Information & Security

Todor Tagarev
vol. 43, no. 1 (2019): 7-10
https://doi.org/10.11610/isij.4300

Published since 1998 ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Editorial

DIGILIENCE – A Platform for Digital Transformation, Cyber Security and Resilience

Todor Tagarev

Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, http://www.iict.bas.bg/EN/index.html

ABSTRACT:

The ongoing digital transformation requires significant investments and innovation to provide security of cyberspace and variety of critical infrastructures and essential services that increasingly depend on the digital infrastructure, as well as to enhance the resilience of organizations, communities, industries, nations, and alliances in the face of malicious use of cyberspace.

This volume presents 28 of the papers, accepted for presentation at the DIGILIENCE 2019 conference, dealing with cyber information sharing and situational awareness, the benefits and challenges of emerging technologies, such as artificial intelligence, the human factor, education and training for cyber security and resilience, the need to incorporate the cybersecurity efforts into the search for effective and efficient exploitation of information technologies, policies and solutions for security and resilience of Industry 4.0 and critical infrastructures, analysing and countering hybrid influence through social networks and more traditional media. The DIGILIENCE series of conferences will promote the sharing of knowledge and experience and facilitate the spread of good practice in IT governance, cyber security and resilience.

ARTICLE INFO:

ONLINE: 24 SEP 2019

KEYWORDS:

digital transformation, cybersecurity, cyber resilience, artificial intelligence, emerging technologies, information sharing, cooperation, intuitionist fuzzy logic, hybrid influence, social networks, industry 4.0, human factors, DIGILIENCE

✉ E-mail: tagarev@bas.bg

The rapid development and massive incorporation of advanced technologies transform industries, services, conflict, government, leisure and social interaction. In the strive for competitive positioning, developers and users often underestimate safety and security considerations, which in turn provides ample opportunities for exploitation by malicious actors.

The series of DIGILIENCE conferences, the first of which will take place in the hearth of Sofia, the capital city of Bulgaria, in the beginning of October 2019, aims to establish the state of the art and future demands in the provision of security and resilience of processes, services and systems that are heavily reliant on information technologies.

This volume features 28 of the papers, accepted for presentation at DIGILIENCE 2019 upon peer review, arranged in six sections. The first section includes seven papers analysing benefits and challenges in implementing artificial intelligence and other emerging technologies for cyber security and resilience, from the role of blockchains for international security [1] and critical energy infrastructure protection [2] to the use of quantum solutions for securing the future Internet.[3] The next group of papers looks into the provision of cybersecurity as integral part of effective and efficient IT governance. Section 3 includes four papers examining the role of the human in cybercrime, cognitive challenges of information flow analysis,[4] and advanced understanding of and platforms for cybersecurity education and training. The fourth section presents studies on more 'traditional' cybersecurity issues such as identifying and countering malware,[5] information sharing, and cyber situational awareness. Section 5 contains four papers on policies and solutions for Industry 4.0 and critical infrastructures, as well as the use of advanced decision support to increase the security and resilience of the energy sector.[6] The final section is dedicated to hybrid threats and includes papers presenting results of media content analysis,[7] comparative analysis of Russian and US views on cyberwar in the 'hybrid' context,[8] and advanced methods and tools for understanding the dynamics of information flows on the basis of data from social networks [9] and inferring status and predictive information from that dynamics.[10]

In the 'Monitor' section of this volume the reader can find the DIGILIENCE 2019 agenda with resumes of the papers that are not included in this volume.

Bringing about 100 participants and some 55 reports to DIGILIENCE 2019—the first conference in the series on "Digital Transformation, Cyber Security and Resilience"—is considered a success.[11] It already provides for exchange of research results and identified good practices in providing cyber security and resilience. A separate session brings together presentations on ongoing national and international research projects intended to support networking, knowledge sharing, standardisation, and innovation.

Networking is of particular importance. In the fluid cybersecurity landscape and resource constraints, it is hardly possible to elaborate, not to mention – implement, comprehensive cyber security and resilience research and technology programs. Networking may alleviate the problem, especially if relevant approaches and frameworks [12] are available to integrate top-down guidance, practitioners' requirements and the multitude of research and innovation projects and bottom-up initiatives. In our view, DIGILIENCE can serve as a platform for networking and knowledge exchange in support of digital transformation, cyber security and resilience.

The final piece in this volume lists the priority themes and the timelines for the second conference on "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2020), that will be conducted in the Black Sea coastal city pf Varna, Bulgaria, 30 September – 2 October 2020, with the Bulgarian Naval Academy as the local co-organizer.

In addition to regular research papers, of particular interest will be studies that examine systems in their interdependence or place their operation in a human context, as well as evidence- and data-based studies and presentations of the respective datasets.

We look forward to your sustained interest and contribution for a successful conference.

References

[1] Sean Costigan and Greg Gleason, "What If Blockchain Cannot Be Blocked? Cryptocurrency and International Security," *Information & Security: An International Journal* 43, no. 1 (2019): 13-20.

[2] Notis Mengidis, Theodora Tsikrika, Stefanos Vrochidis and Yiannis Kompatsiaris, "Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities," *Information & Security: An International Journal* 43, no. 1 (2019): 21-33.

[3] Marcin Niemiec, Andrzej Dziech, Miłosz Stypiński and Jan Derkacz, "Quantum-based Solutions for the Next-generation Internet," *Information & Security: An International Journal* 43, no. 1 (2019): 21-33.

[4] Valerii P. Mygal and Galina V. Mygal, "Problems of Digitized Information Flow Analysis: Cognitive Aspects," *Information & Security: An International Journal* 43, no. 2 (2019): 134-144.

[5] Vesselin Bontchev and Veneta Yosifova, "Analysis of the Global Attack Landscape Using Data from a Telnet Honeypot," *Information & Security: An International Journal* 43, no. 2 (2019): 264-282.

[6] Volodymyr Zaslavskyi and Maya Pasichna, "System Approach Towards the Creation of Secure and Resilient Information Technologies in the Energy Sector," *Information & Security: An International Journal* 43, no. 3 (2019): 318-330.

[7] Ralitsa Kovacheva, "Hybrid Threats in Bulgarian Media," *Information & Security: An International Journal* 43, no. 3 (2019): 333-348.

[8] Yavor Raychev, "Cyberwar in Russian and US Military-Political Thought: A Comparative View," *Information & Security: An International Journal* 43, no. 3 (2019): 349-361.

[9] Diego F.M. de Oliveira and Kevin S. Chan, “Diffusion of Information in an Online Social Network with Limited Attention,” *Information & Security: An International Journal* 43, no. 3 (2019): 362-374.

[10] Maksym Shchoholiev and Violeta Tretynyk, “The System of Operative Determination of the Level of Tension in Society Based on Data from Social Networks,” *Information & Security: An International Journal* 43, no. 3 (2019): 375-382.

[11] The full program of the 2019 conference is available at http://digilience.org/content/DIGILIENCE2019-program.

[12] See, for example, Todor Tagarev, Nikolai Stoianov, and George Sharkov, “Integrative Approach to Understand Vulnerabilities and Enhance the Security of Cyber-Bio-Cognitive-Physical Systems,” in *Proceedings of the 18th European Conference on Cyberwarfare and Security (ECCWS19)*, edited by Tiago Cruz and Paulo Simoes, University of Coimbra, Portugal, 4-5 July 2019, pp. 492-500.

About the Author

Todor **Tagarev** is professor in the Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, and Head of its Centre for Security and Defence Management. With background in cybernetics and experience in senior governmental positions, he is the main organiser of the DIGILIENCE 2019 conference.

https://orcid.org/0000-0003-4424-0201