

Preface: Conflict management in global information networks

Sergiy Gnatyuk^{1,†}, Maksim Iavich^{2,†}, Roman Odarchenko^{1,†}, Marek Aleksander^{3,†} and Maksym Zaliskyi^{1,*,†}

¹National University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

²Caucasus University, Paata Saakadze Str., 1, Tbilisi, 0102, Georgia

³Nowy Sacz School of Business - National Louis University, Grunwaldzka Str., 17, Nowy Sacz, 33-300, Poland

Abstract

This document is the preface of the Fifth International Workshop on Conflict Management in Global Information Networks (CMiGIN'26), June 26–27, 2026, held at the University of the National Education Commission, Krakow, Poland.

Keywords

computer science, data processing, conflict management, information networks, artificial intelligence, software, algorithms, risk analysis

1. Introduction

The Fifth International Workshop on Conflict Management in Global Information Networks (CMiGIN'26) took place on June 26–27, 2026, at the University of the National Education Commission (Krakow, Poland). This Workshop was part of Fifth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks 2026.

The CMiGIN'26 brought together scientists, researchers, experts, and practitioners working in the field of security of modern information systems and networks. The main focus of the event was on current issues of ensuring cybersecurity and confidentiality of critical applications, information and communication technologies, digital infrastructure and network systems. An important place in the workshop program was given to the issues of identifying, analyzing, and effectively managing cyber incidents, as well as developing modern approaches to countering cyber threats and minimizing their consequences. A separate direction of CMiGIN'26 is research related to information confrontation, cyber conflicts, and modern forms of cyber warfare, including methods of predicting, preventing, and resolving conflict situations in global information networks. Considerable attention was also paid to the use of intelligent data processing technologies.

The workshop became a platform for presenting new theoretical results, practical methods, models, algorithms, and technological solutions aimed at increasing the resilience and reliability of information infrastructure.

The conference would not have been possible without the support of many people. First of all, we would like to thank the program and organization staff, the members of the Technical Program Committees, and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the workshop and wish them every success in their research. It is the humble wish of the workshop organizers that the professional dialogue among the researchers,

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ s.gnatyuk@kai.edu.ua (S. Gnatyuk); miavich@cu.edu.ge (M. Iavich); roman.odarchenko@npp.kai.edu.ua (R. Odarchenko); aleksandermarek4@gmail.com (M. Aleksander); maksym.zaliskyi@npp.kai.edu.ua (M. Zaliskyi)

ORCID 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-3109-7971 (M. Iavich); 0000-0002-7130-1375 (R. Odarchenko); 0000-0003-2619-1063 (M. Aleksander); 0000-0002-1535-4384 (M. Zaliskyi)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

scientists, engineers, and doctors continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

The main topics of these Workshop included:

- Management of Cyber Incidents, Warfare and Conflicts.
- Modern Information and Communication Technologies.
- Secure Digital Content Processing for Modern Applications.
- Intelligence Systems of Data Processing.
- Secure ICT and Social Services.
- AI-based Technologies in Cyber Space.
- Legal Aspects of Cyber Security and Digital Resilience.
- Conflict Management.

The CMiGIN'26 was in a hybrid format. Most of papers were presented at the University of the National Education Commission in Krakow, Poland. However, participants from places with a high from Ukraine are invited to participate in a virtual format. Participants from Poland, Ukraine, Georgia, Kazakhstan, and Czech Republic joined the conference.

The CMiGIN'26 received 28 submissions in total. All papers were reviewed by two reviewers. Out of these, 20 papers were accepted for this volume, 16 as regular papers and 4 as short papers.

Paper [1] presents a hybrid explainable machine learning and deep learning framework for IoT network anomaly detection. The results of research demonstrate that explainable ensemble learning can provide both high detection performance and interpretable insights for IoT cybersecurity applications.

Paper [2] deals with the impact of generative artificial intelligence on SEO metrics and web content performance. Experimental results showed a reduction in the content preparation and publication cycle from 120...180 to 12 minutes, a 4...5-fold increase in administrator productivity, and positive dynamics in organic search and audience engagement indicators.

Paper [3] concentrates on cybersecurity-metric-driven software quality assessment for critical information and communication systems. Experimental results showed that even while maintaining correct responses of authentication and access control mechanisms, latency increases and throughput decreases under load, which is reflected in a decrease in the normalized cybersecurity indicator.

Paper [4] discusses a reproducible methodology for investigating network attacks on corporate infrastructure using an open-source cyber range. Experimental evaluation showed rapid environment deployment, 99.86% availability within 72 hours, and high attack detection efficiency with an aggregate F1-score of 97.3%, confirming the practical suitability of the proposed approach for training and reproducible research.

Paper [5] considers the issues of modelling of information security threats for airport infrastructure based on digital twin technology. A methodology for determining the operational and information resilience index was proposed, and the research results showed that a coordinated information attack can reduce its level by 45.6...59.4%, while a digital twin provides means for continuous monitoring, forecasting, and evaluation of resilience measures.

Paper [6] presents the issues of modeling the future splinternet using AI-driven fragmentation scenarios. Using the example of the connectivity of the countries of the Black Sea region, three scenarios of network disruption were investigated and it was found that failures of submarine cable landing stations cause the greatest expected connectivity losses, while kinetic scenarios are characterized by the longest predicted recovery time.

Paper [7] deals with the computational methods for best mathematical model building using a new adequacy criterion. The proposed approach can be used to increase the reliability of mathematical modeling in applied problems where experimental data are unevenly distributed or contain several values in a certain section.

Paper [8] concentrates on fast computational methods for panoramic spectrum analysis with hardware artifacts compensation for SDR-based direction finding applications. A comparison of the speed, efficiency, and accuracy of the proposed methods for the HackRF One and bladeRF micro 2.0 platforms

was conducted, which allows for increasing the accuracy of detection and direction determination of radio emission sources with an unknown frequency.

Paper [9] discusses a logical inference models based on fuzzy production rules for intelligent cyberthreat detection systems. Simulation results demonstrated accuracy of over 95% and the ability to form interpretable decisions regarding the level of cyber threats in systems such as Security Information and Event Management solutions and Intrusion Detection Systems.

Paper [10] considers comparative analysis of datasets with X-ray image for dangerous objects detection tasks.

Paper [11] presents a trust-aware reliability-based aggregation framework for resilient federated learning in critical infrastructure systems. The proposed framework was evaluated in a server-client federated learning simulation under mixed unreliable-client behavior.

Paper [12] deals with comprehensive analysis of machine learning classification metrics, algorithmic models, and the nuances of the neutral class.

Paper [13] concentrates on security-aware centralized network configuration management with automated compliance verification. Experimental validation confirmed the effectiveness of the approach for detecting and automatically remediating configuration deviations while ensuring compliance with existing standards.

Paper [14] discusses the issues of authentication of air traffic controllers in LDACS networks based on voice biometrics. The proposed system does not replace the standard security mechanisms, but it can effectively supplement them by verifying the physical identity of the controller during the establishment or confirmation of a service communication session.

Paper [15] considers information system for the strategic recruitment and retention of academic talent at the technical university.

Paper [16] presents criminal law mechanisms for countering cyberterrorism and its financing taking into account the use of virtual assets and the development of cyberphysical threats. Based on an analysis of Ukrainian legislation, international standards, and foreign practice, the authors substantiate proposals for improving the provisions of the Criminal Code of Ukraine and the draft of the new Criminal Code to form a comprehensive mechanism for countering cyberterrorism.

Paper [17] deals with analysis of the legal status of civilians participating in cyber operations during armed conflicts. The research showed that the main criterion for a civilian to lose protection from an attack is direct participation in hostilities, which requires the simultaneous presence of three elements: threshold of harm, direct causation, and belligerent nexus.

Paper [18] concentrates on test-driven development approach and tools enhanced by artificial intelligence. Using the example of a password reset module, it is demonstrated that AI-enhanced test-driven development can help improve the quality and maintainability of software systems, expand the set of test scenarios, and accelerate iterative development under developer control.

Paper [19] discusses the issues of zero trust architecture for cyber resilience.

Paper [20] considers a real-world incident of a cyberattack on university infrastructure in 2026. Research findings demonstrate that network segmentation, immutable backup technology, multi-factor authentication, and continuous auditing are essential defensive measures.

All our team invites you to visit the CMiGIN'26 workshop website <https://cyberconf.kai.edu.ua/CMGIN/CMGIN5/> where you can find all the relevant information about this event.

The materials of previous CMiGIN workshops were published in CEUR Workshop Proceedings:

- Volume 4024, URL: <https://ceur-ws.org/Vol-4024/>
- Volume 3925, URL: <https://ceur-ws.org/Vol-3925/>
- Volume 3530, URL: <https://ceur-ws.org/Vol-3530/>
- Volume 2588, URL: <https://ceur-ws.org/Vol-2588/>

2. Acknowledgments

CMiGIN'26 would not been possible without the support of the University of the National Education Commission, Poland (www.uken.krakow.pl/en/), National University "Kyiv Aviation Institute", Ukraine (www.nau.edu.ua), Tomas Bata University in Zlin, Czech Republic (www.utb.cz/en/), and CEUR Workshop Proceedings team (ceur-ws.org). Organizers and all participants of the Fifth International Workshop on Conflict Management in Global Information Networks express a lot of thanks.

Program Committee

- Roman Jasek, Tomas Bata University in Zlin, Czech Republic
- Bronislav Chramcov, Tomas Bata University in Zlin, Czech Republic
- Jugoslav Achkoski, Military Academy, North Macedonia
- Audrius Lopata, Kaunas University of Technology, Lithuania
- Rui Luis Aguiar, University of Aveiro, Portugal
- Rat Berdibayev, Almaty University of Power Engineering and Telecommunications, Kazakhstan
- Haruna Chiroma, University of Hafr Al Batin, Saudi Arabia
- Thierry Oscar Edoh, University of Bonn, Technical University of Munich, Germany
- Emil Faure, Cherkasy State Technological University, Ukraine
- Solomia Fedushko, Lviv Polytechnic National University, Ukraine
- Natalia Shakhovska, Lviv Polytechnic National University, Ukraine
- Tetiana Okhrimenko, Scientific Cyber Security Association of Ukraine, Ukraine
- Valentín Cardeñoso Payo, University of Valladolid, Spain
- Jamil Al-Azzeh, Al Balqa Applied University, Jordan
- Vishnu Narayan Mishra, Indira Gandhi National Tribal University, India
- Zhengbing Hu, University of Bonn, Central China Normal University, China

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] M. Turdalyuly, N. Baisholan, S. Gnatyuk, K. Baisholanova, A hybrid explainable machine learning and deep learning framework for IoT network anomaly detection, in: CEUR Workshop Proceedings, 2026, pp. 6–15.
- [2] O. Anisimova, O. Prihunov, H. Lukash, The impact of generative artificial intelligence on SEO metrics and web content performance, in: CEUR Workshop Proceedings, 2026, pp. 16–28.
- [3] R. Hamretskyi, V. Gnatyuk, K. Pytel, Cybersecurity-metric-driven software quality assessment for critical information and communication systems, in: CEUR Workshop Proceedings, 2026, pp. 29–42.
- [4] M. Delembovskyi, A reproducible methodology for investigating network attacks on corporate infrastructure using an open-source cyber range, in: CEUR Workshop Proceedings, 2026, pp. 43–56.
- [5] Z. Poberezhna, T. Konrad, D. Malnov, L. Dorotik, Modelling of information security threats for airport infrastructure based on digital twin technology, in: CEUR Workshop Proceedings, 2026, pp. 57–67.
- [6] M. Iavich, V. Svanadze, Modeling the future splinternet using AI-driven fragmentation scenarios, in: CEUR Workshop Proceedings, 2026, pp. 68–81.

- [7] V. Kuzmin, Y. Petrova, A. Osipchuk, Computational methods for best mathematical model building using a new adequacy criterion, in: CEUR Workshop Proceedings, 2026, pp. 82–93.
- [8] F. Katushonok, O. Shcherbyna, O. Zadorozhnyi, A. Simchuk, Fast computational methods for panoramic spectrum analysis with hardware artifacts compensation for SDR-based direction finding applications, in: CEUR Workshop Proceedings, 2026, pp. 94–106.
- [9] Y. Kostiuk, P. Skladannyi, K. Khorolska, B. Bebesko, V. Sokolov, Logical inference models based on fuzzy production rules for intelligent cyberthreat detection systems, in: CEUR Workshop Proceedings, 2026, pp. 107–137.
- [10] S. Bielov, M. Zaliskyi, K. Sulkowski, O. Shcherbyna, R. Saiko, S. Janczura, Baggage X-ray datasets with prohibited items: A survey, in: CEUR Workshop Proceedings, 2026, pp. 138–148.
- [11] S. Kudrenko, V. Alkema, V. Kozlovskyi, D. Kozlovska, Trust-aware reliability-based aggregation framework for resilient federated learning in critical infrastructure systems, in: CEUR Workshop Proceedings, 2026, pp. 149–159.
- [12] O. Tkachenko, A. Ilyenko, Y. Meleshko, O. Ulichev, Comprehensive analysis of machine learning classification metrics, algorithmic models, and the nuances of the neutral class, in: CEUR Workshop Proceedings, 2026, pp. 160–173.
- [13] O. Yeremenko, M. Trubeko, R. Savchenko, Systematic review on quantum algorithms for solving tasks of linear algebra and statistics, in: CEUR Workshop Proceedings, 2026, pp. 174–184.
- [14] G. Konakhovych, O. Holubnychyi, S. Doroshenko, Authentication of air traffic controllers in LDACS networks based on voice biometrics, in: CEUR Workshop Proceedings, 2026, pp. 185–200.
- [15] R. Odarchenko, M. Krasnoshapka, A. Lelechenko, B. Chumachenko, S. Chumachenko, A. Polozhentsev, Information system for the strategic recruitment and retention of academic talent at the technical university, in: CEUR Workshop Proceedings, 2026, pp. 201–215.
- [16] V. Kubalskyi, P. Kasyanov, M. Kysil, Problems of criminalising cyberterrorist offences and their financing in Ukraine: Doctrinal analysis and proposals for legislative amendments, in: CEUR Workshop Proceedings, 2026, pp. 216–225.
- [17] V. Filinovich, A. Mukasheva, Legal status of civilian participants in cyber operations during armed conflict, in: CEUR Workshop Proceedings, 2026, pp. 226–234.
- [18] V. Pechenko, S. Kryvyi, Test-driven development approach and tools enhanced by artificial intelligence, in: CEUR Workshop Proceedings, 2026, pp. 235–242.
- [19] R. Topala, B. Chramcov, V. Gnatyuk, Zero trust architecture for cyber resilience: Mathematical modelling and human factor minimisation, in: CEUR Workshop Proceedings, 2026, pp. 243–251.
- [20] M. Urazymbetov, B. Akhmetov, Weak passwords and absence of 2FA: Analysis of a ransomware attack on university, in: CEUR Workshop Proceedings, 2026, pp. 252–257.