Methods and Algorithms for Performing Separate Operational Tasks for the Protection of the State Information Space

Andriy Peleshchyshyn [0000-0002-5022-0410], Volodymyr Vus [0000-0003-4980-5195], Oleksandr Markovets [0000-0001-8737-5929] and Ruslana Pazderska [0000-0002-0845-5304]

Lviv Polytechnic National University, Lviv, Ukraine
apele@ridne.net1, volodumur.a.vus@lpnu.ua, oleksandr.v.markovets@lpnu.ua3, pazderskaruslana@gmail.com

Abstract. The proposed methods make it possible to generate generalized indicators of information subjects and to build on base them a common system of measures to protect the information space of the state. The issues of fulfillment of separate operational tasks that arise in the process of implementation of such plan are investigated. In particular, methods are proposed to identify users of certain roles that are harmful to the state, identifying possible ways of effective counteraction. The proposed methods will provide the formation of a consolidated system of indicators for the analysis and prioritization of communities from the point of view of national security. They help to plan and organize measures to protect the state's information space. These methods ensure the effective performance of individual operational tasks to protect the information space of the state.

Keywords: social networks, user activity, socially significant con-tent, roles of users.

1 Introduction

One of the most effective types of organization of harmful influences in the information space of the state is the formation, popularization and resource support of opinion leaders with appropriate anti-state direction. Leaders of opinion with a certain level of influence are able to implement a wide range of ideas, carry out psychological and ideological diversions, and manipulate public opinion.

According to the materials on the investigation of Russian influences on political via social networks in the USA and EU countries, there is a tendency to form an entire system of opinion leaders with hidden motivations and tasks.

The identification of such users allows for a number of information and operational activities, minimizing their impact on the mass consciousness.

The paper proposes to apply the term «opinion leader» to a particular class of users based on behavioral traits. Often, this term is applied to various users with a large audience of content consumers. However, this approach has several disadvantages:

- failure to take into account behavioral characteristics inevitably leads to a decrease in the effectiveness of communication methods of counteraction;
- only individuals with large audiences are identified, which complicates forceful methods (spreading negativity in society);
- much of the adverse effects have already taken place, and society has responded to them in an undesirable form (a particularly urgent problem in the event of a rapid escalation of tension).

The behavioral determination of the opinion leader allows us to identify the following complementary tasks:

- early identification of potential opinion leaders – allows you to achieve opinion leadership goals with high efficiency and relatively low risks and resources, but reach a large number of users;
- identifying dynamic opinion leaders (with rapid growth in popularity) – covers a rather narrow set of potential opinion leaders for whom high dynamics of increasing popularity can be traced; accordingly, a wide range of activities can be involved;
- identifying popular opinion leaders (of high public importance) – covers only a small number, but, as stated above, is fraught with additional risks and requires a comprehensive approach.

Let's take a closer look at these tasks. The distribution between potential, dynamic and popular will be based on the popularity of the user.

2 Related works

A practical focus that has been actively used in recent years is the impact through communities. To some extent, it is similar to the previous one, but is different in its tools and tasks of influence. In addition to spreading opinions on behalf of the individual, it is possible to organize more systematic pressure on public opinion by creating a sense of solidarity between the participants. This impact is characterized by a certain level of support, because of the feedback mechanisms in the communities the marketer can expect to attract additional participants without the need to provide them with rewards. This factor is especially important in political propaganda, as it allows the use of the resources of indifferent citizens for their own purposes.

There are several ways to exert influence on the community itself, although usually the support is received from the community administration and several active participants. Similar approaches are used to collaborate with communities as opinion leaders, and additional areas of work with communities are being actively developed:

- • formation of own, fully controlled communities;

- • the destruction of underserved communities.

The first area is characteristic and actively used in the marketing of large corporations, especially those aimed at the general public. Thanks to these communities, corporations are able to bring together productive consumers, receiving powerful additional resources to further promote them. In addition to purely promotional tasks, these communities play an extremely important role for consumer-producer feedback. Thanks to them, the manufacturer is able to form a large knowledge base on the efficient operation of products (such as Microsoft TechNet) and obtain information on necessary improvements and changes.

In addition to corporations, the formation of their own communities is an important tool for the activities of political forces that use them both as a tool of propaganda and as an information technology to account for supporters and coordinate their actions.

Considering this tendency, the opposite direction of activity is also manifested - purposeful destruction of useful opponent of communities. In business, this phenomenon is hardly traced, but it is widespread in political confrontation as a tool to weaken the enemy.

3 Identification of opinion leaders influencing the information space of the state

The simplest way to determine the popularity of a opinion leader is by the number of users of his or her content:

$$UserPop(User_i) = Count(UF_i) \tag{1}$$

Other ways of determining this metric, other than those of (1), are possible, including those that take into account the graph model of social connections and material citation, but this is not fundamental from the point of view of further approaches. More complex definitions of popularity are likely to be fully correlated with the above, but are much more complicated in computing and collecting information.

The popular opinion leader will be considered a user who responds to a strong sign) and a sign of high popularity:

$$UserPop(User_i) \geq \overline{C}_{UP}^{(OL)} \tag{2}$$

where $\overline{C}_{UP}^{(OL)}$ – constant, determines the minimum number of content consumers for a popular opinion leader.

We consider a potential opinion leader a user, who meets the strongest sign, the activity sign and has the minimum acceptable popularity:

$$UserPop(User_i) \geq \underline{C}_{UP}^{(OL)} \tag{3}$$

where $\underline{C}_{UP}^{(OL)}$ is constant, determines the minimum number of content consumers for a potential opinion leader.

The dynamic opinion leader is a user, who responds to one of the signs or, the sign (3) at the end of the period and has a high popularity gain over a certain period:

$$UserPop(User_i, T + \Delta T) - UserPop(User_i, T) \geq C_{Dyn}^{(OL)} \quad (4)$$

where $C_{Dyn}^{(OL)}$ is the minimum popularity gain over the period, T is the beginning of the period, ΔT is the defined time period of monitoring (in practice, a month or a week depending on the dynamics and intensity of the situation in the society).

In most operational tasks, it is advisable to take a running moment of time as the end of the period. Identification of these types of opinion leaders should be carried out consistently, taking into account previous results. The following algorithm is proposed.

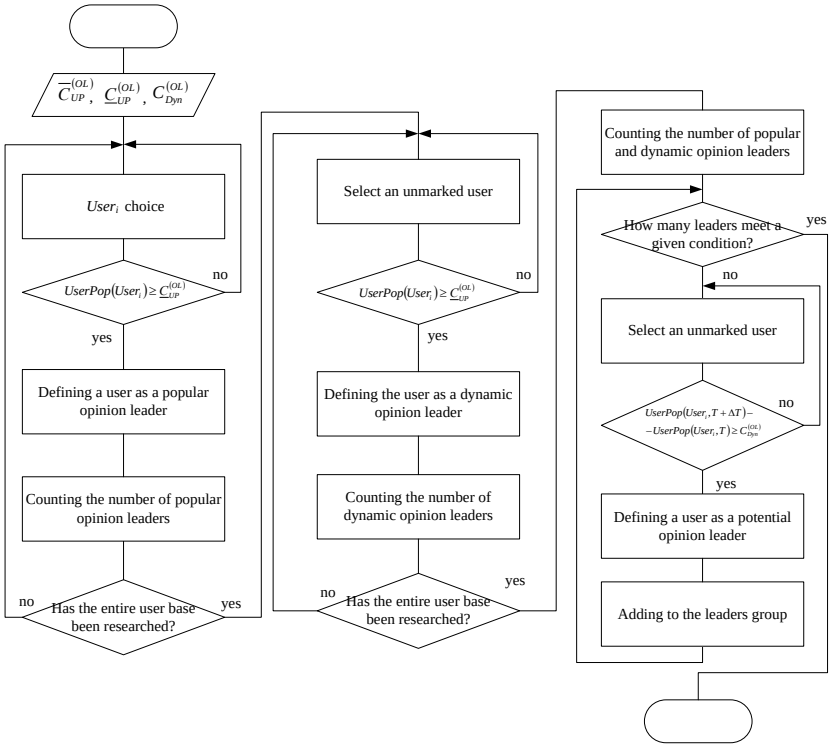

Fig. 1. The algorithm for forming a base of opinion leaders

Searching further to counter potential leaders is advisable in the absence of a good number of popular and dynamic leaders. This is due not to the low value of potential

leaders, but to the fact that in the case of a large number of real leaders, it is unlikely that they will be transferred to the "higher" category.

Given the temporary nature of dynamic leadership, it is important that the algorithm is practiced often enough, at least $\frac{\Delta T}{2}$ (see. (4)).

3.1 Opposition to the leaders of opinions that exert harmful influence in the information space of the state

The opinion leaders can exercise different influences in the state's information space. In some cases, opinion leaders may intentionally or unintentionally engage in harmful activities (hostile propaganda, incitement, animosity, etc.). It is critically important to effectively counteract such sites, taking into account their current characteristics.
The following are considered leaders who have a qualifying influence:

$$USG_i \le C_{Enemy}^{(USG)} \tag{5}$$

where $C_{Enemy}^{(USG)}$ – the constant that determines the threshold of hostility for the USG «Attitude to the State». In practice, the value of the constant is advisable to choose from a range [-1,-0.75].

We next define the following methods of counteraction to each of the categories of opinion leaders engaging in governmental harm according to (5).

It is important to note that it is important to apply methods of counteraction only to those leaders of opinion, for which ordinary public political debate cannot be applied, with the possibility of reaching mutual understanding and eliminating anti-state actions. For this purpose it is advisable to use the proposed indicators of flexibility of the user's position and attitude to the state.

Dynamic leaders are just users who move from the lower to the highest category. At this stage, they are quite vulnerable (as potential leaders), but their value is approaching popular. In this case, dealing with harmful dynamic leaders is one of the most important tasks in terms of process efficiency.

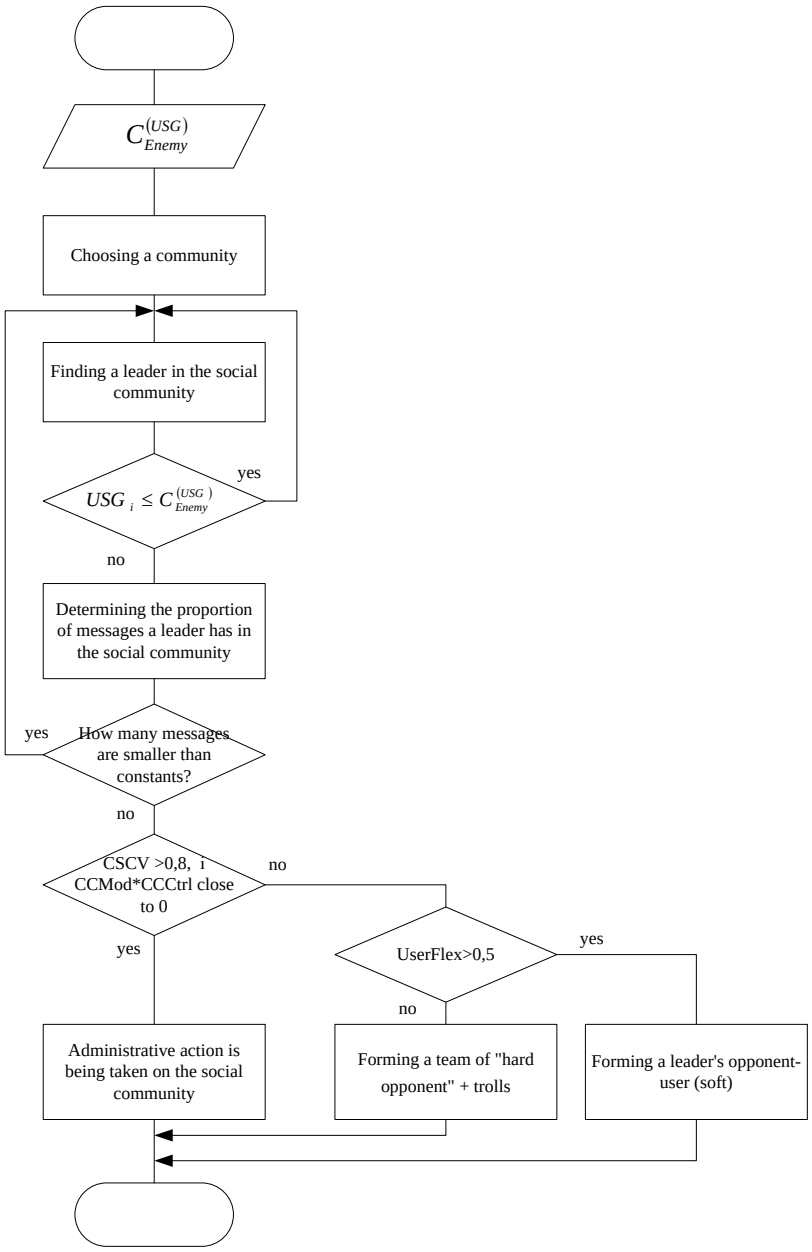

Fig. 2. The algorithm of communication counteraction to the potential opinion leader

The main communication tools to counteract dynamic and potential leaders are to use skilled opponents and reduce the popularity of the communities in which they operate. Figure 2 shows the corresponding algorithm.

For dynamic leaders, the algorithm presented is completely up-to-date, only the requirements for the actions of opponents differ. Opponents should be more active and proactive, given the dynamics of the leader. It is also advisable to attract trolls to reduce the status and motivation of broadcasters of the dynamic opinion leader. The community actions mentioned in the algorithm are explored further in the paper.

In addition to communicating opposition to potential and dynamic leaders, other forms of influence are also effective, primarily organizational and legal. Leaders who do not yet have significant public influence often engage in ill-advised or other-minded activities and are not fully aware of the consequences of the activity. As a result, interviews, warnings, and legal instruments can be effective, but their application is beyond the scope of this work.

Neutralizing the influence of popular opinion leaders is a more difficult task, but is imperative to address in the event of a real threat to national security. Regardless of other tools, the aspect of communicative counteraction is important. Popular opinion leaders are characterized by:

- the authorial nature of the material;
- the high popularity;
- the sufficient material preparation activity.

In general, the content of the set of characteristics boils down to the fact that, in today's competitive environment, the opinion leader needs significant resources, which makes him vulnerable. This opens up the possibility of counteraction, which is summarized below in table 1.

Table 1. Directions to counter popular harmful opinion leaders

Characteristic	**Vulnerability of leader**	**Possibilities of use**
Author material	The Unreliable data	Opponent's criticism of information transfer
	Subjectivity	Opponent's criticism of information transfer
	Lack of culture	Criticism of opponent, trolling
	Bad linguistics	Trolling
High popularity	The broad spectrum of reader	Dissemination of own information in the comments, counter-narratives
	Low criticality	Conducting special operations of communicative and psychological nature
	Competition with other leaders	Using a platform to compromise other harmful leaders
Active preparation	Lack of content	Possibility to influence the theme and content of messages of the opinion leader
	Financial support	

For some leaders, as a result, individual positions in the table may be more or less relevant, which accordingly influences the leader's engagement strategy.

3.2 Detection of trolls and opponents operating according to a defined plan and task

A common element of social media confrontation is engaging users with specific communication skills in destructive activities toward opinion leaders and communities. Formally, such users rarely violate the law, but in practice can offset the positive influence of authoritative individuals in society. Such a phenomenon could destroy the patriotic community, thus eliminating a certain public resource available to support public interests. The large social communities involving tens and hundreds of thousands of citizens can be destroyed. The result is either the degradation of the social community or the loss of motivation to engage in socially beneficial actions (volunteering, mutual assistance, information support, etc.).

The methods for detecting trolls are based on the hypothesis that the troll is, to a certain extent, “attached” to individual users with “opinion leader” roles opinions, «moderator», «translator».

In addition, identifying malicious trolls, as opposed to detecting malicious opinion leaders, only makes sense in the context of protecting predefined communities and users that are important to the protection of the state.

Thus, we obtain the following algorithm for detecting harmful trolls (see fig. 3).

Like opinion leaders, trolls can have varying degrees of popularity among users, but at a psychological level, users understand the technical importance of trolls, leading to low public authority. Thus, the entire range of communication and legal measures can be applied to counteract trolls. The vulnerability of trolls to communication activities is usually increased due to their anonymity or the inaccuracy of personal data.

An effective method of counteraction is also to enhance communication skills and introduce specific communication strategies for opinion leaders and communities valuable for national security. In this case, the efforts of harmful trolls can be spent intentionally or at all to act in the public interest, there is a possibility of exploitation of hostile users in the interests of the state.

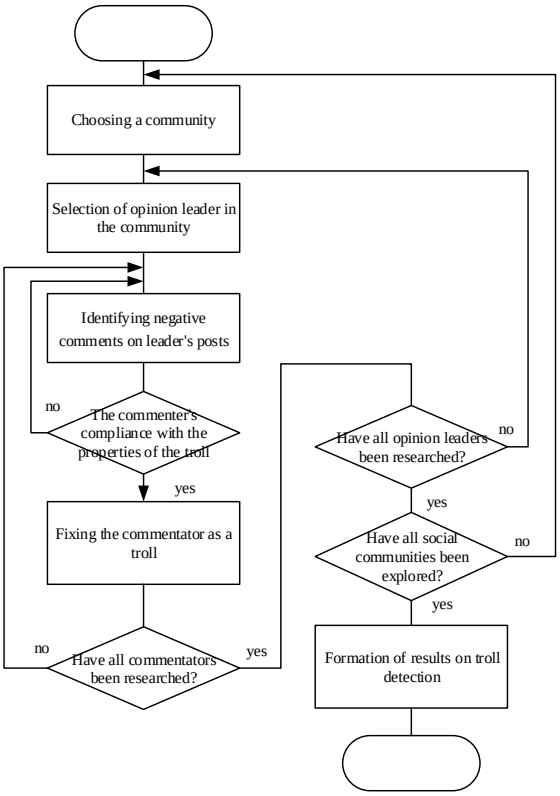

Fig. 3. Detection algorithm for malicious trolls

A key element of such strategies is the hypothesis of a material or other interest in the troll and its accountability to management. This is based on the method of indirect counteraction, as follows:

1. bringing the troll to the brink of breaking the rules of communication – communication rules should be strengthened if necessary;
2. putting it in the face of virtually inevitable blocking – there is a threat of the troll's failure to fulfill its tasks;
3. not blocking him, but revealing his behavior as a troll, – the troll is forced to formally adjust behavior and act within the social community.

When done properly, the resources of the troll are directed to intensive communication within the community. These actions address one of the key problems in most communities – low user engagement in content creation. In addition, there are other, additional, benefits (the possibility of a «live» demonstration of caricature behavior of harmful trolls in social communities, etc.).

Note that today in the social media of the Internet there is a certain division of trolls into «thick» and «thin». The first category includes users of this role with low communication skills and quality of the material, the second – with high. The above

method of indirect counteraction is advisable to use only against «thin» trolls. In addition, this approach should also be applied to harmful users of the role of «opponent», given the fact that the «thin troll» and «opponent» are quite close and differ only in nature of influence (psychological and informational).

3.3 Identification of moderators performing resource support for harmful influences

Identifying moderators that are harmful to the information security of the state is based on an analysis of impact actions (see section 2.1.4 "Formal description of user activity"), taking into account the nature of changes in visibility and the nature of the content to which it applies. Identify the following types to identify the moderator as harmful:

- property of controlled resources;
- austerity towards patriotic opinion leaders;
- condescension to hostile opinion leaders.

The simplest is the property of controlled resources. That is, the moderator who manages the social community defined as harmful (see. section 2.2.6 «Characteristics of State Security»), so at least one of two conditions must be fulfilled:

- $CmL_i \le C_{Enemy}^{(CmL)}$ is harmful on the basis of loyalty or
- $CmA_i \le C_{Enemy}^{(CmA)}$ is harmful on the basis of communicative direction for at least one community in which the user acts as a moderator.

This property allows identifying moderators who explicitly support the development of communities harmful to the state. However, in practice, harmful activity can be carried out in a less obvious way. The moderator can formally administer a politically neutral community with a broad spectrum of opinions (the indicator is close to zero), but implement a policy of moderation in such a way that leaders of patriotic thinking are in a losing situation. In particular, the following steps may be taken:

The overly strict application of the rules to patriotic opinion leaders, that is, the indicator of his personal comfort is much lower than the general:

$$CmComf_i > CmComf_i^* \tag{6}$$

where $CmComf_i^*$ is a measure of comfort for patriotic opinion leaders.

Not strict enough to apply rules to harmful users, to create them comfortable conditions

$$CmComf_i < CmComf_i^{**} \tag{7}$$

where $CmComf_i^{**}$ is a measure of comfort for harmful opinion leaders, opponents, and trolls.

Performing at least one of the following attributes makes it possible to attribute a community moderator to such users who carry out activities harmful to the security of the state.

Conclusion

Methods and algorithms of planning of measures for counteraction to propaganda are developed and the general distributed information and technological algorithm of organization of actions in web communities. One of the key tasks of the early stage of the state's information space protection activities is to establish a catalog of significant personalities that are in the CSI. To solve it, an algorithm for personalization of information subjects was created. To detail one of its stages, an algorithm for individual user processing has been developed, which provides for the collection and systematization of user data according to the proposed formal model. The fulfillment of individual operational tasks that arise during the implementation of such a plan is investigated. Methods are identified for identifying users who perform roles that are harmful to the state, identifying possible ways to effectively counteract them. A method of identifying thought leaders influential in the information space of the state has been developed. It is suggested to use the term "opinion leaders" for a particular class of users based on behavioral traits. The behavioral determination of the thought leader makes it possible to solve the complementary tasks of identifying thought leaders: potential, dynamic, popular, based on given thresholds.

References

1. Deebha Mumtaz, Bindiya Ahuja,"A Lexical Approach for Opinion Mining in Twitter", International Journal of Education and Management Engineering(IJEME), Vol.6, No.4, pp.20-29, 2016.
2. Prajit Limsaiprom, Prasong Praneetpolgrang, Pilastpongs Subsermsri,"Visualization of Influencing Nodes in Online Social Networks", IJCNIS, vol.6, no.5, pp.9-20, 2014.
3. Mouna El Marrakchi, Hicham Bensaid, Mostafa Bellafkih, "E-Reputation Prediction Model in Online Social Networks", International Journal of Intelligent Systems and Applica-tions(IJISA), Vol.9, No.11, pp.17-25, 2017.
4. Ali M. Meligy, Hani M. Ibrahim, Mohamed F. Torky,"Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks", International Journal of Computer Net-work and Information Security(IJCNIS), Vol.9, No.1, pp.31-39, 2017/
5. I. Korobiichuk, S. Fedushko, A. Juś, Y. Syerov "Methods of Determining Information Support of Web Community User Personal Data Verification System". In: Szewczyk R., Zieliński C., Kaliczyńska M. (eds) Automation 2017. ICA 2017.

Advances in Intelligent Systems and Computing, vol 550, 2017, Springer, pp 144-150.
6. O. Markovets, R. Korzh, U.Yarka , “Research of means used in communication of Internet users with local authorities”. Eastern-European Journal of Enterprise Technologies, 2013, Vol. 3, Issue 9 (63), pp. 38–41.
7. S. Fedushko, "Development of verification system of socio-demographic data of virtual community member," Radio Electronics Computer Science Control, Article no. 3, pp. 87-92, 2016.
8. O. Markovets, A. Peleschyshyn, "Modeling of citizen claims processing by means of queuing system" in International Journal of Computer Science and Business Informatics (UCSBI), India:IJCSBI.ORG, vol. 15, no. 1, pp. 36-46, 2015.
9. A. Peleshchyshyn, R. Korzh, "Basic features and a model of university units: University as a subject of information activity", Eastern-European Journal of Eenterprise Technologies, vol. 2/2, pp. 27-34, 2015.
10. Gnatyuk, S., Sydorenko, V., Aleksander, M.: Unified data model for defining state critical information infrastructure in civil aviation, In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, Kyiv, Ukraine, May 24-27, pp. 37-42 (2018).
11. Gnatyuk, S., Akhmetova, J., Sydorenko, V., Polishchuk, Yu., Petryk, V.: Quantitative Evaluation Method for Mass Media Manipulative Influence on Public Opinion, Proceedings of International Conference Computational Linguistics and Intelligent Systems (COLINS 2019), pp. 71-83 (2019).