Conference Paper

Social Bots As an Instrument of Influence in Social Networks: Typologization Problems

V.V. Vasilkova and N.I. Legostaeva

Saint-Petersburg State University, Russia, Saint-Petersburg

Abstract

Nowadays, in the field of social bots investigations, we can observe a new research trend — a shift from a technology-centered to sociology-centered interpretations. It leads to the creation of new perspectives for sociology: now the phenomenon of social bots is not only considered as one of the efficient manipulative technologies but has a wider meaning: new communicative technologies have an informational impact on the social networks space. The objective of this research is to assess the new approaches of the established social bots typologies (based on the fields of their usage, objectives, degree of human behavior imitation), and also consider the ambiguity and controversy of the use of such typologies using the example of botnets operating in the VKontakte social network. A method of botnet identification is based on comprehensive methodology developed by the authors which includes the frequency analysis of published messages, botnet profiling, statistical analysis of content, analysis of botnet structural organization, division of content into semantic units, forming content clusters, content analysis inside the clusters, identification of extremes — maximum number of unique texts published by botnets in a particular cluster for a certain period. The methodology was applied for the botnet space investigation of Russian online social network VKontakte in February and October 2018. The survey has fixed that among 10 of the most active performing botnets, three botnets were identified that demonstrate the ambiguity and controversy of their typologization according to the following criteria: botnet "Defrauded shareholders of LenSpetsStroy" — according to the field of their usage, botnet "Political news in Russian and Ukrainian languages" — according to their objectives, botnet "Ksenia Sobchak" — according to the level of human behavior imitation. The authors identified the prospects for sociological analysis of different types of bots in a situation of growing accessibility and routinization of bot technologies used in social networks.

Keywords: social bots, botnets, classification, VKontakte social network.

Corresponding Author:
V.V. Vasilkova
v-vasilkova@list.ru

Published: 21 January 2021

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the XXIII International Conference Conference Committee.

1. Introduction

Studies of bot technologies operating in social networks are among the youngest ones but at the same time it is a highly promising research field. However, over the past

How to cite this article: V.V. Vasilkova and N.I. Legostaeva, (2020), "Social Bots As an Instrument of Influence in Social Networks: Typologization Problems" in *Culture, Personality, Society in the Conditions of Digitalization: Methodology and Experience of Empirical Research Conference*, KnE Social Sciences, pages 823–830. DOI 10.18502/kss.v5i2.8433

years within this field, we can distinguish the newest research trends, one of which is the shift of the theoretical-methodological paradigm explaining the communicative nature of social bots.

In the beginning, social bots were seen as automated computer programs that allow spreading information in online social networks with high speed and efficiency, imitating the behavior of social networks real users [5]. This interpretation of social bots appeared in the field of computer sciences and was connected to the research of computer security. A technology-centered interpretation directed researchers towards the goal of identifying social bots and fighting against them as bots were seen as an instrument of public opinion manipulation.

The emergence of a broader and more flexible interpretation of bots is connected to a socially centered version. It has been initiated by sociologists who expressed their interest in different forms of automatization in social networks [11]. In this context, a social bot is seen as a program that automatically produce and share content and interact with humans on social media [6, 10]. This interpretation transforms social bots into new research subject for sociology and brings new research perspectives to sociologists. First of all, the range of the investigated social bots is increasing: now these are not only fake accounts but also operating within social networks chatbots, spambots, scan bots, semi-automatized cyborg bots, etc. Secondly, there is a shift in research focus: now the social bot phenomenon is seen not only as one of the efficient manipulative technologies but in a broader sense — as a new communicative technology of informational impact in the social network space. Thirdly, this approach allows investigating structural and functional features of social bots and, specifically, the objectives of their usage by different social actors more broadly and diversely. At the same time, it is important to highlight the routinization of bot technologies. Their growing accessibility allows us to expect that more and more actors will be using this instrument to broaden their influence in the information space of social networks. Fourthly, this interpretation makes us re-consider the conventional approaches to social bots' investigation, including their typologization approaches.

The objective of this research is a characterization of major established types of social bots' classifications and identification of their usage controversies, that are being revealed during the research of social bots operating in the VKontakte social network. As a case, we took bots identified during empirical research of bot–space of Russian online network VKontakte.

First classification criteria for social bots is a field of activity where the bots are used. Among them we highlight the most significant — politics [14, 16, 17, 20, 22, 25, 26], marketing [15, 17, 18], social problems solutions [2, 12, 19, 24].

The second classification criteria is a division of social bots according to their goals into benign and malicious bots [10]. Benign bots generate content, automatically react to the messages, perform useful services (these are mostly news bots and also sport bots, traffic-bots, etc). Malicious bots are being developed for performing the harmful activities (spam, stealing of private information, the spread of misinformation and information noise during political debates, the spread of harmful software, etc.) The majority of bots that are being used for political electoral practices and astroturfing have malicious effects [3, 12, 13] as they create the distortion in perceiving of information product and, therefore, provoke a conflict situation.

Third classification criteria — division of bots according to a degree of human behavior imitation [5]. Some bots imitate the behavior of real social media users both in a way they create content and build interactions with other users. Some bots do not hide the fact that their performance is based on certain algorithms. Their profile descriptions clearly show that they are bots [1, 6]. Still, it is noted that human behavior imitation is mostly used in the operation of malicious political bots [21].

We will consider the features (and the controversies identified by us) of usage of these typologies concerning social bots' performance in the VKontakte online social network.

2. Methodology and Methods

Drawing on the broader understanding of social bots, authors created a method of botnet identification in VKontakte social network, based on content replication criteria combining with two other set parameters: 1) the network should have at least 10 bots, 2) the spread of one unique content should be no more, than 2 hours. This approach allows authors to identify the clusters of social bots that form a botnet. Authors consider a botnet as a publishing complex in the VKontakte social network that consists of 5 components: technological accounts (social bots), content locations, content, software and operator(s). The botnet uses social bots to form a coherent publication of information materials on certain topics in specific publication locations. Data was collected over a limited period — February and October of 2018, based on 44 topics, including politics-related topics, marketing-related and topics related to the social sphere. In February 2018 we have collected a data set composed of 10,744,103 posts and comments with keywords. Out of the total number, 7,634,936 are the posts and 3,109,167 are the comments. In October 2018 we have collected a second data set composed of 23,350,241 posts and comments with initial keywords. Out of the total number, 15,697,341 are the posts and 7,652,900 are the comments. Thus, the final data set reached 34,094,344 publications (including the duplicated ones).

The author's methodology of botnet structure identification is complex and combines a method of frequency analysis of published messages; botnet profiling, that includes static and behavioral analysis of the user's profile data; statistical analysis of the content with the use of timing histograms showing the periods of content spread with the concurrent visualization of graphs of "content-author" ratio; analysis of structural organization of bot network and also the content analysis to identify the topic of the botnet.

For the research purposes, the following software was used: ElasticSearch, Kibana, Tableau Desktop, Tableau Server and PHP scripts for data download using VK API and data processing. To identify the botnet structures from the ratio graphs "author-content" we used clustering algorithms of the Natural library for the software platform Node.js based on JavaScript. As a result of the automatic data processing, 42 botnets have been identified. During the analysis of the content published by those 42 botnets, we have created a data set, consisting of 384 unique (non-replicated) texts. As a result of content division into "unigrams", "bigrams" and "trigrams" we have created clusters of content. While making a graph where the nodes represented texts and semantic units we used the metric «Class modularity». The calculation of the «Class modularity» metric for every node within the given networks was based on the algorithm described in the article written by Blondel V.D., Guillaume J.-L., Lambiotte R., Lefebvre E. [4]. As a result of automated data classification, 43 content clusters published by the botnets were formed. Analysis of content extremes allowed us to form top-10 botnets which made it possible to characterize thematic zones of the bot technologies' most active performance in the VKontakte social network during a chosen period [23].

3. Results and Discussion

During the analysis of the 10 most influential botnets in the VKontakte social network, we have identified three botnets that cannot be accurately classified based on existing typologies.

Botnet «Defrauded shareholders of LenSpetsStroy» (within this botnet there have been 34 bots, the botnet duplicated one unique text 34 times, number of unique content

— 54 texts, number of duplicated texts during the research period — 1836). When classifying this botnet according to the activity areas authors found out that the bot belongs to two topic areas. Content analysis of the botnet has shown that it belongs to the topic area «Solution of social problems» (informing the members and followers of the botnet groups about the events and initiatives organized by the united group of the defrauded shareholders). At the same time this botnet mobilizes its supporters for battle against inaction and red tape of government officials in solving problems of the defrauded shareholders; also for battle against the fraud in the real estate field, that shifts this botnet into politics related sphere and also gives it some protest potential.

Botnet «Political news in Russian and Ukrainian languages» (within this botnet there have been 41 bots, the botnet duplicated one unique text 41 times, number of unique content — 30 texts, number of duplicated texts during the research period — 1230). This bot shows ambiguity when classifying it upon the “objective” criteria. As this botnet is performing as news botnet it can be attributed to benign social botnets (publication of neutral news). But, on the other hand, when analyzing its content, we can distinguish multiple protest opposition publications either on Russian politics or political events happening in other countries (the USA, Germany, etc.), what could classify it as a malicious botnet. Such publications have a clear provocative and manipulative tone, provoking a situation of political conflict, that makes us define it as a malicious botnet.

Botnet Ksenia Sobchak (within this botnet there have been 29 bots, the botnet duplicated one unique text 29 times, number of unique content — 39 texts, number of duplicated texts during the research period — 1311). This bot shows an ambiguity when is identified from the standpoint of the criterion ”imitation of human behavior”. Botnet consists of groups and users — social bots, that, on the one hand, imitate the real users behavior based on static characteristics of the profile (name of the user, photos, date of birth, friends, followers, audio content) and, on the other hand, are easily identified as social bots (absence of the unique photos in the profile, absence of unique posts on the wall, high frequency of the publications on the wall, etc.). Most probably, this botnet can be attributed to this hardly defined bot type — cyborg — these accounts can be real humans that use the automatization methods or bots, managed by humans [8]. We need to highlight that several researchers consider the possibility of the wider spread of this type of social bots as social bots are becoming more and more ingenious and their identification is getting more and more complicated [7, 9].

4. Conclusions

In the context of new sociology-centered explanation of the social bot phenomenon we have studied the established approaches to the social bot typology (according to the spheres of their usage, goals, degree of human behavior imitation), and also using the example of three botnets identified during the empirical research in Russian social network VKontakte we showed the ambiguity and inconsistency of the use of such typologies.

These findings make us assume that the development prospects for sociological analysis of social bots will not only be focused on specifying their classification criteria but on investigating the most efficient combined strategies of bot-technologies use by different actors for informational influence in social networks.

Acknowledgment

The researches were conducted with the use of software from the Center for Sociological and Internet Research of Saint Petersburg State University.

References

[1] Abokhodair, N., Yoo, D. and McDonald, D. W. (2015, March). Dissecting a Social Botnet. Presented at *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15, Canada, Vancouver*, Association for Computing Machinery, New York, NY, United States. pp. 839–851.

[2] Arnaudo, D. (2017). Computational Propaganda in Brazil: Social Bots During Elections. Oxford: Oxford University Press, p. 39.

[3] Bessi, A. and Ferrara, E. (2016). Social Bots Distort the 2016 US Presidential Election Online Discussion. *First Monday*, vol. 21, issue 11-7. https://firstmonday.org/article/view/7090/5653. [Accessed January 12 2020].

[4] Blondel, V. D., *et al*. (2008). Fast Unfolding of Communities in Large Networks. *Journal of Statistical Mechanics: Theory and Experiment*, vol. 10, pp. 1-12.

[5] Boshmaf, Y., *et al*. (2011, December). The Socialbot Network: When Bots Socialize for Fame and Money. Presented at *Proceedings of the 27th Annual Computer Security Applications Conference. Orlando, Florida, USA*, Association for Computing Machinery, New York, NY, United States. pp. 1-10.

[6] Boshmaf, Y., *et al*. (2013). Design and Analysis of a Social Botnet. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 57, issue 2, pp. 556–578.

[7] Chavoshi, N., Hamooni, H. and Mueen, A. (2016, December). DeBot: Twitter Bot Detection via Warped Correlation. Presented at *2016 IEEE 16th International Conference on Data Mining (ICDM), Barcelona, Spain*, IEEE Computer Society, Los Alamitos, CA, USA. pp. 817–822.

[8] Chu, Z., *et al*. (2010, December). Who is Tweeting on Twitter: Human, Bot, or Cyborg? Presented at *Twenty-Sixth Annual Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA*, Association for Computing Machinery, New York, NY, United States. pp. 21– 30.

[9] Everett, R. M., Nurse, J. R. C. and Erola, A. (2016, April). The Anatomy of Online Deception: What Makes Automated Text Convincing? Presented at *Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy*, Association for Computing Machinery, New York, NY, United States. pp. 1115–1120.

[10] Ferrara, E., *et al*. (2016). The Rise of Social Bots. *Communications of the ACM*, vol. 59, issue 7, pp. 96–104.

[11] Gorwa, R. and Guilbeault, D. (2018). Unpacking the Social Media Bot: A Typology to Guide Research and Policy. *Policy & Internet*, vol. 9999, pp. 1-30.

[12] Hofeditz, L., *et al*. (2019, June). Meaningful Use of Social Bots? Possible Applications in Crisis Communication During Disasters. Presented at *Proceedings of the 27th European Conference on Information Systems (ECIS2019), Stockholm & Uppsala, Sweden*, Stockholm University, Kista, Sweden. pp. 1-16.

[13] Howard, P. N., *et al*. (2017). Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing over Twitter? *Data Memo*. Oxford: Project on Computational Propaganda.

[14] Howard, P. N. (2003). Digitizing the Social Contract: Producing American Political Culture in the Age of New Media. *The Communication Review*, vol. 6, issue 3, pp. 213–245.

[15] Mitter, S., Wagner, C. and Strohmaier, M. (2013, May). A Categorization Scheme for Social Bot Attacks in Online Social Networks. Presented at *Proceedings of the 3rd ACM Web Science Conference, Paris, France*, Association for Computing Machinery, New York, NY, United States. pp. 1-6.

[16] Pasquale, F. (2016). *The Black Box Society: The Secret algorithms That Control Money and Information*. Cambridge: Harvard University Press, pp. 320.

[17] Ratkiewicz, J., *et al*. (2011, March). Truthy: Mapping the Spread of Astroturf in Microblog Streams. Presented at *Proceedings of the 20th International Conference Companion on World Wide Web, Hyderabad, India*, Association for Computing Machinery, New York, NY, United States. pp. 249-252.

[18] Rowley, J. (2000). Product Searching with Shopping Bots. *Internet Research*, vol. 10, issue 3, pp. 203–214.

[19] Savage, S., Monroy-Hernandez, A. and Hollerer, T. (2016, February). Botivist: Calling volunteers to action using online bots. Presented at *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '16), San Francisco, CA, USA*, Association for Computing Machinery, New York, NY, United States. pp. 813-822.

[20] Sia, S., *et al*. *A Comparative Study of Chinese Online Agents on Facebook – an Anti–Taiwan Independence Expedition*. (Forthcoming)

[21] Stieglitz, S., *et al*. (2017, December). Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts. Presented at *Australasian Conference on Information Systems, Hobart, Australia*, University of Tasmania, Australia. pp. 1-11.

[22] Vasilkova, V. V. and Legostaeva, N. I. (2019). Social Bots in Political Communication. *Bulletin of the RUDN University. Series: SOCIOLOGY*, vol. 19, issue 1, pp. 121—133.

[23] Vasilkova, V. V., Legostaeva, N. I. and Radushevsky, V. B. (2019). Thematic Landscape of the Bot Space of the VKontakte Social Network. *Journal of Sociology and Social Anthropology*, vol. 22, issue 4, pp. 202–245.

[24] Velázquez, E., Yazdani, M. and Suárez–Serrato, P. (2018, February). Socialbots Supporting Human Rights. Presented at *AIES '18 Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, New Orleans, LA, USA,* Association for Computing Machinery, New York, NY, United States. pp. 290-296.

[25] Woolley, S. C. (2016). Automating Power: Social Bot Interference in Global Politics. *First Monday*, vol. 21, issue 4. https://firstmonday.org/article/view/6161/5300. [Accessed January 12 2020].

[26] Woolley, S. C. and Howard, P. N. (Eds.). (2018). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford: Oxford University Press, pp. 263.