Problems of Analysis and Forecasting of Information and Psychological Influences in Social Networks

Mykola Brailovskyi [1], Serhii Toliupa [2]

[1] *Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine*

Abstract

To protect against information and psychological influence, it is necessary to use not only defensive methods, but also preventive ones. Such tools include analysis and forecasting of events, information about which is beginning to appear and discuss on social networks with increasing frequency. The issues of influencing people and society through "soft power" and the use of network structures that can effectively calculate, predict and counteract the manifestation of manipulation in the digital space are considered.

Keywords

Social networks, analysis, forecasting, management, information impact, soft power.

1. Introduction

Today, online social networks are extremely popular and are one of the main tools of information and psychological impact on a large part of the population, and for the most part on young people. The need to counter information security threats that can be implemented through online social networks is confirmed by the National Security Strategy and the Information Security Doctrine of Ukraine, which indicates the significant relevance of the study of information processes in online social networks, which are weighted heterogeneous networks.

Profound changes in the attitude of most countries of the world, including Ukraine, to their own information and, consequently, cyber security prompt to pay more and more attention to the development of recommendations on short- and long-term priorities for security sector transformation in search and collection of information from open and relatively open sources. , as well as its extraction from closed electronic sources, while caring about the protection of its own information resource from outside cyber influence [1]. Many publications of foreign and domestic authors, such as V. Horoshko, V. Buryachok, A. Korchenko, V. Domarev, V. Bogdanovich, J. Koziol, M. Kuznetsov, Kr. Kaspersky, K. Mytnyk, I. Simdyanov.

2. Main part

With the development of information systems and the global Internet, in addition to gaining significant opportunities for information exchange, the world community has become too vulnerable to outside cyberspace, namely from blatant attempts to influence each other's information and cyberspace through the use of modern computing and / or special equipment and related software (so-called cyber interventions) and other manifestations of their destabilizing negative impact on a particular object, which are realized through the use of technological capabilities of information and cyberspace, creating a danger both for themselves and for human consciousness as a whole (so-called cyber threats) [2].

In the era of global intensification of information processes and their penetration into

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine

EMAIL: bk1972@ukr.net (A.1) ; tolupa@i.ua (A. 2)
ORCID: 0000-0002-3148-1148 (A.1); 0000-0002-1919-9174 (A. 2)

all areas (social, political, economic) of human activity, when almost everyone has to perform various tasks interacting with many elements of IT infrastructure, the dependence of each individual on information systems and networks and its vulnerability in relation to extraneous cybernetic influence are constantly growing. Eventually, the human psyche is traumatized, and this, in turn, can motivate it to disclose information with limited access (R&D). That is why social engineers in search of the objects of their attacks take into account primarily the psychological state of those involved [3,4].

The most important tasks of information and analytical support for working with online social networks are their monitoring, analysis, as well as forecasting and management.

The first two tasks are used to understand the processes taking place in social networks. Monitoring includes obtaining and structuring primary data. This collects the texts of messages, links between users and links to external resources. The capabilities of these systems are largely determined by the richness of the data used and the mode of their processing. If possible, data analysis of the monitoring system and analysis of social networks can be divided into three types:

- systems that do not perform data analysis;
- systems that perform retrospective data analysis;
- systems that perform real-time data analysis [5-7].

Real-time monitoring systems are more complex to design and operate than complexes that use retrospective data collection. Therefore, the role of data obtained earlier and on the basis of which some conclusions and forecasts have already been made, as well as the creation of appropriate knowledge bases, becomes obvious. The analysis involves several stages of primary data processing. First of all, basic indicators are calculated that answer simple quantitative questions, such as "how many users are online?", "How many messages did the user write?", "How many of them are active?", "How many of them have a high level of authority. », Etc. Then the identification of statistical and structural patterns in the obtained data, which allows to understand the nature of the studied network. For example, the types of distributions that include discussions of certain topics. From the point of view of practical application, the greatest interest is the identification of specific patterns in narrow subject discussions. Identifying the most popular topics for discussion and, most importantly, user reactions to them.

The forecasting stage is used to predict with a certain degree of probability the state of a social network over a period of time under certain conditions.

They can focus on the analysis of various objects of the social network [8], such as:

- the network as a whole (using aggregate global indicators);
- subnets and communities;
- individual users;
- information messages;
- opinions (with the help of indicators of the tone of the message on some information objects);
- external nodes − information resources of the Internet. It should be noted that the information object may be a person, event, organization, etc.

According to the authors, to date, little attention is paid to such a process as event forecasting. This may be due to the fact that the tasks of analysis, forecasting and management may be different. First, depending on who sets the task, who is the end user of the system, who is interested in the topic. There are different types of users who need to analyze, predict and manage online social networks [9]:

- bodies of state power and local self-government;
- enterprises of the public and private sector of the economy (commercial, research organizations, mass media);
- society (political parties, individuals).

Secondly, how much the expected forecast is beneficial to the user. Will this forecast lead to a general deterioration of the political or economic situation of the user, and even national security in general. There are cases, and there are many, when after the analysis there is no reaction to the situation or information about the event. Or assumptions, forecasts of expected development of a situation are not resulted. There is no alarm signal for negative information. The question arises: "Do we not see the threat or do not want to see it?". This is especially true of cultural events such as literature, cinema, pop, painting, etc.

As you know, man lives in three dimensions − in the real world, the information world and the symbolic world. However, it is in today's world that new technologies and means of communication have such a powerful effect on consciousness that real actions and events only become significant when they are presented in the media, ie become a function of virtuality. As if the event does not exist in real life, if it is not written about on the site or it is not reflected in the social network. This is one side of the issue. It is also important that modern technology allows you to easily and quickly manipulate the minds of large masses of people, to form the necessary manipulator images and symbols [10-12].

The best example of such a situation, taking into account the mass public social networks, is just − cinema, called not for nothing one of the classics of the world proletariat − the most important of the arts. It allows you to embody all possible methods of psychological influence − video, sound, rhythm, ideas, guidelines, etc. In movies, it is quite easy to inspire the viewer with the words and actions of the protagonist algorithm of actions and "correct" perception of the problem. Examples are popular films made in Russia at one time − "Brother" and "Brother-2", "72 meters", "Kandahar", which represent Ukrainians as a second-rate nation of traitors, unobtrusively forming the necessary stereotype in the viewer.

Such approaches begin to control the user. Therefore, it is necessary to recognize external influences and predict what it may lead to in the future.

The management phase is to provide targeted influences on the social network to translate information processes into the desired state. At this stage, high-quality recommendations to the user are possible, the so-called "soft power".

The concept of "soft power" (MS) was introduced into scientific circulation ("Soft power") by Joseph Nay − an American political scientist, professor at Harvard University in the early 90's of last century.

The basic meaning of soft power is the formation of attractive power or living conditions, that is, the ability to influence people's behavior, indirectly forcing them to do what they would otherwise never have done. Such power becomes not only based on persuasion, persuasion, or the ability to motivate people to do something with arguments, but also on the "assets" that produce its attractiveness. To achieve this, according to Nay, is possible using the "power of information and images", the power of meaning. In other words, the core of "soft power" is intangibility, and informativeness and mobility.

Mild force on large masses of people can be carried out in a relatively short period − it usually does not exceed a few months. In this case, the most effective soft power tools are the media, traditional and new social media.

In the long run, soft power is less dependent on rhetoric, but more related to practice. In this case, effective tools of "soft power" are: the provision of services for language learning, culture, history, higher education, as well as the development of science, including social, whose main task is to produce meanings − theories and concepts, legitimizing the position and views of the state, which pursues a policy of promoting their worldview, traditions of life. The combination of these strategies allows you to influence the system of socio-cultural filters or "matrix of beliefs" of a particular individual, society, to which this type of influence is applied, forcing him to eventually change his behavior to the desired manipulator.

One of the ways to solve the above problematic issues is to automate the management of the protection of society from negative information and psychological impact (IPI). This automation should be understood as a set of measures for the development, implementation and use of hardware and software by the appropriate officials in the interests of making informed decisions to eliminate the destructive influences on people of information flows generated by the enemy or other unfriendly forces.

Automation of control over the defense of society from the enemy's IPI, first of all, presupposes the presence at control points of complexes of automation equipment (CAE) of protection with the corresponding special software (SSS).

The creation of the latter can be based on a logical-mathematical model, which is a formalized description of the processes of receiving, transforming and processing input information, formulating the necessary conclusions and proposals.

As the input information necessary for modeling the protection of society from negative information and psychological impact, one should first of all consider the initial information and data characterizing the direction and scale of the latter. In addition, data on the moral and psychological state (MPS) of people and on the factors that, in the current situation, have (will) have the most significant impact on this state will be of great importance.

Determination (forecasting) of the direction (topic) of negative IPI today, as a rule, is carried out in free formulations after a specialist in the information warfare body has studied the information about the information activity of the attacker. At the same time, this process can be partially automated, provided that a systematic list of possible topics of hostile propaganda is created and included in the database (DB) of STRs.

The scale of the IPI malefactor should be understood as a generalized characteristic of the capabilities of its forces and means of psychological operations (PsO) in terms of the destructive impact on the MPS of society. The scale of the IPI is usually predicted on the basis of a study of operational intelligence information and reference data on the composition, tactical and technical characteristics, the probable nature of use, and the location of the enemy's PsO forces and assets. Formalization of conclusions about the scale of negative IPI in relation to society can be ensured by transforming the initial characteristics indicated above into integral quantitative indicators of the capabilities of the enemy's PsO forces and means:

a) coverage of the target audience (the number of people exposed to IPI);

b) by the strength (intensity) of the impact.

The degree (or coefficient) of coverage of people subjected to IPI by a group of forces and means of the enemy's PSO at a certain point in time (t) is calculated by the formula:

$$K_{\mathrm{I\Pi B}(t)} = \frac{N_{\mathrm{I\Pi B}(t)}}{N_{\Sigma}}\,, \qquad (1)$$

where:

$N_{\mathrm{I\Pi B}(t)}$- the probable number of people falling into the coverage area of the grouping of PsO funds,

N_{Σ}- the total number of personnel of the inhabitants of the region.

The specified coefficient will depend on the number of means of influence of a particular type in the operation area, the size of their coverage areas, the characteristics of settlements (size, infrastructure, people and their views, preferences, living standards, etc.).

Depending on the type of PsO tools, the calculation of the size (area) of their coverage areas has its own specifics. Thus, the coverage areas of sound and television and radio propaganda of the enemy, as well as psychological weapons based on new physical principles (infrasonic, ultrasonic, microwave and psychotronic generators, flash noise ammunition, sources of coherent and incoherent light), are determined mainly by the range of their action and, accordingly, power. And the impacts of social networks are limited only by the Internet coverage area.

The total coverage area of the grouping of PsO means will be determined by the outer boundaries of the coverage areas of individual means when they are overlaid. Calculation $N_{\mathrm{I\Pi B}(t)}$ requires a special technique.

It is advisable to determine the probable intensity of negative IPI on society on an n-point scale (table), which is based on a prognostic assessment of the strength of the influence of various types of enemy psychoactive means on the MPS society. In turn, this force is determined by the form of information presentation (type of psychotechnology), implemented in a specific medium.

When several types of enemy psycho means are functioning, their integral force of impact on the population should be calculated using the formula:

$$F_{\mathrm{I\Pi B}} = \frac{\sum_{i=1}^{n} f_{\mathrm{I\Pi B}_i}}{n}\,, \qquad (2)$$

where: $f_{\mathrm{I\Pi B}_i}$ is the force of influence of the i-th type of psychoactive means, n is the number of types of the enemy's psychoactive means in the area of forthcoming actions.

The scale of the intensity of the impact of the main means of the enemy's PsO on the population will be measured from 1 to 10, where 1 is the lowest level of influence, and 10 is the highest.

Ultimately, the probable scale of the enemy's IPI, reflecting the potential of his forces and means of PsO in the area of influence at the moment t, can be calculated as the product of the values of the capabilities of these forces and means, measured in the range from 0 to 1, both in terms of the coverage of society and by the intensity of the impact:

$$M_{\mathrm{I\Pi B}(t)} = \mathrm{K}_{\mathrm{I\Pi B(t)}} \cdot \mathrm{F}_{\mathrm{I\Pi B}}\,, \qquad (3)$$

with $M_{\mathrm{I\Pi B}(t)}$ <0.3, the scale (level) of negative IPI should be considered insignificant, with 0.3 < $M_{\mathrm{I\Pi B}(t)}$- 0.7 − significant (average), and with $M_{\mathrm{I\Pi B}(t)}$> 0.7 − critical (extreme).

The quantitative value of the indicator of the scale of the enemy's information and psychological impact, first of all, allows us to draw a conclusion about the place of the task of protecting against this impact in a number of other tasks of moral and psychological support (MPS). Mathematically, this conclusion determines the specific amount of time, effort and funds allocated for the implementation of measures to eliminate destructive influences on the personality. So, already at $M_{\mathrm{I\Pi B}(t)}$ - 0.3, the model for managing protection against negative IPI should initiate the inclusion in the content of MPS of preparation for measures to identify, physical and informational blocking (suppression) of sources of destructive information, neutralizing carriers of demoralizing views and moods, informing the population about the expected nature of the impact enemy. At higher values of the $M_{\mathrm{I\Pi B}(t)}$ considered model, a request for the allocation of additional resources to protect against negative IPI is activated.

A prerequisite for the logical and mathematical modeling of the optimal content of protection against negative IPI is the availability of information about the most effective methods (measures) of such protection in the database (DB) of IPO measures. This mainly presupposes their preliminary accumulation and structuring, as well as the formulation of rules (like "if ...

then…") for a reasonable selection of measures to neutralize demoralizing influences on the population in relation to the current situation. The main source of this information should be considered expert knowledge obtained through studying the opinions of experts, analysis of guidance documents, practical experience and conclusions of scientific research in the field of information warfare. On the basis of the collected information, a matrix (spreadsheet) is constructed containing the most complete list of measures to protect against negative IPI and the parameters of each of them, including: its information basis (subject matter); time, effort and resources required to prepare and carry out measures to protect one object; the number of objects to be protected; the total amount of work (time) for the preparation and conduct of the event (hours) in order to solve the problem on a regional or national scale. The matrix of measures to protect against negative IPI and the database of IGO activities as a whole should be maximally coupled with the database of IGO information resources (national security).

The choice of the specific content of protection against negative information and psychological impact is primarily due to the direction of the latter, as well as the conclusions expressed in numerical values from the assessments of the moral and psychological state of the population, the socio-political situation and other factors that have a significant impact on the Ministry of Railways of society, taking into account the available temporary resource of forces and means of MPO. At the formalized level, the choice is made by means of logical links to the database cells containing the codes of the information basis and the names of the activities that satisfy the previously formulated rules of the specified choice. As a result, "at the output" of the model, proposals are formed on the most appropriate measures to protect against negative IPI, indicating their subject matter, duration (time) of carrying out, the necessary forces and means.

Daily life practice convincingly proves that information and cyber security is a continuous, extremely complex and multifaceted process, and success in its implementation is determined by society and depends on each of its representatives, but above all on the steady implementation of public policy in this area, purposeful efforts of all branches. authorities, the scientific community, leaders at all levels [6]. At the same time, systematized measures to prevent numerous threats should not hinder the increasingly rapid formation of the national information and cyberspace, as well as the integration of Ukraine into the global information society [7]. That is why the strategic task of state policy should be the formation of a comprehensive system of information and cyber security, which is based on scientifically sound political, social and economic criteria and world experience in legal and organizational aspects of functioning [13-15].

3. Conclusion

Thus, it becomes obvious the need to pay more attention to the processes taking place in social networks and the information circulating in them. As they say in the famous saying: "There is no smoke without fire", that is, if some information appears on the network and begins to be heatedly discussed by users, then someone needs it. And it can be an artificial excitement.

Therefore, it is necessary to pay special attention not only to its individual components, but also to their totality. It is necessary to create criteria, algorithms and software for forecasting, preventing the situation and making the right decisions in a timely manner. It is clear that the government, which seeks to preserve sovereignty, must have a set of tools that limit (minimize) the effectiveness of manipulative influence of "soft power". States need to develop and implement those network structures that can effectively detect, predict and counter the manifestation of manipulation in the digital space, to work in the same operational field as their potential and real opponents.

4. References

[1] M. Brailovskyi, V. Khoroshko, V. Artemov, O. Lytvynenko Information war in modern conditions. Part 1 // Scientific & practical cyber security journal (SPCSJ) VOL 5. №2. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-modern-conditions-part-1-3/

[2] V.L Buryachok, S.V Toliupa., V.B Tolubko, V.O Khoroshko. "Information and cybersecurity: socio-technical aspect" // Textbook. − K.: Nash format, 2015. – 288p.

[3] V.L Buryachok, S.V Toliupa, V.V. Semko Information and cyberspace. Security issues, methods and means of control. Tutorial. K .: LLC "Our format", 2016. − 176p.

[4] NN Brailovsky, VA Khoroshko Methods of recognizing cyberattacks taking into account the monitoring of the information

environment. Information security. Volume 27, № 1 (2021) pp.6-13

[5] S.V Toliupa., V.S. Nakonechny, N.N. Brailovskyi. Building Cyber-Security Systems of Information Networks Based on Intellectual Technologies // Scientific & practical cyber security journal (SPCSJ) №1. [Electronic journal]. URL: http://journal.scsa.ge/issues/ 2017/09/432.

[6] N. Lukova-Chuiko., I. Ruban, V. Martovytskyi. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System.Cybernetics and Systems Analysis.Vol. 54. № 2. 2018. pp. 142 – 150.

[7] N. Lukova-Chuiko, V. Saiko, V. Nakonechnyi, T. Narytnyk, M. Brailovskyi. Terahertz Range Interconnecting Line For LEO-System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine. 2020. pp. 425– 429.

[8] I. Ruban, V. Martovytskyi & N. Lukova-Chuiko. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System. Cybernetics and Systems Analysis. Vol. 54, 2018.pp.302–309.

[9] Mashkov V.A. and Barabash O.V. Self-Testing of Multimodule Systems Based on Optimal Check-Connection Structures. Engineering Simulation. Amsterdam: OPA, 1996. Vol. 13, pp. 479 – 492.

[10] V. Sobchuk, V. Pichkur, O. Barabash, O. Laptiev, K. Igor and A. Zidan, Algorithm of Control of Functionally Stable Manufacturing Processes of Enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 206-210, doi: 10.1109/ATIT50783.2020.9349332.

[11] Maksymuk O., Sobchuk V., Salanda I., SachukYu. A system of indicators and criteria for evaluation of the level of functional stability of information heterogenic networks. / // Mathematical Modeling and Computing. – 2020. – Vol. 7, No. 2. – pp. 285 – 292

[12] Korchenko, A., Breslavskyi, V., Yevseiev, S., Sievierinov, O., Tkachuk, S. Development of a Method for Constructing Linguistic Standards for Multi-Criteria Assessment of Honeypot Efficiency.Eastern-European Journal of Enterprise Technologiesthis link is disabled, 2021, 1(2(109)), pp. 14–23

[13] Androshchuk, A., Yevseiev, S., Melenchuk, V., Lemeshko, O., Lemeshko, V. Improvement of project risk assessment methods of implementation of automated information components of non-commercial organizational and technical systems. EUREKA, Physics and Engineeringthis link is disabled, 2020, 2020(1), pp. 48–55

[14] Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615

[15] N. Brailovskyi, V. Khoroshko, V. Artemov, I. Opirskyi, I. Ivanchenko Information war in Ukraine // Scientific & practical cyber security journal (SPCSJ) VOL 4. №4. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-ukraine-2/