Advances in Social Science, Education and Humanities Research, volume 315

International Conference on Pedagogy, Communication and Sociology (ICPCS 2019)

Extensive and Intensive Models of Botnet Influence over Target Audience

Valeria Vasilkova
Faculty of Sociology
St. Petersburg State University
St. Petersburg, Russia

Natalia Legostaeva
Faculty of Sociology
St. Petersburg State University
St. Petersburg, Russia

Vladimir Radushevskii
Center for Sociological and Internet Research
St. Petersburg State University
St. Petersburg, Russia

***Abstract*—In the article, authors make an overview of existing approaches to typologization of bots and suggest their own approach for distinguishing botnets based on the influence of botnets over target audience. Using the logic of this approach, authors have performed a comparative analysis of two botnets found in the "VKontakte" social network, which revealed existence of two models of influence over target audience: extensive and intensive. Among the criteria for comparative analysis, botnets are characterized by "number of technological accounts in the botnet", "intensity of publication activities". Authors assume that the choice of one of these two models depends on thematic orientation of botnets, which involves different types of potential audiences.**

***Keywords*—bots, botnets, typology of bots, botnet detection techniques, intensive and extensive models**

I. Introduction

Networks of social bots (bot – networks, botnets) – automated programs that allow transmitting information with high speed and effectiveness (also through imitating behavior of real social networks users) drew specific attention due to the huge potential of their use in different spheres and their manipulative influence that can significantly affect macro level processes (for example, outcomes of political elections) [1,6,8]. Modern information technologies increasingly offer new possibilities for botnets creation and operation. Nowadays, even a moderate user with basic media literacy and software developing skills can develop and introduce a bot [9], not mentioning specialized media developing organizations (for example, "bot factories"). Thus, the number of real and potential developers of political bots and, accordingly, their customers is growing rapidly, as well as the forms of bot-programs themselves and the ways to use them are diversifying. All of this encourages researchers and programmers to analyze the various forms and ways in which bots function, primarily in order to develop increasingly effective techniques for detecting and identifying the bots.

II. Classification of Bots in Theories

Comparative analysis of different types of bots reveals that there are various criteria for their comparison and typologization allowing to explaining specific nature of different types of bots and botnets. First, bots can be classified according to spheres (practices) of their use. Based on these criteria we can distinguish political, trade and marketing, media, chat-bots, HR-bots, bots in education, Wikipedia bots (Wiki-bots) [5,10,12-14,16-20] and others. Also, there are types of botnets related to the characteristics of the subjects – developers and customers. The most common, according to the researchers themselves, is the division of social bots into benevolent (benign) and malevolent (malign) bots [4] based on the subjects' intentions. Benign bots generate an aggregate content, automatically respond to messages, and perform useful services (news bots, weather bots, sports bots, traffic bots, etc.). Malign bots are designed for malicious activities (spam, identity theft, disinformation and information noise propagation during political debates, malware propagation, etc.). Another widely used classification of bots is based on their degree of imitation of human behavior [2]. Some accounts of bot profiles in social networks are very hard to distinguish from real users" profiles, as these accounts have completed profile fields and use popular models of the users' communication behavior in social media: they create messages that are very similar to the content created by real users, are able to discuss with the audience, etc. Other bots are being classified according to degree of human control, type of activity and external / conceptual characteristics. Accounts in social networks can be real users who use automation methods through their profiles, or profiles are already bots, which are controlled by operators and set the parameters of account activity and the replicated content [2-4,7,11,15, etc.].

At the same time researchers point out that different types of bots are used and demonstrate their productivity depending on the purposes of their creation and operation [7], in other words, depending on the choice of appropriate communicative strategy. The authors of the article present a new approach to bot typology related to the choice of communication strategy – their separation by the nature of the impact on the target audience. Authors assume that among the parameters for target audience impact when choosing bot - network communication strategy are: 1)

Corresponding Author: Natalia Legostaeva, Faculty of Sociology, St. Petersburg State University, St. Petersburg, Russia.

Fund Project: the reported study was funded by RFBR according to the research project No 18-011-00988 'The bot-space structure of online social networks: network analysis'.

quantity of technological accounts within bot network; 2) intensiveness of publication activeness. Depending on correlation of these parameters, we can speak about extensive or intensive model of target audience impact. For demonstration of this approach we used a comparative analysis of these parameters within two cases – botnets, performing in "VKontakte" social network during the period from January 1, 2018 till October 31, 2018.

III. Research Method

The analyzed botnets were found during the pilot study of the botnet space of the "VKontakte" social network, conducted as part of the research grant of the Russian Foundation for basic research on the subject "Structure of botnet space of social networks: network analysis". In order to promptly identify botnets in the "VKontakte" social network, consisting of groups of technological accounts, a special technique was developed, in which the "replicability of content" parameter was used as a link between technological accounts. On the basis of this parameter the publication complexes have been revealed and the tops of replicated texts for a certain period of time have been constructed. Also, when identifying botnets, the parameter "number of technological accounts in the botnet" and the parameter "intensity of publication activities" were taken into account, which was used to select botnets for comparative analysis. Botnet detection algorithm within the framework of the author's methodology was developed using Elastic Search software, Kibana (Discovery, Visualize, Dashboard), Tableau and PHP scripts for downloading and processing information, using VK API. The algorithm itself includes the following steps: 1) compilation of a list of keywords based on the 'frequency of mentionability' parameter in the texts in the VKontakte social network; 2) determination of the research period; 3) analysis of data integrity in Kibana / Discovery for each keyword for the selected period; 4) analysis of top-text (replicability); 5) analysis of the structure of 'text-author' correlations on the graph; 6) profiling of authors (groups) that make up the identified botnets. In the course of analysis of the profiles of technological accounts (groups) replicating the content one considered the static and behavioral features of bot profiles: a uniform design of bot profiles, the same published content on the walls of technological accounts, the same contacts and links on the profile pages.

IV. Results

Two botnets included into case study were chosen by the authors because both had similar structural organization, in other words, both botnets consisted of groups – accounts in "VKontakte" social network, but significantly varied in numbers of automated accounts in the botnet and the intensity of online publication activities. First botnet consists of 66 automated accounts, which starting from October 1, 2018 to October 31, 2018 published 3 texts (Figure 1). These texts are about advertising, repairing and on Apple products technical support. Botnet developer is the network of smartphone repairing centers in 90 cities in Russia. In the course of analysis of the network publication activities of botnet accounts, it was revealed that the average number of publications for 10 months, which falls on one technological account of the botnet No 1, is 69 publications. A median value of the coverage of botnet No 1 audience is 134,925 users of the "VKontakte" social network. Median audience of the botnet (in case of automated accounts of groups) is the sum of the average statistics of the number of followers.

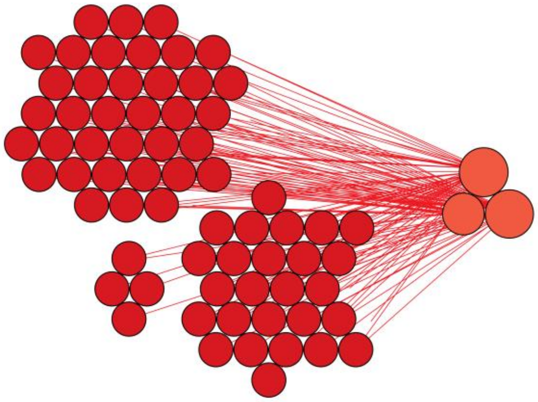

Fig. 1. Botnet No1. Nodes – authors (to the left) and content publications (to the right), edges – relationship "text - author"

The second botnet consists of 15 technological accounts, which in the period of October 1, 2018 to October 31, 2018 distributed 19 texts (Figure 2). These texts are devoted to the news and social problems of Kudrovo residents: the important objects of social service, the drug addiction problem in Kudrovo, the construction of an orange subway line to the 'Kudrovo' station, the search for missing people, and the development of the transport system, etc.

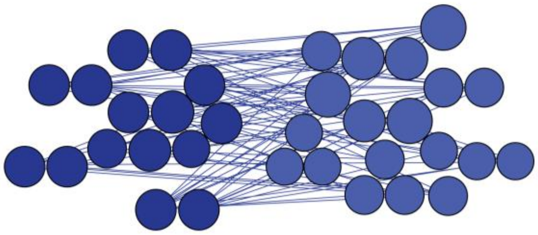

Fig. 2. Botnet No2. Nodes – authors (to the left) and publications (to the right), edges – relationship "text-author"

With much fever number of automated accounts of the botnet No 2, it's network publication activeness is much higher than of the botnet No 1. Average number of publications during the year per every automated account of the botnet No2 is 307 publications. At the same time median value of the audience outreach of the botnet No 2 is also higher than of the first botnet - 212 390 users of "VKontaakte" social network.

Results of the conducted research showed that, first, different botnets with the similar structural organization, which is reduced to connected groups – bot profiles, have different number of automated accounts within bot network. First botnet has 66 automated accounts, second – 15. Second, the botnets under study differ in their online publication activities. The first botnet in October 2018 published 3 texts, the second one – 19. During the analyzed period from January 1, 2018 till October 31, 2018 the average number of publications of one technological account of the first botnet is 69, and of the second one – 307. It shows that botnets under our investigation used different communicative strategies in terms of the intensity of interaction with potential audiences. According to our classification, the first botnet functioned according to the parameters of the extensive model, while the second botnet functioned according to the parameters of the intensive model. The authors hypothesize that the choice of any of these two models can depend on the botnet theme and need to outreach different target audiences. First extensive model of communicative strategy is targeted to more diversified audience (potential clients of the Apple products), second intensive model is targeted to more homogeneous audience localized in the same place and based on specific thematical interest (social problems of the residents of the town in town Zanevskoe, of Vsevolozhsky district of Leningrad region). Meanwhile, the second model of communication strategy proved to be quite effective, as evidenced by the greater coverage of the potential audience.

V. Conclusion

The authors are aware that the suggested typology of the models of botnets' impact on the audience, when choosing a communication strategy, requires its development related to the identification of additional parameters of modeling, as well as further verification, including through the comparative analysis of different types of botnets operating on the platform of various online social networks. In terms of future research, the authors plan to introduce additional parameters when studying botnet communication strategies. The parameters such as "botnet topics", "target group features", "number of likes", and "number of reposts" will allow the researchers to speak not only about the processes of botnets' impact on the audience, but also about the processes of interaction between bots and real users, which in the end will give a broader understanding of the degree of bot influence over the social networks users.

VI. Acknowledgment

The study was conducted using the software of the Resource Center of the Scientific Park of St. Petersburg State University "Center for Sociological and Internet Research".

References

[1] A. Bessi, E. Ferrara, "Social Bots Distort the 2016 US Presidential Election Online 8 Discussion", First Monday, 2016, vol. 21 (11).

[2] Y. Boshmaf, I. Muslukhov, K. Beznosov, M. Ripeanu, "The socialbot network: when bots socialize for fame and money", In Proceedings of the 27th Annual Computer Security Applications Conference. Orlando, Florida, USA. New York, 2011, pp. 93–102.

[3] R. Calo, "Robotics and the Lessons of Cyberlaw", Cal. L. Rev., 2015, vol. 103 (3).

[4] E. Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini, "The rise of social bots", Communications of the ACM, vol. 59(7), 2016, pp. 96–104.

[5] A. Følstad, P.B. Brandtzæg, "Chatbots and the new world of HCI. Interactions", vol. 24(4), July-August 2017, pp. 38-42.

[6] M.C. Forelle, P.N. Howard, A. Monroy-Hernandez, S. Savage, "Political bots and the manipulation of public opinion in Venezuela", Oxford, UK: Project on Computational Propaganda, 2015.

[7] R. Gorwa, D. Guilbeault, "Unpacking the Social Media Bot: A Typology to Guide Research and Polic", Policy & Internet, 2018.

[8] P.N. Howard, G. Bolsover, B. Kollanyi, S. Bradshaw, L.-M. Neudert, "Junk news and bots during the U.S. Election: What were Michigan voters sharing over Twitter?", Working Papers & DataMemos. Oxford, UK: Project on Computational Propaganda, 2017.

[9] P.N. Howard, S. Woolley, R. Calo, "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration", Journal of Information Technology & Politics, vol. 15(2), 2018, pp. 81-93.

[10] D. Murthy, A.B. Powell, R. Tinati, N. Anstead, L. Carr, S.J. Halford, M. Weal, "Automation, algorithms, and politics | Bots and political influence: A sociotechnical investigation of social network capital", International Journal of Communication, vol. 10, 2016, pp. 4952–4971.

[11] S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, N. Borisov, "Stegobot: a covert social network botnet", in International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 2011, pp. 299-313.

[12] G. Neff, P. Nagy, "Automation, algorithms, and politics| talking to bots: symbiotic agency and the case of tay", International Journal of Communication, vol. 10, 2016, pp. 4915–4931.

[13] F. Schäfer, S. Evert, P. Heinrich, "Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe's Hidden Nationalist Agenda", Big data, vol. 5 (4), 2017, pp. 294-309.

[14] S. Shorey, P.N. Howard, "Automation, Algorithms, and Politics| Automation, Big Data and Politics: A Research Review", International Journal of Communication, vol. 10, 2016, pp. 5032–5055.

[15] S. Stieglitz, F. Brachten, B. Ross, A-K. Jung, "Do Social Bots Dream of Electric Sheep? A Categorisation of Social Media Bot Accounts", Australasian Conference on Information Systems. Hobart, Australia, 2017.

[16] M. Tsvetkova, R. Garc ía-Gavilanes, L. Floridi, T. Yasseri, "Even good bots fight: The case of Wikipedia", PLoS ONE 12(2): e0171774, 2017.

[17] B. Waugh, M. Abdinpanah, O. Hashemi, S.A. Rahman, D.M. Cook, "The Influence and Deception of Twitter: The Authenticity of the Narrative and Slacktivism in the Australian Electoral Process", Proceedings of the 14th Australian Information Warfare Conference. Edith Cowan University, Perth, Western Australia, 2013, pp. 27-38.

[18] J.A. Williams, D.M. Miller, "Netizens Decide 2014? A Look at Party Campaigning Online. In Japan Decides", 2nd ed. Palgrave Macmillan, London, 2016, pp 144-152.

[19] S.C. Woolley, "Automating power: Social bot interference in global politics", First Monday, vol. 21 (4), 2016.

[20] S.C. Woolley, P.N. Howard, "Automation, algorithms, and politics| political communication, computational propaganda, and autonomous agent – Introduction", International Journal of Communication, vol. 10, 2016, pp. 4882–4890.