Botnets as an election campaign tool: a methodology for identification and analysis of network publication activity[1]

N. Legostaeva, V. Vasilkova, V. Radushevskii

St. Petersburg State University, e-mails: n.legostaeva@spbu.ru, v.vasilkova@spbu.ru, v.radushevsky@spbu.ru

Abstract

In recent years, political botnets are becoming an important tool of political communication, particularly in the course of election campaigns, which makes examination of their functioning and ways of their detection relevant. In the paper, taking into account the existing methods of botnets detection, the authors propose their own mixed-method approach to detect botnets. The core parameter of this approach is a "replicable publication". The algorithm presented in the paper combines the method of analyzing the graph structure of an author's relation to a publication, that of constructing time diagrams for the distribution of identical publications and structural botnet analysis that builds on profiling accounts and includes static characteristics of detection of technological agents. This method was tested in the analysis of the March 2018 presidential elections in the Russian Federation. As a result, in VKontakte social network, the study detected several botnets related to the names of two presidential candidates. The study concluded that different botnet structures help political leaders use different communicative tactics when interacting with their potential electorate.

Keywords: political bots, election campaigns, techniques of botnet detection, VKontakte social network, network publication activity, content's replicability.

Introduction. Botnets in the practices of election campaigns

The space of political communication has transformed with the emergence of social networks that brought into existence a new massive social platform where people can express their civic position. This function becomes more relevant in the periods of important political events: referendums, presidential and municipal elections.

However, in recent years in the context of social control and political manipulation, an ambivalent nature of social networks has become an important focus of research. On the one

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

hand, social networks are a factor in the development of democratic institutions, on the other hand, they are a source of threats to democratic freedoms.

Researchers have identified and described practices of bot technologies use in election campaigns of different levels - from municipal to presidential – in different countries (Cook et al., 2014).

First studies of bot technologies use in the USA addressed the 2010 mid-term elections to the U.S. House of Representatives and elections in Massachusetts (Massachusetts Special Election - MASEN) in 2010 (Metaxas, Mustafaraj, 2012; Ratkiewicz et al., 2010). The studies detected bot attacks on candidates from both sides – from representatives of different political forces. In 2010, researchers from Indiana University detected bot campaigns against Chris Coons, the presidential candidate from the Democrats who won early elections from the state of Delaware in 2010. In the course of the 2012 election cycle, organizers of Mitt Romney's campaign were accused of using bot accounts on Twitter in order to increase the number of supporters and the popularity of Mitt Romney (Howard, Woolley & Calo, 2018, p. 87).

The 2016 U.S. presidential campaign registered the most frequent use of bot technologies directed at both Democratic and Republican candidates (see Howard et al., 2017; Bessi, Ferrara, 2016). During only one month of observation, Bessi and Ferrara counted almost 400,000 bots that accounted for almost one-fifth of all tweets related to political discussions about the presidential elections (Bessi, Ferrara, 2016, p. 14). The bots employed helped construct a positive image of the candidate and delegitimize images of political opponents. In particular, the study detected bots that mimicked Latin-American voters supporting Trump. This became in contrast with Trump's anti-immigration rhetoric that turned away many Latin-American voters. During the same time, Twitter and Facebook botnets accused Hilary Clinton of her engagement in scandalous stories related to pedophilia and corruption. These accusations implied that Russian automated cyber teams participated in the bot attacks. In these elections, political bots aimed to manipulate political discussions, demobilize opposition and form a non-existing army of political supporters (Howard et al., 2017, p. 1).

During the referendum in Great Britain, bot-campaigns advocated the country's exit from the European Union (Howard, Kollanyi, 2016).

In Mexico, the 2012 presidential elections registered first examples of computer outreach. The eve of general 1 July 2018 elections saw similar strategies of automated accounts use aimed to increase political polarization. In form of headlines discrediting some of the presidential candidates, their photos supplemented with false statistics and political statements, a huge amount of disinformation appeared on Twitter, Facebook and WhatsApp platforms (Glowacki et al., 2018).

In Venezuela, political bots were instrumental for the far-right opposition forces (Forelle et al., 2015). There are studies focusing on the use of automated accounts by the leading politicians in Brazil during the 2014 presidential elections, 2016 impeachment and in the course of 2016 municipal elections in Rio de Janeiro (Arnaudo, 2017).

The 2014 elections in Japan revealed that political Twitter bots disseminated information in favor of the prime-minister Shinzo Abe (Schäfer, Evert, Heinrich, 2014). Other examples that link together political VIPs and bot technologies relate to agents of the North Korea National Intelligence Agency. The agents disseminated more than 1,2 million messages on Twitter in order to shape public opinion in favor of the presidential candidate Park Geun-hye who won the 2012 elections (Woolley, 2016).

Summarizing the analysis of practices of bot-campaigns carried out in election campaigns of different levels, the authors identify three main communication strategies that get implemented with the help of bot-campaigns: 1) attracting a great number of potential candidate supporters, 2) constructing a positive politician's image and 3) discrediting a political opponent. Tactics of implementation of these base strategies depend upon a particular electoral situation.

Drawing from this analysis of bot-campaigns, political communication researchers can say that botnets are becoming a communication tool in election campaigns (Howard, Woolley, Calo 2018, p. 86). Different bot-types engender a wide variety of bot detection mechanisms and techniques that presuppose studies combining both programming methods and that used in social sciences because programmers of automated algorithms themselves can hardly forecast the outcomes of using bots (Woolley, Howard, 2016, p. 4883).

Comparing and contrasting the existing mechanisms and techniques of bot detection, this paper presents the authors' method to detect political botnets and the results of applying this method to the analysis of the 2018 presidential elections in the Russian Federation.

Mechanisms and techniques to detect and analyze political bots and botnets

The examination of bot detection methods and techniques has shown that different researchers use similar mechanisms to detect automated algorithms but the combinations of algorithms vary. The literature reveals the following known mechanisms: frequency analysis of posts and comments (Bolsover&Howard, 2018; Howard, Kollanyi, 2016), analysis of bot static characteristics (whether a profile has unique photos, biographic information, number of friends and followers, date of account's creation, etc.) (Howard, Woolley&Calo, 2018; Chu, Gianvecchio, Wang&Jajodia, 2010; Grimme et al., 2017), machine-learning techniques (Bessi, Ferrara, 2016; Schäfer, Heinrich, 2017), method of automated bot detection (Grimme et al., 2017) and other mechanisms.

G. Bolsover и P. Howard have searched Twitter and Sina Weibo social networks for the evidence of automated accounts in China. They used a mixed-method approach that combined a frequency analysis of posts and comments and Botometer developed by the researchers from Indiana University (Bolsover&Howard, 2018). With the help of BotOrNot framework they detected 54,7% of automated accounts in the dataset consisting of 100 users. The content generated by such automated accounts accounted for 30% of their data. Christian Grimme, Mike Preuss, Lena Adam and Heike Trautmann presented a different view on the use of the automated tool of bot programs detection. They concluded that the tool is imperfect because 'a friendship network' and 'account's activity over time' are parameters not sufficient enough to differentiate between a bot and a real user. The content of posts and comments and some profile characteristics are the only indicators of a bot profile (Grime et al., 2017, p.21).

P. Howard и B. Kollanyi have found bot accounts on Twitter during the UK referendum on EU membership. They collected 1,5 million tweets produced by 313,832 distinct Twitter user accounts. To collect the data they followed hashtags associated with the argument for leaving the EU, that associated with the argument for staying in EU and hashtags that did not specifically relate to leaving or remaining in EU (Howard, Kollanyi, 2016, p. 3). Based on the frequency analysis (the frequency that particular hashtags are used by users or bots), they found out that accounts using exclusively neutral hashtags were rarely automated, while one-third of the tweets using a mixture of all hashtags were generated by accounts that used heavy automation. The other finding is that only less than one percent of the sampled accounts generated almost a third of all Twitter traffic about the UK referendum.

When examining U.S. political bots on Twitter, P. Howard, S. Woolley and R. Calo analyzed bot static characteristics such as a screen name, whether a profile had unique photos, biographic information, number of friends and followers, account creation date, etc. (Howard, Woolley&Calo, 2018; Chu, Gianvecchio, Wang&Jajodia, 2010). The researchers have distinguished between two types of Twitter bot platforms that help users create and manage a botnet. One is TweetDeck and TwitterWebClient platforms that allow users to manage several accounts, with a limited number of accounts that can be managed. The other type is Botize, MasterFollow и UberSocial platforms that can load massive amounts of content which are distributed by many already existing accounts with adjustable delivery schedule. These platforms limit users in their bot management. The researchers have noted that, in Venezuela, Botize and MasterFollow were the most popular bot platforms through which the information related to political leaders was distributed (Forelle et al., 2015).

When detecting bots on Twitter during the 2016 U. S. elections, A. Bessi and E. Ferrara used several machine-learning methods that helped measure conversation dynamics in social media over time. In their study, they focused on exogenous factors (such as information on political debates and press-releases), endogenous factors (for instance, who supports who) and a geographical dimension of the conversation (Bessi, Ferrara, 2016). When studying Twitter bots during the 2014 election in Japan, F. Schäfer, S. Evert, and P. Heinrich employed a corpus linguistics method with using algorithms to automatically detect duplicates (Schäfer, Evert, Heinrich, 2017).

Russian researchers developed mechanisms to discern botnets and methods of their examination. For instance, for bot identification, Alymov A.S., Baranyuk V.V. and Smirnova O.S. look at account's activity and static characteristics. To discern a bot profile from that of a human user, they developed a list of indicators, each having a different weight in a summary profile score (Alymov, A.S., Baranyuk, V.V., Smirnova, O.S., 2016). Like other researchers, they distinguish two types of bots: automated ones that follow simple pre-programmed instructions and manageable bots that are controlled by an operator who takes part in discussions in a semi-automated mode. This method of bot identification includes two mechanisms of discerning bot from human users. One is analysis of information collected during the time when users are logged in (on-line analysis). The other mechanism is analysis of users' profile information (off-line analysis) (Alymov, A.S., Baranyuk, V.V., Smirnova, O.S., 2016, p. 57). The first mechanism focuses on account activity characteristics such as user's posting quick comments, comments posted from different accounts but from one IP address during a short time, trivial comments or comments unrelated to the topic and duplicate comments (drones). Off-line analysis explores static characteristics of a bot profile: no account verification, abnormal number of friends and followers, account that posts many comments having too few friends and followers, many incomplete profile fields, no unique user's avatar, no unique author's publications (only reposts of other users' comments), invalid account's name, no comments from other users on account's wall, lots of advertising posts, harmful links and other characteristics.

Analyzing automated virtual users, Chesnokov V.O. employs a graph analysis of immediate environment. To analyze bot profiles, he advocates using a mixed-method approach that combines analysis of a bot profile activity, static and semantic analyses of texts, and analysis of user connections with the help of an algorithm that finds communities (Chesnokov V.O., 2017). To study botnets, Katasev A.S., Kataseva D.V. and Kirpichnikov A.V. use machine-learning methods such as neural networks, decision tree and logarithmic regression (Katasev, A.S., Kataseva, D.V., Kirpichnikov, A.V., 2015). When examining botnets on Twitter, in addition to the machine-learning methods, they analyze static and account actitvity characteristics.

Instead of focusing on unique bot profiles, Kotenko I.V., Konovalov A.M. and Shorov A.V. examine a botnet – a computer network consisting of many hosts with its own software which is a bot (Kotenko, I.V., Konovalov, A.M., Shorov, A.V., 2011, p.24). Drawing on the mechanism of traffic generation to model botnets, they use algorithms with static characteristics that are similar to the characteristics of real network's traffic. They test different architecture of modeling environment meant for botnet analysis.

To detect political bots, D.S. Martyanov looks at static characteristics such as almost incomplete profile, no photos, subscribing to publics that are unrelated and other characteristics. Martyanov notes the recent increase in the use of political automated bots in order to change topics of political discussions. But bots inability to have a dialogue and their repetitive content has resulted in a greater involvement of human resources to improve robot's functions (Martyanov, D.S., 2016, p. 74). Bot factories become part of a political discourse and an important factor of political cyber-environment. The author notes that a crucial role is played not by large 'bot factories' but by press offices of political leaders and that of parties that administer official websites and weblogs and lead information wars with the help of bots.

Thus, development of information infrastructure leads to the development of automated algorithms. Bot accounts get more sophisticated and complex, thus, in the near future, making the analysis of static and account activity characteristics for their detection insufficient. Therefore, the near future research of automated records lies in the multidisciplinary perspective and mixed method approach to detect bots, in the so-called 'hybrid detection systems that are able to judge on content, background strategies and distributed narratives by the inclusion of human intelligence' (Grimme et al., 2017, p. 22).

The authors note that in Russia despite works on the mechanisms of bot detection, there are no works on application of these mechanisms to the analysis of political practices including online political practices. This makes the present research relevant and of forward-looking nature.

Mechanism of rapid detection of political bots in VKontakte social network

Taking into account the existing mechanisms of bot and botnet detection, the authors have developed their own tool to detect botnets on VKontakte social network. The mechanism includes the frequency analysis of comments and posts, bot account profiling that examines static characteristics of user profile, static analysis of texts when constructing time histograms at the time of content distribution, building graphs that depict 'author-text' relation and structural botnet analysis. This tool was tested in the analysis of the March 2018 presidential elections in the Russian Federation.

We called bot accounts that disseminate political propaganda about presidential candidates the 'technological accounts' which is one component of the automatic or semi-automated (human participation is needed) publishing complex in VKontakte social network. The other four components of the publishing complex are the following: publication sites, publications, software, operator(s). We define a botnet as a publishing complex consisting of N1 technological accounts that coordinate the publication of N2 theme-based issues in N3 places (where Nn – a given quantitative parameter).

In order to detect botnets consisting of several technological accounts, we looked at a 'replicable publication' through which technological accounts are linked. By means of a 'replicable publication' we have detected publication complexes and have built a top list of replicable texts over a given time period. In this the proposed mechanism differs from other discussed above tools which focus on account automation and the structure of user connections.

The other distinctive feature of this mechanism is the structural analysis of botnets which includes the examination of profiles of technological accounts. These accounts can consist of such components as: users, events, groups, pages, users+groups+pages, events+groups and other components. A chosen combination of components determines the audience size of the distributed content. The VKontakte users are more likely to trust the content distributed by a bot account that has real users in its contact groups compared to the content distributed by groups that have technological accounts as their contacts.

For the purposes of the study, the following software programs were used: Elastic Search, Kibana (Discovery, Visualize, Dashboard), Tableau and, for data downloading and processing, PHP scripts, including VK API. To build time histograms, we used the following parameters: time of publication distribution, visualization of 'text - authors' relationships. In the 'text - author' field, the graph nodes represent publication authors, the edges are number of publications. The content analysis of texts includes a publication date, time of publication distribution, number of replications, and content structure (text+link, text+picture, text+video , etc.). When studying pages of technological accounts replicating content, we look at static and account activity characteristics of bot profiles.

The procedure of botnet detection includes nine steps. Step One is making a list of keywords based on the analysis of online media, results of surveys, focus groups, reports, rating lists and lists of replicated texts over a certain time period. Step Two is determining a study's duration. Step Three is, with the use of Kibana /Discovery, for every keyword, to examine data completeness over a given time slot. Step Four is putting lacking keywords into the PHP scripts that get data from VK API and save them in the Elastic Search program. Step Five is adding to work assignment procedures on making data complete (filling blanks resulted from extension of the study duration or from technical failures when accessing VK API).

Step Six is analyzing network publication activity and 'text - author' relationships. This step includes two parts: one (6.1) is examination of top list of replicable texts and time histograms of their publication. The other step (6.2) is analysis of 'text - author' relationship structure shown at a graph. Step Seven is analyzing content and profile structure: step 7.1 is looking at the content of texts (altering keywords to better focus on particular texts) and step 7.2 is profiling of the author (groups, pages, events and users) that the detected botnets consist of (see steps 6.1 and 6.2).

Step Eight is making inferences and getting interim results: step 8.1 is making lists, tables, graphs and maps and step 8.2 is focusing on research subjects (communities, authors, study duration, themes and other subjects). Finally, Step Nine is deciding to make changes in the study – extending or refining a keyword list, extending or changing study duration (in case of deciding to make changes in the study, return to Step One).

Research Findings

To examine network publication activity of technological publication complexes on VKontakte[2], we made a list of last names of presidential candidates for 18 March 2018 elections

[2] VKontakte (internationally known as VK) is a Russian social network comprised of 97 million active users a month, 6,5 billion messages a day. As of 20 June 2018, judged on the duration of staying logged in, it is a number one network. Like users of other social networks, VKontakte users have access to such capabilities as: creating a profile with personal information, creating and distributing content, flexible features of account settings, private interaction with other users (via personal messages) and public interaction (through posting comments on the walls and by means of groups and meetings), following activities of friends and communities through newsfeeds. Besides writing messages, users can make comments to already published content. Photos, audio- and video recordings (including feature films), documents and survey links can be attached to messages. The capabilities of uploading user own recordings and using files uploaded by other users make VKontakte one of the biggest Runet's media archives. In addition, there are applications for iOS, Android and Windows Phone platforms.

in the Russian Federation. The list included the following last names: Baburin, Grudinin, Zhirinovsky, Putin, Sobchak, Suraikin, Titov and Yavlinsky. In January and February 2018, the top-20 list of replicable publications consisted of texts that referred to Sobchak[3] and Grudinin[4].

When refining the study's duration (January 24 - 31, 2018) using 'Sobchak' keyword, we have collected a data set consisting of 34,334 posts and comments (namely, 20,240 posts and 14,094 comments) which were written by 22,576 authors and posted on 15,416 publication sites (groups, pages, events, user walls). During the selected time slot, we have detected two botnets. Publications on the first botnet addressed news about entertaining 'Dom-2' reality show. Publications on the second botnet informed VKontakte users about 2018 presidential elections. Information distributed by both botnets contained 'Sobchak' keyword, with news on the first botnet referring to Ksenia Sobchak's personal and social life, while news on the second botnet related to her political activity.

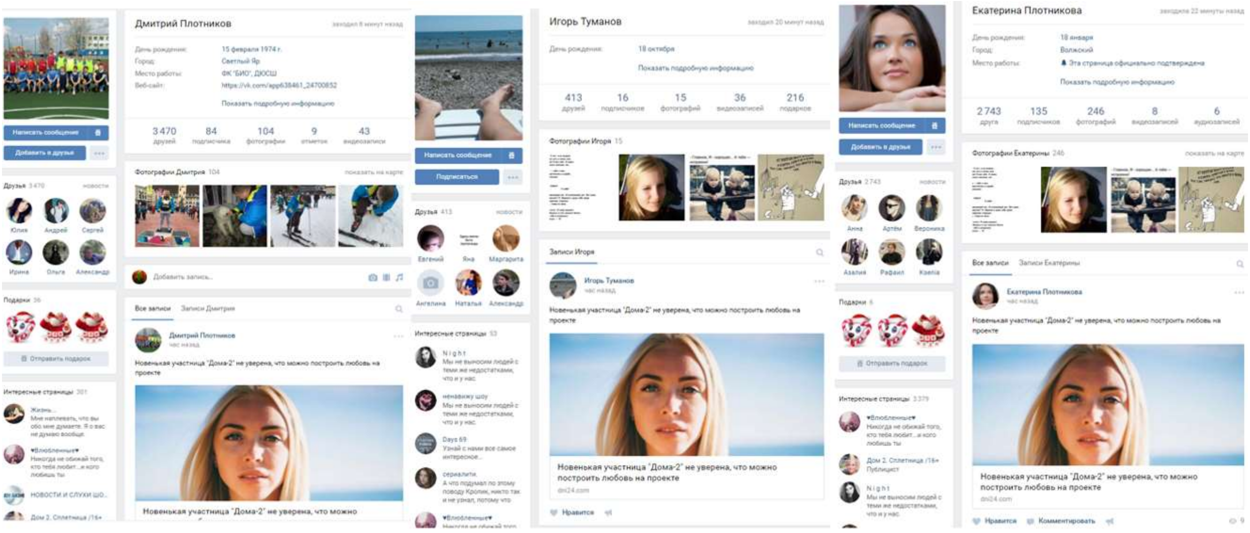
The first botnet consisted of 24 technological accounts – accounts of VKontakte users, groups and pages. On their own walls, these accounts distributed posts with the same content (text+link) over 30-40 seconds, with one publication being distributed 24 times (on each of the 24 technological accounts). When profiling these technological accounts, we have identified the following static characteristics: abnormal number of friends and followers, no unique content on authors' walls, no unique photos, same photos on walls of different accounts, incomplete profile fields, high network publication activity, the same published content on technological accounts' walls (Picture 1). The total number of botnet's friends and followers accounted to 339,945 VKontakte users[5] (see Attachment 1).

Picture 1. Technological accounts of #1 botnet formed by 'Sobchak' keyword (#1 user, #2 user, #3 user).

[3] Sobchak Ksenia Anatolyevna (born 11.05.1981, Leningrad, USSR) is a Russian politician, anchorwoman and a radio host, journalist, public figure, an actress. She is known for her roles in 'Dom-2' reality show, 'Blonde in Chocolate', and 'Last Hero' films and for being an anchorwoman on 'Sobchak live' TV show (on 'Rain' TV channel). She was a member of the Coordinating Council of the Russian opposition (starting with 10.22.2012 till 10.19.2013). In 18 March 2018 presidential elections, she ended up at fourth place, with 1,237,692 (1,68 %) votes.

[4] Grudinin Pavel Nikolaevich (born 10.20.1960, Moscow, RSFSR, USSR) is a Russian politician, mechanical engineer, lawyer, businessmen. Since 1995, he has managed 'Lenin Sovkhoz' farming cooperative in Lenin Sovkhoz rural settlement of the Lenin region of Moscow district. He is the honored worker of agriculture of the Russian Federation (2001). In 2018 presidential elections, he was a presidential candidate from the Communist Party of the Russian Federation (CPRF) and ended up at second place having gathered 11,77 % of votes.

[5] Number 1 botnet audience was counted on February 20, 2018.



Дмитрий Плотников

День рождения: 15 февраля 1974 г.
Город: Светлый Яр
Место работы: ФК "БИО", ДЮСШ
Веб-сайт: https://vk.com/app638461_24700852

3 470 друзей · 84 подписчика · 104 фотографии · 9 отметок · 43 видеозаписи

Дмитрий Плотников
Новенькая участница "Дома-2" не уверена, что можно построить любовь на проекте

Игорь Туманов

День рождения: 18 октября

413 друзей · 16 подписчиков · 15 фотографий · 36 видеозаписей · 216 подарков

Игорь Туманов
Новенькая участница "Дома-2" не уверена, что можно построить любовь на проекте

Новенькая участница "Дома-2" не уверена, что можно построить любовь на проекте
dni24.com

Екатерина Плотникова

День рождения: 18 января
Город: Волжский
Место работы: Эта страница официально подтверждена

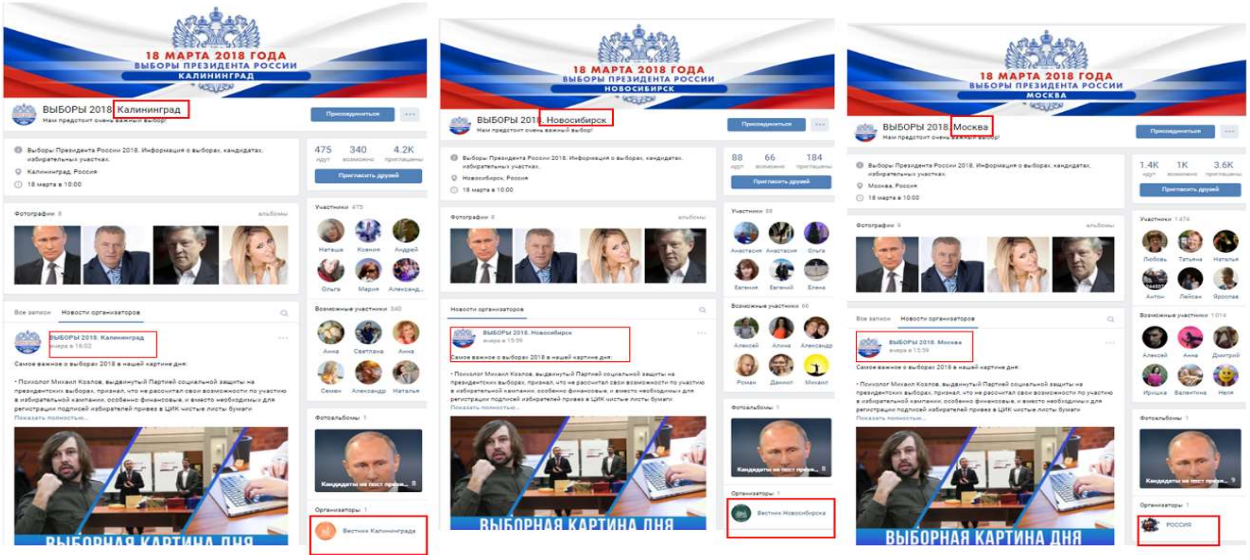
2 743 друга · 135 подписчиков · 246 фотографий · 8 видеозаписей · 6 аудиозаписей

Екатерина Плотникова
Новенькая участница "Дома-2" не уверена, что можно построить любовь на проекте

Новенькая участница "Дома-2" не уверена, что можно построить любовь на проекте
dni24.com

The second botnet with news about 2018 presidential elections, had a more complex structure and consisted of 23 events (Picture 2). Like the characteristics of the first botnet profiles, the characteristics of the second botnet profiles have included same photos on walls of different accounts, same published content on the walls, same publication period of same-type content.

Picture 2. Technological accounts of #2 botnet formed by 'Sobchak' keyword (#1 event, #2 event, #3 event).



ВЫБОРЫ 2018 Калининград
Нам предстоит очень важный выбор!
Выборы Президента России 2018. Информация о выборах, кандидатах, избирательных участках.
Калининград, Россия
18 марта в 10:00
475 идут · 340 возможно · 4.2K приглашены
ВЫБОРЫ 2018. Калининград
Самое важное о выборах 2018 в нашей картине дня:
• Психолог Михаил Козлов, выдвинутый Партией социальной защиты на президентских выборах, признал, что не рассчитал свои возможности по участию в избирательной кампании, особенно финансовые, и вместо необходимых для регистрации подписей избирателей привез в ЦИК чистые листы бумаги
Организаторы: Вестник Калининграда

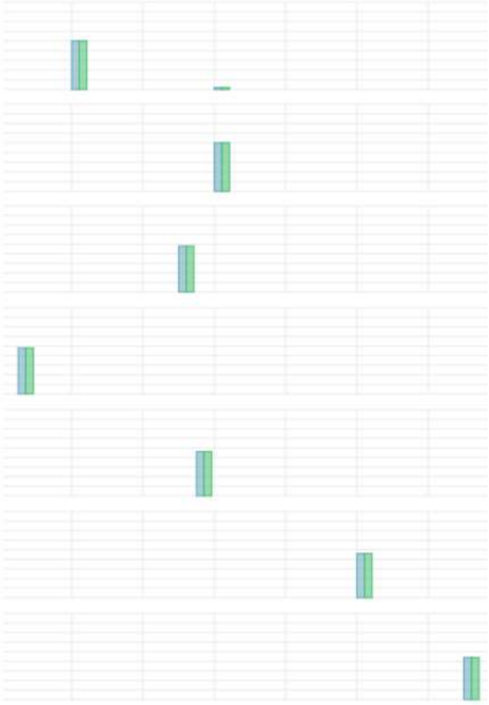
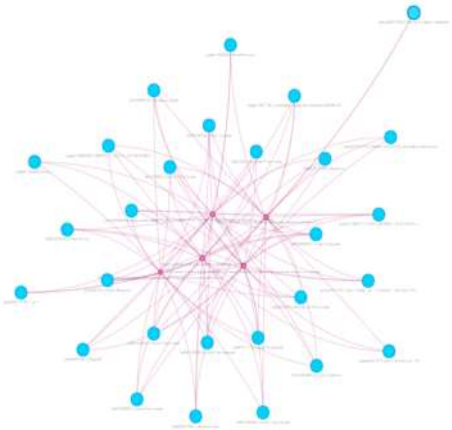
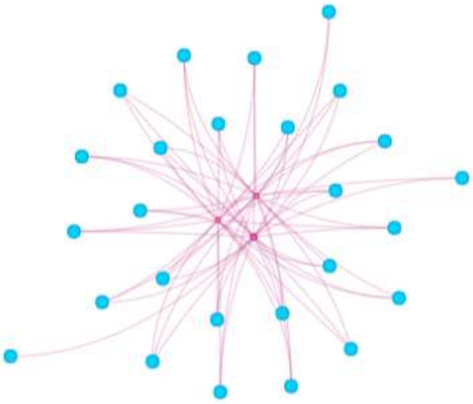
ВЫБОРЫ 2018 Новосибирск
Нам предстоит очень важный выбор!
Выборы Президента России 2018. Информация о выборах, кандидатах, избирательных участках.
Новосибирск, Россия
18 марта в 10:00
88 идут · 66 возможно · 184 приглашены
ВЫБОРЫ 2018. Новосибирск
Самое важное о выборах 2018 в нашей картине дня:
Организаторы: Вестник Новосибирска

ВЫБОРЫ 2018 Москва
Нам предстоит очень важный выбор!
Выборы Президента России 2018. Информация о выборах, кандидатах, избирательных участках.
Москва, Россия
18 марта в 10:00
1.4K идут · 1K возможно · 3.6K приглашены
ВЫБОРЫ 2018. Москва
Самое важное о выборах 2018 в нашей картине дня:
Организаторы: РОССИЯ

Given that distribution of identical publications depends on the number of publications and that of authors, we have built time histograms and have simultaneously visualized 'text – author' relationship in order to capture the distribution process over time. Thus, we have identified the processes of artificial distribution of content of the same type in the same numbers by the same number of authors over a short time slot. The same content (text+photo) containing

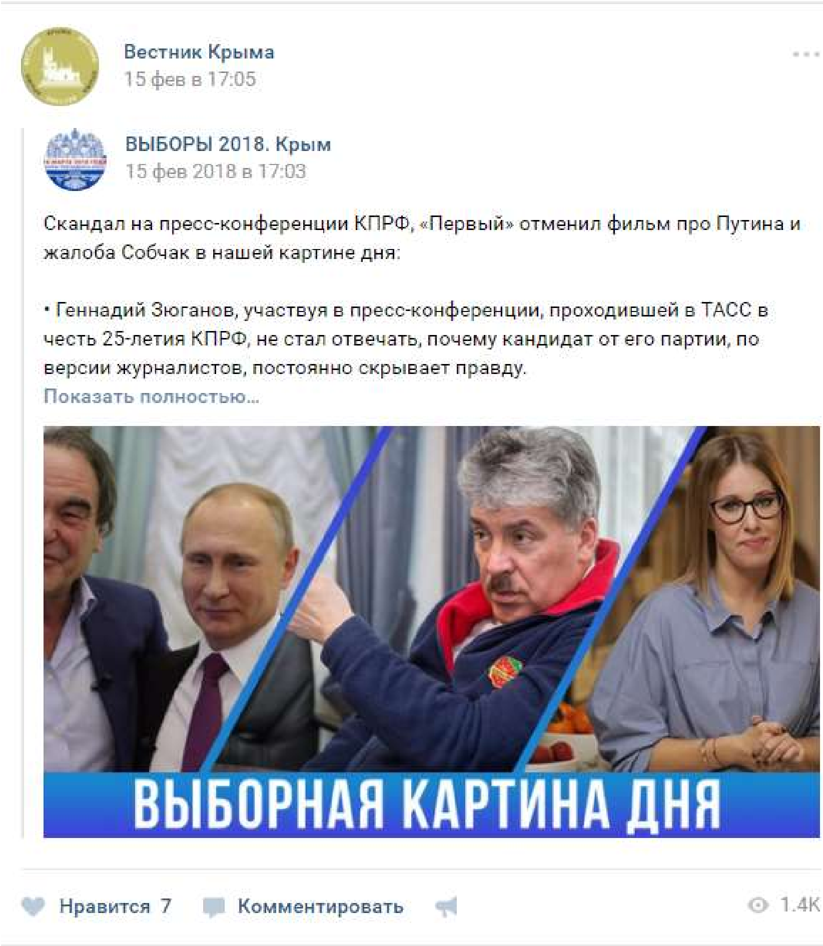
‘Sobchak’ keyword was replicated over 8-9 minutes, with one publication being distributed 23 times (on each of the 23 technological accounts).

Table 1. Visualization of network publication activity of #1 and #2 botnets in form of histograms (on the right), where column 1 is the number of authors, column 2 is the number of publications and (on the left) graphs depicting ‘text – author’ relationship on #1 and #2 botnets.

Top list of replicable publications selected using ‘Sobchak’ keyword	#1 botnet, #2 botnet selected using ‘Sobchak’ keyword
	
	

Number 1 botnet differed from #2 botnet in that the 23 technological accounts – events - that distributed the content with ‘Sobchak’ keyword were linked to the regional media having a big audience. The two-level botnet structure helped increase the audience to which content got replicated because the #1 botnet audience (consisting of 2018 presidential election events) got extended to the audience of the regional media (duplicating on #2 botnet’s newsfeed) (Picture 3). The total #2 botnet audience included event participants, potential event participants, those invited to 2018 ELECTION and followers of the regional media and accounted for 1,243,128 VKontakte users.[6]

Picture 3. 'Crimea's Vestnik' regional newspaper and VK duplicating #2 botnet newsfeed on '2018 Election. Crimea' technological accounts (one of the 23 technological accounts (events)).



Вестник Крыма
15 фев в 17:05

ВЫБОРЫ 2018. Крым
15 фев 2018 в 17:03

Скандал на пресс-конференции КПРФ, «Первый» отменил фильм про Путина и жалоба Собчак в нашей картине дня:

• Геннадий Зюганов, участвуя в пресс-конференции, проходившей в ТАСС в честь 25-летия КПРФ, не стал отвечать, почему кандидат от его партии, по версии журналистов, постоянно скрывает правду.
Показать полностью...

Нравится 7 Комментировать 1.4K

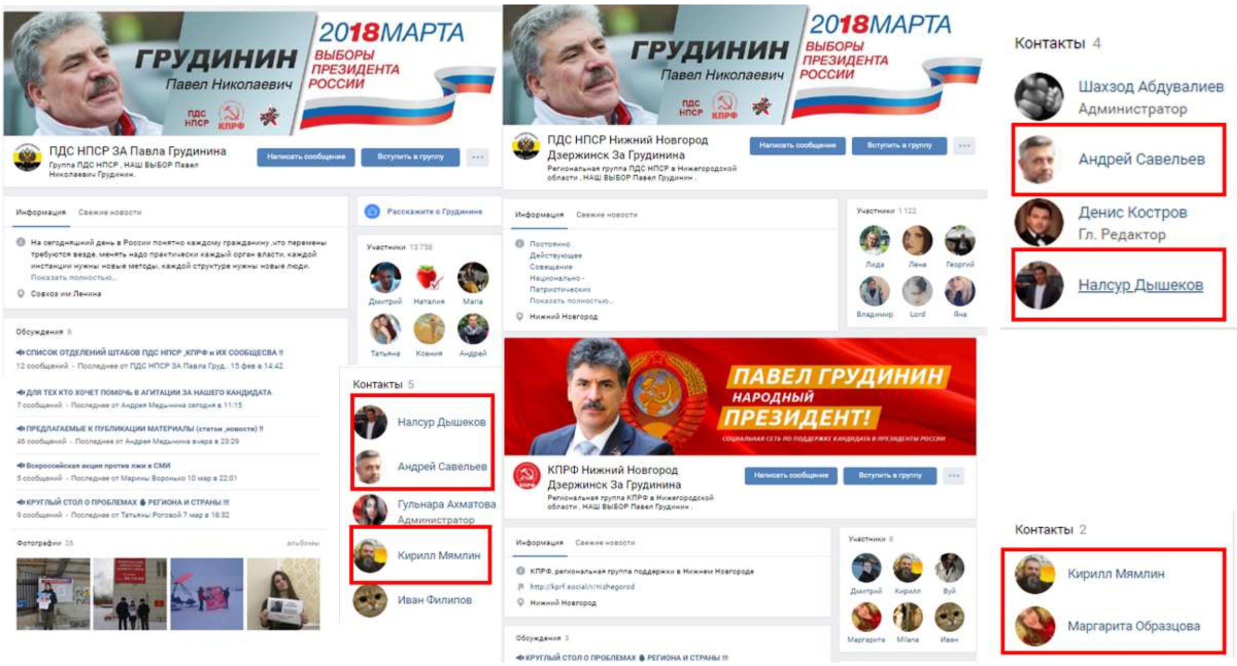
When refining the study's duration (March 8 - 9, 2018) using 'Grudinin' keyword, we have collected a data set consisting of 256,458 posts and comments (namely, 132,451 posts and 124,007 comments) which were written by 73,685 authors and posted on 45,461 publication sites (walls of groups, pages, events and users) (see Attachment 2).

During the selected time slot, we have detected a botnet consisting of 175 technological accounts – 'For Pavel Grudinin' groups: 91 'PC NPFR + city name' groups and 84 'CPRF + city name' groups (where PC NPFR stands for Permanent Conference of National Patriotic Forces of Russia and CPRF stands for the Communist Party of the Russian Federation) (Picture 4). The following features characterized bot profiles of the #3 botnet: identical page profiles, same replicable content (text+photo, text+video) and same time period of duplicating publications.

[6] Number 2 botnet audience was counted on February 20, 2018.

The content was replicated over 10 seconds to 1 minute, with one publication being distributed 175 times (on each of the 175 technological agents). The total #3 botnet audience included friends and followers and accounted for 54,829 VKontakte users.[7]

Picture 4. Technological accounts (#1 group, #2 group, #3 group) of #3 botnet formed by ‘Grudinin’ keyword.



ПДС НПСР ЗА Павла Грудинина
Группа ПДС НПСР , НАШ ВЫБОР Павел Николаевич Грудинин.

На сегодняшний день в России понятно каждому гражданину ,что перемены требуются везде, менять надо практически каждый орган власти, каждой инстанции нужны новые методы, каждой структуре нужны новые люди.

Совхоз им Ленина

Участники 13 738

Дмитрий, Наталия, Maria, Татьяна, Ксения, Андрей

Обсуждения 6

СПИСОК ОТДЕЛЕНИЙ ШТАБОВ ПДС НПСР ,КПРФ и ИХ СООБЩЕСВА !!
12 сообщений · Последнее от ПДС НПСР ЗА Павла Груд.. 15 фев в 14:42

ДЛЯ ТЕХ КТО ХОЧЕТ ПОМОЧЬ В АГИТАЦИИ ЗА НАШЕГО КАНДИДАТА
7 сообщений · Последнее от Андрея Медынина сегодня в 11:15

ПРЕДЛАГАЕМЫЕ К ПУБЛИКАЦИИ МАТЕРИАЛЫ (статьи ,новости) !!
46 сообщений · Последнее от Андрея Медынина вчера в 23:29

Всероссийская акция против лжи в СМИ
5 сообщений · Последнее от Марины Воронько 10 мар в 22:01

КРУГЛЫЙ СТОЛ О ПРОБЛЕМАХ ● РЕГИОНА И СТРАНЫ !!!
9 сообщений · Последнее от Татьяны Роговой 7 мар в 18:32

Контакты 5

Налсур Дышеков
Андрей Савельев
Гульнара Ахматова
Администратор
Кирилл Мямлин
Иван Филипов

ПДС НПСР Нижний Новгород Дзержинск За Грудинина
Региональная группа ПДС НПСР в Нижегородской области , НАШ ВЫБОР Павел Грудинин .

Постоянно Действующее Совещание Национально - Патриотических

Нижний Новгород

Участники 1 122

Лида, Лена, Георгий, Владимир, Lord, Яна

Контакты 4

Шахзод Абдувалиев
Администратор
Андрей Савельев
Денис Костров
Гл. Редактор
Налсур Дышеков

КПРФ Нижний Новгород Дзержинск За Грудинина
Региональная группа КПРФ в Нижегородской области , НАШ ВЫБОР Павел Грудинин .

КПРФ, региональная группа поддержки в Нижнем Новгороде
http://kprf.social/r/nizhegorod
Нижний Новгород

Участники 8

Дмитрий, Кирилл, Вуй, Маргарита, Milana, Иван

Обсуждения 3

КРУГЛЫЙ СТОЛ О ПРОБЛЕМАХ ● РЕГИОНА И СТРАНЫ !!!

Контакты 2

Кирилл Мямлин
Маргарита Образцова

The technique used in this study has helped detect botnets in the Russian political space on VKontakte social network. Applying ‘a replicable publication’ parameter, we have examined publication activity of authors that include users, groups and events. Depending on their structural organization, we have identified types of botnets such as botnet-users, botnet-pages, botnet-events and botnet-groups. When analyzing #2 botnet structure (formed by ‘Sobchak’ keyword), we have found that the more sophisticated the botnet structure is, the greater is the size of its audience. At the same time, the audience size is not the main indicator of botnet productivity. The research has shown that, collected over 24-hour period, formed by ‘Grudinin’ keyword, the dataset of publications was 7,5 times larger than that of publications with ‘Sobchak’ keyword collected over eight days (256,458 posts and comments referred to Grudinin versus 34,334 posts and comments related to Sobchak).

[7] Number 1 botnet audience was counted on March 9, 2018.

Conclusions

Based on our mechanism of bot identification, over certain time slots, we have detected three botnets that distributed content with keywords related to Ksenia Sobchak and Pavel Grudinin - two presidential candidates for 2018 election in the Russian Federation.

In regards to Sobchak and Grudinin, the botnets aimed to attract a great number of supporters and, as such, served as a tool to rapidly increase the politicians' popularity during a relatively short period of the election campaign. The reason for choosing this bot communication strategy is political biographies of the candidates. In the political space of the Russian Federation, Sobchak and Grudinin were known less compared to their counterparts.

Ksenia Sobchak is a well-known media person (she is known as a journalist and a TV anchorwoman of "Dom-2" reality show). The fact that she was not perceived as a politician by the Russian voter asked for Sobchak's image rebranding. On October 18, 2017 Sobchak officially announced her intention to participate in 2018 presidential elections and shortly gained high popularity on "VKontakte" and Twitter social networks.

In the beginning of the election campaign, Pavel Grudinin was completely unknown in the political space of the Russian Federation. He was not a media person and became a "dark horse" for the voter. Only on December 23, 2017, he was nominated as a presidential candidate and became an easily recognizable and the most discussed political figure by March 2018.

In the course of the study, we have uncovered differences in the structure of the botnets. In addition to the above mentioned communication strategy, the first two botnets distributing the content with 'Sobchak' keyword utilized the tactics of *extensive influence* over potential voters. This extensive influence was realized through technological accounts (in form of users, pages and groups) and regional media that made it possible to reach a wide audience of potential voters. For instance, the first botnet distributing the content with 'Sobchak' keyword had an audience of 339,945 VKontakte users. The second botnet distributing the content with 'Sobchak' keyword had an audience of 1,243,128 VKontakte users. The third botnet distributing the content with 'Grudinin' keyword had an audience of 54,829 VKontakte users.

The third botnet distributing the content with 'Grudinin' keyword utilized the tactics of *intensive influence* over the audience through high frequency distribution of the content. We have found 256,458 posts and comments with 'Grudinin' keyword during 8 – 9 March 2018, while there were only 34,334 posts and comments with 'Sobchak' keyword during 24 – 31 January 2018.

In conclusion, the study has shown that different botnet structures help realize different communication tactics that politicians employ in their interaction with potential voters.

References

1. Alymov, A.S., Baranyuk, V.V., Smirnova, O.S. 2016. “Detecting bot programs that mimic people's behavior in the social network "Vkontakte." *International Journal of Open Information Technologies*. 8: 60-55.
2. Bessi, A., and E. Ferrara. 2016. “Social Bots Distort the 2016 US Presidential Election Online Discussion” *First Monday*. 21 (11). https://ssrn.com/abstract=2982233.
3. Bolsover, G., Howard, P. 2018. "Chinese computational propaganda: automation, algorithms and the manipulation of information about Chinese politics on Twitter and Weibo." *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2018.1476576.
4. Chesnokov, V.O. 2017. “Application of the algorithm for the allocation of communities in the information confrontation in social networks.” *Questions of cybersecurity*. 1 (19): 44-37.
5. Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S. 2010. “Who is tweeting on Twitter: human, bot, or cyborg?” *In Proceedings of the 26th annual computer security applications conference*. New York: ACM, 21-30. https://www.eecis.udel.edu/~hnw/paper/acsac10.pdf
6. Evseeva, A.O., Gumerova, R.I., Katasev, A.S., Kirpichnikov, A.V. 2017. “Identification of bots in social networks based on data mining technology.” *Vestnik of Kazan Technological University*. 20 (5): 90-87.
7. Forelle, M., Howard, P. N., Monroy-Hernandez, A., Savage, S. 2015 “Political Bots and the Manipulation of Public Opinion in Venezuela.” July 25. http://dx.doi.org/10.2139/ssrn.2635800
8. Glowacki, M., Narayanan, V., Maynard, S., Hirsch, G., Kollanyi, B., Neudert, L.-M., Howard, P., Lederer, T., Barash, V. 2018. “News and Political Information Consumption in Mexico: Mapping the 2018 Mexican Presidential Election on Twitter and Facebook.” Working Paper, University of Oxford. Computational Propaganda Project: Working Paper Series. http://comprop.oii.ox.ac.uk/research/working-papers/mexico2018/
9. Grimme, C., Preuss, M., Adam, L., &Trautmann, H. 2017. “Social Bots: Human-Like by Means of Human Control?” *Big data*. 5(4): 293-279.
10. Howard, P. N., Woolley, S., Calo, R. 2018. “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*. 15 (2): 93-81.

11. Howard, P. N., Kollanyi, B. 2016. "Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum." (June 20). http://dx.doi.org/10.2139/ssrn.2798311.
12. Howard, P. N., Kollanyi, B., & Woolley, S. 2016. "Bots and Automation over Twitter during the US Election." Working Paper, University of Oxford. Computational Propaganda Project: Working Paper Series. http://comprop.oii.ox.ac.uk/research/working-papers/bots-and-automation-over-twitter-during-the-u-s-election/
13. Katasev, A.S., Kataseva, D.V., Kirpichnikov, A.P., Evseeva, A.O. 2015. "Neural network model of bot identification in social networks." *Vestnik of Technological University*. 18 (16): 256-252.
14. Katasev, A.S., Kataseva, D.V., Kirpichnikov, A.V. 2015. "Neural network diagnostics of abnormal network activity." *Vestnik of the Technological University*. 18 (6): 167-163.
15. Kotenko, I.V., Konovalov, A.M., Shorov, A.V. 2011. "Agent-oriented modeling of botnets and protection mechanisms against them." *Questions of information protection*. 3: 29-24.
16. Lyfenko, N.D. 2014. "Virtual users in social networks: myths and reality." *Cybersecurity issues*. 5: 20-17.
17. Martyanov, D.S. 2016. "Political bot as a profession." *Political expertise*. 12 (1): 89-74.
18. Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A., &Menczer, F. 2011. "Detecting and tracking political abuse in social media." *In Proceedings of the 5th AAAI International Conference on Weblogs and Social Media.* 11: 304-297.
19. Schäfer, F., Evert, S., Heinrich, P. 2017. "Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzo Abe's Hidden Nationalist Agenda." *Big Data*. 4 (5): 309-294.
20. Woolley, S., Howard. P. 2016. "Automation, algorithms, and politics| political communication, computational propaganda, and autonomous agents—Introduction." *International Journal of Communication*. 10. http://ijoc.org/index.php/ijoc/article/view/6298
21. Woolley, Samuel C. 2016. "Automating Power: Social Bot Interference in Global Politics." *FirstMonday*. 21 (4). https://doi.org/10.5210/fm.v21i4.6161

Attachment 1. An array of publications with the keyword "Sobchak" from 24.01.18-31.01.2018.

Type of author	Type of place	Type of publication	Number of publications	Number of unique authors	Number of unique places
User	User's wall	Comments	-	-	-
		Posts	12 501	9 411	9 411
		Total	12 501	9 411	9 411
	Group's/ page's / event's wall	Comments	13 741	10 213	3 478
		Posts	-	-	-
		Total	13 741	10 213	3 478
	Total	Comments	13 848	10 292	3 570
		Posts	12 501	9 411	9 411
		Total	26 349	19 465	12 776
Group / page / event	User's wall	Comments	-	-	-
		Posts	-	-	-
		Total	-	-	-
	Group's/ page's / event's wall	Comments	242	104	118
		Posts	7 739	3 423	3 423
		Total	7 981	3 493	3 486
	Total	Comments	246	105	120
		Posts	7 739	3 423	3 423
		Total	7 985	3 495	3 487
Total	User's wall	Comments	-	-	-
		Posts	12 501	9 411	9 411
		Total	12 501	9 411	9 411
	Group's/ page's / event's wall	Comments	13 983	10 333	3 521
		Posts	7 739	3 423	3 423
		Total	21 722	13 667	6 260
	Total	Comments	14 094	10 412	3 615
		Posts	20 240	12 590	12 590
		Total	34 334	22 576	15 416

Attachment 2. An array of publications with the keyword "Grudinin" from 08.03.18-09.03.2018.

Type of author	Type of place	Type of publication	Number of publications	Number of unique authors	Number of unique places
User	User’s wall	Comments	-	-	-
		Posts	114 782	33 417	33 417
		Total	114 782	33 417	33 417
	Group’s/ page’s / event’s wall	Comments	122 110	37 829	8 869
		Posts	-	-	-
		Total	122 110	37 829	8 869
	Total	Comments	122 572	38 052	9 140
		Posts	114 782	33 417	33 417
		Total	237 354	68 303	42 694
Group / page / event	User’s wall	Comments	-	-	-
		Posts	-	-	-
		Total	-	-	-
	Group’s/ page’s / event’s wall	Comments	1 341	463	691
		Posts	17 669	5 366	5 366
		Total	19 010	5 601	5 636
	Total	Comments	1 435	465	737
		Posts	17 669	5 366	5 366
		Total	19 104	5 604	5 681
Total	User’s wall	Comments	-	-	-
		Posts	114 782	33 417	33 417
		Total	114 782	33 417	33 417
	Group’s/ page’s / event’s wall	Comments	123 451	38 261	8 983
		Posts	17 669	5 366	5 366
		Total	141 120	43 318	11 743
	Total	Comments	124 007	38 489	9 297
		Posts	132 451	38 791	38 791
		Total	256 458	73 685	45 461