Information & Security

V. Shalamanov, N. Stoianov & Y. Yanakiev
vol. 46, no. 1 (2020): 7-10
https://doi.org/10.11610/isij.4600

Published since 1998

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

Editorial

ICT Governance, Human Factors and Cyber Situational Awareness

Velizar Shalamanov , ***Nikolai Stoianov*** ,
Yantsislav Yanakiev (✉)

ABSTRACT:

The article summarises the results from the four sessions during the Second International Scientific Conference Digital Transformation, Cyber Security and Resilience DIGILIENCE 2020. These are ICT Governance and Management for Digital Transformation, Cyber Situational Awareness and Information Exchange, Human Systems Integration Approach to Cybersecurity and Education and Training for Cyber Resilience.

This volume is the outcome of the Second International Scientific Conference Digital Transformation, Cyber Security and Resilience DIGILIENCE 2020. In the volume are included accepted papers that are covering big part of what was expected as research topics.

The first part of this volume includes papers presented at DIGILIENCE 2020 conference, covering the theme of ICT Governance and Management for Digital Transformation. In this area our aim was to explore innovative ideas on governance and management of Collaborative Networked Organizations (CNOs) as one of the main venues for digital transformation and resilience.

A key element of any governance and management concept for digital transformation is the proper definition of the function of the CIO/CISO (Chief Information Officer / Chief Information Security Officer) or CDO (Chief Digital Officer). So, we explore the experience and new ideas for the development of this function in various national or international organisation. Separate round table is organized in parallel of the conference with CIO of key institutions in Bulgaria as well as a workshop on the CIO function in academic institutions, co-organized with the British Embassy in Bulgaria.

✉ E-mail: yantsislavyanakiev@gmail.com

In the first article Velizar Shalamanov, Vasil Sabinski and Trayan Georgiev explore the opportunity for Optimization of the Chief Information Officer Function in Large Organizations, looking at the experience in NATO, EU, some countries and especially the developments in Bulgaria. Other paper "A Concept for Establishing a Security Operations and Training Centre at the Bulgarian Naval Academy" by Borislav Nikolov addresses the achievements in design of training support environment. The CIO of IICT - Daniela Borissova with a team of young scientists in their article "How to Support Teams to be Remote and Productive: Group Decision-Making for Distance Collaboration Software Tools" is proposing review of responsibilities in ICT resource management with focus on decision making for selection of the key tools for critical functionalities in an academic institution.

Our colleagues from Finland, working on ECHO project - Kirsi Aaltola and Harri Ruoslahti are presenting their study "Societal Impact Assessment of a Cyber Security Network Project" to share experience from societal perspective. "Organizational Learning in the Academic Literature – Systematic Literature Review" by Harri Ruoslahti and Amir Trent is presenting a comprehensive review of resources on organizational learning and the next article of Yantsislav Yanakiev is adding value by presenting the experience in development of a governance alternative in ECHO project with focus on research and development – "A Governance Model of a Cyber Security Collaborative Networked Organization for Cybersecurity Research". Next paper "A Governance Model for an EU Cyber Security Collaborative Network – ECSCON" by Georgi Penchev and Antoniya Filipova-Shalamanova is presenting initial work on development of a White paper on governance to be further investigated through collaborative work of the four EU pilot projects on cyber competence, together with ECSO. Last, but not least is the paper of Silvia Matern – "e-Platform to maintain digital competencies for collaborative network organisation" addressing the key issue of development and maintaining the digital competencies, required for the success of the transformation process.

The second part of the volume includes papers presented at DIGILIENCE 2020 conference, covering the theme of Cyber Situational Awareness and Information Exchange.

The paper of George Sharkov, Yavor Papazov, Christina Todorova, Georgi Koykov, and Georgi Zahariev focuses on MonSys which is a flexible, robust, and scalable monitoring platform, developed by the authors and implemented as a cloud-based platform and an on-premise solution. It provides a number of standardized services availability checks (like web-based services from multiple points) and a flexible platform and tools for defining customized complex services.

The paper of Valentin Nekhai, Mariia Dorosh and Valentin A. Nekhai presents a study on the directions for the Situational Awareness Concept for the protection agricultural enterprises corporate networks.

The third paper of Nikolai Stoianov and Maya Bozhilova proposes a model of the system that is intended to provide network behaviour awareness, attacks

awareness, malicious web content awareness, with a primary focus on injection and the distribution of malicious information.

The paper of Jyri Rajamäki and Vasilis Katos is the result of a qualitative multiple-case study analysis. It consists of theory development by systematic reviews of academic articles, seven case studies, and cross-case conclusions, from which a set of system requirements and features were established to support a model that promotes information sharing among partners, while also meeting regulatory requirements.

Finally, the paper of Tuomo Sipola, Samir Puuska and Tero Kokkonen presents find a list of methods to fool artificial neural networks used in medical imaging. Specifically, the focus of the stress is laid on pathological whole slide images used to study human tissues.

The third part of the volume includes papers presented at DIGILIENCE 2020 conference, covering the theme of Human Systems Integration Approach to Cybersecurity and Education and Training for Cyber Resilience.

The first article of Ivana Ilic Mestric, Arvid Kok, Giavid Valiyev, Michael Street, and Peter Lenk from NCIA focuses on, possible approaches to gain greater understanding of document content by applying rule-based methods in addition to open source machine learning models. The performance of two approaches to sentiment analysis are assessed, when operating on document sets from NATO sources.

Next paper of Elitsa Pavlova focuses on Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation.

The third paper with authors Lisa de Kok, Deborah Oosting and Marcel Spruit from the Hague University of Applied Sciences aims at understanding how people's knowledge of and attitude (cognitive and an affective components) towards both cyber threats and cyber security controls affect intention to adopt cyber secure behaviour.

Next paper of Velizar Shalamanov, Silvia Matern, Vladimir Monov, Ivaylo Blagoev, Gergana Vassileva, and Ivan Blagoev, presents a conceptual framework for development of a model for building of advanced digital competences for digital transformation in cyber resilient environment. In addition, it identifies key research areas to support the development and implementation of the model and describes the current results of engaging with the key stakeholders from administration, academia and industry.

The key contribution of the paper of Harri Ruoslahti is in presenting a practical example of rapid transition from classroom to on-line learning in under the conditions of COVID19 pandemic in Laurea University of Applied Sciences.

The next paper of Yavor Dechev, Borislav Nikolov and Mariyan Rachev, Distance Learning at the Nikola Vaptsarov Naval Academy is also related to utilising online platforms during the COVID-19 Crisis. The report examines some of the technologies, used for distance learning in Nikola Vaptsarov Naval Academy. After a comparison analysis, an option is presented for the integration of the Microsoft Teams platform in the Academy's distance learning system.

The paper of Michal Turčaník, highlights the concept of a cyber range and the use of cyber range for educational purposes in the armed forces. The paper takes into account the use cases, the topology and software tools of the newly created cyber range in Slovakia.

The paper of Nikoleta Georgieva from the Bulgarian Naval Academy presents a comparative study between the Cyber Operations majors in the United States Naval Academy and the Bulgarian Naval Academy. It compares the goals of the major, the length of the degree, the courses, the lab hours, and their respective learning objectives to conclude.

Last but not least, the paper of Evgeni Andreev, Mariya Nikolova and Veselka Radeva presents research and numerical experiments in connection with the participation of authors and students from Nikola Vaptsarov Naval Academy in the NASA International Program: Simulation Exploration Experience 2020 for the creation of computer simulations of federations on the moon. Conclusions have been made regarding the security of the systems for cyber and space security of the Mobile Lunar Base.

Disclaimer

The views expressed and opinions expressed in this book are responsibility of the authors and do not necessarily represent the views of the Bulgarian of Defence Institute “Prof. Tsvetan Lazarov” and the Institute for Information and Communication Technologies of the Bulgarian Academy of Sciences.

About the Authors

Assoc. Prof. Dr. Velizar **Shalamanov** is deputy director of the Institute for Information and Communication Technologies of the Bulgarian Academy of Sciences.

Colonel Assoc. Prof. Dr. Nikolai **Stoianov** is deputy director of the Bulgarian Defence Institute “Prof. Tsvetan Lazarov”.

Captain (BGR-N) (ret.) Yantsislav **Yanakiev** is a full professor in sociology at the Bulgarian Defence Institute “Prof. Tsvetan Lazarov”.