Information & Security

Published since 1998

G. Sharkov & W. Mees
vol. 53, no. 1 (2022): 7-8
https://doi.org/10.11610/isij.5300

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

Editorial

Enhanced Collaboration for Cyber Security and Resilience

George Sharkov[1] (✉), *Wim Mees*[2]

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

[2] *Koninklijke Militaire School – Ecole Royale Militaire, Brussels, Belgium*
https://www.rma.ac.be/en/

ABSTRACT:

This editorial article introduces the structure and content of articles accepted for presentation at the Fourth International Scientific Conference "Digital Transformation, Cyber Security and Resilience, DIGILIENCE 2022. The volume includes articles presenting results on six particular topics: Advanced Threat Intelligence and Information Sharing; Digitalization and Privacy Preservation; Governing Cybersecurity Networks and Ecosystems; Developing Critical Cyber Skills; Human Factors for Safety and Resilience to Cyber/Hybrid Influence; and Cyber Ranges, Simulation and Training.

KEYWORDS: digital transformation, threat intelligence, artificial intelligence, privacy, collaborative network organization, human factor, cyber digital skills, situational awareness, cyber range, ECHO project

In 2018, a group of senior researchers with policymaking experience decided to launch a series of international scientific conferences to address the rapidly growing demand for enhanced collaborative models, skills frameworks, research and innovation for cyber defense, and resilience under the title "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE). Three leading Bulgarian research institutions initially supported the initiative: 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. The new endeavor attracted multiple international partners, NATO's NCI Agency, the European Defense Agency, European Cybersecurity Agency ENISA, international universities, and research centers.

✉ Corresponding Author: George Sharkov; E-mail: gesha@esicenter.bg

Results from European research projects under Horizon 2020 and other programs have been regularly reported, with a significant number of contributions from the ECHO [1] project, including in the selection for this volume.

Traditionally, a pre-selection of the accepted papers is published prior to the conference in volumes of this journal. As a reference, in Volume 43 of the 2019 edition of DIGILIENCE we had 28 papers, while 32 appeared in a dedicated Springer volume post-conference. In 2020, fifty accepted papers were pre-published in volumes 46 and 47, and 34 were submitted for publication in a Springer Series volume. Despite the covid-19 pandemic, the DIGILIENCE 2021 conference was conducted in a hybrid mode, with more than 30 talks, of which sixteen were published in the dedicated Volume 50 of this journal.[2]

The papers included in this volume are grouped in six thematic sections.

In the section *"Advanced Threat Intelligence and Information Sharing"* the first paper presents a use-case from the ECHO project for applying the Early Warning System in the energy sector. The second presents a novel technique for OSINT on the dark web of child abuse material without exposing the researchers to sensitive content. The third outlines preliminary research results by the European Cybersecurity Agency ENISA towards establishing a unified ontology for cyber incident and crisis information sharing and management.

The section "*Digitalization and Privacy Preservation" presents* an approach to preserving privacy in Security-as-a-Service model and a technique to transform classical UML models of InfoSec systems into agent-based simulation models. The third paper covers personal data leakage prevention improvement of web video streaming, and the fourth is dedicated to the optimisation of automated fire control systems.

The *"Governing Cybersecurity Networks and Ecosystems"* section includes three approaches to developing the cybersecurity ecosystem, and the governance consulting services and tools developed within the ECHO project.

The section *"Developing Critical Cyber Skills"* covers simulation-based training, piloting ECHO e-skills and training toolkit, designing a modern training program, hackathons, and cyber hygiene in the naval security environment.

The *"Human factor"* is addressed in two papers studying the safety and resilience problems in the evolving industrial environment and the cyber/hybrid influence.

Three different approaches toward simulation-based and gamified training, red teaming, orchestration and federation of cyber ranges are presented in the last section, *"Cyber Ranges, Simulation and Training"*.

The reader may consult the final conference program and the full list of contributions at the conference website http://www.digilience.org/.

[1] ECHO project: European network of Cybersecurity centres and competence Hub for innovation and Operations, https://echonetwork.eu/

[2] Information & Security: An International Journal, https://isij.eu/.