ISSN 2664-9969

UDC 355/359
DOI: 10.15587/2706-5448.2023.276544

Andrii Shyshatskyi,
Taras Hurskyi,
Yevhenii Vdovytskyi,
Roman Vozniak,
Oleksii Nalapko,
Halyna Andriishena,
Lyubov Shabanova-Kushnarenko,
Nadiia Protas,
Yuliia Vakulenko,
Serhii Pyvovarchuk

DEVELOPMENT OF METHOD FOR THE IDENTIFICATION OF HYBRID CHALLENGES AND THREATS IN THE NATIONAL SECURITY MANAGEMENT SYSTEM

As a result of Russian aggression against Ukraine, some fundamental theses regarding the nature of hybrid military operations will require clarification and even revision. First of all, this refers to the widespread perception of the asymmetric nature of hybrid threats as those used by a weaker opponent against a party with significantly greater military, technological and human potential. This, in turn, requires the use of modern and proven mathematical apparatus, which is capable of processing a large array of various types of data in a short period of time with a given reliability of making management decisions. The object of research is the system of strategic management of national security. The subject of the research is the method of detection and identification of hybrid challenges and threats in the national security management system. In the research, the method of detection and identification of hybrid challenges and threats in the national security management system was developed. The novelty of the research:

– a destructive effect on the system of national security management by adding an appropriate correction factor;

– the use of an improved procedure of deep learning of the database of the system of detection and identification of hybrid challenges and threats to the national security of the state;

– a mechanism for resolving conflicting cases of classification is used due to additional training, adaptation of detectors to the type and intensity of the hybrid challenge and threat to the national security of the state;

– the procedure for automatically calculating the detector activation threshold and the universality of the structure of their representation due to the hierarchy and flexibility for the available hardware resources of the detection and identification system.

It is advisable to implement the specified method in algorithmic and software while studying the state of the national security system.

Keywords: *hybrid warfare, national security system, research methods, intellectual management methods.*

Received date: 28.02.2023
Accepted date: 29.03.2023
Published date: 05.04.2023

How to cite
Shyshatskyi, A., Hurskyi, T., Vdovytskyi, Y., Vozniak, R., Nalapko, O., Andriishena, H., Shabanova-Kushnarenko, L., Protas, N., Vakulenko, Y., Pyvovarchuk, S. (2023). Development of method for the identification of hybrid challenges and threats in the national security management system. Technology Audit and Production Reserves, 2 (2 (70)), 26–29. doi: https://doi.org/10.15587/2706-5448.2023.276544

1. Introduction

Hybrid war is a consequence of changes in the forms and methods of armed aggression due to changes in the principles of the geopolitical system, the development of scientific opinion on the conduct of armed struggle [1–5]. The researches [1–5] describe changes in approaches to information exchange, approaches to complex information processing, directions for creating information infrastructure, new forms and methods of influencing information systems in conditions of hybrid influence of the enemy.

Changes in the forms and methods of armed struggle are quite clearly illustrated with the use of hybrid actions in Ukraine, which were divided into the following stages:

– the hidden start of the war beginning (stage 1), during which the opposition to the current government was formed, an informational and psychological operation was conducted, as a result of which the values of the servicemen of the Armed Forces of Ukraine were revised, who, as a result, betrayed their oath and the rest of the servicemen were demoralized;

– escalation (stage 2) of political and military leaders in the regions are informed about the developing conflict.

The russian federation exerted and is exerting political, diplomatic or economic pressure on the regime or non-political entities;

– the beginning of the conflict, namely the third stage began with more hostile actions of the opposing forces – demonstrations, protests, sabotage, murders, intervention of paramilitary groups, etc. At this stage, the russian federation began the strategic launch of its forces into conflict regions in the event of a strategic or national security interest;

– the start of military operations (stage 4), accompanied by strong diplomatic and economic support, along with a constant stream of information aimed at swaying public opinion towards Russian intervention.

In such conditions, a change in the strategic management of the national security system is needed. This, in turn, requires the use of a modern and proven mathematical apparatus capable of processing a large array of various types of data in a short period of time with a given reliability of making management decisions [6–10].

The existing approaches to the identification of hybrid challenges and threats to the national security of the state are narrowly focused and directed to the research of only certain issues and do not allow [6–10]:

– comprehensively and in a short time to identify and assess hybrid challenges and threats to national security;

– to process various types of data with different units of measurement, different in origin and sources of information extraction;

– to identify new and unusual hybrid challenges, threats to national security and assess the degree of their destructive impact.

All this requires a review of approaches to identifying challenges and threats to the state's national security with the use of hybrid actions.

Taking into account the above, *the aim of research* is to develop a method for identifying hybrid challenges and threats to the state's national security.

The object of research is a system of strategic management of national security.

The subject of research is a method of detection and identification of hybrid challenges and threats in the national security management system.

2. Materials and Methods

In the course of the research, let's use:

– classic methods of analysis – to solve the problem of analyzing the conditions and factors affecting the effectiveness of functioning the system of strategic management of national security;

– the theory of artificial intelligence – for processing various types of data during the identification and assessment of challenges and threats to national security, detection and identification of challenges and threats to the national security of the state in conditions of hybrid destructive influence.

3. Results and Discussion

3.1. Development of methods for detection and identification of hybrid challenges and threats in the national security management system. Artificial intelligence methods are actively used in many areas of human activity. The state's national security management systems were no exception to this. At the same time, taking into account the large number of challenges and threats to the national security of the state, the constant and rapid development of information technologies, problematic issues arise related to the identification of the destructive impact on the national security system of the state, which are hybrid challenges and threats [7–10].

The use of artificial intelligence systems in the interests of ensuring the national security of the state will allow to increase the efficiency and reliability of the decisions made by the persons who make them. Detecting and identifying the destructive impact of hybrid challenges and threats to the state's national security is quite difficult. In the mentioned research, the intentional destructive influence on the national security system will be understood as:

– informative messages aimed at discrediting the state leadership;

– cyber attacks aimed at denial of service;

– measures of indirect destructive influence on the national security system;

– cyber intelligence, aimed at gathering information about the leadership of the state and the security and defense sector.

The use of ready-made artificial intelligence methods to detect and identify the destructive impact on the national security management system is not effective. This does not allow to identify new challenges and threats to the state's national security, to carry out their identification and, as a result, to promptly make decisions by the persons who make them.

To identify challenges and threats to the national security of the hybrid influence, it is proposed to develop a method for identifying challenges and threats to the national security of the state based on the artificial immune system.

Step 1. Entering initial data about the national security system.

Step 2. Initialization of the mathematical model for detection and identification of hybrid challenges and threats to national security, which is described as:

$$AISEA = \langle D_\tau, D_M, S_A, S_N, G, R, \Psi \rangle, \quad (1)$$

where $D_\tau \subset D$ is a set of detectors for identifying hybrid challenges and threats to national security; D_M is a set of memory detectors in which hybrid challenges and threats to national security are recorded; $S_A \subset S$ is an educational sample consisting of a set of known challenges and threats to the national security of the state; $S_N \subset S$ is a test set consisting of a set of normal parameters of the functioning of the state's national security system; $D = D_\tau \bigcup D_M$ is a set of detectors used to detect and identify challenges and threats of a hybrid nature to the national security of the state; $G = \{G_1,...,G_K\}$ are the strategies for optimizing detectors for detection and identification of threats to national security; $R: D \times 2^{S_A} \times 2^{S_N} \times G \to D$ are the rules for training detectors for detection and identification of challenges and threats to the state's national security; S is a set of possible input events, $\Psi: D \times S \to R_+$ is a function of calculating the correspondence rule between detectors $d \in D$ and test indicator $s \in S$, where $R_+ = R \bigcap [0, +\infty)$.

Each detector for detection and identification of hybrid challenges and threats to the national security of the state from the set $d \in D$ is described as a tuple of the following form:

ISSN 2664-9969

$$d = \langle representation, threshold, life\_time, state \rangle, \quad (2)$$

where

$$representation \in$$
$$\in \{BitString, RealVector, NeuralNetwork, PetrNet..., \}$$

is the internal structure of detector d for detection and identification of hybrid challenges and threats to the national security of the state; $threshold \in R_+$ is the detector activation threshold d for detection and identification of hybrid challenges and threats to the state's national security; $life\_time \in R_+$ is the validity period of detector d for detection and identification of hybrid challenges and threats to the state's national security; $state \in \{immature, semimature, mature, memory\}$ is the current state of the detector.

Step 3. Determination of the correction coefficient for the degree of awareness of the forces and devices of destructive influence on the state's national security system. The degree of awareness can be: complete uncertainty, partial uncertainty, full awareness.

Step 4. Selection of the internal structure of each detector $d \in D$: *representation.* Calculation for each detector $d \in D$, its activation value $a_d = \Psi(d,s) - threshold$, thus, the transition from an inactive state to an active one. It is believed that if $a_d \geq 0$, then detector d is activated, otherwise the corresponding detector does not respond to input data.

Step 5. Formation of the training data set S_A, containing pre-selected hydride challenges and threats to the national security of the state.

Step 6. Formation of a test data set S_N, which contains pre-selected hydride challenges and threats to the national security of the state, which have been identified and are in the detector's memory.

Step 7. Choosing a strategy for genetic optimization of immune detectors.

Step 8. Training R immune detectors D.

Step 9. Selection of the matching rule Ψ *between the immune detector and the input object.*

The end of the algorithm.

3.2. Research results and discussion. The method of detection and identification of hybrid challenges and threats in the national security management system was developed.

The specified method is proposed for use during the settlement of military conflicts, assessment of hybrid challenges and threats to the national security of the state. This will increase the efficiency of data processing and transmission and the reliability of decisions by those who make them.

However, the developed method additionally:

– takes into account the type of uncertainty of information about the available possibilities of destructive influence on the system national security management by adding an appropriate correction factor;

– uses an improved procedure of deep learning of the database of the system of detection and identification of hybrid challenges and threats to the national security of the state;

– uses a mechanism for resolving conflicting cases of classification due to additional training, adaptation of detectors to the type and intensity of the hybrid challenge and threat to the national security of the state;

– uses the procedure for automatically calculating the threshold of activation of detectors and the universality of the structure of their representation due to the hierarchy and flexibility for the available hardware resources of the detection and identification system.

The limitations of the mentioned research are:

– time limits for the transmission of informational messages in the system of detection and identification of challenges and threats to the national security of the state;

– the need for a primary base of destructive influences on the national security system.

It is expedient to implement the specified method in algorithmic and program software while detecting and identifying challenges and threats to the national security of the state in conditions of hybrid destructive influence.

The directions of further research will be aimed at the development of the methodology of intelligent management of the national security system.

4. Conclusions

In the research, the method of detection and identification of hybrid challenges and threats in the national security management system was developed.

The results of the research will be useful for:

– the development of new algorithms for managing the national security system at the stage detection and identification of challenges and threats to the state's national security in conditions of hybrid destructive influence;

– a substantiation of recommendations on increasing the effectiveness of operational management of the national security system at the stage detection and identification of challenges and threats to the state's national security in conditions of hybrid destructive influence;

– creating promising technologies for increasing the efficiency of operational management of the national security system at the stage detection and identification of challenges and threats to the state's national security in conditions of hybrid destructive influence;

– the development of new and improvement of existing models, methods of managing the national security system.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The research was performed without financial support.

Data availability

The manuscript has no associated data.

References

1. Shyshatskyi, A. V., Bashkirov, O. M., Kostina, O. M. (2015). Rozvitok integrovanikh sistem zv'iazku ta peredachi danikh dlia potreb Zbroinikh Sil. *Ozbroennia ta viiskova tekhnika, 1 (5)*, 35–40.
2. Timchuk, S. (2017). Methods of Complex Data Processing from Technical Means of Monitoring. *Path of Science, 3 (3)*, 4.1–4.9. doi: http://doi.org/10.22178/pos.20-4
3. Sokolov, K. O., Hudyma, O. P., Tkachenko, V. A., Shyiatyi, O. B. (2015). Main directions of creation of IT infrastructure of the Ministry of Defense of Ukraine. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen, 3 (6)*, 26–30.

4. Shevchenko, D. G. (2020). The set of indicators of the cyber security system in information and telecommunication networks of the armed forces of Ukraine. *Suchasni informatciini tekhnologii u sferi bezpeki ta oboroni, 38 (2),* 57–62. doi: https://doi.org/10.33099/2311-7249/2020-38-2-57-62
5. Makarenko, S. I. (2017). Perspektivy i problemnye voprosy razvitiia setei sviazi spetcialnogo naznacheniia. *Sistemy upravleniia, sviazi i bezopasnosti, 2,* 18–68. Available at: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf
6. Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O. (2020). Development of complex methodology of processing heterogeneous data in intelligent decision support systems. *Eastern-European Journal of Enterprise Technologies, 4 (9 (106)),* 14–23. doi: http://doi.org/10.15587/1729-4061.2020.208554
7. Brownlee, J. (2011). *Clever algorithms: nature-inspired programming recipes.* LuLu, 441.
8. Gorokhovatsky, V., Stiahlyk, N., Tsarevska, V. (2021). Combination method of accelerated metric data search in image classification problems. *Advanced Information Systems, 5 (3),* 5–12. doi: http://doi.org/10.20998/2522-9052.2021.3.01
9. Meleshko, Y., Drieiev, O., Drieieva, H. (2020). Method of identification bot profiles based on neural networks in recommendation systems. *Advanced Information Systems, 4 (2),* 24–28. doi: https://doi.org/10.20998/2522-9052.2020.2.05
10. Rybak, V. A., Shokr, A. (2016). Analysis and comparison of existing decision support technology. *System analysis and applied information science, 3,* 12–18.

✉***Andrii Shyshatskyi,*** *PhD, Senior Researcher, Educational and Scientific Institute of Public Administration and Civil Service of Taras Shevchenko Kyiv National University, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-6731-6390, e-mail: ierikon13@gmail.com*

Taras Hurskyi, *PhD, Associate Professor, Head of Research Department, Research Institute of Military Intelligence, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-7646-853X*

Yevhenii Vdovytskyi, *Adjunct, The Scientific and Methodological Center of the Organization of Scientific and Scientific and Technical Activities, The National University of Defense of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-0930-525X*

Halyna Andriishena, *Educational and Scientific Institute of Public Administration and Civil Service of Taras Shevchenko Kyiv National University, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-8863-7027*

Roman Vozniak, *PhD, Deputy Head of Department of Information Technology Application and Information Security, Institute for Providing Troops (Forces) and Information Technologies, The National University of Defense of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-3789-2837*

Oleksii Nalapko, *PhD, Senior Research Fellow, Scientific-Research Laboratory of Automation of Scientific Researches, Central Scientifically-Research Institute of Armaments and Military Equipments of the Armed Forces of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-3515-2026*

Nadiia Protas, *PhD, Associate Professor, Department of Information Systems and Technologies, Poltava State Agrarian University, Poltava, Ukraine, ORCID: https://orcid.org/0000-0003-0943-0587*

Yuliia Vakulenko, *PhD, Associate Professor, Department of Information Systems and Technologies, Poltava State Agrarian University, Poltava, Ukraine, ORCID: https://orcid.org/0000-0002-6315-0116*

Lyubov Shabanova-Kushnarenko, *PhD, Associate Professor, Department of Intelligent Computer Systems, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0002-2080-7173*

Serhii Pyvovarchuk, *Head of Department of Combat Use of Communication Units, Military Institute of Telecommunication and Information Technologies named after the Heroes of Kruty, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-9410-5951*

✉*Corresponding author*