locations that were under attack in the first week like Donetsk and Luhansk,
- The county name under attack and its nationality,
- Some critical words related to war and conflict.

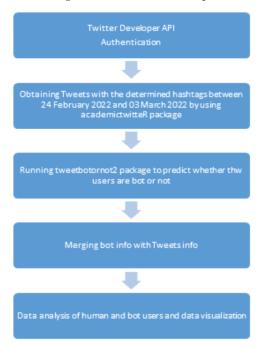
2022,13-04-2022,28-04-2022

- Popular hashtags supporting Putin and Russian military power.

After data collection, we performed the bot prediction process. In our analysis, we got some Not-Available (NA) values for bot prediction. It tells us that these accounts were either deleted or suspended users. Given that Twitter's attempts to suspend and delete the users completely increased (especially after the 2016 US elections) and Twitter became more sensitive about Russia during the period we analysed, we assume that users who cannot be assigned (accounts that are detected as NA) as a bot. In other words, Twitter users that could not be reached at the time of our bot prediction analysis can be considered as bots. These accounts were also cross-checked by botometer. The results were the same; botometer gave us two types of outputs about them: "unauthorized" and "not found".

The steps during the data collection are summarized in Figure 1:

Figure 1. Data Collection Steps



4. Findings

We collected our data on 08 April 2022. We performed the bot prediction on three different days (12 April 2022, 13 April 2022, and 28 April 2022) due to our limited technical abilities. Dates are important here because some users (30.873 users) were either suspended or deleted in the period between data collection and bot prediction. After evaluating the related literature and Twitter's company policies, we assume that those users, which cannot be assigned a bot, score as bots. Here are the first findings after data collection and bot prediction analysis:

Total Count of Tweets: 889,193

Total Count of Tweets that cannot be defined: 65.500

Total Count of Tweets that can be defined: 823.693

Total Count of Bot Tweets (Prob>0.5): 12.865

Total Count of Human Tweets: 810.828

A pie chart of bot prediction results is given in Figure 1. As seen, both probabilities of accounts can be defined for most accounts, however, some of the remaining accounts can't be defined based on bot prediction method. Defined accounts are split into two parts: human-like accounts and bot accounts.

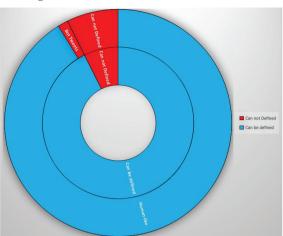


Figure 2. Pie Chart of Bot Prediction Results

The average bot probability of each user was obtained after assuming the probability value of 1 for each tweet belonging to users who were assigned as a bot (Figure 2). After the merging process, we managed to obtain bot probabilities for each user for each time.

Following this step, we needed to define the probabilities for all analysis times. To this end, we calculated the average probabilities of each user and defined bots based on this calculated average to find out whether it is below 0.5 or above 0.5. Finally, in terms of users' perspective, all Twitter users were counted as 183.287 users and bots consisted only %15,93 of all users, as shown in Figure 3. When it comes to the number of tweets, human-like tweets were 747.510, whereas bot-like tweets were 141,683.

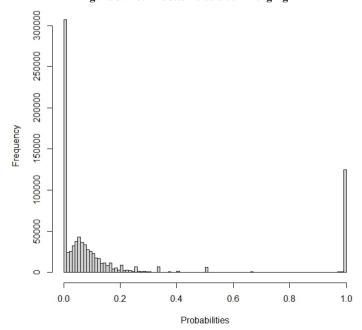
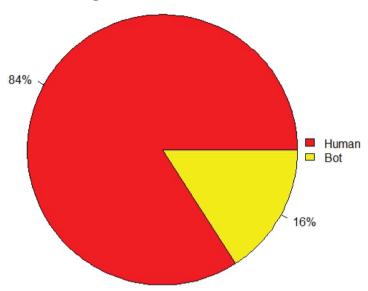


Figure 3. Bot Probabilities after Merging

Figure 4. Bot Classes of Twitter Users



According to the findings we obtained (Figure 4.) on the daily fluctuations of tweet counts, nearly %14,9-%24,2 of users were bots. While the number of tweets decreased day by day, the number of users did not decrease accordingly.

Figure 5. Bot Probabilities for Each Day

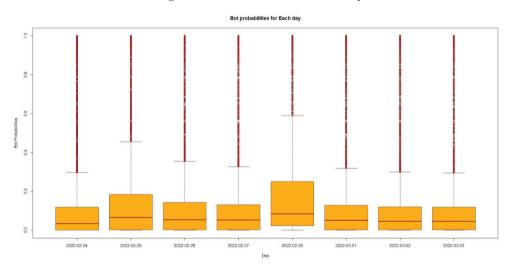


Table 2. Daily Distribution of Tweets and Users

Date	Human-like Tweets	Bot-like Tweets	Human-like User	Bot-like User	Bot Percent- age (by Users)	Bot Percentage (by Tweets)
24 February 2022	131,308	23,865	56,324	10,600	0.158389	0.153796
25 February 2022	121,131	26,759	44,805	12,931	0.223968	0.180939
26 February 2022	106,008	19,392	40,695	8,450	0.17194	0.154641
27 February 2022	90,307	15,421	36,644	6,642	0.153445	0.145855
28 February 2022	73,151	17,907	28,891	9,224	0.242004	0.196655
1 March 2022	84,074	14,287	35,006	6,281	0.15213	0.145251
2 March 2022	74,286	12,461	32,092	5,643	0.149543	0.143648
3 March 2022	67,245	11,591	30,220	5,453	0.152861	0.147027

Table 2 and Figure 6 show us the number of tweets and users on a daily basis. As seen, since 25 February 2022 was the day with the highest number of bot users, it was chosen for visualization of bot interaction. The interaction dataset was generated with a username and who he/she/it mentioned on this filtered date. This type of data is generally considered directional data because it denotes a communication network from one to the other.

Figure 6. Daily Tweets' Count

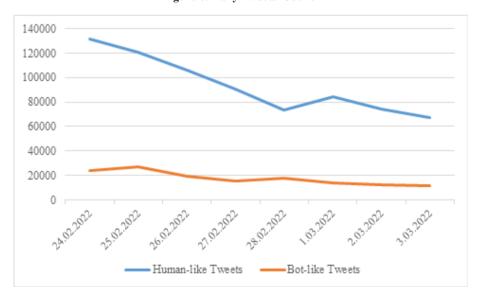


Table 3. Sample Tweets of Bots

Tweet ID	Activity Type	Russian(Original) Tweet	Translated Tweet	Bot Probability	
1498316510883897344	Retweet	RT @aleks_roza: Пожалуйста эти кадры миру, как украинская антитеррористическая операция началась, как убивали мирных жителей Донб	RT @aleks_roza: Please give this fo- otage to the world, how the Ukrainian anti-terrorist operation began, how the civilians of Donb were killed	1	
1498319687792406528	Retweet	RT @velien84: Украина, которая несет "какие плохие русские, в метро прошлось ночь посидеть"!Посмотрите что делают ваши нацики с простым народом!	RT @velien84: Ukraine, which says "how bad the Russians are, I spent the night sitting in the subway"! Look what your Nazis are doing to the common people!	1	
1498273776517402624	Retweet	RT @RusEmbassyMinsk: 4 Переговоры в Гомельской области начались.	RT @RusEmbassyMinsk: 4 Negotiations in the Gomel region have begun.	1	
		RR В состав российской делегации входят представители администрации През	RR The Russian delegation includes representatives of the administration of the President		
1498331243775205376	Tweet	Война на Украине (28.02.22 на 18:00): сводки с полей сражений, Бердянск, https://t.co/lyQqiVLvgt через @YouTube	War in Ukraine (28.02.22 at 18:00): reports from the battlefields, Berd- yansk, https://t.co/lyQqiVLvgt via @YouTube	0.97	
1498322919264509952	Tweet	НАТО не планирует вводить бесполетную зону над Украиной https://t.co/JW8pjbysqo	NATO has no plans to introduce a no-fly zone over Ukraine https://t.co/ JW8pjbysqo	0.94	
1497929825671131136	Tweet	Ядерная война? Путин предупреждает "силами сдерживания" - обиделься на "агрессивные высказывания" https://t.co/FtdCoPoSRi	Nuclear war? Putin warns of "forces of containment" - offended by "aggressive statements" https://t.co/FtdCoPoSRi	1	
1498412524051574784	Tweet	Сиярто: Венгрия не размещает ядерные силы НАТО на своей территории https://t.co/rJemwF4YIZ	Szijjártó: Hungary does not host NATO nuclear forces on its territory https://t.co/rJemwF4YIZ	0.87	
1498643803879661568	Mention	@KremlinRussia Ребята, Украина - вы победили космическую гонку, теперь время работать на вас! Просим вас, пошлите освобождение Украины против нас от фашистского путлеровского ига!	@KremlinRussia Guys, Ukraine - you won the space race, now it's time to work for you! We ask you, send the liberation of Ukraine against us from the fascist Putlerite yoke!	0.88	
1499070389493846016	Tweet	Мнение: операция по демилитаризации и денацификации Украины будет доведена до конца https://t.co/fK9VT12mhO	Opinion: the operation to demilitarize and denazify Ukraine will be completed https://t.co/fK9VTI2mhO	0.95	
1497226770243735552	Mention	@antiputler_news a что он сделал за 2.5 года для обороны Украины: не финансировал в должном объеме армию, не выполнил обещанный заказ,отдал территорию,отдал террористов, вагнеровцев Цемаха преследовал боевых генералов Павловского и Марченко и мн др а сейчас опять хочет говорить с хулом уже о неуступке в НАТО	@antiputler_news what did he do in 2.5 years for the defense of Ukraine: did not adequately finance the army. did not fulfill the promised order, gave up the territory, gave up the terrorists, the Wagnerites Tsemakh persecuted the military generals Pavlovsky and Marchenko and many others, and now he again wants to talk with blasphemy about non-concession in NATO	1	
1497493081255469056	Mention	@bbcrussian Украина говорит, что уничтожила нашу армию, но все сидят в метро Что-то как-то не логично	@bbcrussian Ukraine says it destroyed our army, but everyone is sitting in the subway Something is somehow not logical	1	

We generated a bot network from the dataset by using bilateral interactions from username to name of the mentioned account by using a looping structure in R. It gave us all existing interactions in the dataset for all available 147.890 tweets, however, we needed to remove non-mentioned interactions and filter with interaction from only bots. Total interactions counted 6.464.779, while interactions from only the bots counted 816.336, which constituted only 12.62% of total interactions. For graphical implementation, we found 125.293 bot-related bilateral interactions and 6,452 unique interactions.

To show bot interactions, we generated a network graph from the network dataset with 6.381 nodes and 6.452 edges by using the "graph_from_dataframe" function in the "igraph" package in R.89 We also applied ForceAtlas2 for the graph layout algorithm.

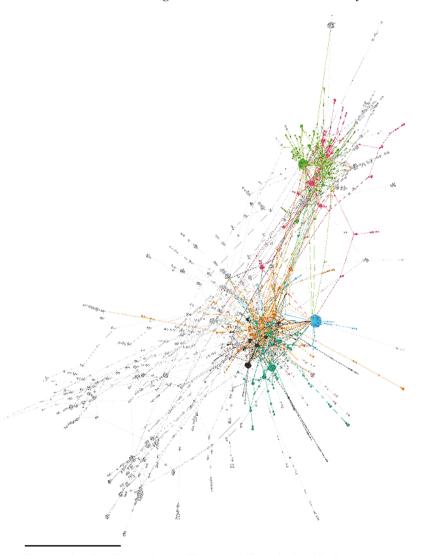


Figure 7. Bot Interaction on 25 February 2022

⁸⁹ Gabor Csardi and Tamas Nepusz, "The Igraph Software Package for Complex Network Research", *InterJournal* Complex *Systems*, 2006, pp. 1695-1704.

As seen from the bot interaction visualization in Figure 6, three different bot clusters produced a bigger number of interactions. All coloured accounts represented the interacted accounts from bots or to bots. Whereas some accounts reacted as Twitter bots, some accounts represented the mentioned accounts by bots and these accounts could be used by bots as an intermediary for spreading disinformation.

Some important bots were media organs like news, radio channels etc. Besides, some bot accounts which were different from those media organs could be seen as interactive in the social media environment. These bots did not only post tweets they also provided interactions such as mentions to other users.

Overall, the findings can be summarized as:

- 1- There are bots that post about the war on Russian Twitter-sphere during the first week of the Russian attacks,
 - 2- There is a large number of users that are not available at the time of bot prediction,
- 3- Twitter reacts more quickly than ever to suspend bot accounts in the war between Russia and Ukraine so 30.873 users were already suspended or deleted between the data collection and bot prediction,
- 4- The number of bots can be reached to a meaningful level after merging NA users with bots,
- 5- Bots in the Russian Twitter-sphere do not only post content, they also mention other users to raise interaction.

Discussion and Results

In the last decade, researchers have shown a great interest in shedding light on the issue of bots in social media. The 2014 Crimean conflict, the 2016 US Presidential elections, and the 2016 Brexit Referendum have been the hot moments when bots were put into play by Russia. Especially Twitter is one of the platforms which have been exploited by Russia through bots for disinformation campaigns. In this paper, we focused on bots in the Russian Twitter-sphere in the first eight days of the Russian war on Ukraine.

This paper, first, provided evidence that there were bots in Russian Twitter-sphere employed by Russia. These bots were active in the discussions related to the war during the first eight days of the war. This means that Russia did not hold back from putting bots into action together with its physical attack on Ukraine.

Secondly, there is a large number of users, which were not available for bot prediction. It means that the tweets including selected keywords were posted by the users, which were later on either deleted or suspended by Twitter, as the study of Pohl Seiler, Assenmacher and Grimme (2022) proved. Our study showed that the users, which were labelled as bots (1.658)

⁹⁰ Janina Susanne Pohl, et al., "A Twitter Streaming Data Set Collected before and after the Onset of the War between Russia and Ukraine in 2022", *Zenodo*, 2022.society, and world events. Their reach enables the global dissemination of information in the shortest possible time and thus the individual participation of people all over the world in global events in almost real-time. However, equally efficient, these platforms can be misused in the context of information warfare in order to manipulate human perception and opinion formation. The outbreak of war between Russia and Ukraine on February 24, 2022, demonstrated this in a striking manner. Here we publish a dataset of raw tweets collected by using the Twitter Streaming API in the context of the onset of the war which Russia started on Ukraine on February 24, 2022. A distinctive feature of the dataset is that it covers the period from one week before to one week after Russia's invasion of Ukraine. We publish the IDs of all tweets we streamed during

users), only account for 1,01 % of total collected tweets. These findings neither comply with the bot literature in general⁹¹ nor with those focusing on Russia's interference⁹² nor with the studies on account suspension.⁹³ However, when we added deleted/NA accounts (30.873 users) to bots, we reached % 15,93 of all users in our study. The results are similar on the subject of tweet counts. The number of tweets posted by accounts labelled as bots was 12.865 and it only consists of 1,44 % of all tweets. When we added tweets posted by NA to those posted by bots, we reached 78.365 tweets which constituted 8,81% of all tweets. In the end, we had 747,510 human-like tweets and 141.683 bot-like tweets.

We can deduce from these findings that Twitter reacted quickly to the bots in the Russian Twitter-sphere during the first days of the Russian war on Ukraine and did not let Russia pollute the Twitter environment. More importantly, this paper aims to uncover the Russian disinformation strategy using bots. Our analysis suggests that Russia tried to exploit Twitter by using bots during its attack on Ukraine, but it seems that Twitter reacted quickly. In the end, Russia chose to block Twitter in Russia when it turned out that it could not benefit from it.

Although our study reveals some results related to Russian bots during its attack on Ukraine, English tweeting bot analysis may contribute to the literature as well. Also, the content analysis of tweets posted by bot accounts may shed light on the Russian disinformation strategy. It is also clear that Russia has passed to other platforms to strengthen its disinformation strategy. Thus the studies to be performed on platforms like TikTok may help a better understanding of disinformation war.

Conflict of Interest Statement:

The authors declare that there is no conflict of interest.

Author Contribution Statements:

The authors contributed to the study equally.

that time, the time we rehydrated them using Twitter's API as well as the result of the rehydration. If you use this dataset, please cite our related Paper: Pohl, Janina Susanne and Seiler, Moritz Vinzent and Assenmacher, Dennis and Grimme, Christian, A Twitter Streaming Dataset collected before and after the Onset of the War between Russia and Ukraine in 2022 (March 25, 2022

⁹¹ Venkatramanan S. Subrahmanian et al., "The DARPA Twitter Bot Challenge", *Computer*, 49:6, 2016, pp. 38-46; Varol et al., "Online Human-Bot Interactions"; Woolley and Howard, "Computational Propaganda in Russia."

⁹² Badawy et al., "Characterizing the 2016 Russian IRA Influence Campaign"; Stukal et al., "Detecting Bots on Russian Political Twitter."

⁹³ Farhan Asif Chowdhury et al., "On Twitter Purge: A Retrospective Analysis of Suspended Users", in Companion Proceedings of the Web Conference, Taipei Taiwan, 2020, pp. 371-378; Silvia Majó-Vázquez et al., "The Role of Suspended Accounts in Political Discussion on Social Media: Analysis of the 2017 French, UK and German Elections", Social Media + Society, 7:3, 2021.

REFERENCES

Published Works

- AHMED Faraz and ABULAISH Muhammad (2013). "A Generic Statistical Approach for Spam Detection in Online Social Networks", *Computer Communications*, 36:10-11, 1120-1129.
- AGRALI Özgür SÖKÜN Hakan and KARAASLAN Enis (2022). "Twitter Data Analysis: Izmir Earthquake Case", *Journal of Emerging Computer Technologies*, 2:2, 36-41.
- ALIAKSANDRAU Andrei (2014). "Brave New War: The Information War between Russia and Ukraine", Index on Censorship, 43:4, 54-60.
- ATABEK Ümit (2020). "Twitterda Yerel Siyasal İletişim: Türkiye'de İki Farklı Tarz", *Galatasaray Üniversitesi İletişim Dergisi*, 33, 32-54.
- BADAWY Adam ADDAWOOD Aseel LERMAN Kristina and FERRARA Emilio (2019). "Characterizing the 2016 Russian IRA Influence Campaign", Social Network Analysis and Mining, 9:1, 1-11.
- BARRIE Christopher and JUSTIN Ho (2021). "AcademictwitteR: An R Package to Access the Twitter Academic Research Product Track v2 API Endpoint", *Journal of Open Source Software*, 6:62, 3272.
- BASTOS Marco T. and MERCEA Dan (2017). "The Brexit Botnet and User-Generated Hyperpartisan News", Social Science Computer Review, 37:1, 38-54.
- BESSI Alessandro and FERRARA Emilio (2016). "Social Bots Distort the 2016 US Presidential Election Online Discussion", First Monday, 21:11.
- BLANK Stephen (2013). "Russian Information Warfare as Domestic Counterinsurgency", *American Foreign Policy Interests*, 35:1, 31-44.
- BRADSHAW Samantha and HOWARD Philip N. (2018). "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs*, 71:1.5, 23-32.
- BRONIATOWSKI David A. JAMISON Amelia M. SIHUA Qi ALKULAIB Lulwah TAO Chen, BENTON Adrian QUINN Sandra C. and DREDZE Mark (2018). "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate", *American Journal of Public Health*, 108:10, 1378-1384.
- CALDARELLI Guido DE NICOLA Rocco VIGNA Fabio Del PETROCCHI Marinella and SARACCO Fabio (2020). "The Role of Bot Squads in the Political Propaganda on Twitter", *Communications Physics*, 3:1, 1-15.
- CAM Handan CAM Alper Veli DEMIREL Ugur and SANA Ahmed (2024). "Sentiment Analysis of Financial Twitter Posts on Twitter with the Machine Learning Classifiers", *Heliyon*, 10:1, e23784.
- CHAVOSHI Nikan HAMOONI Hossein and MUEEN Abdullah (2016). "Identifying Correlated Bots in Twitter", Emma Spiro & Yong-Yeol Ahn (eds.), *Social Informatics*, Springer International Publishing, Cham, 14-21.
- CHOWDHURY Farhan Asif LAWRENCE Allen YOUSUF Mohammad and MUEEN Abdullah (2020). "On Twitter Purge: A Retrospective Analysis of Suspended Users", In *Companion Proceedings of the Web Conference*, Taipei Taiwan, 371-378.
- CHU Zi, GIANVECCHIO Steven, WANG Haining and JAJODIA Sushil (2010). "Who Is Tweeting on Twitter: Human, Bot, or Cyborg?", In *Proceedings of the 26th Annual Computer Security Applications Conference on ACSAC*. Austin, Texas: ACM Press.
- CORNELISSEN Laurenz A., BARNETT Richard J., SCHOONWINKEL Petrus, EICHSTADT Brent D. and MAGODLA Hluma B. (2018). "A Network Topology Approach to Bot Classification", In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists, Port Elizabeth South Africa, 79-88.
- CRESCI Stefano LILLO Fabrizio REGOLI Daniele TARDELLI Serena and TESCONI Maurizio (2019). "Cashtag Piggybacking: Uncovering Spam and Bot Activity in Stock Microblogs on Twitter", ACM Transactions on the Web, 13:2, 1-27.
- CRESCI Stefano DI PIETRO Roberto PETROCCHI Marinella SPOGNARDI Angelo and TESCONI Maurizio (2015). "Fame for Sale: Efficient Detection of Fake Twitter Followers." *Decision Support Systems*, 80, 56-71.
- CSARDI Gabor and NEPUSZ Tamas (2006). "The Igraph Software Package for Complex Network Research", InterJournal Complex Systems, 1695-1704.
- DAVIS Clayton Allen VAROL Onur FERRARA Emilio FLAMMINI Alessandro and MENCZER Filippo (2016). "BotOrNot: A System to Evaluate Social Bots." In *Proceedings of the 25th International Conference Companion on World Wide Web*, Montreal: Canada, 273-274.
- DICKERSON John P., KAGAN Vadim and SUBRAHMANIAN V.S. (2014). "Using Sentiment to Detect

- Bots on Twitter: Are Humans More Opinionated than Bots?" In 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 620-627.
- EFTHIMION Phillip George PAYNE Scott and PROFERES Nicholas (2018). "Supervised Machine Learning Bot Detection Techniques to Identify Social Twitter Bots", *SMU Data Science Review*, 1:2, 1-70.
- FERRARA Emilio VAROL Onur DAVIS Clayton MENCZER Filippo and FLAMMINI Alessandro (2016). "The Rise of Social Bots", *Communications of the ACM*, 59:7, 96-104.
- GILANI Zafar, KOCHMAR Ekaterina and CROWCROFT Jon (2017). "Classification of Twitter Accounts into Automated Agents and Human Users." In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Sydney Australia, 489-496.
- GOLOVCHENKO Yevgeniy HARTMANN Mareike and ADLER-NISSEN Rebecca (2018). "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation", *International Affairs*, 94:5, 975-994.
- GORODNICHENKO Yuriy PHAM Tho and TALAVERA Oleksandr (2021). "Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #USElection", *European Economic Review*, 136, 103772.
- GUESS Andrew M. and LYONS Benjamin A. (2020). "Misinformation, Disinformation, and Online Propaganda", Nathaniel Persily & Joshua A. Tucker (eds.), *Social Media and Democracy: The State of the Field, Prospects for Reform* (1st ed.), Cambridge University Press, Cambridge, 10-33.
- HEGELICH Simon and JANETZKO Dietmar (2016). "Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet", *Proceedings of the International AAAI Conference on Web and Social Media*, 10:1, 579-582.
- HEIDARI Maryam, JONES James H. and UZUNER Özlem (2020). "Deep Contextualized Word Embedding for Text-Based Online User Profiling to Detect Social Bots on Twitter", In 2020 International Conference on Data Mining Workshops (ICDMW), Sorrento, Italy, 480-487.
- HOWARD Philip N. and KOLLANYI Bence (2016). "Bots,# StrongerIn, And# Brexit: Computational Propaganda during the UK-EU Referendum." SSRN Electronic Journal.
- KELLER Tobias R. and KLINGER Ulrike (2019). "Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications", *Political Communication* 36:1, 171-189.
- KORTUNAY Nevin (2023). "Turkish Universities' Use Of Twitter: A Content Analysis", *Pamukkale Social Sciences Institute Journal*, 56, 267-279.
- KUDUGUNTA Sneha and FERRARA Emilio (2018). "Deep Neural Networks for Bot Detection", *Information Sciences*, 467, 312-322.
- MAJÓ-VÁZQUEZ Silvia CONGOSTO Mariluz, NICHOLLS Tom and NIELSEN Rasmus Kleis (2021). "The Role of Suspended Accounts in Political Discussion on Social Media: Analysis of the 2017 French, UK and German Elections", *Social Media + Society*, 7:3.
- MEHMETCIK Hakan KOLUK Melih and YÜKSEL Galip (2023). "Perceptions of Turkey in the US Congress: A Twitter Data Analysis", *Uluslararası İlişkiler Dergisi*, 19:76, 69-89.
- MILLER David, ROBINSON Piers and BAKIR Vian (2017). "Propaganda and Persuasion in Contemporary Conflict", Piers Robinson, Philip M. Seib & Romy Fröhlich (eds.), Routledge Handbook of Media, Conflict and Security, Routledge, New York, NY, 308-320.
- MILLER Zachary DICKINSON Brian DEITRICK William HU Wei and WANG Alex Hai (2014). "Twitter Spammer Detection Using Data Stream Clustering", *Information Sciences*, 260, 64-73.
- MINNICH Amanda CHAVOSHI Nikan KOUTRA Danai and MUEEN Abdullah (2017). "BotWalk: Efficient Adaptive Exploration of Twitter Bot Networks", In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Sydney Australia, 467-474.
- ORABI Mariam MOUHEB Djedjiga AL AGHBARI Zaher and KAMEL Ibrahim (2020). "Detection of Bots in Social Media: A Systematic Review", *Information Processing & Management*, 57:4, 102250.
- PIERRI Francesco and CERI Stefano (2019). "False News On Social Media: A Data-Driven Survey", ACM SIGMOD Record, 48:2, 18-27.
- POHL Janina Susanne, MORITZ Vinzent Seiler, ASSENMACHER Dennis and GRIMME Christian (2022). "A Twitter Streaming Data Set Collected before and after the Onset of the War between Russia and Ukraine in 2022", Zenodo.
- SANOVICH Sergey (2019). "Computational Propaganda in Russia: The Origins of Digital Misinformation", Samuel Woolley & Philip N. Howard (eds.), Computational Propaganda Political Parties, Politicians, And Political Manipulation On Social Media, Oxford University Press, Oxford, 21-40.
- SAYYADIHARIKANDEH Mohsen VAROL Onur YANG Kai-Cheng FLAMMINI Alessandro and MENCZER Filippo (2020). "Detection of Novel Social Bots by Ensembles of Specialized

- Classifiers", In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management*, Virtual Event Ireland, 2725-2732.
- SHAO Chengcheng CIAMPAGLIA Giovanni Luca VAROL Onur YANG Kai-Cheng FLAMMINI Alessandro and MENCZER Filippo (2018). "The Spread of Low-Credibility Content by Social Bots", *Nature Communications*, 9:1, 1-9.
- SHU Kai SLIVA Amy WANG Suhang TANG Jiliang and LIU Huan (2017). "Fake News Detection on Social Media: A Data Mining Perspective", ACM SIGKDD Explorations Newsletter, 19:1, 22-36.
- SPANGHER Alexander RANADE Gireeja NUSHI Besmira FOURNEY Adam and HORVITZ Eric (2018). "Analysis of Strategy and Spread of Russia-Sponsored Content in the US in 2017", *ArXiv Preprint ArXiv:1810.10033*.
- STUKAL Denis SANOVICH Sergey BONNEAU Richard and TUCKER Joshua A. (2017). "Detecting Bots on Russian Political Twitter". *Big Data*, 5:4, 310-324.
- STUKAL Denis SANOVICH Sergey BONNEAU Richard and TUCKER Joshua A. (2022). "Why Botter: How Pro-Government Bots Fight Opposition in Russia", *American Political Science Review*, 1-15.
- SUBRAHMANIAN Venkatramanan S. AZARIA Amos DURST Skylar KAGAN Vadim GALSTYAN Aram LERMAN Kristina ZHU Linhong FERRARA Emilio FLAMMINI Alessandro and MENCZER Filippo (2016). "The DARPA Twitter Bot Challenge", *Computer*, 49:6, 38-46.
- TAŞDELEN Birgül (2020). "Twitter'da Suriyeli Mültecilere Karşı Çevrimiçi Nefret Söylemi: #suriyelileriistemiyoruz", Gümüşhane Üniversitesi Sosyal Bilimler Enstitüsü Elektronik Dergisi, 11:2, 562-575.
- THORNTON Rod (2015). "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *The RUSI Journal*, 160:4, 40-48.
- VAROL Onur FERRARA Emilio DAVIS Clayton MENCZER Filippo and FLAMMINI Alessandro (2017). "Online Human-Bot Interactions: Detection, Estimation, and Characterization", In *Proceedings of the International AAAI Conference on Web and Social Media*, 11, 280-289.
- VAROL Onur and ULUTURK Ismail (2020). "Journalists on Twitter: Self-Branding, Audiences, and Involvement of Bots", *Journal of Computational Social Science*, 3:1, 83-101.
- WANG Alex Hai (2010). "Detecting Spam Bots in Online Social Networking Sites: A Machine Learning Approach", Sara Foresti and Sushil Jajodia (eds.), Data and Applications Security and Privacy XXIV, 335-342.
- WARDLE Claire and DERAKHSHAN Hossein (2017). "Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking", In *The Computational Propaganda Project* edited by Woolley, Samuel C., and Philip Howard.
- WOOLLEY Samuel C. and HOWARD Philip N. (2019). "Introduction", Samuel C. Woolley & Philip N. Howard (eds.), Computational Propaganda Political Parties, Politicians, And Political Manipulation On Social Media, Oxford University Press, Oxford, 3-18.
- WOOLLEY Samuel C. and HOWARD Philip N. (2017). "Social Media, Revolution, and the Rise of Political Bot", Piers Robinson, Philip M. Seib & Romy Fröhlich (eds.), Routledge Handbook of Media, Conflict and Security, Routledge/Taylor & Francis Group, London/New York, 282-292.
- YANG Chao HARKREADER Robert and GU Guofei (2013). "Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers", *IEEE Transactions on Information Forensics and Security*, 8:8, 1280-1293.
- YANG Kai-Cheng VAROL Onur DAVIS Clayton A. FERRARA Emilio FLAMMINI Alessandro and MENCZER Filippo (2019). "Arming the Public with Artificial Intelligence to Counter Social Bots", *Human Behavior and Emerging Technologies* 1:1, 48-61.
- YILMAZ Fahri ELMAS Tugay and ERÖZ Betil (2023). "Twitter-Based Analysis of Anti-Refugee Discourses in Türkiye", *Discourse & Communication*, 17:3, 298-318.

Internet Sources

- "No Reason to Lift Russian Ban on Twitter Roskomnadzor," April 10, 2023. https://interfax.com/newsroom/top-stories/89467/, accessed 11.12.2023.
- "Russia Criminalizes Independent War Reporting, Anti-War Protests," March 7, 2022. https://www.hrw.org/news/2022/03/07/russia-criminalizes-independent-war-reporting-anti-war-protests, accessed 11.12.2023.
- Aleksejeva, Nika, Andriukaitis, Luiza Bandeira, Donara Barojan, Graham Brookie, Eto Buziashvili, Andy Carvin, et al. "Operation Secondary Infektion." Digital Forensic Research Lab: The Atlantic Council, June 22, 2019. https://www.atlanticcouncil.org/in-depth-research-reports/report/operation-secondary-infektion/, accessed 15.12.2023.

- Clayton, James. "Twitter Moves to Limit Russian Government Accounts," April 5, 2022. https://www.bbc.com/news/technology-60992373, accessed 03.05.2022.
- European Commission. "Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions," 2018. https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf, accessed 20.11.2022.
- European Parliament. "European Parliament Resolution of 23 November 2016 on EU Strategic Communication to Counteract Propaganda against It by Third Parties," November 23, 2016. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441 EN.html?redirect, accessed 11.12.2023.
- Giles, Keir. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016. https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook,%20Russian%20Information%20 Warfare.pdf., accessed 15.12.2023,
- Graham Timothy, Bruns Axel, Zhu Guangnan and Campbell Rod (2020). "Like a Virus: The Coordinated Spread of Coronavirus Disinformation." The Australia Institute, 2020. https://eprints.qut.edu.au/202960/1/P904 Like a virus COVID19 disinformation Web .pdf, accessed 18.10.2022.
- Gregory Paul Roderick (2014). "Inside Putin's Campaign Of Social Media Trolling And Faked Ukrainian Crimes Paul Roderick Gregory." Forbes, May 11, 2014. https://www.forbes.com/sites/paulroderickgregory/2014/05/11/inside-putins-campaign-of-social-media-trolling-and-faked-ukrainian-crimes/?sh=15dbee407140, accessed 11.12.2023.
- Harding, Luke. "Russia Blocks Access to Facebook and Twitter," March 4, 2022. https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter, accessed 03.05.2022.
- Jack, Caroline. "Lexicon of Lies: Terms for Problematic Information." Data & Society Research Institute, 2017. https://datasociety.net/wp-content/uploads/2017/08/DataAndSociety_LexiconofLies.pdf, accessed 11.11.2023.
- Lucas, Edward, and Peter Pomeranzev. "Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda," 2016. https://cepa.ecms.pl/files/?id_plik=2715, accessed 20.12.2023.
- Office of The High Commissioner for Human Rights. "Ukraine: Emergency-UNHCR Data Portal", October 08, 2023, https://data.unhcr.org/en/documents/download/104244, accessed 11.11.2023.
- PAUL Christopher and Miriam Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model", RAND Corportation, 2016. https://www.rand.org/pubs/perspectives/PE198.html, accessed 11.12.2023.
- POMERANTSEV Peter. "Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare", The Atlantic, 2014. https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/, accessed 15.12.2023.
- Statista, "Number of Social Media Users Worldwide as of October 2023", https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%20 2023&text=Of%20this%20total%2C%204.95%20billion,population%2C%20were%20social%20 media%20users, accessed 28.12.2023.
- Twitter. "Update on Twitter's Review of the 2016 US Election", January 19, 2018. https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html, accessed 03.05.2022.
- US. Department of Justice. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", 2019. https://www.justice.gov/archives/sco/file/1373816/download, accessed 03.05.2022.
- Weir, Fred. "In Russia, Critiquing the Ukraine War Could Land You in Prison", The Christian Science Monitor, December 5, 2022. https://www.csmonitor.com/World/Europe/2022/1205/In-Russia-critiquing-the-Ukraine-war-could-land-you-in-prison, accessed 11.12.2023.
- Wojcik, Stefan, Solomon Messing, Smith, Aaron, Lee Rainie, and Paul Hitlin. "Bots in the Twittersphere," 2018. https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/, accessed 11.12.2023.
- Wright Jordan and Anise Olabode (2018). "Don't @ Me, Hunting Twitter Bots at Scale", Duo Labs, 2018. https://i.blackhat.com/us-18/Wed-August-8/us-18-Anise-Wright-Dont-@-Me-Hunting-Twitter-Bots-at-Scale-wp.pdf, accessed 15.12.2023.
- Yin, Leon, Roscher Franziska, Bonneau Richard, Nagler Jonathan and Tucker Joshua A. (2018). "Your Friendly Neighborhood Troll: The Internet Research Agency's Use of Local and Fake News in the 2016 US Presidential Campaign", SMaPP Data Report, 2018. https://csmapnyu.org/assets/publications/2018_01_IRA_Presidential_Campaign.pdf, accessed 15.12.2023.