Information & Security

Published since 1998

T. Tagarev, G. Sharkov, K. Kaloyanova,
Y. Yanakiev & N. Stoianov,
vol. 55, no. 1 (2024): 7-12
https://doi.org/10.11610/isij.5500
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Editorial

Open Source Intelligence, Artificial Intelligence, and Human-centered Approaches to Cyber-security and Countering Disinformation

Todor Tagarev [1] (✉), ***George Sharkov*** [1,2], ***Kalinka Kaloyanova*** [3], ***Yantsislav Yanakiev*** [4], ***and Nikolai Stoianov*** [4]

[1] *Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, Bulgaria, http://www.iict.bas.bg/EN*

[2] *European Software Institute, Sofia, Bulgaria, https://esicenter.bg/*

[3] *Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski," Sofia, Bulgaria, https://www.fmi.uni-sofia.bg/en*

[4] *Bulgarian Defence Institute "Prof. Tsvetan Lazarov," Sofia, Bulgaria, https://www.di.mod.bg*

ABSTRACT:

This editorial article introduces the reader to the Fifth International Scientific Conference "Digital Transformation, Cyber Security and Resilience," DIGILIENCE 2024. It summarises the findings presented in this volume in the areas of Methodological and IT Support to Cybersecurity and Critical Infrastructure risk assessment, methodological and IT support to critical infrastructure protection, the implementation of open-source and commercial-off-the-shelf technologies in the military domain, novel technologies and norms for maritime communications, situational awareness, critical infrastructure protection, and cybersecurity, civilian and security applications of advanced machine learning methods, the importance of the human factor in cybersecurity, and Russia's concept of reflexive control.

KEYWORDS: digital transformation, open-source intelligence, OSING, artificial intelligence, maritime security, human factors, human-centered cybersecurity, cyber skills framework, ethics, privacy, disinformation, reflexive control

✉ E-mail: tagarev@bas.bg

The unprecedented speed of technological advances provides opportunities for states and businesses to enhance performance and meet existing and emerging security challenges. To utilise the technological potential and remain competitive, organisations need to innovate and transform. Innovation, however, needs to go hand in hand with defence against malicious actors and attacks from cyberspace in a comprehensive approach that combines prevention, protection, reaction, and recovery measures and increases overall organisational resilience.

To reflect on these developments, in 2018, a group of senior researchers with policy-making experience launched a series of international scientific conferences under the title "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE). Three leading Bulgarian research institutions—the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences, the Bulgarian Defence Institute, and the European Software Institute—joined their forces in the pursuit of the new endeavor in cooperation with partner institutions from several European countries. The goal was to establish DIGILEINCE not only as an internationally recognised scientific conference but also as a platform that brings together senior policymakers, academics, and practitioners from governmental and business organisaitons to present and discuss trends, operational concepts, requirements, lessons from the experience, novel ideas, and emerging innovative solutions.

The first conference, DIGILIENCE 2019, was a resounding success. It took place in Sofia, 2-4 October 2019, and brought together over 100 participants and an agenda with 55 presentations. Twenty-eight of the papers were published in volume 43 of this journal [1] prior to the conference, while 32 of the presented papers appeared in a dedicated Springer volume.[2]

The second conference, DIGILIENCE 2020, was hosted by the Nikola Vaptsarov Naval Academy in Varna, Bulgaria. Fifty of the accepted papers were published in two volumes of *Information & Security: An International Journal*. Volume 46 addressed the challenges of ICT governance and management in the process of digital transformation, information exchange and situational awareness in cyberspace, the role of the human factor in systems integration, education and training, and ways of enhancing cyber resilience.[3] The articles in volume 47 covered the ways of protecting critical infrastructures from attacks from cyberspace, IoT systems, the application of big data and artificial intelligence methods for enhancing cybersecurity, and secure communications, and presented advanced ICT security solutions.[4] Updated and revised versions of presented papers were published in a post-conference volume of the Springer Series "Communications in Computer and Information Science."[5]

The third conference was hosted by the National Military University "Vassil Levski," located in the old Bulgarian capital, Veliko Tarnovo, and the fourth conference took place in Plovdiv, Bulgaria. Some of the accepted papers were published in pre-conference volumes of *Information & Security: An International Journal*, respectively vol. 50 and vol. 53, and selected papers are under publication in the same Springer series.

The fifth conference returns back to Sofia on 13-15 November 2024. For the first time, a DIGILIENCE event incorporates a well-established international workshop on Data Processing in Information Systems, Embedded Systems, and Intelligent Applications. The Computer Informatics Department of the Faculty of Mathematics and Informatics, Sofia University "St. Kliment Ohridski," and the Bulgarian Chapter of the Association for Information Systems are the lead organisers of the workshop.

The aim of the workshop is to bring together researchers, practitioners, and experts from different disciplines to share practical experience, challenges, and best practices in data modeling, data analysis and machine learning algorithms, security and privacy. A specific objective of this workshop is to encourage mentorship and support for early-career professionals.

This volume includes 20 original research articles to be presented at DIGILIENCE 2024, structured in six blocks: Methodological and IT Support to Cybersecurity and Critical Infrastructure Risk Assessment; Implementing Open-source and Commercial-off-the-Shelf Technologies for Enhanced Security; Advanced Technologies and Norms for Maritime Communications, Situational Awareness, Critical Infrastructure Protection, and Cybersecurity; Machine Learning and Artificial Intelligence Challenges and Applications; Enhancing Skills and Promoting Design Principles in a Human-centered Cybersecurity; and Understanding Cognitive Influence through Reconceptualization of Russia's Reflexive Control.

Methodological and IT Support to Cybersecurity and Critical Infrastructure Risk Assessment

With massive interconnections and reliance on a variety of information technologies, data, and communications, modern organisations are increasingly vulnerable to attacks from cyberspace. Of particular importance is to protect the organisations designated as critical infrastructures and/or providing services essential for the functioning of states, economies, and society.

Implementing rigorous risk assessment is the key to enhancing the understanding of main risks and transparent decision-making on investments in cybersecurity measures,[6] as well as measures for the protection of critical infrastructures.[7] The articles in this volume will contribute to the discourse in several ways. First, recognising the power of open-source intelligence [8] (OSINT), Rajamäki and co-authors present results from a study of the applicability of sets of open-source tools for assessing the risks of cyberattacks. They demonstrate that OSINT, properly used, may increase the effectiveness of organisational cybersecurity efforts. In the second article, Jakimoski et al. review the main cybersecurity standards and present an easy-to-use online tool developed to assist organisations, independent of their size, to better understand the salient risks for specific to them. In the third article, Radulov and coworkers present a step-by-step methodology to assess risks related to critical infrastructures, developed in view of norms and regulations applicable to owners and operators of critical infra-

structure in Bulgaria. In the fourth article, Grigorov et al. present an implementation of a geographic information system to visualize the levels of risks in the area surrounding a selectd critical infrastructure object in a variety of scenarios. Tikanmäki and coworkers wrap up this block of articles by reviewing standards addressing the intersection of cybersecurity and business continuity management. The authors also elaborate on the benefits that the certification according to one or more standards will bring to an organisation.

Implementing Open-source and Commercial-off-the-Shelf Technologies for Enhanced Security

In this block of articles, Stevanoski et al. continue the tread of using open-source tools to validate concepts and speed up the process of developing operational systems. They present the architecture and the tools used in a testbed for an integrated Network Operations Center and a Security Operations Center. The testbed allows the research team to gain real-time insights into the network's behavior, detect faults, identify potential vulnerabilities and, generally, evaluate cybersecurity and test additional risk reduction measures.

Another study by Veigl and coworkers demonstrates how relatively simple methods and algorithms for digital image stabilization can enhance the performance of thermal cameras in security applications—surveillance of green borders and critical infrastructures—and thus avoid the need for using more expensive equipment with mechanical gimbal, sensors, actuators, and servo electronics.

Maritime (Cyber) Security

In the first article in this block, Yavor Todorov reviews the cyber risks and threats for the maritime industry. Then, the focus shifts to the cybersecurity capabilities of the Black Sea littoral countries and those of the relevant threat actors, and the potential consequences for maritime security. He wraps-up the study by providing recommendations, including enhanced regional cooperation and countering hybrid threats.

The second article, contributed by Dimitrov and Karakolev, deepens our understanding of maritime security challenges in the Black Sea by examining critical infrastructures on the seabed, potential threat scenarios, and consequences. Further, they propose a model for analyzing the protection seabed critical infrastructure elements, reviewing protection technologies and systems, and wrapping up by outlining a protection strategy.

The third article describes the use of satellite imagery for rapid mapping and object detection in maritime environments. In the fourth, Brama et al. present a data exchange protocol in a novel approach to underwater communication.

Machine Learning and AI Challenges and Applications

Security, and in particular, the military applications of artificial intelligence pose considerable ethical challenges,[9] and this will be a main topic for discussions at DIGILIENCE 2024. One of the articles in this block, contributed by Maria

Lachova, examines the legal and ethical considerations in AI-based defence and security systems. Two additional articles examine respectively the augmentation of scarce data sets for fraud detection by using diffusion models and a hybrid optimization of feature sets for machine learning-based disease prediction.

Human-centered Cybersecurity

This block includes studies on human factors and the utility of cyber skills frameworks for enhancing cybersecurity, as well as ways to promote design principles in human-centered information security systems.

Russia's Reflexive Control

The final block includes two articles by Mitrakiev and Dimitrov centered on Russia's concept of reflexive control, examined as part of its cognitive influence, or information warfare more broadly. The first article substantiates the need for analyzing emotional cues in OSINT, while the second tracks how Russia's application of reflexive control leads to the realignment of political forces and individual politicians in the United States, the United Kingdom, Germany, and France.

References

[1] Todor Tagarev, ed., *Digital Transformation, Cyber Security and Resilience*, *Information & Security: An International Journal*, vol. 43 (2019), https://doi.org/10.11610/isij.v43.

[2] Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk, eds., *Digital Transformation, Cyber Security and Resilience of Modern Societies*, in *Studies in Big Data*, vol. 84 (Cham, Switzerland: Springer, 2021), https://doi.org/10.1007/978-3-030-65722-2

[3] Velizar Shalamanov, Nikolai Stoianov, and Yantsislav Yanakiev, eds., *DIGILIENCE 2020: Governance, Human Factors, Cyber Awareness*, *Information & Security: An International Journal*, vol. 46 (2020), https://doi.org/10.11610/isij.v46.

[4] Todor Tagarev, George Sharkov, and Andon Lazarov., eds., *DIGILIENCE 2020: Cyber Protection of Critical Infrastructures, Big Data and Artificial Intelligence*, *Information & Security: An International Journal*, vol. 47 (2020), https://doi.org/10.11610/isij.v47.

[5] Todor Tagarev and Nikolai Stoianov, eds., *Digital Transformation, Cyber Security and Resilience*, in *Communications in Computer and Information Science*, vol. 1790 (Cham, Switzerland: Springer, 2024), https://doi.org/10.1007/978-3-031-44440-1.

[6] Stephen C. Phillips, Steve Taylor, Michael Boniface, Stefano Modafferi, and Mike Surridge, "Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems," *IEEE Access* 12 (2024): 82482–505, https://doi.org/10.1109/ACCESS.2024.3404264.

[7] Jovana Ilkic, Milos Milovanovic, and Valentina Marinkovic, "A Novel Multiple-expert Protocol to Manage Uncertainty and Subjective Choices in Probabilistic Single and

Multi-hazard Risk Analyses," *International Journal of Disaster Risk Reduction* 110 (2024), 104641, https://doi.org/10.1016/j.japh.2024.102081.

[8] Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, Basel Katt, Mohammad Hijji, and Khan Muhammad, "Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security," *Mathematics* 2022, 10(12), 2054; https://doi.org/10.3390/math10122054.

[9] James Cook, Kirsi Helkala, George Lucas, Frank Pasquale, Gregory Reichberg, and Henrik Syse, "Artificial Intelligence in Strategic Planning and Military Operations," in *Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons*, edited by Mehmet Emin Erendor (CRC Press, 2024), Chapter 9.

About the Authors

Todor **Tagarev**, PhD, is an experienced security and defence policymaker with a background in cybernetics and control. He is currently a professor in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and leads its Centre for Security and Defence Management.
https://orcid.org/0000-0003-4424-0201

George **Sharkov**, PhD, is Director of the European Software Institute in Sofia, Bulgaria and Associate Professor at the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences. He also leads the Cybersecurity Lab at Sofia Tech Park. https://orcid.org/0000-0001-5086-311X

Kalinka **Kaloyanova**, PhD, is a Professor at the Faculty of Mathematics and Informatics at Sofia University "St. Kliment Ohridski," Bulgaria, and a Researcher at the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. She has extensive experience in many national and international projects, both as a project manager/ software developer and researcher. She is the founder and long-time President of the Bulgarian Chapter of the Association for Information Systems. Prof. Kaloyanova is the author of more than 100 publications on data science, database systems, information systems, project management. https://orcid.org/0000-0003-0222-7607

Captain (BGR-N, ret.) Yantsislav **Yanakiev**, PhD, is a full professor in sociology at the Bulgarian Defence Institute "Prof. Tsvetan Lazarov." Professor Yanakiev has been a principal national representative to the NATO STO Human Factors & Medicine Panel since 2005. He received the 2018 Individual Scientific Achievement Award of NATO Science and Technology Organization. https://orcid.org/0000-0003-0664-1661

Nikolai **Stoianov**, PhD, is Colonel in the Bulgarian Armed Forces, and Professor in the Bulgarian Defence Institute. Dr. Stoianov is Bulgaria's national representative in the NATO Science and Technology Board and chair of the STO IST Panel.
https://orcid.org/0000-0002-4953-4172