Information & Security

T. Tagarev, N. Stoianov, G. Sharkov & Y. Yanakiev, vol. 50, no. 1 (2021): 5-8
https://doi.org/10.11610/isij.5000

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Editorial

AI-driven Cybersecurity Solutions, Cyber Ranges for Education & Training, and ICT Applications for Military Purposes

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

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

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

[3] *European Software Institute – Center Eastern Europe, Sofia, Bulgaria, https://esicenter.bg/*

ABSTRACT:

This editorial article introduces the reader to the Third International Scientific Conference "Digital Transformation, Cyber Security and Resilience," DIGILIENCE 2021, and summarises the results from four of its sessions: AI-driven Cybersecurity Solutions; Organisational and Ethical Considerations in Providing Cybersecurity; Cyber Ranges for Innovative Education & Training; and Advanced ICT Solutions with Military Applications.

KEYWORDS: digital transformation, artificial intelligence, intrusion detection, collaborative network organisation, human factors, situational awareness, cybersecurity ethics, cyber range, ECHO project

Rapid technological developments provide numerous opportunities to enhance performance and create new security and defence capabilities. To utilise their potential, organisations need to innovate and transform while paying due attention to their protection against attacks from cyberspace and overall resilience. To reflect on these developments, a group of senior researchers with policy-making experience decided in 2018 to launch a series of international

✉ E-mail: tagarev@bas.bg

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–Center Eastern Europe—joined their forces in the pursuit of the new endeavour. We aimed to establish DIGILEINCE as an internationally recognised scientific conference and as a platform bringing together academics, senior policy-makers, and practitioners to present and discuss current and future requirements, lessons from the experience, novel ideas, and forthcoming innovative solutions.

The first conference, DIGILIENCE 2019, was a resounding success. It took place in the Central Military Club 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 focused on ICT governance and management for digital transformation, cyber situational awareness and information exchange, human systems integration, and education and training for cyber resilience.[3] The articles in volume 47 covered the protection of critical infrastructures from cyberattacks, IoT systems, the utilisation of big data and artificial intelligence for cybersecurity, secure communications, and presented advanced ICT security solutions.[4] Forty-five of the conference papers were submitted for publication in a post-conference volume of the Springer Series "Communications in Computer and Information Science."

As announced in 2020, the third conference, DIGILIENCE 2021, will be hosted by the National Military University "Vassil Levski," located in the old Bulgarian capital, Veliko Tarnovo. Unfortunately, the uncertainty surrounding travel restrictions during the Covid-19 pandemic was not conducive to the further expansion of the conference. Nevertheless, 42 papers were submitted for peer-review, and the conference agenda will include invited presentations from leading Bulgarian policy-makers, the European Defence Agency, ENISA, Bournemouth University, UK, the National Aerospace University "KhAI," [5] Kharkiv, Ukraine, and others.[6]

This volume includes 16 papers to be presented at the conference, structured four sections as follows:

- AI-driven Cybersecurity Solutions;
- Organisational and Ethical Considerations in Providing Cybersecurity;
- Cyber Ranges for Innovative Education & Training;
- Advanced ICT Solutions with Military Applications.

AI-driven Cybersecurity Solutions

Researchers continue to expand the applications of machine learning (ML) and artificial intelligence (AI) methods and techniques to strengthen cybersecurity. This section starts with a review of strategies, policies, and standards used by the European Union and its relevant bodies to direct the development of robust and trustworthy AI applications and their certification.

The following three articles present relevant results in developing cybersecurity prototypes with the Horizon 2020 project ECHO,[7] and delve respectively into adding heuristics to enhance intrusion detection functionalities in a Snort environment, combining signature-based and AI-driven anomaly detection methods to improve host-based detection, and strengthening detection by sharing cyber threat intelligence. The final two articles in this section apply clustering. In the first case, the technique is used to identify network users with risky behaviour. In the second, it is applied to automate the analysis of natural language, e.g., posts in social networks, and the creation of digests.

ML and AI techniques enhancing cybersecurity will continue to be covered by the conference. In its future editions, we will invite as well contributions on the reverse aspect – the security of AI applications.

Organisational and Ethical Considerations in Providing Cybersecurity

This section includes three articles. The first one is dedicated to cybersecurity collaboration and presents a structured methodological approach for transforming a project consortium into a self-sustainable collaborative network organisation.

The second is focused on ethical considerations and provides tools and guidelines to developers of health and wellbeing services with an account of privacy of information and confidentiality of communication.

The final contribution analyses information campaigns in support of recruitment in the armed forces and suggests improvements to current practice.

Cyber Ranges for Innovative Education & Training

Cybersecurity experts are in short supply while the demand continues to increase. The use of cyber ranges is seen as the most promising approach in training and educating the cyber workforce.

This section includes three articles. The first one provides a critical analysis of the experience of using hybrid cyber ranges in multiagency exercises and draws important recommendations for the future enhancement of the approach. The other two articles look into the experience for the purposes of higher education, with a specific focus on the needs of a masters' programme in cybersecurity management.

Advanced ICT Solutions with Military Applications

The final section includes four articles. The first one provides an analysis of the vulnerabilities of the widely used RSA cryptographic algorithm due to commonly used random number generators. The second contribution looks into the use of

augmented reality to enhance command and control applications. It is followed by a presentation of a method of planning the path of an autonomous vehicle so that it uses features of the terrain to remain hidden from an adversary observer. The last article outlines the main challenges to applying graph theory to the analysis of network security.

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] An extended version of the article Vyacheslav Kharchenko, Ihor Kliushnikov, Herman Fesenko, and Oleg Illiashenko, "Multi-UAV Mission Planning for Monitoring Critical Infrastructures Considering Failures and Cyberattacks," *Information & Security: An International Journal*, vol. 49 (2021), https://doi.org/10.11610/isij.4906.

[6] The reader may check the final conference agenda at https://digilience.org/content/digilience-2021-program.

[7] European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO), https://echonetwork.eu/.

About the Authors

Todor **Tagarev** 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.

Nikolai **Stoianov** is Colonel in the Bulgarian Armed Forces, Associate Professor and Deputy Director of the Bulgarian Defence Institute. Dr. Stoianov is Bulgaria's national representative in the NATO Science and Technology Board and vice-chair of the STO IST Panel.

Dr. George **Sharkov** – see p. 22 of this volume, https://doi.org/10.11610/isij.5030

Captain (BGR-N, ret.) Yantsislav **Yanakiev** 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.