future internet

MDPI

Article

Detection of Induced Activity in Social Networks: Model and Methodology

Dmitrii Gavra [1], Ksenia Namyatova [1] and Lidia Vitkova [2,*]

[1] Department of Public Relations in Business, St. Petersburg State University, 7-9 Universitetskaya Embankment, 199034 St. Petersburg, Russia; d.gavra@spbu.ru (D.G.); ksnsun@mail.ru (K.N.)

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 39, 14th Line V.O., 199178 St. Petersburg, Russia

* Correspondence: vitkova@comsec.spb.ru; Tel.: +7-(981)-977-9101

Abstract: This paper examines the problem of social media special operations and especially induced support in social media during political election campaigns. The theoretical background of the paper is based on the study fake activity in social networks during pre-election processes and the existing models and methods of detection of such activity. The article proposes a methodology for identifying and diagnosing induced support for a political project. The methodology includes a model of induced activity, an algorithm for segmenting the audience of a political project, and a technique for detecting and diagnosing induced support. The proposed methodology provides identification of network combatants, participants of social media special operations, influencing public opinion in the interests of a political project. The methodology can be used to raise awareness of the electorate, the public, and civil society in general about the presence of artificial activity on the page of a political project.

Keywords: network operations; network combatants; social bots; social network analysis; induced activity; induced activity detection; election campaigns

check for updates

Citation: Gavra, D.; Namyatova, K.; Vitkova, L. Detection of Induced Activity in Social Networks: Model and Methodology. *Future Internet* **2021**, *13*, 297. https://doi.org/10.3390/fi13110297

Academic Editor: Eirini Eleni Tsiropoulou

Received: 30 September 2021
Accepted: 17 November 2021
Published: 22 November 2021

1. Introduction

In classical mass society, political reality was shaped by traditional media owned by government institutions and political elites. The situation has changed, and more than once. Political reality itself, which used to be unified for the majority of audiences united by the mass media, has now disintegrated into a number of local areas. A plural network political reality is created by horizontal communities based on their hierarchies. Local realities are constructed in "bubbles"—closed communities with their own hierarchy, distribution of social roles, leadership, etc. Partial identities are formed in them, and partial models of political reality are constructed. Moreover, such models can radically differ from community to community.

A fragmented and disconnected set of networked realities has become a breeding ground for new approaches to the manipulation of public opinion, mass consciousness and finally, electoral choice. This eventually created ground for so-called "special operations in social networks". This refers to the covert influence on audiences for political purposes.

There are quite a number of studies and papers devoted to the detection of bots during election campaigns [1–4], models [5,6], algorithms and techniques for detecting artificial activity [7] and ways to detect information dissemination paths [8]. However, in all these works there is a wide variety of terms and basic concepts for similar objects or operations. Therefore, it is first necessary to define the basic concepts, select the related concepts, and outline the framework.

It can be said that attempts are being made to manipulate public opinion as part of election campaigns. By manipulating public opinion, we, following Forell, Howard, Monroy-Hernandez, Savage and Mexico, understand the deliberate hidden influence on public opinion in order to form positions and assessments beneficial to the manipulator [9,10]. From our point of view, within the framework of general theoretical approaches to the analysis of the processes of manipulation of public opinion in the digital environment, it is necessary to expand and clarify the terminological apparatus. In particular, we propose to use a subjective approach and introduce the concept of a special information operation implemented in social networks (Social Media Special Operations). To solve this problem, we borrow the concept of special operations from the theory of wars and the art of war. There, special operations are defined as "special missions to achieve strategic goals in which the use of conventional armed forces would create unacceptable risks. Overcoming these risks requires special operations forces..." [11]. In line with this approach, we further suggest that Social Media Special Operations could be defined as a set of coordinated technological solutions implemented by software and means of social engineering that covertly manage the co-consciousness and behavior (both online and offline) of social media users for the benefit of political actors. Among such special operations we suggest to include operations on giving the users an impression or image of large public network support for certain political projects. This illusion creates a high online reputation for these projects and psychologically encourages those who have not yet formed their attitudes to join the majority and support these projects. We propose that special network operations of this type be labelled as operations to generate the illusion of public support or operations to generate induced support for a political project. This interpretation of Social Media Special Operations makes them one of the technologies used for manipulating public opinion in the digital environment.

We propose the term Network Combatants (NC or Combatants). These are active and specifically engaged participants in conflicts or special operations in social media. They could be bots as well as real people who deliberately carry out their activities, in some cases for compensation. The use of the term stems from a basic understanding of Combatants as persons taking a direct part in the combat operations of armed forces during an armed conflict [12,13]. In the case of international conflicts, the Geneva Convention is known to give combatants a special status [14]. In the case of information confrontations on social media, NC confront the so-called "online citizenry".

Induced support for a project is further understood to mean the network social capital artificially generated for the project through the network activities of the actors (Network Combatants) who create traffic of induced content beneficial to the project in the interested communities. Such engaged actors, or in other words agents of induced activity, can be paid agents from the real world as well as virtual agents or bots.

There are many terms for Network Combatant accounts in the academic literature: (1) Sybils are automatic/semi-automatic profiles designed to mimic human profiles [15]; (2) Imposters—fake accounts [16]; (3) False identity—a made-up identity with a stolen photo and/or false information [17]; (4) A fake-account is an active user account created and monitored by an intruder for illegal purposes, including the collection of personal data [18]; (5) Social bots—computer-based, robotic programs that pretend to be people [19]. There are now many publications devoted to the search for traces of artificial activity in political election campaigns. As [20] points out, the possibility of fake/fake personalities in the political arena certainly existed before. However, the development of digital reality and social networks has made it possible to use induced activity more widely. Bots, trolls, fake or stolen accounts, etc., are all in the election campaign. All this has created additional opportunities for special operations in which the impact is directed at network horizontal communities with their own hierarchies.

When we talk about the dynamics of political consciousness and political behavior of social network users in a specific situation such as election campaign, then we are talking about the fact that these dynamics can unfold in two modes. We denote them as spontaneous (natural) and induced (artificial). In the first mode, competing political actors campaign in all forms allowed by law, including social media. The voter perceives this campaign information and forms his electoral preferences. There is what we call a natural (spontaneous) process of electoral preference formation. However, if any of the competing political actors resort to a special operation to create imaginary support during an election campaign, and these artificial activities are effective, we see an induced dynamic of electoral preference formation. To emphasize an important point once again, these transactions are generally outside the scope of electoral legislation.

This article focuses on two aspects, firstly, on the methodology of identifying induced activity in social media during project implementation, and secondly, on the phenomenon of induced activity itself during political campaigns. In our work we aim not to show that artificial activity in social networks takes place, but rather to focus the attention of both the professional community and the wider public on the fact that it is an extremely common practice and, in our view, it is important to raise the need for such techniques and practices that can conditionally "distinguish" such activity from the general population for the voter. That is, models, techniques and algorithms are needed to ensure that individuals are protected from the effects of special operations.

This paper proposes a model, algorithm and technique for monitoring and diagnosing the activities of combatants that differs from existing approaches and solutions in that it provides detection of special operations Network Combatants during the implementation of a political project.

The paper is structured as follows: the second section presents an overview of relevant works. The third section contains a model of induced activity and methods of monitoring and detection of induced activity. The empirical basis is the results of case studies on the use of induced activity during election campaigns in a major Russian region in 2019. The fourth section contains the results of the experiment and the fifth section, the conclusion and discussion, concludes the paper.

2. Related Works

Since the advent of social media, the research community has been puzzled by the problem of reliably identifying social media fake accounts. Research can be divided into two parts: (1) social and political sciences (who and what a bot is; its scope; social and political functions; case studies devoted to analyzing specific examples of induced activity); (2) technical sciences (methods for detecting bots and fake activity or features of spreading false information). According to the main directions of research, the review of relevant works is divided into two parts: the first part is dedicated to a group of social and political studies, the second part contains a description of models and algorithms of detection of bots or information dissemination.

The first strand of research, in our view, focuses more on the socio-political effects and regulatory aspects of the use of NC.

All terminology is in one way or another based on the functional characteristics of the accounts and is mostly related to information security in the information space. Thus, [16,17] states that the main purpose of creating fake accounts involves malicious activities related to extremism, fraud, identity theft, bullying and violence. As highlighted by the researchers in [17], robot accounts—bots—are most commonly used for malicious activity in an automated mode. In this case, a social media bot is akin to a chatbot in an app; it works according to a predetermined algorithm for human-defined purposes. The difference between a chatbot in apps and a malicious bot is that a "chat-bot" is easily identifiable by its association with a social networking project or channel (community). At the same time there are those fake social media accounts that tend to mimic a real person as much as possible. Detecting them is the main problem. Detecting a bot whose behavior is automated is much easier.

It should be noted that if we characterize a fake account as a social network user who has some inaccurate information on his page, then theoretically all social network accounts can be classified as fake accounts. Because human beings can be inaccurate, they can make mistakes, they have a right to misrepresent themselves on social media. They can put on masks and play games. In our opinion, the problem of distinguishing real accounts from fake ones seems to be more complex, which also lies in the field of communication deontology. This begs the question: where is the line between freedom of expression, role-playing and malicious misleading of other network users?

After all, fake accounts are very often used both for commercial and political purposes. We agree with the researchers who argue that fake accounts are neither good nor bad, rather it is the intention behind them that matters [21]. Let us consider, for example, the field of commercial applications. This is where fake accounts are used to increase the number of contributors, views, and likes, and there are plenty of exchanges where you can order everything from likes to comments, see for example Amazon Mechanical Turk [22], qcomment [23], freelancer [24], zbj [25] and buyaccs [26]. The scientific community uses a special term for such exchanges—crowdturfing [17,27–30]. On these stock exchanges, anyone can buy the services of robotic accounts.

In parallel to the commercial sphere, fake accounts have become more widespread in the field of political communication. Research to identify fake activity is ongoing around the world, with local, regional, and federal elections coming under the scrutiny of researchers. For example, Ferrara et al. analyzed the presence of artificial activity during Trump's 2016 US election, Macron's 2017 election in France [1], Keller and Klinger focused on elections in Germany [2], Borge-Holthoefer et al. analyzed the presence of artificial activity during the 15 May movement in Spain [3], Ruediger et al. conducted an extensive study from the 2014 presidential election in Brazil to the referendum vote in 2017 [4]. It is not just elections that have come to their attention, but also local conflict situations, such as the strike in 2017 or the US impeachment debate and the Catalan referendum. The increasing popularity of the use of fake accounts in political campaigns is clearly demonstrated in the work of Pastor-Galindo and colleagues [31]. Whereas in 2014 they noted artificial activity in two countries, in 2019 they noted 13 countries where fake Twitter activity was used during election campaigns. The strength of the research to detect such activity is undoubtedly to capture the fact and to draw attention to the problem, the weakness is that researchers focus on the social network Twitter, whereas there are other networks such as Facebook, Instagram, TikTok, YouTube, etc. and that often this research is focused on finding bot farms from robotic accounts.

Summarizing the review of relevant works from the social and political sciences, it should be noted that the heterogeneity of concepts and terms for the same objects leads to collisions. As a consequence, the task of developing an algorithm for detecting induced activity, NC, and signs of special network operations becomes more complicated. It is therefore necessary to classify fake accounts.

The second line of study focuses more on the techno-mathematical realm. Here the category of Influence is put in the center of discussion. Influence in these approaches is interpreted as the process and result of a subject changing the behavior of another subject (individual or collective object of influence). Influence can be seen from two perspectives: (1) on the side of the recipient, (2) on the side of the disseminator of information.

Studies aimed at finding purposeful Influence are divided into those in which the authors look for communities or major nodes in communities. In such a case, the aim is to detect and assess the disseminator and the way the information is disseminated (diffusion). Studies are also divided into those in which the authors assess from the recipient's reaction or the audience's response to the Influence.

Let us consider the models and algorithms that we propose to place in the first group (recipient side):

In 1962, a penetration of innovation model was proposed by E. Rogers. This model is still used in research aimed at detecting the management or manipulation of users in social networks [32]. Algorithms based on this model find innovators and then their contributors in social media.

Frank Bass' multiple penetration of innovation model: According to Bass's model [7] agents in a network can be either active or inactive, i.e., agents have a binary state. Bass distinguishes two types of agents: (1) innovators; (2) imitators. In [8], the authors propose a new model, an improved version of Bass's model, which allows identifying influential channels on YouTube.

The spiral of silence is a theory proposed by Noelle-Neumann in 1974 [33,34]. His theory claims that people, driven by a fear of isolation, constantly monitor their opinions to assess whether they conform or contradict the majority opinion [35]. As social networks become more popular for co-social interaction and political participation, the spiral theory of silence in social networks has become a popular subject of research [34,36] and can be used to detect Influence in social networks.

Models and algorithms that we propose to classify into the second group (the disseminator side) are, as follows:

Independent cascade models: Such models describe an information cascade, i.e., the dissemination of information through neighbors. To block propagation of the cascade between communities, the maximum value for the link fraction is calculated [5,6]. In a cascade, a central node is singled out, and it is basically a disseminator of information. Algorithms based on a cascade model allow for the detection of the most influential agents through their connection to multiple recipients. In [6], algorithms based on independent information, cascade models are proposed.

Granovetter threshold model (threshold model) [37]: In [38], the authors show how the linear threshold model GLT (an evolution of the Granovetter model) can more accurately simulate the dissemination of information in social media and detect disseminators.

Graph models: Social network graph models are used to analyze information dissemination processes, finding communities and related subgroups into which the entire social network can be broken down. In [39], the authors suggest an approach to detecting bots by visualizing the graph of communication between social network users. In [40], the authors presented an approach for detecting fake accounts based on their online interactions with other users.

Summarizing the review of relevant models and algorithms for detecting signs of processes and results of a subject changing the behavior of another subject, i.e., the Influence on public opinion, we can say that the most effective would be to measure user activity within a political project. This corresponds, for instance, to Everett Rogers' penetration of innovation model, Spiral of silence, and the Granovetter model. However, relevant studies have not considered the task of identifying NC (innovators, initiators, agitators) and there is no methodology for detecting induced activity in the known studies.

Summing up the first and second part of the review, we note that a review of relevant works suggests that there are a sufficient number of tools, approaches that can be adapted to the task of detecting induced activity, NC or features of network operations. However, it is necessary to select and combine their strengths to detect induced activity during the implementation of a political project. Our aim in this paper is to propose a methodology for detecting and diagnosing induced support for a political project in social media.

3. Methodology for Identifying and Diagnosing Induced Support for a Political Project

According to most models and algorithms that analyze the reactions of recipients, the entire audience is divided into quiet observers and activists. Thus, the most important difference between Influence actors (Network Combatants) and the civilian population in a political project would be the level of activity: the number of messages, the number of likes, etc. A methodology is needed to separate the civilian population from the combatants in the social network.

The proposed methodology includes an induced activity model, an algorithm for segmenting the audience of a political project by activity level, and a technique for detecting induced activity. Thus, the methodology provides the identification and diagnosis of induced support for a political project.

3.1. Model of Induced Activity in Social Networks

The set-theoretic model of induced activity in a social network includes such basic elements as:

- IO—set of information objects;
- IA—set of induced activity;
- Text—a set of textual attributes of the information object;
- Feature—the set of discrete characteristics of the information object;
- Com—the set of links between objects in the social network;
- Feedback—many signs of feedback from the audience;
- Event—event, political project.

The model can be represented as follows (Figure 1)

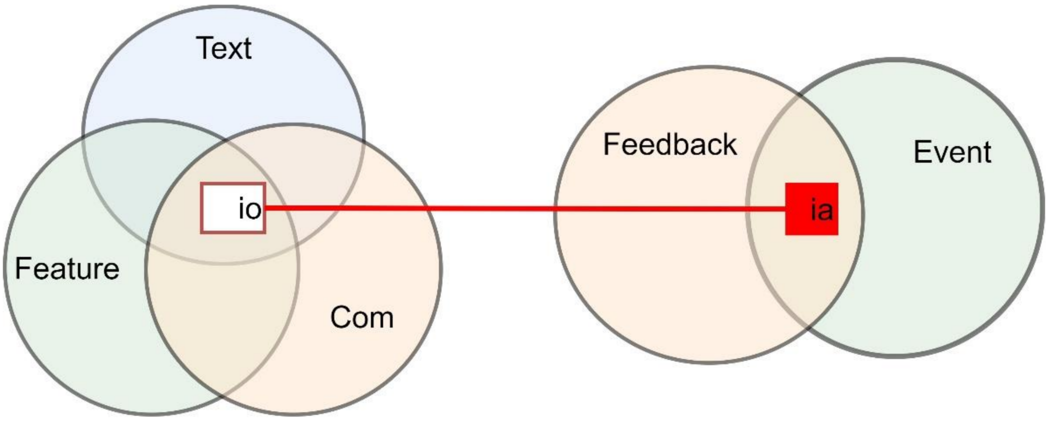

Figure 1. A model of induced activity in social media.

Let the information object in social networks have a number of properties:

1. Textual features;
2. Discrete features;
3. Connections with another information object.

Let us suppose the following:

- It is possible to identify information objects that deviate from the norm, i.e., have anomalous characteristics by textual characteristics, connections, or by discrete features;
- It is possible to identify feedback characteristics for information objects that will differ from the norm;

Then:

- Those objects that differ from the norm in terms of the set of discrete features and the level of feedback from the audience belong to the set of guided/induced activity.

In accordance with the proposed model, we will formulate the concept of induced activity:

An induced activity is a set of information objects united by textual features, discrete characteristics, and connections with another information objects around one event, activity, or theme, designed to increase the level of feedback from the audience and form a necessary point of view.

The proposed model of induced activity differs from the existing ones in that it takes into account the level of audience feedback in the social network of the political project, connection between informational objects, as well as their textual and discrete characteristics. At the same time, the model allows to form the requirements for the algorithm of segmentation of the audience of the political project.

3.2. The Algorithm of Segmentation of the Audience of a Political Project

Let us consider an algorithm that assesses the audience of a political project by their activity on the social network. By activity we mean the number of comments and/or "likes" left by the social network user.

At the first step, the "Passive" segment is distinguished from the whole audience of the political project, which includes users who have viewed the posts, comments, but have never shown communicative activity. Users who are not in the "Passive" segment will be referred to as communicative core (Figure 2).

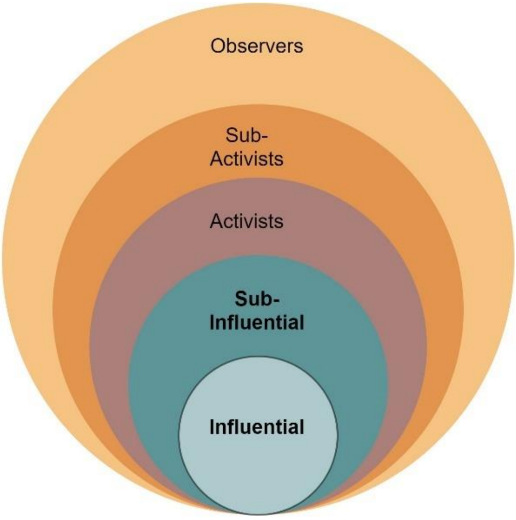

Figure 2. Communicative core of a political project.

The second step in the communication core summarizes the activity of each social network user and then calculates the average of the number of messages left and "likes". All communicators with activity below the average are classified as "Observer".

The third step follows the same steps as the second step for users who are not in the "Passive" and "Observer" segments. Users with below average activity are placed in the "Sub-Activist" segment.

The fourth step follows the same steps as the third step for users who are not in the "Passive", "Observer", and "Sub-Activist" segments. Users with below average activity will be placed in the "Activist" segment.

The fifth step proceeds in the same way as the fourth step for users who are not in the "Passive", "Observer", "Sub-Activist", and "Activist" segments. Users with below average activity are placed in the "Sub-Influential" segment and above average users are placed in the "Influential" segment.

The algorithm results in six user segments. The segmentation significantly reduces the number of profiles for analysis and comparison when identifying NC. The algorithm identifies the most active group of users who form the online social capital artificially created for a political project. They create induced content traffic and thereby influence public opinion.

The proposed algorithm is an elaboration of the authors' previous studies, which presented the results of an analysis of information dissemination sources in social networks [41,42].

3.3. Technique for Identifying and Diagnosing Induced Support

According to the induced activity model and algorithm of segmentation, the technique for identifying and diagnosing induced support for a political project can be presented as follows (Figure 3).

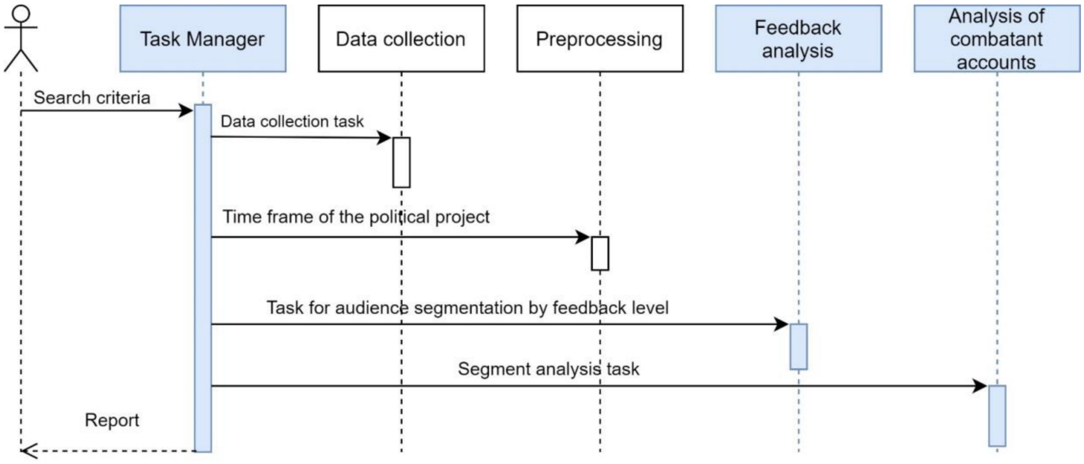

Figure 3. Technique for identifying and diagnosing induced support for a political project.

According to the proposed technique, to detect induced activity in social networks, five tasks need to be carried out:

1. To select "Search criteria"—event, activity, topic, and keywords to be searched for on the social network;
2. To collect data from the social network;
3. To identify the time frame of the event;
4. To analyze the level of feedback from the audience;
5. To analyze of the network combatant accounts

According to the proposed technique, only step 1 is carried out manually or in automatic mode. The remaining four steps can be carried out in automatic or automated mode. The components "data collection" and "data pre-processing" are not special. It is assumed that any available tools, algorithms, commercial designs, etc., can be used for data collection and preprocessing. The proposed technique supports the process of induced activity detection.

4. Experiment

To conduct the experiment, the study received confirmation from experts about the presence of artificial induced activity on the page of the candidate for the position of the head of the city administration (hereinafter referred to as the political project). The task was to detect the actors of induced activity, including combatants, to pass the list to the experts and to obtain confirmation or denial for each actor detected.

4.1. Description of the Stand and the Original Data

A stand with the following characteristics was prepared for the experimental evaluation:

1. Server supermicro: Intel Xeon CPU E5-2630/6 cores per processor, 12 virtual threads per processor (2 virtual threads per core), 1200–3100 MHz CPU frequency/128GB/HDD4+1Tb. Operating system: Debian Jessie 8.11;
2. A framework for collecting data from the VKontakte social network, which was developed as part of the grant of RSF #18-71-10094-P in SPC RAS;
3. Desktop computer: Intel (R) Core (TM) i5-9600CPU 3.10 GHz / DDR16.00G / 128SSD/1000HDD; Operating system: "Windows 10 Education Version 20H2". Microsoft Office Standard 2019.

The data sets contain the following fields:

1. Project (social network page of a political leader);
2. Author (identifier of the author of the message);
3. Name_author (name of the author of the message);

4. Date (date of message);
5. Text (message);
6. Like (the number of "likes" to the message);
7. Comm (the number of comments on the message);
8. Repost (the number of "repost" messages);
9. View (the number of views of the message)
10. Type (message type: post on page, comment).

All the fields in the dataset are connected to each other, e.g., the "like" field contains information about the author who left it on the page of the political project. It should be noted that all author IDs and names were anonymized.

The data collection was conducted in three iterations, allowing us to examine updates on the political leader′s page, to see traces of moderation (deleted posts) and to further compare the ambivalent history of active participants during and after the election campaign. The data collection period was from 1 March 2019 to 31 December 2019. A total of 222 posts were published on the political leader′s page. More than 130,000 comments and more than 300,000 likes to the posts and comments on the political project page were collected in the study.

4.2. *Analysis of Induced Support for a Political Project*

The experiment used the algorithm of segmentation of the audience of a political project according to their level of feedback. According to the algorithm, of all the many feedback signs, only comments were taken into account (see Table 1) [43].

Table 1. Segments of the communicative core and their characteristics for a political project.

Segment	Number of Users	Percentage of Users from the Total	Average Number of Comments from a User
Observer	18,360	83.52%	$\geq$6.046
Sub-Activist	2946	13.4%	$\geq$26.32
Activist	557	2.53%	$\geq$87.6
Sub-Influential	100	0.45%	$\geq$296.75
Influential	20	0.09%	<296.75

In total, 21,983 participants showed some activity on the page of the political project. According to the algorithm of segmentation, the following segments and characteristics of the communicative core of a political project were obtained using the comments analysis.

Only five users from the Influential segment are subscribed to the political project page. The numbers of comments left only by the first three Influential users are the following: 7863, 2400, and 2292. Together, 20 users of the Influential segment wrote 20,600 comments.

A detailed study was conducted for users who made up the Influential segment. An additional analysis of the profiles of such authors in the social network showed that at the time of their previous activity in the social network, they had other nicknames (for example, Ivan Ivanov was previously called "the Government"). Or they had other avatars or other posts on the wall. After the end of the election campaign, all information from the pages was deleted. Separately, the dynamics of network combatant activity was analyzed by the number of comments. An example of the results of such an analysis on the example of the author "Ivan Ivanov" (Figure 4).

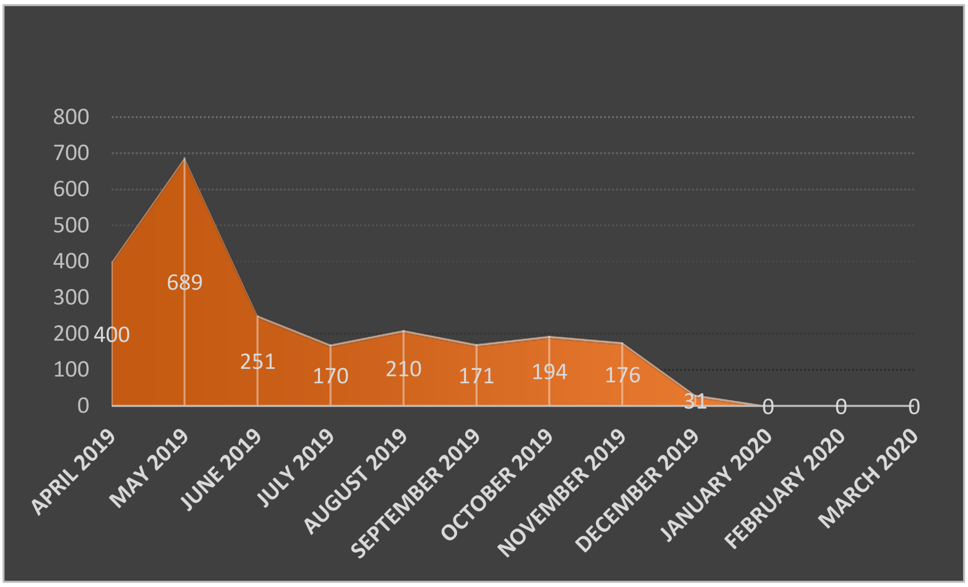

Figure 4. Dynamics of the activity of a Network Combatant on the page of a political project.

It is important to note that all 20 Influential essentially acted as Network Combatants (agents of induced activism). They wrote messages only in support of the candidate, and acted either as official representatives of regional government agencies or as extremely active supporters of the candidate. However, it should be stressed that the candidate served as the head of the regional government during the election period.

Content analysis of comments from NC (Influential) revealed that the user "Prist Sergeev" (old username [id58 . . . | Ivan Sor . . . mov]) wrote messages agitating in support of the subject of the information operation. In addition, co-messaging in support of the candidate during the campaign were actors with the nicknames "Ekaterina G . . . ova", "Nina Ko . . . .va", and "Vyacheslav La . . . ov". A retrospective analysis revealed that these users had worked directly in support of the gubernatorial candidate as part of their previous activities on the social network. Thus, all of them were found to have previously participated in processing negative information on the candidate's page. All of these users wrote their last comments in September 2019, 2–3 days after the end of the elections.

Among the 100 Sub-Influential, 26 users participated in commenting on the candidate's page for 10 months and ceased their activity immediately after the end of the campaign.

Comments and "like" marks on the page of a candidate on a social network were collected by connecting to the social network API in different sessions, once every two days, during the entire election campaign. Often the comments were deleted by the moderators of the page, but due to the different sessions, the comments were kept in the database for research.

Remarkably, the second and third most popular regions, as reported by social network users, were Uzbekistan and, surprising as it may seem, Barbados. Both extremely far from the region where the campaign took place.

An analysis of user registration dates revealed a sign of induced activity such as a spike in the number of users registered in 2019 in February and March. This was the period when the election campaign kicked off.

The experiment resulted in a list of alleged NC, actors of artificial induced activity on the candidate's page. This list was presented to the experts engaged for the study, which included professional campaign managers, journalists, and political communication experts. When reviewing the material provided, all experts confirmed that the induced support agents were correctly identified. Thus, the experiment confirms the effectiveness of the methodology.

5. Discussion

In the broader context of the use of the findings, it should be noted that, to date, the electoral laws of most states do not regulate the use of social bots or, more generally, the use of ad hoc social media operations during election campaigns. Meanwhile, research, including that described in this article, shows that this tool is increasingly being used in the arsenal of applied political technology. Moreover, this tool can influence the consciousness and behavior of large groups of voters, especially those who have not yet made a definitive choice and are still in search of a candidate or party to vote for. The bandwagon effect, repeatedly described in electoral technology theory, is that undecided voters join the vote for a potential winner, in favor of whom there appears to be a so-called "climate of opinion" [44,45].

In our view, there are to be suggested some useful innovations in the electoral legislation of democratic states to regulate the use of those voter influencing techniques that we discussed in this article. As a first step, we would propose the introduction of mandatory marking of candidate pages with signs of induced activity. This would give voters the right to know if a particular politician or candidate's page shows features of a specific operation, in particular the presence of bots that create additional induced activity. This gives voters the false impression that the candidate has widespread support on the social network. By doing so, they give the false impression to voters that the candidate has widespread support on social media. The informed voter is then already aware that there is a special online operation in favor of that candidate and he or she, the voter, is able to make a more informed responsible electoral decision.

In addition, candidates who use social bots in their campaigns to generate induced online support could also be encouraged to voluntarily inform voters on their social media pages.

Anyway, from our point of view, the proposed algorithmic approach and related legislative solutions will be able to ensure higher awareness of voters and protect them from the use of shady special network technologies. Thereby, this would improve the quality of electoral democracy and protect individual rights in social networks. Therefore, in the future, the study will be continued and the number of experimental tests for the methodology on other political projects will be increased. We are also going to expand the methodology to investigate special network operations in the field of business projects and in social media market.

6. Conclusions

When concluding our findings, we note the following.

Above all, we show that ad hoc network operations such as supporting a candidate through induced activities to give voters the impression of high public support from the network community are widely used in electoral practices.

Secondly, the experiment confirmed the effectiveness of the proposed methodology. Essentially, the basis for constructing a focused feature vector for identifying participants in an information network ad hoc operation or, in this case, agents of induced support for a political actor—Network Combatants—has been formed.

Experiment and empirical materials obtained has shown that the proposed model, algorithm, and technique make it possible to detect induced activity on the platform of the subject of an information operation and to identify Network Combatants, and therefore to record the presence of a special information operation for the latent influence on the consciousness of voters.

Author Contributions: Conceptualization, methodology—L.V., K.N. and D.G.; software, project administration—L.V.; validation, formal analysis, review and editing—L.V., K.N. and D.G.; investigation, writing original draft preparation, visualization—L.V. and K.N; supervision—L.V. and D.G.; All authors have read and agreed to the published version of the manuscript.

Funding: Part related to the social networks data analysis (Sections 3.2 and 4.1) was supported by the grant of RSF #18-71-10094-P in SPC RAS, all other sections and research in general was funded by Russian Foundation for Basic Research project № 20-011-00371 A «Mediatization of local incidents as a mechanism for mobilizing political protest in the information and network society» in SPbSU.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in https://www.kaggle.com/lidiaiskin/segmentation-of-the-audience (accessed on 18 November 2021).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ferrara, E. *Bots, Elections, and Social Media: A Brief Overview*; Shu, K., Wang, S., Lee, D., Liu, H., Eds.; Springer: Cham, Switzerland, 2020; pp. 95–114.
2. Keller, T.R.; Klinger, U. Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications. *Political Commun.* **2018**, *36*, 171–189. [CrossRef]
3. Borge-Holthoefer, J.; Rivero, A.; García, I.; Cauhé, E.; Ferrer, A.; Ferrer, D.; Francos, D.; Iñiguez, D.; Pérez, M.P.; Ruiz, G.; et al. Structural and Dynamical Patterns on Online Social Networks: The Spanish May 15th Movement as a Case Study. *PLoS ONE* **2011**, *6*, e23883. [CrossRef] [PubMed]
4. Ruediger, M.A. Bots, Social Networks and Politics in Brazil: A Study on Illegitimate Interferences with the Public Debate on the Web, Risks to the Democracy and the 2018 Elections. Available online: http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/ (accessed on 17 November 2021).
5. Cheng, J.; Adamic, L.; Dow, P.A.; Kleinberg, J.M.; Leskovec, J. Can cascades be predicted? In Proceedings of the 23rd International Conference on World Wide Web, Seoul, Korea, 7–11 April 2014; pp. 925–936.
6. Kumari, A.; Singh, S.N. Online influence maximization using rapid continuous time independent cascade model. In Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science & Engineering—Confluence, Noida, India, 12–13 January 2017; pp. 356–361.
7. Bass, F.M. A New Product Growth for Model Consumer Durables. *Manag. Sci.* **2004**, *50*, 1825–1832. [CrossRef]
8. Susarla, A.; Oh, J.-H.; Tan, Y. Social Networks and the Diffusion of User-Generated Content: Evidence from YouTube. *Inf. Syst. Res.* **2012**, *23*, 23–41. [CrossRef]
9. Forelle, M.; Howard, P.N.; Monroy-Hernández, A.; Savage, S. Political bots and the manipulation of public opinion in Venezuela. *arXiv* **2015**, arXiv:1507.07109. [CrossRef]
10. Syuntyurenko, O.V. Network technologies for information warfare and manipulation of public opinion. *Sci. Tech. Inf. Process.* **2015**, *42*, 205–210. [CrossRef]
11. Spulak, R. *A Theory of Special Operations*; JSOU Press Report: Hulburt Field, FL, USA, 2007.
12. MacKuen, M.; Wolak, J.; Keele, L.; Marcus, G.E. Civic Engagements: Resolute Partisanship or Reflective Deliberation. *Am. J. Political Sci.* **2010**, *54*, 440–458. [CrossRef]
13. D'Urso, M. The Cyber Combatant: A New Status for a New Warrior. *Philos. Technol.* **2015**, *28*, 475–478. [CrossRef]
14. Eghbali, K. Information Warfare in Terms of the Principle of Distinction between Combatants and Civilians in the Armed Conflicts. *J. Leg. Res.* **2018**, *17*, 71–109.
15. Gurajala, S.; White, J.S.; Hudson, B.; Voter, B.R.; Matthews, J.N. Profile characteristics of fake Twitter accounts. *Big Data Soc.* **2016**, *3*, 2053951716674236. [CrossRef]
16. Khaled, S.; El-Tazi, N.; Mokhtar, H.M.O. Detecting Fake Accounts on Social Media. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 3672–3681.
17. Romanov, A.; Semenov, A.; Mazhelis, O.; Veijalainen, J. Detection of Fake Profiles in Social Media-Literature Review. In Proceedings of the 13th International Conference on Web Information Systems and Technologies, Porto, Portugal, 25–27 April 2017; pp. 363–369.
18. Boshmaf, Y.; Ripeanu, M.; Beznosov, K.; Santos-Neto, E. Thwarting Fake OSN Accounts by Predicting their Victims. In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, Denver, CO, USA, 16 October 2015; pp. 81–89.
19. Igawa, R.A.; Jr, S.B.; Paulo, K.C.S.; Kido, G.S.; Guido, R.C.; Júnior, M.L.P.; da Silva, I.N. Account classification in online social networks with LBCA and wavelets. *Inf. Sci.* **2016**, *332*, 72–83. [CrossRef]
20. Farkas, J.; Schou, J.; Neumayer, C. Platformed antagonism: Racist discourses on fake Muslim Facebook pages. *Crit. Discourse Stud.* **2018**, *15*, 463–480. [CrossRef]
21. Smith, L.R.; Smith, K.D.; Blazka, M. Follow Me, What's the Harm? Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. *J. Leg. Asp. Sport* **2017**, *27*, 32–45. [CrossRef]
22. Amazon Mechanical Turk. Available online: https://www.mturk.com/ (accessed on 8 November 2021).
23. Exchange of Comments and Social Promotion. Available online: https://qcomment.ru/ (accessed on 8 November 2021).

24. The Freelancing and Crowdsourcing Marketplace. Available online: https://www.freelancer.com/ (accessed on 8 November 2021).
25. The Freelancing and Crowdsourcing Marketplace. Available online: https://www.zbj.com/ (accessed on 8 November 2021).
26. Account Store. Available online: https://buyaccs.com/ (accessed on 8 November 2021).
27. De Cristofaro, E.; Friedman, A.; Jourjon, G.; Kaafar, M.A.; Shafiq, M.Z. Paying for Likes? In Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver BC, Canada, 5–7 November 2014; pp. 129–136.
28. Thomas, K.; McCoy, D.; Grier, C.; Kolcz, A.; Paxson, V. Trafficking fraudulent accounts: The role of the underground market in Twitter spam and abuse. In Proceedings of the 22nd USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 195–210.
29. Wang, T.; Wang, G.; Li, X.; Zheng, H.; Zhao, B.Y. Characterizing and detecting malicious crowdsourcing. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 12–16 August 2013; pp. 537–538.
30. Liu, B.; Sun, X.; Ni, Z.; Cao, J.; Luo, J.; Liu, B.; Fu, X. Co-Detection of crowdturfing microblogs and spammers in online social networks. *World Wide Web* **2019**, *23*, 573–607. [CrossRef]
31. Pastor-Galindo, J.; Zago, M.; Nespoli, M.Z.P.; Bernal, S.L.; Celdran, A.H.; Gil Perez, M.; Ruiperez-Valiente, J.A.; Perez, G.M.; Marmol, F.G. Spotting Political Social Bots in Twitter: A Use Case of the 2019 Spanish General Election. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2156–2170. [CrossRef]
32. Forest, J.J. *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas: How Terrorists and Governments Fight to Shape Perceptions in a War of Ideas*; Praeger Security International: London, UK, 2009.
33. Noelle-Neumann, E. The Spiral of Silence a Theory of Public Opinion. *J. Commun.* **1974**, *24*, 43–51. [CrossRef]
34. Chen, H.-T. Spiral of silence on social media and the moderating role of disagreement and publicness in the network: Analyzing expressive and withdrawal behaviors. *New Media Soc.* **2018**, *20*, 3917–3936. [CrossRef]
35. Kennamer, J.D. Self-Serving Biases in Perceiving the Opinions of Others. *Commun. Res.* **1990**, *17*, 393–404. [CrossRef]
36. Cheng, C.; Luo, Y.; Yu, C. Dynamic mechanism of social bots interfering with public opinion in network. *Phys. A Stat. Mech. Appl.* **2020**, *551*, 124163. [CrossRef]
37. Berestycki, H.; Nordmann, S.; Rossi, L. Modeling the propagation of riots, collective behaviors and epidemics. *Math. Eng.* **2022**, *4*, 1–53. [CrossRef]
38. Ran, Y.; Deng, X.; Wang, X.; Jia, T. A generalized linear threshold model for an improved description of the spreading dynamics. *Chaos Interdiscip. J. Nonlinear Sci.* **2020**, *30*, 083127. [CrossRef]
39. Kolomeets, M.; Chechulin, A.; Kotenko, I. Bot detection by friends graph in social networks. *JoWUA* **2021**, *12*, 141–159.
40. Breuer, A.; Eilat, R.; Weinsberg, U. Friend or Faux: Graph-Based Early Detection of Fake Accounts on Social Networks. In Proceedings of the Web Conference 2020, New York, NY, USA, 20–24 April 2020.
41. Vitkova, L.; Kolomeets, M. *Approach to Identification and Analysis of Information Sources in Social Networks*; Springer: Saint-Petersburg, Russia, 2019; pp. 285–293.
42. Vitkova, L.; Chechulin, A.; Kotenko, I. Feature Selection for Intelligent Detection of Targeted Influence on Public Opinion in Social Networks. In Proceedings of the Fifth International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'21), Sirius, Russia, 30 September–4 October 2021; pp. 421–430.
43. Dataset "Segmentation_of_the_Audience". Available online: https://www.kaggle.com/lidiaiskin/segmentation-of-the-audience (accessed on 8 November 2021).
44. Shamir, J. Information Cues and Indicators of the Climate of Opinion. *Commun. Res.* **1995**, *22*, 24–53. [CrossRef]
45. Zerback, T.; Koch, T.; Krämer, B. Thinking of Others. *J. Mass Commun. Q.* **2015**, *92*, 421–443. [CrossRef]