The European Proceedings of
Social & Behavioural Sciences
EpSBS

ISSN: 2357-1330

https://doi.org/10.15405/epsbs.2019.12.04.27

SCTCMG 2019

International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism»

FEATURES OF TERRORISM THREAT TRANSFORMATION UNDER THE GLOBAL INFORMATION SECURITY CRISIS

Vladimir Kotenko (a), Konstantin Rumyantsev (b), Kamila Bamatgireeva (c)*
*Corresponding author

(a) Southern Federal University, 44D, Nekrasovsky Lane, Taganrog, Rostov Region, Russia
virtsecurity@mail.ru,
(b) Southern Federal University, 44D, Nekrasovsky Lane, Taganrog, Rostov Region, Russia
rke2004@mail.ru,
(c) Grozny State Oil Technical University, 100, H.A. Isaev Av., Grozny, Russia
puma-i@mail.ru

Abstract

The influence of information security on terrorism threat transformation is described. The solution is based on the theory of virtualization and the virtual analogization method. Identification of the influence of information security on terrorism threats; justification of information security crisis based on crisis symptoms; identification of features of terrorism threat transformation as a result of the global information security crisis were studied. The purpose of the study is to substantiate peculiarities of terrorism threat transformation under global information security crisis. Terrorism threat sources can influence behavioral forms of intellectual systems acting as targets through information environment. Hence, the basis for countering threats of terrorism is protection of the information environment. By changing the degree of protection of the information environment, one can transform threats of terrorism. Symptoms and diagnosis of the information security crisis were described. The symptoms are application of information security methods and systems incapable of providing absolute information protection; emergence of an uncontrollable community of hackers. The diagnosis is a failure to comply with conditions of theoretical undecipherability. A strategy for overcoming information security crisis is suggested. The hacker community generated by information security crisis is a developing structure with pronounced centripetal tendencies, own philosophical concept, etc. The global information security crisis transforms terrorism threats. The forecast of crisis consequences shows possible emergence of a supranational terrorist monster structure aimed at intellectual and spiritual enslavement of humanity. The first step towards this goal is intellectual and spiritual terrorism, merging with ordinary terrorism in its manifestations.

Keywords: Information security, terrorism threats, virtual analogization, information environment, cryptanalysis, information influence of terrorism threats.

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Today information security as an integral part of human safety is experiencing a deep crisis. Under the globalization of terrorism, the consequences of this crisis can be critical. Analysis and assessment of terrorism threat transformation is relevant.

2. Problem Statement

Against the background of the scientific and engineering information security achievements, the crisis requires justification. It is necessary to justify the relationship of information security and terrorist threats. The solution can be obtained on the basis of the theory of virtualization (Kotenko, 2011, 2007) by applying a virtual analogization method (Kotenko, 2011; Kotenko & Rumyantsev, 2014; Polikarpov, Kotenko, & Polikarpova, 2013; Polikarpov, Kotenko, & Polikarpova, 2015). The main condition of virtualization is that the concept of crisis determines a sharp change in something, for example, in a disease. One can talk about the crisis of a disease if its "symptoms" were identified and the disease was diagnosed. The task is to determine the influence of information security on terrorism treat transformation.

3. Research Questions

The following issues were studied:

- identification of the influence of information security on terrorism threats;
- justification of the information security crisis by identifying symptoms and diagnosing the crisis state;
- identification of features of terrorism threat transformation as a result of the global information security crisis.

4. Purpose of the Study

The aim of the study is to substantiate features of transformation of terrorism threats under the global information security crisis.

5. Research Methods

The Impact of Information Security on Counterterrorism

It was established that the basis of counterterrorism is information and communication technologies (Kotenko, 2011; Kotenko & Polyakov, 2018; Kotenko & Rumyantsev, 2009; Kotenko, Rumyantsev, & Kotenko, 2014; Polikarpov, Kotenko, & Polikarpova, 2015; Polikarpov, Kotenko, Polikarpova, & Rumyantsev, 2016). The main goal and source of terrorism threats is a person as an intellectual system (IP). The mathematical model of the intelligent systems can be reduced to the form:

$$Q + I_{П} + I_{ПП} \Rightarrow D + D_{М} + E + E_{П}\ , \quad (1)$$

$$E + E_{П} + D + D_{М} \Rightarrow Q + I_{П} + I_{ПП}\ , \quad (2)$$

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

where Q is the intellegince; $I_П$, $I_{ПП}$ - information of the field of knowledge of the conscious and subconscious levels, respectively; D - spiritual motivation; D_M - moral incentives and goal setting; E and $E_П$ - energy of knowledge of the conscious and subconscious levels, respectively.

The mathematical model (1) - (2) allows for synthesizing a risk model of the information impact of terrorist threats on intellectual systems presented in Figure 01.

Terrorism threat sources can influence on the behavioral IF forms through the information environment. The information environment includes: a) a conscious-level information environment represented by an information field of knowledge (IFC); b) the information environment of the subconscious level (IES). The IFC and IES are formed by intelligent systems (IS): a) directly; b) indirectly from sources of terrorism threats (STT). The IFC is formed from information $I_П$ (2) which results from the creative work of the IS at the conscious level, and from information $I_П$ from the STT at the conscious level. The material form $I_П$ can be constant and variable.

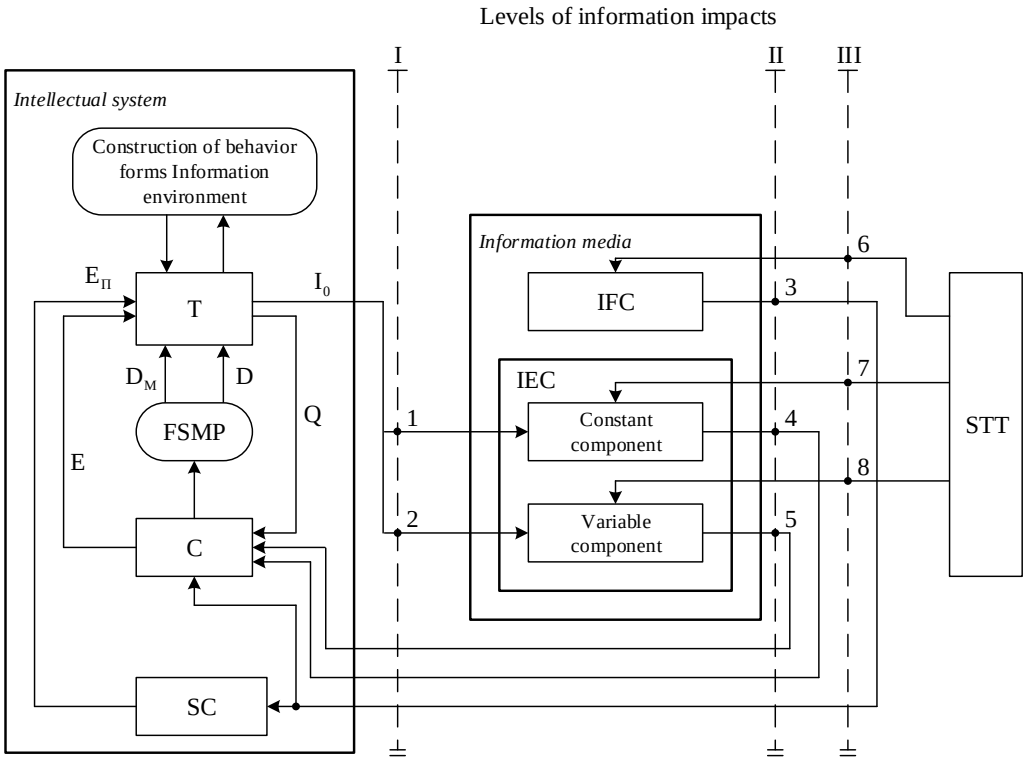

Figure 01. The model of risks of information impacts of terrorism threats on intellectual systems

Thus, the IES includes two constant and variable components. The IS cognition includes two components: a) conscious cognition (C); b) subconscious cognition (SC). C and SC determine formation of spiritual and moral purposes (FSMP) by influencing Dand D_M (1). Creativity at the information level determines construction of behavioral forms of the IS. The results of the construction of behavioral forms of the IS influence the creative process.

Thus, the sources of terrorism threats can influence behavioral forms of the IS through the information environment. Hence, the basis for counterterrorism is protection of the information

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

environment, that is, information security. A change in the degree of protection of the information environment will transform terrorism threats.

6. Findings

Symptoms and diagnosis of the information security crisis

When analyzing the history of development of information security systems and methods, two destructive phenomena can be revealed. First, methods and systems of information security were initially incapable of providing absolute protection of information. However, if at the dawn of development and application of these methods and systems, successful cryptanalysis was an exception, today, due to their mass character, it is a rule. This is no longer a symptom of the "disease" itself - it is a symptom of its crisis. Second, the emergence of information security systems caused the emergence of individuals involved in their cryptanalysis. At the initial stage, training and behavior of these persons were under strict control of public services. However, over time, these processes became uncontrollable. An uncontrollable community of hackers was created (Bhargava & Choudhaiy, 2001). Having identified "symptoms," one can diagnose the "disease".

Improvement of modern methods and information security systems is accompanied by an increase in their complexity.

Today we can only guess how the first algorithms of this class were created, since everything happened under strict secrecy. However, it can be argued that scientists and developers who participated in this process were familiar with the works by famous mathematicians who determined conditions for theoretical (absolute) undecipyability of cryptographic systems. In order to achieve absolute non-decipherment of the system, the keys should be formed according to a random law, and their number should tend to infinity. However, initially, these algorithms did not meet absolute undecipherability requirements. One can only assume why this approach has been chosen. The hope that determined the whole subsequent process of development of these algorithms both along the hardware and software paths. The number of recurrent sequences that formed a key sequence increased, hash conversions were introduced, associated algorithms of imitation protection, authentication, signature, etc. were created. A powerful mathematical apparatus explaining validity of practical steps was created (Shannon, 1963). Unfortunately, today we see that the crisis of “disease” has come. Its diagnosis is a failure to comply with the conditions of theoretical undecipherability.

The diagnosis and causes of the information security crisis were established. Unfortunately, the resulting diagnosis was not encouraging. Is it possible to treat this disease? Treatment should involve treatment of causes and possible consequences.

“Treatment of causes” involves the search for new approaches to solving information security problems, ensuring absolute non-decipherment conditions:

1) the keys must be formed by an absolutely random law;

2) the number of keys must be infinite.

The use of any known method for analyzing the effectiveness of information security leads to the same conclusion. It is not possible to ensure thsese conditions using the currently accepted approach. This approach assumes a discrete set of keys, that is, it practically eliminates the condition.

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In addition, it is impossible to form identical key sequences in transmission and reception. If we take into account unsolvable synchronization problems, skepticism becomes evident. Skepticism explains the dogging of the opinion that it is practically impossible to ensure the fulfillment of the conditions of theoretical non-decipherment.

The path determined by these frames is the same – increasing the complexity of the security algorithms. This is the only way to ensure maximum concealment of the pseudo-random nature of the key sequence. One more problem is important – protection algorithms themselves. It is quite clear that the more complex the algorithm, the more difficult it is to prevent an unauthorized access. Is there a limit of complexity? This question has not been studied yet.

It would seem that treatment of the disease "information security crisis" impossible. But the preliminary results of research conducted by the authors are positive.

If we return to the conditions of absolute non-decipability (Kotenko & Rumyantsev, 2009), it is easy to see that they can ensured under equality. The key must be an analog value. Thus, we can conclude that in order to fulfill the conditions of absolute undecipherability, it is necessary to move from the discrete sample space of the ensemble of keys to the continuous one. It is obvious that in the framework of the generally accepted approach to information security, this transition is impossible. This is due to the fact that the transition to a continuously-valued sample space denies the expediency of using the discrete key generation algorithms themselves, including those based on the formation of pseudo-random sequences of a maximum period. In addition, this transition creates a rather serious problem of reconciling continuously-valued key ensembles with the digital strategy for the development of information processing and transmission systems. These considerations determined the fact that until now the possibility of using analog key ensembles has no been considered as a research object. However, the way out can be found in this direction (Morelos-Zaragoza, 2006; Peterson & Weldon, 1976).

It turned out that setting the goal of studying the possibility of using analog key ensembles to protect information in digital systems, one can get encouraging results. This possibility opens up the use of the apparatus of the theory of virtual sample spaces. Due to the fact that this device is only under development and testing, it is still premature to talk about final success. However, the initial results of its use are encouraging. There is at least one way out of the crisis. Of course, there are other more efficient methods.

Features of terrorism threat transformation as a result of the global information security crisis

Initially, the hacker community consisted of amateur enthusiasts. Today, this community is a global structure with pronounced centripetal trends, own philosophical concepts, ideology and sources of funding. Over time, humanity may encounter a powerful and organized structure, more dangerous than traditional terrorism, since it will embody terrorism at intellectual and spiritual levels.

The information security crisis can be compared with the situation when doctors use conservative treatment instead of surgical intervention. In case of a developing disease, more and more potent drugs are required. The disease will gradually violate natural functions of the body and causes death. Is the situation similar to information security today? It becomes clear why the use of more and more complex and efficient information security algorithms leads to opposite results.

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

The situation when the doctor does not choose surgical intervention may be due to two reasons. He believes that this intervention will damage the patient. Unfair doctors do it because it is beneficial for them. Business laws distorting medical ethics are dominant.

Cryptography as art and science has developed in strict accordance with the basic law of philosophy - unity and struggle of opposites, when efforts directed in opposite directions (cryptographic protection and cryptanalysis) contributed to the development of information security. This law operated in the 1950s when information security systems were created. The stimulating factors for the development of cryptographic protection and cryptanalysis were ideological, patriotic, national and state interests (McEliece, 1978; Niederreiter, 1986).

However, financial interests became decisive when information security development processes became uncontrollable. This brings into effect new philosophical laws based on pure business philosophy. The developers of information security algorithms are no longer interested in absolute undecipability of these algorithms. Development of efficient algorithms that are in demand becomes optimal for them. Then it becomes possible to develop a new, more complex algorithm and sell it to the same buyer. In addition, the developers are interested in a certain opposing force (e.g., hackers) whose threat will keep the buyer in constant tension. Psychologically, this tension will prepare for higher prices, higher profits for the developers. On the other hand, this position is beneficial for the hacker community. Effective information security algorithms create an incentive to work. The hacker community is interested in advertising the effectiveness of existing algorithms, and the developer community is interested in advertising the effectiveness of hackers. There is a unity of economic and financial interests. The most unfavorable forecast is the emergence of a self-contained, closed supranational centralized structure with its own ideology, philosophy, culture, financial flows, division of labor and authorities aimed at the intellectual and spiritual enslavement of humanity. This forecast is terrifying. However, there are some prerequisites: monopolization of information security developments at the level of transnational monopolies (Polikarpov et al., 2016); centripetal processes in the hacker community; convergence of these structures; involvement of hackers into transnational corporations. These prerequisites are provided with huge financial resources. As a consequence, recent political events are perceived in a different way.

7. Conclusion

The following conclusions can be drawn:

1. The information security crisis is a real global fact.
2. The consequences of this crisis can be tragic for humanity.
3. It is necessary to change the existing approach to information security.
4. Successful search for new approaches is possible.
5. It is necessary to discuss issues of information security crises in the context of terrorism threats.

The global information security crisis transforms terrorism threats. The forecast of crisis consequences shows possible emergence of a certain supranational terrorist monster structure aimed at the intellectual and spiritual enslavement of humanity. The first step towards this goal is intellectual and spiritual terrorism, merging with ordinary terrorism in all its manifestations.

https://doi.org/10.15405/epsbs.2019.12.04.27
Corresponding Author: Kamila Bamatgireeva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

References

Bhargava, H., & Choudhaiy, V. (2001). Information goods and vertical differentiation. *Journal of Management Information Systems, 18*, 89–106.

Kotenko, V. V. (2007). The strategy of applying the theory of information flow virtualization in solving information security problems. *News SFU. Technical science, 76*(1), 26–37.

Kotenko, V. V. (2011). *The theory of virtualization and telecommunication protection.* Taganrog: SFU.

Kotenko, V. V., & Polyakov, A. I. (2018). Virtual immediate coding. *International Journal of Engineering and Technology (UAE), 7*(13), 14–16.

Kotenko, V. V., & Rumyantsev, K. E. (2009). *Information theory and telecommunication protection.* Rostov-on-Don: Southern Federal University.

Kotenko, V. V., & Rumyantsev, K. E. (2014). *Theoretical foundations of information countering the threats of terrorism.* Rostov-on-Don: Southern Federal University.

Kotenko, V. V., Rumyantsev, K. E., & Kotenko, S. V. (2014). *Methodology of identification analysis of information and communication systems.* Rostov-on-Don: Southern Federal University.

McEliece, R. J. (1978). A Public-Key Criptosystem Based on Algebraic Theory. In *DGN Progress Report 42–44* (pp. 114–116). Pasadena: Jet Propulsi on Lab.

Morelos-Zaragoza, R. (2006). *The art of noise-immune coding. Methods, algorithms, application*. Moscow: Technosphere.

Niederreiter, H. (1986). *Knapsack-Type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory, 15,* 19–34.

Peterson, W., & Weldon, E. (1976). *Codes correcting mistakes.* Moscow: Mir.

Polikarpov, V. S., Kotenko, V. V., & Polikarpova, E. V. (2013). *Information sovereignty of Russia and information and intellectual wars.* Rostov-on-Don: Southern Federal University.

Polikarpov, V. S., Kotenko, V. V., & Polikarpova, E. V. (2015). *The strategic importance of NBICS technologies in the formation of ethical values.* Rostov-on-Don: Southern Federal University.

Polikarpov, V. S., Kotenko, V. V., Polikarpova, E. V., & Rumyantsev, K. E. (2016). *Information countering threats of terrorism in a global world.* Taganrog: Southern Federal University.

Shannon, K. (1963). *Works on the theory of information and cybernetics.* Moscow: Foreign literature.