The risk-models and risk-criteria for information confrontation in social media

Alexey Nazarov
Professor
Moscow Institute of Physics and Technology
State University
MIREA - Russian Technological University
Moscow, Russia
Expert ITU
a.nazarov06@bk.ru

Artem Sychev
Head of analytical department LLC «SSEC-Service»
Moscow, Russia
sychev@ssec.ru

***Abstract*—On the basis of logical-probabilistic approach proposed risk model successful attacks on social media on the Internet in terms of information warfare. We formulated and investigated the criterion of decision-making framework to achieve the goals of information warfare. Proposed algorithmic foundations of the developed criteria in Hadoop cluster.**

Keywords-warfare; polynomial; risk-models; risk-criteria

I. INTRODUCTION

By "information warfare on the Internet" should be understood rivalry between political actors through the use of specialized information technology resources of the Internet to influence the information environment of the opposing side, the impact on its audience and different spheres of political and power relations in order to establish control over the sources of virtual and electronic policy Resources actor-opponent and achieve information superiority [2]. In other words, the actor aggressor for information superiority over-actor advocate making information attack against an object in the web-space, whose success is a victory, in the sense of achievement of information superiority.

In fact, citizens become an extensive network of ground-based social touch, reflecting the structure of society in real time in nearly every corner of the world, and the speed and volume of the sensor network, especially in terms of "Internet of Things" is growing every day.

Hidden information and psychological impact on the population in social networks used to solve the following problems: informational influence on individuals, social and other groups, society as a whole; informational influence on the feasibility and efficiency of administrative decisions by the government and law enforcement agencies adopted on the basis of this information; manipulation of public opinion through the mass media and, in particular, through social networking services; discrediting the leaders of objectionable; automated information dissemination in the major social networks and the organization of information support activities for prepared exposure scenarios and given a mass audience of social networks.

A. Risk models of information influence and destabilizing factors

The model makes it possible to influence the information to study the dependence of the behavior of the subject of his awareness and, consequently, on the impact of information. Having a model of informational influence, can pose and solve the problem of synthesis of information management - what should be the impact of information (in terms of the control of the subject), managed to get on the subject of the desired behavior. Finally, unable to solve the problem of information management, information warfare can be modeled - the interaction of several actors, whose interests have engaged in information and effects on the same managed object. If the model of informational influence (social impact in terms of sociology and social psychology) are the subject of numerous studies for over half a century, the issues of mathematical modeling is information management and information confrontation in social networks almost never investigated, due to the recent emergence of these.

Based on the above it can be concluded on the relevance of studying the problem of social networks in terms of improved security of its members by building risk models of information and psychological warfare for the users of social networking.

II RISK-ATTACK MODELS

A. THE APPLICABILITY OF LOGICAL-PROBABILISTIC APPROACH FOR THE INTEGRATED RISK ASSESSMENT

Risk Y - an object social media are being attacked by the intruder, consists of two components [1,2]:

- The probability of failure counter attack against him (hereinafter - the failure of the object Y) or the probability of a successful attack

- Evaluation (e.g., financial, material, time to repair the damage, etc.) scale consequences (damage) of a successful attack.

The object of risk is considered to be sufficiently protected if given the opportunity to overcome potential barriers probability of a successful attack (the probability of the risk,

the probability of failure or vulnerability of the object of risk) $P_A^Y = \left(1 - P_3^Y\right)$ than minimum value P_{A-ACC}^Y , i.e.,

$$P_3^Y \geq 1 - P_{A-ACC}^Y \text{ -} \quad (1)$$

- the condition of the feasibility, where P_3^Y - the probability of a successful counter attack (immunity, the success of the object of risk) subject to risk.

For any object risk Y of [1,3] in the general case, there is a complete system (list) security functions or attributes, each of which is in Table 1 denote the binary logic variable X with the appropriate subscript.

Table 1. Security Functions

Designation of security functions	Appointment of security functions
X_1	Preventing the occurrence of conditions conducive to the generation of (occurrence) destabilizing factors (hereinafter - DF)
X_2	Warning immediate manifestations of DF
X_3	Detection manifested DF
X_4	Prevention of exposure to risk in the manifested and revealed DF
X_5	Prevention of exposure to risk on the manifest, but the undetected DF
X_6	Detecting the impact of DF on the subject of risk
X_7	Localization (restriction) found the impact of DF on the subject of risk
X_8	Localization of undetected exposure to risk by DF
X_9	Dealing with the consequences of the localized impact of the detected object on the destabilizing factors risk
X_{10}	Dealing with the consequences of undetected localized exposure to risk by DF

The result of each of the security functions, or the outcome is a random event and can take two values - success or failure. It is assumed that a binary logical variable X_j, $j = 1 \div n, n = 10$ is equal to 1 with probability P_j if the execution of the $j-$ security function has led to the failure risk of the object Y, and this binary logical variable equal to 0 with a probability $Q_j = 1 - P_j$ otherwise. The barriers that are created to counteract the negative effects of destabilizing factors on the subject of risk, perform certain security functions that prevent the implementation of the attacks on the subject of risk. At the same time, technology, one barrier can consistently perform multiple security functions. Obstruction may perform the security functions against different objects risk.

In general, the logic function (L-function) the success of the attack, realizing the impact of destabilizing factors as [1,3]

$$Y = Y\left(X_1, \ldots, X_n\right),$$

and the probability function (P-function, P-polynomial) the risk of failure of the object –

$$P\left(Y = 1/X_1, \ldots, X_n\right) = \Psi\left(P_1, \ldots, P_n\right) = PY .$$

According to the general case of [1,3] L-function (L-polynomial) of the success of an attack is a type of

$$Y = X_1 X_2 \left(\overline{X_3} X_4 \vee X_3 X_5\right) \bullet$$

$$\bullet \left(\overline{X_6 X_7} X_9 \vee X_6 \overline{X_8} X_{10} \vee \overline{X_6} X_7 \vee X_6 X_8\right) \quad (2)$$

and the probability of success of an attack can be calculated using the B-polynomial

$$PY = PY\left(P_1, P_2, \ldots, P_{10}\right) = P_1 P_2 \left[\left(1 - P_3\right) P_4 + P_3 P_5\right] \times$$

$$\times \left[\left(1 - P_6\right)\left(1 - P_7\right) P_9 + P_6 \left(1 - P_8\right) P_{10} + \right.$$

$$\left. + \left(1 - P_6\right) P_7 + P_6 P_8\right] . \quad (3)$$

Destabilizing factors for social networks, of course have their own specifics. DF appear in text messages, the network structure of society, and others. To assess the socio-economic system DF used markers of social stress - stress quantitative active Internet users.

A. Social markers

There are 6 types of social markers [4]:

1. Markers activity. The values are calculated by direct marker of counting the number of messages and users per unit time. Higher values of these markers indicate increased activity in a certain period of time, of mass reaction to some event or "stuffing" of information.

2. Psycholinguistic markers. Display the emotional state of the author's text message. The massive increase in the indicators of emotional stress indicates the emotional contamination - the grouping process on the basis of common passion.

3. Lexical tokens. Analysis is carried out tone text messages (words denoting negative emotional states; words with destructive semantics).

4. Semantic markers. Express elementary sense, for example, destructive, directives, liquidators, results.

5. Network markers. In the process of dissemination of information among people there is a greater number of connections with like-minded people. Normally the graph model satisfies users "small world." Thus, the marker is an integral indicator of the following parameters of the graph: the

diameter of the graph; the average coefficient of betweenness, clustering; the density of the graph; connectivity, and others.

6. Markers consumption. Is an integral indicator that takes into account intra-regional studies the following indicators: number of calls, average call duration, size, frequency, and the total amount of airtime purchases.

The causal completeness of [1] security functions is an important property of logical-probabilistic approach. At the same time, within the framework of refinement and specification information in the context of the attack on the object based on the risk characteristics of the social markers and information warfare practices for each of the security functions that are introduced graduation security functions.

B. New graduation security functions based on social markers

By analogy with the foregoing, we assume that the binary logical variable X_j, $j=1\div n, n=10$ corresponding r-th gradation j-th security function is 1 with probability P_{jr}, if because it perform j-th security function has led to failure. And this X_j equal to 0 with probability $Q_{jr}=1-P_{jr}$ otherwise. Each group of gradations for X_j is a full group of events $\{X_{jr}\}_{r=1}^{N_j}$, so we can use Bayes' formula [1]

$$P(X_{jr}/X_j)=\frac{P(X_{jr})P(X_j/X_{jr})}{\sum_{r=1}^{N_j}P(X_{jr})P(X_j/X_{jr})}. \quad (4)$$

Formula (4) can be used for iterative learning (configuration identification) L-B-polynomials (2), (3) on the statistical data to clarify the value of this risk. This calculation algorithm can organize some rational way, for example, is given in [1].

In order to develop constructive solutions, including architecture, circuit design and algorithmic solutions for the automation of the identification information and counter attacks it is advisable to extend the functionality, the introduction of new grades of these security functions, putting them in line the new indexed binary logic variables are shown in Table 2.

Table 2. New gradation extending functionality security functions from information attacks on social media

Designation of security functions	Appointment of security functions
X_{11}	Preventing an environment conducive to the generation (emergence) DF exposure to the object itself on the basis of the risk of social markers
X_{12}	Collect information about information attack against object risk Y in social media in some Enterprise Networks in the domain on the basis of all the information about changes in the social markers
X_{13}	Collect information about information attack in centralized organization, based on all the information it received
X_{31}	Detection of information attack based on information from a centralized organization
X_{32}	Detection of information attack based on information from other Enterprise Networks in the domain
X_{33}	Detection of information attack based on information from other domains
X_{51}	Prevention through social markers of exposure to the risk of undetected object DF based on information from other Enterprise Networks in the domain
X_{52}	Prevention through social markers of exposure to the risk of undetected object DF based on information from a centralized organization in this domain
X_{53}	Prevention through social markers of exposure to the risk of undetected object DF based on information from other domains.

New L-polynomial for social-media must be taken into account new components according to the table. 2, namely:

$$X_1 = X_{11}\overline{X}_{12}\overline{X}_{13} \vee \overline{X}_{11}X_{12}\overline{X}_{13} \vee \overline{X}_{11}\overline{X}_{12}X_{13} \vee X_{11}X_{12}\overline{X}_{13} \vee X_{11}\overline{X}_{12}X_{13} \vee \vee \overline{X}_{11}X_{12}X_{13} \vee X_{11}X_{12}X_{13},$$

$$X_3 = X_{31}\overline{X}_{32}\overline{X}_{33} \vee \overline{X}_{31}X_{32}\overline{X}_{33} \vee \vee \overline{X}_{31}\overline{X}_{32}X_{33} \vee X_{31}X_{32}\overline{X}_{33} \vee \vee X_{31}\overline{X}_{32}X_{33} \vee \overline{X}_{31}X_{32}X_{33} \vee X_{31}X_{32}X_{33},$$

$$X_5 = X_{51}\overline{X}_{52}\overline{X}_{53} \vee \overline{X}_{51}X_{52}\overline{X}_{53} \vee \vee \overline{X}_{51}\overline{X}_{52}X_{53} \vee X_{51}X_{52}\overline{X}_{53} \vee \vee X_{51}\overline{X}_{52}X_{53} \vee \overline{X}_{51}X_{52}X_{53} \vee X_{51}X_{52}X_{53}.$$

Substituting the obtained logical expressions in (2) we obtain the L-function of the success of information attack in social-media.

Similar to the previous theoretical results can be generated for each specific gradation of 6 social markers. Thus the analytical expressions for the L-function and B-polynomial information attack can easily methodically refined as new knowledge, including intelligence on new DF influencing the behavior of social markers for specific cases of information warfare. The power of the set of security functions is increasing.

II. RISK ASSESMENT CRITERIA OF PROTECTED OBJECT OF INFORMATION WARFARE. PRICE RISK

From (2) the failure of information attack logical condition (L-criteria) can be written as follows:

$$Y_A = 0,$$

is satisfied if at least one of the conditions

$$\begin{cases} X_1 X_2 = 0, \\ \overline{X_3} X_4 \vee X_3 X_5 = 0, \\ \overline{X_6 X_7} X_9 \vee X_6 \overline{X_8} X_{10} \vee \overline{X_6} X_7 \vee X_6 X_8 = 0. \end{cases}$$

Accordingly (3), the failure of information attack probability condition (P-criteria) can be written as follows:

$$PY = 0,$$

is satisfied if at least one of the conditions

$$\begin{cases} P_1 P_2 = 0, \\ (1-P_3)P_4 + P_3 P_5 = 0, \\ (1-P_6)(1-P_7)P_9 + P_6(1-P_8)P_{10} + (1-P_6)P_7 + P_6 P_8 = 0. \end{cases}$$

In general, the ratio of the calculated values of L-function and B-polynomial allow us to estimate the action actor aggressor, attacking the object in social-media on the basis of information from the intelligence, used protecting barriers, peculiarities of the security functions, as well as the existing vulnerabilities in them. Technically, it would be written as actor aggressor known model (2) and (3) with security functions $X_1^A \div X_n^A$ and the probability of failure $P_1^A \div P_n^A$. As the allowable probability of failure risk object (see (1)) can take the value calculated by (3) in the probabilities of failure $P_1^A \div P_n^A$. For actor-aggressor assessment of security risk to the value of the object is $1 - P_{A-ACC}^Y$. Then the value of the difference is defined as [1]

$$\Delta = P_3^Y - (1 - P_{A-ACC}^Y), \quad (5)$$

where the value of P_3^Y calculated by the formula (3), characterized by the implementation of the objective conditions of the reachability (1) and the quality of "armor" barriers, implementing security functions object risk.

We introduce a new measure

$$\Delta Y = YY_A.$$

From (5) it follows that if at least one of the conditions (criterion of exhaustion of reserve risk the stability of the object)

$$\begin{cases} \Delta < 0, \\ \Delta F = 1, \end{cases}$$

it is evidence of an urgent need to strengthen the security of the object of risk.

If carried out at least one of the conditions (a criterion of the presence of the stability margin of the object of risk)

$$\begin{cases} \Delta \geq 0, \\ \Delta F = 0, \end{cases}$$

it indicates the presence of the stability margin of the object to the risk of attacks by actor aggressor. Accordingly, it is necessary actor aggressor invest additional resources in the improvement of the attack on the object of risk.

Cost of risk can be estimated by the following formula

$$CY = \begin{cases} CY_{ACC}, & when\ \Delta \geq 0\ or\ \Delta Y = 0, \\ CY_{ACC} + C, & when\ \Delta < 0\ or\ \Delta Y = 1, \end{cases}$$

where CY_{ACC}- the cost of acceptable risk, C - a term that depends on many factors specific information warfare, the choice of values which is an independent problem.

III. CLUSTER INFORMATION WARFARE AMONG HADOOP

The authors, in a team, doing research on the automation of the information counter attacks in social media. Methodological approaches to the creation of algorithms and software solutions in the environment of web-programming Hadoop for a wide class of problems of monitoring sites in the web-space. Designed cluster topology Monitoring Hadoop, having common application [5]. The research and the algorithm of the measurement attributes of monitoring facilities in the web-space to meet the requirements of unity of measurements. On the basis of neuro-fuzzy approaches developed recommendations following the creation of technological procedures - Assessment of the object of monitoring and identification of its information model. Formulated system requirements for the design of the monitoring cluster Hadoop [5].

According to the creators of such monitoring cluster must have its functionality required for the functioning of the fullness of the control system (CS) Social Media (SM). In other words CS should receive from it all the necessary information to make decisions. Technologically, formally Hadoop cluster management system module (Fig. 1) can be represented as two daemons - **DataNode_Social_Media** responsible for the formation of information model of attacks on social media and **TaskTraker_ Social_Media** daemon responsible for the control actions to curb attacks on social media. Then the proposed new cluster topology information warfare among Hadoop, is schematically illustrated in Fig. 1.

The ability to reliably predict on the basis of SM, such as looming social unrest, ranging from riots and protests and ending assassinations and coups, enables timely decisions to prevent such disasters, without waiting for the bloody conflict, eventually contributing to the stability, peace and order as in individual countries, regions and globally.

It can be concluded that the forecast of the actual behavior of a certain scenario social networking in the future. This

objective can be accomplished by the construction and study of high-quality models of complex social and economic systems, including social, political, economic, informational and other factors. The result is a set of modeling scenarios of the social network, depending on the state of its information infrastructure, and by environmental factors. In addition, the ultimate goal of simulation is to develop recommendations for the development of effective in terms of achieving a given set of objectives and performance criteria of control actions.

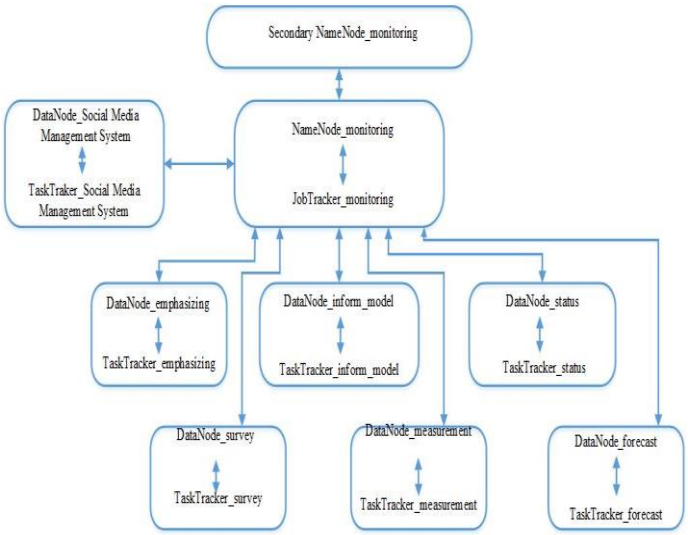

Figure 1. Cluster Topology information warfare among Hadoop. Description daemons are given in [5].

A. Synthesis of new daemons

On the basis of the above, the following guidelines designing software modules ***DataNode_Social_Media*** and ***TaskTraker_Social_Media*** daemons in the form of the following sequence of steps.

1. Definition of the monitoring object. Formation of its information models in a software module into a daemon ***DataNode_Social_Media***.

2. Formation of the complete set of security functions and their grades in a software module ***DataNode_Social_Media*** daemon.

3. Development of software modules that implement the L-polynomial and B-polynomial into a daemon ***TaskTraker_Social_Media***.

4. Development of software modules risk assessment criteria of a protected object of information warfare in the daemon ***TaskTraker_Social_Media***.

5. Development of software modules into a daemon ***TaskTraker_Social_Media*** for calculating the price risk of the object information warfare.

6. Development of software modules into a daemon ***TaskTraker_Social_Media*** to take decisions on further actions based on the results in steps 4 an 5.

7. Set-up Hadoop-cluster information warfare.

Decisions points 1-6 are specified in the operation of the cluster of information warfare as new knowledge of the security functions and algorithms underlying the above-mentioned software modules and daemons ***DataNode_Social_Media*** and ***TaskTraker_Social_Media***. This is done continuously updated software modules other daemons that cluster.

CONCLUSION

As the scientific and methodological framework is proposed to use the formalism of logical-probabilistic approach, allowing the model to information attacks social-media risk positions. This approach is flexible, based on the new knowledge to clarify the actions of the attacker, which makes it relatively easy to specify, develop models of risk of attack.

To evaluate the DF socio-economic systems used markers of social stress - stress quantitative active Internet users. Proposed a risk-based model of social stress markers.

Developed risk assessment criteria of a protected object of information warfare.

For the proposed cluster topology information warfare among Hadoop developed guidelines synthesis algorithmic bases and program modules, and daemons ***DataNode_ Social_Media*** and ***TaskTraker_ Social_Media.***

REFERENCES

Article in a journal:

[1] A. N. Nazarov, “Estimation of information safety level of modern infocommunication networks on basis of logic-probability approach,” Automation and Remote Control, July 2007, Volume 68 Issue 7, 2007, pp. 1165-1176, doi: 10.1134/S0005117907070053.

[2] A. N. Nazarov, “LOGICAL-AND-PROBABILISTIC MODEL FOR ESTIMATING THE LEVEL OF INFORMATION SECURITY OF MODERN INFORMATION AND COMMUNICATION NETWORKS,” Telecommunications and Radio Engineering, USA, 2010, Vol. 69, № 16, pp. 1453-1463, doi: 10.1615/TelecomRadEng.v**69**.i**16**.60.

Article in a conference proceedings:

[3] Nazarov A. ‘Botnet tracking and global threat intelligence - behavior approaches to identifying distributed botnets‘ paper presented at the IEEE / Collection of proceedings of the *Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012.* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6780878&newsearch=true&queryText=Botnet%20tracking%20and%20global%20threat%20intelligence%20-%20behavior%20approaches%20to%20identifying%20distributed%20botnets

[4] Osipov G.S. Methods and software for assessments of social stress, based on analysis of information online. Access: https://www.gkpromtech.ru/material/view?id=27. Date of circulation: 02.10.2015.

[5] Volkov, D., Nazarov, A. & Nazarov, M 2014, ′A global threat - the dark web′, paper presented in the annual Collection of scientific works of International conference Managing the development of large-scale systems" (MLSD'2014), Institute of control Sciences RAS, pp. 452-459