ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Introduction to Special Issue on Cybersecurity in Digital Systems: Emerging Trends, Models and Technologies

Joanna Kołodziej | NASK – National Research Institute, Warsaw, Poland | ORCID: 0000-0002-5181-8713

Matteo Repetto | Consiglio Nazionale Delle Ricerche, Genoa, Italy | ORCID: 0000-0001-8478-2633

Received: 23.07.2026

Accepted: 24.07.2026

Published: 10.08.2026

Cite this article as:
J. Kołodziej, M. Repetto, "Cybersecurity in Digital Systems: Emerging Trends, Models and Technologies," ACIG, vol. 5, no. 2, pp. 1–5, 2026, doi: 10.60097/ACIG/226529

Corresponding author:
Joanna Kołodziej, NASK National Research Institute, Poland; E-mail: joanna.kolodziej@nask.pl
0000-0002-5181-8713

Modern applications and services are increasingly built on a large, pervasive, and heterogeneous computing continuum, where software, networks, devices, infrastructure, and data from different providers are combined in technology and business-value chains. Ensuring end-to-end confidentiality, integrity, and availability is extremely challenging today because it goes beyond protecting individual networks, software, and hardware from unauthorised access, attacks, or damage. Multi-layered frameworks are required that combine encryption, firewalls, multi-factor authentication (MFA), and endpoint protection in a seamless and homogeneous way across technological and business domains. Moreover, a transition from the prevailing reactive approach to a proactive posture is necessary to anticipate threats before they materialise and cause irreparable damage (e.g. data leaks, ransomware, loss of reputation, and large-scale failures of critical infrastructure).

Tight and complex dependencies in digital service chains require new simulation models, such as digital twins (DTs), which could be used to monitor infrastructures and services, investigate anomalies, detect the new breed of artificial intelligence (AI)-powered threats, and enforce security controls in a homogeneous way across the heterogeneous computing continuum. AI, in its various forms, is an

indispensable tool for detecting, responding to, and orchestrating cybersecurity processes, effectively addressing complexity beyond human capacity. However, it also introduces many vulnerabilities, especially for non-explainable models.

This special issue encompasses theoretical work and practical approaches that advance research in all aspects of securing interconnected digital information technology (IT) systems and infrastructures. The contributions range from advanced technologies, applications, and innovative solutions for modelling, simulation, and predicting cyber threats in complex systems to modern cryptographic methods as well as the development of methods, conceptual and theoretical models, and simulations related to the secure operation of digital chains and services in large, heterogeneous, and multi-ownership systems.

Contents

This volume, comprising eight articles, presents the latest research on complex, intelligent conceptual, and theoretical models and simulations for the secure operation of digital supply chains and services as well as methodologies for securing interconnected digital services within IT systems and infrastructures. This publication also presents innovative solutions for modelling, simulating, and forecasting cyber threats and attacks in complex IT systems as well as modern post-quantum cryptography methods.

In the first article, Repetto and Canavese [1] discuss the concept of secure DTs and their potential application in securing large, interconnected systems owned by multiple parties. The authors first focus on a digital twin model that can detect real-time threats, identify lateral movement, and mitigate attacks using digital assets. Next, the authors discuss hybrid DTs, which incorporate physical devices into the model and can detect threats in critical infrastructures. Both models are characterised by their use in Smart City and Smart Grid projects.

Multidimensional digital twin models are implemented on complex platforms that use container technologies, such as Kubernetes, which has become an essential tool for digital service platforms, and where authorisation is a key security mechanism. Pizzato et al. [2] compare authorisation mechanisms in Kubernetes, based on operational requirements typical of shared clusters. The results of this analysis reveal the limitations of the existing authorisation methods and point to directions for further research in this area.

The modern critical infrastructure systems usually contain complex AI mechanisms embedded to support decision-making. Sood and Zeadally [3] defined a multi-level taxonomy of complex AI systems that accounts for cross-layer interactions and emerging security vulnerabilities. This taxonomy can serve as a basis for a new approach to threat modelling and the identification of architectural weaknesses. Risk mitigation strategies and architectural best practices aimed at building secure and trustworthy AI systems are also presented.

The next two articles focus on the vulnerabilities of AI-based IT systems and adversarial attacks. Kowalczyk et al. [4] survey adversarial attack models, defence methods against them, and the assessment of the resilience of complex AI-based systems. A taxonomy of defence methods was defined, encompassing both proactive and reactive approaches. The essential conclusion from the analysis is the need to build multi-layered defence mechanisms and to assess realistically their effectiveness and the threats they face in complex AI systems. Multimodal malware detection in mobile systems (Android) is discussed by Sackitey et al. [5]. They propose a malware-detection method that leverages image-based and tabular representations of Android applications based on visual and tabular representations of Android Package Kit (APK) files for the Android system. In the experiments, a ResNet-50 network was used to extract visual representations from 'byte plot' images. The tabular data was analysed using an autoencoder pre-trained on a multilayer perceptron (MLP) network to model behavioural correlations.

Sherif [6] analyses IT system vulnerabilities using the MITRE ATT&CK framework. The author proposes a Bayesian co-occurrence model that estimates the conditional probability of common weakness enumeration (CWE) classes, given a specific ATT&CK technique, integrating three publicly available datasets. Experimental analysis shows that probabilistic models are highly effective at generating interpretable, practically useful priorities for corrective actions related to CWEs.

Syed [7] describes an AI-based platform for real-time identity risk assessment and adaptive access control. Anomaly detection using autoencoders is combined here with Bayesian risk assessment methods. The platform also features a built-in Q-learning reinforcement learning agent, which enables real-time adjustment of system access policies. This solution has been enhanced further with graph–theory-based centrality analysis, designed to increase the *a priori* risk for accounts holding structural permissions within the enterprise's permission network, ensuring that identities with a high

degree of exposure are subjected to proportionally greater control. A comprehensive experimental analysis confirms the high performance of AI-based Identity and Access Management (IAM) pipelines, compared to rule-based models under controlled test conditions.

Finally, Dybel and Kołodziej [8] survey post-quantum cryptography (PQC) methods. The authors employed a systematic methodology to evaluate the empirical trade-offs in performance of newly standardised PQC algorithms and to conduct a comparative analysis of data load, computational delay, and resource efficiency. A new, implementation-oriented taxonomy was defined that maps PQC standards to practical use cases, accounting for constraints in Internet of Things (IoT), cloud, and blockchain environments.

The list of authors includes the partners from the HE MIRANDA project, the external collaborators, and invited experts and scientists in the domain. We strongly believe that this issue will be of interest to a broad group of researchers, engineers, and professionals working in computer science and IT business units that use intelligent modelling to support their interdisciplinary projects and applications in distributed complex digital systems and data-intensive computing domains. We believe they would find a valuable survey of emerging technologies for realistic potential infrastructures and use cases.

Acknowledgements

We are grateful to all the contributors of this issue for their willingness to work on this project. We thank the authors for their interesting articles, their time and effort, and their researchful ideas, which make this volume a comprehensive, state-of-the-art compendium of the latest research advances and technology development in next-generation secure digital systems. We would also like to express our sincere thanks to the reviewers who helped us to ensure the quality of this volume. We gratefully acknowledge their time and valuable remarks and comments.

Our special thanks for Prof. Aleksandra Gasztold, Editor-in-Chief of the journal *Applied Cybersecurity & Internet Governance* (ACIG), Prof. Dorota Domalewska, Dr. Agnieszka Wrońska, and the entire editorial team for their patience, valuable editorial assistance, and excellent collaboration on the release of this special issue.

Finally, we would like to extend our warmest gratitude to our friends and families for their patience, love, and support in preparing this volume.

References

[1] M. Repetto, D. Canavese, "A cybersecurity digital twin architecture for modelling threats in interconnected systems," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 6–36, 2026, doi: 10.60097/ACIG/221493.

[2] F. Pizzato, D. Bringhenti, F. Valenza, "A comparative study of authorisation mechanisms in Kubernetes-based service platforms," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 37–65, 2026, doi: 10.60097/ACIG/220492.

[3] A. Sood, S. Zeadally, "Designing secure composite AI systems: Cross-domain holistic threat model and mitigation framework," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 66–89, 2026, doi: 10.60097/ACIG/221578.

[4] M. Kowalczyk, J. Kołodziej, M. Krzysztoń, "Evaluating and defending against adversarial threats in multimodal AI," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 90–130, 2026, doi: 10.60097/ACIG/220237.

[5] P. Sackitey, C.C. Mawunyo Agbesi, T. Graham, "Multimodal malware detection under obfuscated and adversarial attack conditions using ResNet-50 and MLP encoders with contrastive learning and adaptive cross-modal fusion," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 131–154, 2026, doi: 10.60097/ACIG/219075.

[6] E. Sherif, "From ATT&CK technique to remediation priority: Bayesian estimation of weakness-class likelihood for operational cyber defence," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 155–175, 2026, doi: 10.60097/ACIG/224570.

[7] K. Syed, "Artificial intelligence-driven continuous identity risk assessment and adaptive access control for automated cybersecurity," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 176–200, 2026, doi: 10.60097/ACIG/221412.

[8] A.W. Dybel, J. Kołodziej, "Navigating the NIST PQC standards: Trade-offs and case studies," *Applied Cybersecurity & Internet Governance,* vol. 5, no. 2, pp. 201–223, 2026, doi: 10.60097/ACIG/221494.