Scientific and Practical Cyber Security Journal (SPCSJ) 3(3): 18 - 24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

Evaluation of the Level of Cyber Security of Information

Khoroshko Vladimir, National Aviation University of Kiev, Doctor in Technical Sciences, Professor Kiev, Ukraine, professor

Mykola Brailovskyi, Taras Shevchenko National University of Kyiv, PhD in Engineering Science, Associate Professor Kiev, Ukraine

Khokhlachova Yulia, National Aviation University of Kiev, PhD in Technical Sciences, Associate Professor Kiev, Ukraine

Ayasrah Ahmad Rasmi Ali, graduate student of the National Aviation University, Kiev, Ukraine

ABSTRACT

A comparative analysis of the concepts of "cyber threat" and "cybersecurity" is given. However, opposite these concepts may be, they are interdependent and have much in common. It is proved that the level of cyber-threat of information simultaneously characterizes the level of cybersecurity, and the quantitative indicator of this could be - the cybersecurity index. The method of calculation of cybersecurity index of is presented in the work. Mathematical modeling of the cybersecurity index of information has not only practical but also predictive value. By employing the values of variables that are included in mathematical dependencies to calculate a cybersecurity index, one can evaluate the effectiveness of implementing certain measures aimed at its dynamics. Therefore, the functional relationship between the cybersecurity index and the value of the information indicators around the information can be an instrument for an in-depth study of the cybersecurity problem of information.

Keywords: cyber security index, security rating, cyber threat

The gradual transition in the development of the human formation of the "information society" to "high-tech society" causes the evolution of approaches to security in the new conditions at different levels. The gradual transformation of citizen, society and state information security concept requires supplementing it with a new concept of cybernetic security. At the same time, there is a process of distinguishing different types of security at the geopolitical levels and understanding the role of cybernetic security at each of them. The need for awareness of the role of cybernetic security is primarily due to the intensification of international, terrorist, extremist organizations and criminal gangs, individual states that exercise cybernetic effects on citizens, society and the state in order to reach their goals.

Cybersecurity is becoming increasingly important in ensuring the national security of the developed states. The cybernetic affects are probably the most effective in achieving the objective of controlling various objects (i.e. individuals, organizations, regions, states, etc.) in the modern world. In fact, a new phenomenon has emerged in international politics: the possibility of achieving political goals, changing legitimate governments and even political, economic and spiritual subjugation of civilians without any military force. Cyberattacks and cyber impacts are evolving rapidly.

With regard to it, one can make the following conclusions concerning the changes in cyberspace and national security of states in the context of transformation of the existing and new methods of cyber-threats, cyber-impacts and their impact on cybersecurity systems, including national, regional and international.

Recently, there has been a surge in research aimed at shaping the cybersecurity of the state. This is necessary due to the need to provide an opportunity to solve the main tasks of cybersecurity in various areas of the state's activity from the common methodological positions.

On the basis of the definition and essence of cybernetics as a science of the general laws describing processes of management and information transmission in society and information systems, and security as the protection of certain objects from threats, cybersecurity can be defined as the state of security management in all spheres (social, technical, sociotechnical), which ensures its effective implementation [1,2].

In order to implement cyber security, a priority task is to ensure the counteraction towards destructive influences in this area, and this requires relevant information. That is why a powerful counteraction is required.

Cybersecurity is an integral part of information security and of each area of national security. Therefore, the state policy of ensuring high-tech cybernetic security becomes one of the most important components of national security policy, which is becoming increasingly independent.

Accordingly, implementing cybersecurity at the international, national and regional levels is one of the most important components of the national security system for any state.

In addition, a comparison of the concepts of "cybersecurity" and "protection" should be made. The protection of information by its main task means the rejection or reflection of a cyberattack on information or unauthorized access to it. Cyber security, compared to protection, is more complex and multifaceted. The information security is achieved not only through the organization of cyber defense, but also through a variety of activities in the political, economic and through other spheres of public life.

When discussing the concepts of "cyber threats" and "cybersecurity" of information, a range of questions may arise: which of these two phenomena is primary; what are their mutual relationship and influence; what are the criteria for their assessment?

It is obvious that the primary concept of "cyber security" lies in information. It is directed against the information dangers through employing the ways, methods and means of cyber security.

However, despite the semantic prominence of the concepts of cyber-threats of information, much is to be found between them.

First, both concepts of the phenomenon are purposefully arisen in the same spheres of human activity.

Secondly, cyber-threats of information and cyber security of information are created by the same subjects.

Thirdly, both cyber threats and cyber security information can be created using the same methods and tools.

Regarding the differences between cyber-information and cybersecurity, they lie in different contexts.

First and foremost, this is the difference between the cyber threats of information and cyber security in relation to the objects of activity: the object of information hazard - mastering, receiving, while the object of cybersecurity - protection, preservation, provision of conditions for the direct existence, information storage and use.

Another fundamental difference between cyber threats and cybersecurity of information is in their relationship with the objects of activity. Cybersecurity information is for its objects an external hostile factor. Cybersecurity is united with its objects by the commonality of the personal unity of goals and interests, especially in experimental situations. In spatially presented objects of cybersecurity information seems to be surrounded by a protective shell, and the cyber threat of information is aimed

at unauthorized access to it and the destruction of both this protection itself and the information itself (object).

Finally, cyber-threats of information and cyber security of information are also distinguished by the arsenal of means by which these phenomena are created in the sphere of life-type information. If the information cyber threat is, first, the means of attack and the impact on it, the cybersecurity of information, which also relies on active counteraction, should be achieved first, ways to prevent unauthorized actions and attacks on information.

The interdependence of cybersecurity information and cyber threats is unequivocal. It has several important features that greatly affect the situation around information.

First, it is a deterrent effect of cybersecurity on cyber-threat information. The cybersecurity information-suppressive information, if it is carried out mainly by one type of protection, is often temporary if it does not eliminate the root causes of a conflict or does not use integrated security systems.

Secondly, there is a stimulating effect of cyber threats on information. Any increase in the cyber-threat of information causes a certain reaction in society, which, of course, reflects the growth of efforts and strengthening of the integrated information security system.

At the same time, the questions of methodical bases for assessing the level of cybersecurity of information are very relevant. Logical methods for analyzing cybersecurity information problems are quite effective, however, they do not allow the establishment of clear functional relationships between the actions of individual factors and their combined outcomes. Therefore, the initial need is to develop a method for quantitative and qualitative analysis and to objectively determine the level of cyber security information.

When considering the concept of cyber-threat information, one can conclude that the cyber-threat of information can be estimated using an integral indicator (the level of cyber-threat information), related in a way to the degree of application of the situation and the expected scale of potential attack or influence. Turning to the question of assessing the level of cybersecurity of information, it is necessary first, to find out the essence of this assessment.

Let's make a few questions to answer.

First, can we talk about cybersecurity of information in the absence of cyber threats? Obviously yes, because the cyber security of information, in fact, is the lack of cyber threats of information. Thus, the complete lack of cyber-threat information means full cybersecurity of information.

Secondly, can we talk about cybersecurity of information in the presence of cyber-threats of information? At the same time, it is possible with a certain caveat: the higher the level of cyber security information. It could seem to be a paradox at first glance, however, the conclusion can be quite simply proved.

As mentioned before, [3,4], cybersecurity of information is achieved in two main ways:

- Prevention of the attack (threat) associated with the use of passive or active actions against the attacker, i.e. the use of various leverages to influence it in order to prevent attempts to resolve the conflict;

- Counterattack, that is, deterrence (or reflection) of attack, using certain methods and means.

The focus of attention is a potential attack on information as an event that may or may not occur, depending on the degree of attacker’s commitment in it and the effectiveness of the cybersecurity implementation system of the object of potential attack. If the attack is to be started, the ability to provide cybersecurity, however, is preserved through the ability to successfully counteract the attack. In this case, it is the event that could acquire a local, regional, nationwide or global scale, depending on the level of attack.

It is possible to build a corresponding scheme of events related to the implementation of cyber threats of information and the provision of cybersecurity information through identifying the cyber threat of information with a potential attack and its consequences, and the cyber security of information - with the successful protection (in any way) of information and the preservation of its value (figure.1).

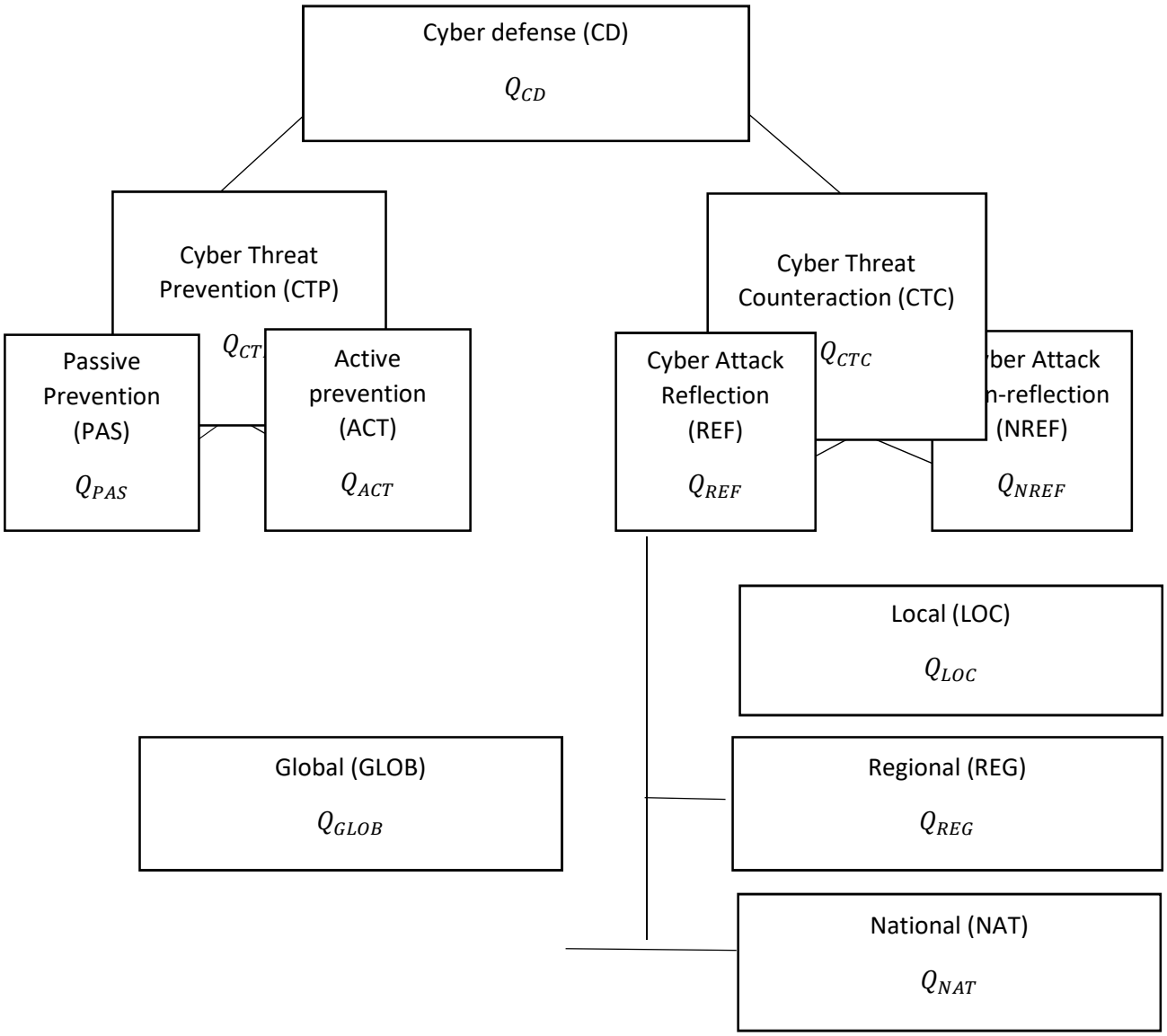

Figure 1. Scheme of events related to cyber s~~ecurity.~~

The key is the following pair of opposite events:
- Dealing with cyberattacks and countering them;
- Passive and active prevention of cyberattacks;
- Repulsing of the cyberattack and its success.

To analyze these events, a mathematical apparatus of probability theory can be used. However, an appeal to the theory of probabilities in this case requires a certain justification.

The fact is that the theory of probabilities operates, as a rule, events and phenomena that have such a property as statistical stability. The story gives thousands of examples of various conflicts, the

conditions for their occurrence, development and completion are so diverse that it is very difficult to distinguish stable statistical features. However, there are many arguments in favor of the probable approach to use in the field of cyber security.

The probability theory has many ways to determine the probability of events indirectly, because of the likelihood of other events associated with the first [5].

Significant help in solving this problem can give rise to the well-known Laplace uncertainty principle [4], the essence of which is that, in the presence of several hypotheses, none of which cannot be defeated, the probability of occurrence of the corresponding events should be considered the same. Since in this case we consider pairs of opposite events, then the starting point can serve as an axiom that for such events the sum of probabilities of their onset is equal to one.

These are the fundamental foundations for the application of the probability theory in the interest of investigating mechanisms for the emergence and termination of conflicts and attacks in the information (cyber) space.

By the way, the probabilistic approach in the analysis of conflict situations is also used in foreign studies [4].

Returning to figure 1, we note that here is the event, which is to provide cybersecurity, is marked as CD, and its probability is marked as Q_{CD}. This event can occur simultaneously with one of two other inconsistent events: with a cyberattack (CTP) with a probability of as Q_{CTP}. or with a cyberattack (CTC) with probability Q_{CTC}. At the same time, since events CTP and CTC form a complete group, then

$$Q_{CTC} = 1 - Q_{CTP} \quad (1)$$

Considering happening of the events CTP and CTC under the conditions of a specific level of cyber-threats, as only two possible hypotheses, in connection with which, with the probability Q_{CD}, according to the expression of complete probability [3] can be written

$$Q_{CD} = Q_{CTP} * Q\left(\frac{CD}{CTP}\right) + Q_{CTC} * Q(\frac{CD}{CTC}) \quad (2)$$

Or considering (1) we write

$$Q_{CD} = Q_{CTP} * Q\left(\frac{CD}{CTP}\right) + (1 - Q_{CTP}) * Q(\frac{CD}{CTC}) \quad (3)$$

where Q (CD / CTP) - conditional probability of occurrence of the event of a short-term damage in a series of offensive HQ; Q (CL / CPZ) - conditional probability of occurrence of a CF event in case of occurrence of the PCZ event.

Note that the onset of the CTP event means that the cyberattack is reflected, the cyber-threat is neutralized. In this case, the event CD is true, i.e :

$$Q\left(\frac{CD}{CTP}\right) = 1 \quad (4)$$

If a CTC event occurs, then the probability of a CD event is determined by the probability of a successful reflection of the cyberattack on the information (1), that is,

$$Q_{CD} = Q_{CD} \quad (5)$$

Then, considering (4) and (5), it is possible to write down

$$Q\left(\frac{CD}{CTC}\right) = Q_{CTP} + (1 - Q_{CTP}) * Q_{CTP} \quad (6)$$

It is important to determine the physical meaning of the value Q_{CTP}. If we denote the maximum damage to national interests and organizations as a result of external cyberattacks on information as G_{max}, then we will assume that with some probability of cyberattack reflection Q_{CTP} loss will be equal to $G_{max}(1 - Q_{CTP})$ and if $Q_{CTP} = 1$ (hypothetical case) the loss will be around zero.

Further consideration of the relationship of events is shown in Fig. 1 can be carried out according to a similar scheme. The probability of averting a cyberattack by passive action (PAS) or active containment of a cyberattack (ACT) is determined as follows:

$$Q_{CTP} = Q_{PAS} + (1 - Q_{PAS}) * Q_{ACT} \quad (7)$$

Note that the probability of deterrence or distraction of a cyberattack can be, to a certain extent, an assumption comparable to the probability of its successful reflection, since a potential attacker, when deciding on unauthorized access to information, derives, above all, from the capabilities of the party protecting the information. Thus, you can write (7) as

$$Q_{CTP} = Q_{PAS}+(1-Q_{PAS}) * Q_{REF} \quad (8)$$

As regards the reflection of a cyberattack on the information we protect, it can occur in the conditions of its local, regional, global or national nature, with the probability that the corresponding hypotheses form a complete group

$$Q_{LOC} + Q_{REF} + Q_{NAT} + Q_{GLOB} = 1 \quad (9)$$

Then

$$Q_{REF} = Q_{LOC} * Q_{REF(LOC)} + Q_{REG} * Q_{REF(REG)} + Q_{NAT} * Q_{REF(NAT)} + Q_{GLOB} * Q_{REF(GLOB)} \quad (10)$$

where $Q_{REF(LOC)}$, $Q_{REF(REG)}$, $Q_{REF(NAT)}$, $Q_{REF(GLOB)}$- is the probability of a reflection of a cyberattack of a corresponding type.

Considering (8) and (10) the level (6) is a mathematical model that reflects the degree of development of cyber threats or cyberattacks and the ability to address them by preventing or countering cyberattacks.

The conducted researches make it possible to draw the following conclusions:

1. As the main quantitative indicator of the level of cyber security, the probability of successful protection of information, preservation of its integrity in the conditions of the projected cyber-threat information may be accepted. This indicator can be determined by the cybersecurity index of information, the quantitative meaning of which makes it possible to draw certain conclusions about the level of cyber security information.

2. The methodology for calculating the cybersecurity information index should be based on the results of the assessment of the cyber-threat of information, since the schemes of events related to the provision of cybersecurity information and the implementation of cyber-threats of information are similar and are characterized by the probabilities of the same events. In addition, the basic output data for calculating the cybersecurity index can be attributed to indicators that characterize the cyber-threat of information, and their quantitative values can be determined when evaluating the latter.

Thus, the assumption that the level of information cyber threats simultaneously characterizes the level of cyber security can be considered proven.

3. Based on the interdependence of cyber-threats and cybersecurity as the main quantitative indicator of cyber-threat information, the probability of causing significant damage to the integrity and value of information as a result of cyberattacks from the outside can be accepted. This indicator should be called the index of cyber-threat information, which, in comparison with the scale of cyber-threat information, allows, in the presence of a certain criterion, to determine the level of cyber-threat information.

4. The indexes of cyber threats of information and cyber security of information are the probabilities of opposite events, which are incompatible and form a complete group, that is,

$$Q_{NCD} = 1 - Q_{CD} \quad (11)$$

Expression (2) makes it possible to argue about the possibility of applying a unified methodological approach to the evaluation of cybersecurity information and cyber security indices.

5. The quantitative assessment of the cybersecurity information index, due to the inevitable errors and the inaccuracy of the initial data, may not be of a predominant importance. More important is another: mathematical modeling of the cyber security index has not only practical but also predictive value. Operating the values of the variables included in the mathematical dependencies for calculating

the index of cybersecurity, one can evaluate the effectiveness of the implementation of certain measures aimed at its dynamics. Therefore, the functional dependence between the cybersecurity index and the value of partial information about the information environment can be an instrument for in-depth study of the cyber security problem.

References:

1. Grishchuk R.V. Fundamentals of cybernetic security / R.V. Gryshchuk, Yu.G. Danik - Zhitomir: ZNAEU; 2016 - 636 pp.

2. Danik Yu.G. National security: prevention of critical situations / Y.G. Danik, Y.I. Katkov, M.F .Pichugin - K: Ministry of Defense of Ukraine; Zhytomyr: Ruta, 2006 – 388pp.

3. Khoroshko V.O. Methodological Approach to Assessing the Level of Information Security / V.O.Khoroshko, V.S. Cherunichenko // Coll. Sci. Works of the Kyiv Taras Shevchenko National University, Vip. 14, 2008. - P. 176-181

4. Saati T.L. Mathematical methods of conflict situations / T.L. Saati - M: Sov.radio, 1997. - 304 pp.

5. Ventsel V.C. Theory of probabilities / VS Ventzel - M: Gos. issuance physical math. Lit., 1962 - 560 pp.