OPINION

by Professor Sevdalina Ilieva Dimitrova, D.Sc., Tel. +359 887 395 307; sevdalinaid_bg@mail.bg Registration No. 45970 in the Scientific Activity Register – https://cris.nacid.bg/public/scientist-preview/14061; Registration No. 14061 in the Academic Staff Register – https://ras.nacid.bg/dissertation-preview/14061; Higher Education Field 9: Security and Defense Professional Field 9.1: National Security Scientific Specialty 05-02-24: Organization and Management Outside the Sphere of Material Production (Defense and National Security)"

of a dissertation work developed by associate professor Dr. Dmytro Igorovich Prokopovich - Tkachenko

on the topic: "Organizational and managerial mechanisms for state information and cybersecurity amidst hybrid threats"

submitted for the acquisition of the scientific degree "Doctor of Sciences" in Higher Education Field 9: "Security and Defense" Professional Field 9.1: "National Security"

The scientific jury was appointed by Order No. 004/03.09.2026 of the Rector of the Academy of National and Information Security, Plovdiv

2026

1. Relevance of the problem addressed in the dissertation from a scientific and applied-scientific perspective

The modern digitized world is accompanied by numerous cyber threats of varying natures that affect the security of every national circumstance that constitutes a serious challenge in itself. Hybrid threats stand out as particularly significant, posing serious challenges to the national security system. Within this broad spectrum, information security and cybersecurity are gaining increasing importance as key policies for the national security system, while also opening up a wide field for scientific research. Consequently, there is a greater-than-ever need to establish a scientifically and practically grounded framework for the organizational and managerial mechanisms governing information security and cybersecurity in the face of hybrid threats that would help enhance the effectiveness of state policy in this area. This underscores the relevance of the dissertation authored and presented by Assoc. Prof. Dr. Dmytro Tkachenko, as well as the scientific novelty achieved therein, thereby filling a significant gap in scientific knowledge within the fields of security and defense.

The author's research was prompted by the digital transformation of all levels of public administration—interconnected via information and communication systems—where the use of such systems entails various risks of cyberattacks. This naturally necessitates a search for solutions to the research problem substantiated and outlined in the dissertation.

The dissertation demonstrates full alignment between its topic and its core content, as well as a well-founded research thesis and hypothesis regarding the defined aim, object, and subject of the study. The research aim is substantiated through specific tasks focused on the theoretical and methodological foundations of organizational and managerial mechanisms for information and cybersecurity amidst hybrid threats, the creation of a conceptual model for "Integrated State Cyber-Resilience" (ISCR), and a methodology for its assessment and practical implementation. Accordingly, the object of Assoc. Prof. Dr. Tkachenko's research is the state's information and cybersecurity system in the context of hybrid threats. The subject of the research is the status and development of information and cybersecurity policies within the broader security system, specifically through the establishment of ISCR as a means to enhance the effectiveness of the unified national cybersecurity policy.

The dissertation is characterized by the clarity and logical structure of the research, an analytical and conceptual style of presentation, and the application of a wide range of general scientific, specialized, expert-analytical, sociological, and applied methods—along with the tools of structural-functional and institutional analysis—to delineate the hierarchy of the Integrated System for

Internal Financial Control (IDKU). Scientifically grounded, practical solutions regarding the conceptual framework of the IDKU are proposed.

2. Extent of knowledge regarding the state of the problem

To achieve the research objective, address the research tasks, and substantiate the scientific and applied results and contributions of the dissertation, Assoc. Prof. Dr. Tkachenko examines and appropriately utilizes a substantial information and empirical base. This comprises legal acts of the Republic of Bulgaria; documents from the European Union and NATO; international standards (ISO/IEC and NIST); analytical reports from ENISA, Microsoft, Mandiant, the EEAS, CISA, Hybrid Coe, and NATO CCDCOE; comparative case studies involving Estonia, Poland, Romania, Ukraine, and other nations; results from expert assessments, sociological surveys, and analytical calculations; as well as the author's own publications, monographs, patents, intellectual property documents, and R&D activities—totaling 321 bibliographic entries. The validity of the conclusions, results, and personal contributions presented in the dissertation is demonstrated through a successful synthesis of theoretical, empirical, and practical-analytical approaches to the subject matter, supported by the necessary evidentiary and illustrative materials—specifically, 43 tables and 46 figures.

3. Compliance of the chosen methodology with the research objective.

The dissertation is structured in accordance with the formulated research objective, the chosen methodology, and the research tools, following a chronological and thematic order. The work is presented in two parts. The first part comprises the introduction and the first three chapters, spanning 354 pages, while the second part contains the fourth and fifth chapters, the conclusion, and the bibliography, totaling 283 pages. The total length of the dissertation is 637 pages.

The methodology employed to achieve the dissertation's objective and address its research tasks encompasses general theoretical and empirical methods of scientific inquiry: the systems approach, the comparative legal method, structural-functional and institutional analysis, risk-based analysis, SWOT analysis, GAP analysis, PESTEL analysis, the Analytic Hierarchy Process, and scenario analysis. The array of analytical tools and instruments used for empirical and sociological research is impressive. A mixed-methods design was applied, combining standardized surveys with semi-structured in-depth interviews involving 245 specialists.

The author's reasoning proceeds from the general to the specific, with each chapter building upon the preceding one. The various components of the dissertation are developed in a logical sequence, demonstrating the necessary

analytical depth and research, and employing the author's own methodology for evaluating and validating the IDKU conceptual model. The proposed IDKU model supports the substantiation of the dissertation's objective and the author's thesis.

As a scholarly work, the submitted dissertation meets the statutory requirements for the award of the academic degree of Doctor of Sciences".

4. Brief analytical overview of the nature and assessment of the reliability of the material upon which the contributions of the dissertation are based.

Associate Professor Dr. Tkachenko's dissertation is based on reliable legal, documentary, and sociological information, which has been utilized in a correct, analytical, and critical manner for the purposes of the research.

5. Scientific and applied scientific contributions

A profound understanding and creative adaptation of contemporary scientific theories, legal and regulatory acts, and publications relevant to the subject matter underpin the scientific and applied contributions resulting from the author's research.

The empirical and sociological studies and analyses in the dissertation make it possible to systematize the scientific and applied-scientific contributions resulting from the author's research. I accept the author's claims in this regard and concur with the contributions he has proposed.

5.1. Scientific Contributions:

5.1.1. Theoretical insights regarding the digital transformation of national security have been further developed, framing the information and cyber dimensions as all-encompassing components of state resilience.

5.1.2. The conceptual and categorical framework, the assessment of actual managerial maturity, and the system of technical, organizational, personnel, legal, communication, and international indicators have been refined.

5.1.3. New knowledge has been generated regarding scientifically grounded, integrated state cyber-resilience—conceptualized as a seven-layer organizational and management architecture—and a toolkit for developing a unified national cybersecurity policy.

5.1.4. The cyber-resilience of critical communication and information systems and networks is scientifically substantiated as a distinct management category of national security.

5.1.5. A multi-component methodology for the assessment and validation of IDKUs has been developed based on the applicable analytical toolkit.

5.2. Scientific and applied contributions

5.2.1. The scientific and expert platform for the research conducted on cyber-resilient public governance has been validated.

5.2.2. An operational matrix for hybrid threats and an interagency coordination mechanism based on situational awareness, crisis protocols, and cooperation have been developed.

5.2.3. The Cyber Intelligence and Innovation Center (CIIC) has been established on a scientifically sound basis to serve as an institutional coordination and analysis hub, and a national MISP-based mechanism for the exchange of indicators of compromise has been proposed.

5.2.4. An original conceptual model titled "Integrated State Cyber-Resilience" (ISCR) has been developed; it ensures the systemic integration of strategic, institutional, operational-coordination, technological, human, legal, and international levels of governance, serving as a practical tool for the development and enhancement of state cybersecurity policy.

5.2.5. A practical roadmap for 2026–2030 has been developed, comprising regulatory, institutional, operational-technical, educational and staffing, and international measures.

The scientific and applied research contributions of the dissertation are based on a profound understanding and creative adaptation of contemporary scientific theories, as well as on analytical calculations performed using a real-world dataset.

6. Evaluation of the scientific results and contributions of the dissertation

The submitted dissertation, the developed and verified theory for the effective management of state cyber-resilience, the methodology for assessing and validating the State Cyber-Resilience Management System (SCRMS), the developed hybrid threat matrix, the rationale for the Cyber-Resilience and Information Center (CRIC) and a national MISP-based information-sharing mechanism, and the roadmap for implementing the SCRMS during the 2026–2030 period are the personal work of Associate Professor Dr. Dmytro Tkachenko. Most of the ideas, approaches, and solutions discussed represent original developments presented to a broad audience for the first time, or constitute novel interpretations of existing concepts, taking into account the impact of changing conditions and factors affecting information and cybersecurity.

This is grounded in the author's indisputable scholarly and literary expertise - meriting praise for the effort to compile, analyze, and interpret a diverse and often conflicting array of sources, including literature, regulations, reference materials, sociological studies, websites, and existing scholarly opinions and research on the subject.

7. Evaluation of publications related to the dissertation and authorship

The results of the author's research presented in this work have been disseminated through numerous publications both in Bulgaria and abroad; this attests to the long-standing, consistent, in-depth, and cumulative research activity of Associate Professor Dr. Tkachenko in the field of information and cyber security amidst hybrid threats. Supporting this assertion are 73 publications in peer-reviewed national and international scientific journals and editions - including monographs (8), chapters in collective monographs, and research articles directly relevant to the dissertation topic (4 of which are indexed in Scopus) - as well as 13 patents. The significance of these publications is confirmed by 126 recorded citations and an h-index of 7. The volume of publications is sufficient and representative for the academic degree of "Doctor of Sciences" and meets the minimum requirements for obtaining this degree as stipulated by the Act on the Development of the Academic Staff in the Republic of Bulgaria (ADASRB) and its implementing regulations. The presented publications account for 1,900.99 points across the various indicators of the minimum national requirements, well exceeding the 350 points required for the "Doctor of Sciences" degree.

No instances of plagiarism were identified during the review of the dissertation. Nor have any reports of plagiarism been received.

8. Utilization of the results of the dissertation

The significance of the scientific and applied scientific contributions to the theory and practice of state information and cybersecurity amidst hybrid threats is indisputable.

9. Motivated recommendations for future use of scientific and applied scientific contributions

It is recommended that the proposed dissertation, along with the scientific and applied scientific contributions substantiated therein, be utilized in the educational process and in the practice of state information and cybersecurity.

The results of the research presented in the dissertation can serve as a methodological basis for the development of a number of research studies.

10. Evaluation of the abstract

The abstract outlines the key issues and the approaches to resolving them as presented in the dissertation. It provides a comprehensive overview of the scientific value and practical applicability of the achieved scientific and applied results and contributions, thereby substantiating the research focus on information and cybersecurity as a subsystem of the national security system.

11. Critical Notes

I have no critical comments regarding the dissertation of Associate Professor Dr. Tkachenko.

12. Conclusion

The dissertation titled "Organizational and Management Mechanisms for State Information and Cybersecurity Amidst Hybrid Threats," authored by Assoc. Prof. Dr. Dmytro Tkachenko, is a comprehensive and well-structured scholarly work addressing a highly relevant issue - namely, the need to safeguard the information and cybersecurity of state governance at all levels in the face of intensifying hybrid threats. The study presents significant theoretical and practical scientific results and contributions. These findings are the author's own work and demonstrate his ability to independently address critical issues in security theory and practice regarding information and cybersecurity, as well as the enhancement of state governance effectiveness within a digitized and dynamic security environment.

This provides grounds for a **positive assessment**, and I believe the dissertation will be highly regarded by the unbiased reader and can serve as a basis for future research.

The dissertation complies with the Law on the Development of the Academic Staff in the Republic of Bulgaria (LDASRB), the Regulations for its implementation, and the regulatory framework of ANIS–Plovdiv. I confidently recommend to the esteemed members of the scientific jury that the academic degree of "Doctor of Sciences" be awarded to Associate Professor Dr. Dmytro Prokopovych-Tkachenko for the dissertation titled "Organizational and Management Mechanisms for State Information and Cybersecurity Amidst Hybrid Threats," submitted for the acquisition of the "Doctor of Sciences" degree in the field of higher education 9 "Security and Defense," professional field 9.1 "National Security"

02.10.2026
Veliko Tarnovo

Member of the scientific jury:
Prof. DSc Sevdalina Dimitrova