ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Letter from the Editor-in-Chief

Corresponding author:
Aleksandra Gasztold, NASK National Research Institute, ul. Kolska 12, 01–045 Warsaw, Poland; E-MAIL: aleksandra.gasztold@acigjournal.pl

ORCID
https://orcid.org/0000-0002-9114-1604

Applied Cybersecurity & Internet Governance
2023;2 (1)

Dear Esteemed Readers,

It is with great pleasure that I introduce the 2023 volume of Applied Cybersecurity & Internet Governance (ACIG). As Editor-in-Chief, I am excited to present to you an array of insightful articles that delve into various facets of cybersecurity and its intersection with governance, technology, and society. At NASK-National Research Institute, the publisher of ACIG, humans are at the heart of technology. As a research institute dedicated to enhancing information and communication networks in Poland, we prioritize research, development, and education to empower users and safeguard the digital landscape, particularly focusing on the advancement of cybersecurity measures and the understanding of cyber threats.

In this issue, we bring together a collection of original research articles that offer diverse perspectives and analyses, catering to readers from academia, the IT sector, policy decision-makers, and beyond. Each article encapsulates cutting-edge research, practical insights, and thought-provoking discussions that contribute significantly to the discourse surrounding cybersecurity and modern online challenges.

Fourteen articles featured in this volume cover a wide range of topics, including supply chain risks in autonomous weapon systems, hybrid warfare, cognitive warfare, cyber resilience at the state level, and the protection of critical infrastructures, among others.

The issue opens with the article “Structured Field Coding and its Applications to National Risk and Cybersecurity Assessments” by William H. Dutton, Ruth Shillair, Louise Axon and Carolin Weisser, which explores the utilization of structured field coding in enhancing national cybersecurity assessments, facilitating cross-national comparative analyses. Moreover, “Predictive Modelling of a Honeypot System Based on a Markov Decision Process and a Partially Observable Markov Decision Process” by Lidong Wang,

Reed Mosher, Patti Duett and Terril Falls, presents innovative approaches to predictive modeling in honeypot systems, crucial for proactive cybersecurity measures. The next paper, titled "Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies" by Patryk Widuliński, provides an overview of artificial immune systems in intrusion detection systems, offering insights into recent advancements and future research directions. Complementing this section, the interview held by Rubén Arcos, "Shielding the Spanish Cyberspace: An Interview with Spain's National Cryptologic Centre (CCN)," aims to present the perspective of security institutions involved in monitoring cyberspace for threats.

Furthermore, "Examining Supply Chain Risks in Autonomous Weapon Systems and Artificial Intelligence" by Austin Wyatt delves into the risks associated with AI-enabled autonomous systems, focusing on the vulnerabilities within supply chains responsible for producing such military technologies. In the context of growing threats in cyberspace, Marco Marsili's article, "Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse," explores the concept of hybrid warfare, particularly within the context of cyber, information, and cognitive hostilities, shedding light on the implications of these phenomena in the modern world. Thereafter, Guillermo Lopez-Rodriguez, Irais Moreno-Lopez and José-Carlos Hernández-Gutiérrez compare cyber attacks on energy infrastructures carried out by Russia and Iran, analyzing their strategies and political implications in the manuscript titled "Cyberwarfare against Critical Infrastructures: Russia and Iran in the Gray Zone." Staying in the area of hybrid warfare in cyberspace, the paper entitled "The Russia-Ukraine Conflict from 2014 to 2023 and the Significance of a Strategic Victory in Cyberspace" by Dominika Dziwisz and Błażej Sajduk examines Russian engagement in cyberspace during the conflict with Ukraine, challenging Western perspectives and discussing Russian cyber warfare strategies.

Moreover, "Tell Me Where You Live and I Will Tell Your P@Ssword: Understanding the Macrosocial Variables Influencing Password's Strength" by Andreanne Bergeron investigates the influence of macrosocial factors on password strength, aiming to offer insights into global cybersecurity policies and configurations. An approach to societal aspects was presented in "Trust Framework on Exploitation of Humans as the Weakest Link in Cybersecurity" by Daudi Morice. This analysis develops a trust framework focusing on the exploitation of human psychology in cyberattacks, highlighting the importance of understanding and mitigating human vulnerabilities in cybersecurity. However, a comprehensive conceptualization of state-level cyber

resilience, offering insights into the capacities required for states to effectively respond to cyber threats is examined by Geoffrey Hubbard in "State-level Cyber Resilience: A Conceptual Framework."

The challenges of the changing digital technology landscape exemplified by efforts in the European Union are presented in two articles. The first, titled "Protection of the EU's Critical Infrastructures: Results and Challenges" by Robert Mikac, analyzes EU legislative acts aimed at improving the resilience of critical infrastructures, focusing on potential weaknesses and suggesting solutions. The next, "Regulating Deep Fakes in the Artificial Intelligence Act" by Mateusz Łabuz, discusses the challenges and limitations in mitigating the negative consequences of deep fake technology. The issue closes with "Creating a Repeatable Nontechnical Skills Curriculum for the University of Southern Maine (USM) Cybersecurity Ambassador Program (CAP)" by Lori L. Sussman and Zachary Leavitt. It presents a case study on the development of a nontechnical skills curriculum for a cybersecurity internship program, aiming to bridge the gap between academia and industry demands in cybersecurity education.

We extend our sincere gratitude to the authors, reviewers, and International Editorial Board whose dedication and expertise have made this volume possible. We hope that the articles presented herein stimulate meaningful discussions and inspire further research in cybersecurity and internet governance.

Thank you for your continued support and readership.

Warm regards,

Aleksandra Gasztold
Editor-in-Chief
Applied Cybersecurity & Internet Governance