Information & Security

T. Tagarev, G. Sharkov & A. Lazarov
vol. 47, no. 1 (2020): 7-10
https://doi.org/10.11610/isij.4700

Published since 1998

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

Editorial

Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions

Todor Tagarev [a] (✉), ***George Sharkov*** [b], ***Andon Lazarov*** [c]

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

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

[c] *Nikola Vaptsarov Naval Academy, Varna, Bulgaria, http://naval-acad.bg/en*

ABSTRACT:

This editorial article introduces the reader to the Second International Scientific Conference "Digital Transformation, Cyber Security and Resilience," DIGILIENCE 2020, and summarises the results from five of its sessions: Protecting Critical Infrastructures from Cyberattacks; Security Implications and Solutions for IoT Systems; Big Data and Artificial Intelligence for Cybersecurity; Secure Communication and Information Protection; and Advanced ICT Security Solutions.

In the fall of 2018, a group of senior researchers from the Institute of Information and Communication Technologies, the Bulgarian Defence Institute, and the European Software Institute–Center Eastern Europe—all with considerable policy-making experience—decided to launch a series of international scientific conferences under the title "Digital Transformation, Cyber Security and Resilience," or DIGILIENCE for short. In addition to typical conference goals, we aimed to bring together researchers, senior policy-makers and practitioners, and to present and discuss needs, requirements, novel ideas and upcoming solutions.

The first conference, DIGILIENCE 2019, took place in the Central Military Club in Sofia, 2-4 October 2019, bringing together over 100 participants and, as a first

✉ E-mail: tagarev@bas.bg

in the series, an ambitious agenda with 55 presentations. Twenty-eight of the papers were published in volume 43 of this journal.[1] The authors of 32 of the presented papers were invited to submit amended versions to a Springer volume.[2]

The assessment of the first conference was overwhelmingly positive. Hence, without hesitation we decided to start the organisation of the second conference, and Adm. Boyan Mednikarov, Rector of the Nikola Vaptsarov Naval Academy in Varna, Bulgaria, kindly agreed to host DIGILIENCE 2020.

108 papers were submitted to peer-review. Fifty of the accepted papers appear in two volumes of *Information & Security: An International Journal*. Volume 46 includes papers for five of the conference sessions: ICT Governance and Management for Digital Transformation, Novel Conceptual Approaches and Solutions, Cyber Situational Awareness and Information Exchange, Human Systems Integration Approach to Cybersecurity, and Education and Training for Cyber Resilience.[3]

This volume includes 26 papers, scheduled for the other five sessions:

- Protecting Critical Infrastructures from Cyberattacks;
- Security Implications and Solutions for IoT Systems;
- Big Data and Artificial Intelligence for Cybersecurity;
- Secure Communication and Information Protection;
- Advanced ICT Security Solutions.

The papers in this volume are arranged accordingly.

The section on critical infrastructure protection starts with an article presenting a framework for multi-sector cyber risk assessment, followed by contributions focusing on cyber risks to the maritime sector, social media, and Internet service providers. The next three articles in the section present conceptual design aspects, addressing respectively the cybernetic approach to building cyber resilient systems,[4] the interplay between resiliency, trust, and information exchange,[5] and the focus on decentralisation to enhance systems' security and resilience.[6]

The section on IoT systems presents studies on managing a logistics system through a digital twin, a tactical approach to cyber defence, and the estimation of network stability in in a big data environment.

The topic of bid data is pursued further in the third section of the volume. The introductory article sets the ground by elaborating on the concept of data science as a service.[7] The remaining five articles focus on the application of machine learning and other AI methods and techniques to enhance cybersecurity and resilience of complex systems.

This volume, as well as the conference agenda, flow into the topic of securing communication and information protection with contributions on public key generation and cybersecurity,[8] steganographic algorithms for hiding messages in music,[9] and an exploration of diceware passphrases.[10]

The final section includes articles addressing a variety of issues related to the security of advanced information and communication technologies and

suggesting practical solutions. Individual articles cover the use of instrumental equipment to create honeypots and facilitate the prevention of cyberattacks,[11] the security of mobile communications, the identification of network traffic anomalies, the performance of hard disks under ransomware attack, etc., as well as a comprehensive study of methods to reconstruct 3D facial images from 2D portraits.[12]

As with DIGILIENCE 2019, the authors of selected papers will be invited to contribute to a Springer volume, dedicated to DIGILIENCE 2020.

And finally, DIGILIENCE 2021 will take place in Veliko Tarnovo, capital of Bulgaria from XII to the end of the XIV century, in the period 29 September – 1 October 2021. For participation and other related information, you can visit the conference website, https://digilience.org.

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* (Cham: Springer, in press).

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 Vyacheslav Kharchenko, Sergiy Dotsenko, Yuriy Ponochovnyi, and Oleg Illiashenko, "Cybernetic Approach to Developing Resilient Systems: Concept, Models and Application," *Information & Security: An International Journal*, vol. 47, no. 1 (2020): 77-90, https://doi.org/10.11610/isij.v4705.

5 Jyri Rajamäki, "Resilience Management Framework for Critical Information Infrastructure: Designing the Level of Trust that Encourages the Exchange of Health Data," *Information & Security: An International Journal*, vol. 47, no. 1 (2020): 91-108, https://doi.org/10.11610/isij.v4706.

6 Nikita Savchenko, Vitaliy Tsyganok, and Oleh Andriichuk, "A Cost-Effective Approach to Securing Systems through Partial Decentralization," *Information & Security: An International Journal*, vol. 47, no. 1 (2020): 108-121, https://doi.org/10.11610/isij.v4707.

7 Peter Lenk, Michael Street, Ivana Ilic Mestric, Arvid Kok, Giavid Valiyev, Philippe Le Cerf, and Barbara Lorincz, "Data Science as a Service: The Data Range," *Information & Security: An International Journal*, vol. 47, no. 2 (2020): 157-171, https://doi.org/10.11610/isij.v4711.

[8] Nikolai Stoianov and Andrey Ivanov, "Public Key Generation Principles Impact Cybersecurity," *Information & Security: An International Journal*, vol. 47, no. 2 (2020): 249-260, https://doi.org/10.11610/isij.v4717.

[9] Michał Bajor and Marcin Niemiec, "A New Steganographic Algorithm for Hiding Messages in Music," *Information & Security: An International Journal*, vol. 47, no. 2 (2020): 261-275, https://doi.org/10.11610/isij.v4718.

[10] Petar Antonov and Nikoleta Georgieva, "Security Analysis of Diceware Passphrases," *Information & Security: An International Journal*, vol. 47, no. 2 (2020): 276-282, https://doi.org/10.11610/isij.v4719.

[11] Alexander Kolev and Pavlina Nikolova, "Instrumental Equipment for Cyberattack Prevention," *Information & Security: An International Journal*, vol. 47, no. 3 (2020): 285-299, https://doi.org/10.11610/isij.v4720.

[12] Matthew Caruana and Joseph G. Vella, "3D Facial Reconstruction from 2D Portrait Imagery," *Information & Security: An International Journal*, vol. 47, no. 3 (2020): 328-340, https://doi.org/10.11610/isij.v4724.

About the Authors

Todor **Tagarev** – see p. 26 of this volume, https://doi.org/10.11610/isij.4701

Dr. George **Sharkov**, former National Cybersecurity Coordinator (2014-2017), is currently an Adviser to the Minister of Defence. He led the development of the National Cybersecurity Strategy of Bulgaria, adopted in 2016. Since 2003, he is the Director of the European Software Institute – Center Eastern Europe and Lead of the Cyber Resilience Lab (CyResLab).

Andon **Lazarov** – see p. 43 of this volume, https://doi.org/10.11610/isij.4703