ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Letter from the Editor-in-Chief

Aleksandra Gasztold

Corresponding author:
Aleksandra Gasztold,
NASK–National Research
Institute, ul. Kolska 12,
01–045 Warsaw, Poland;
E-mail: aleksandra.gasztold@acigjournal.pl
0000-0002-9114-1604

Dear Readers,

The year 2025 marked a period of profound structural transformation in the global landscape of cybersecurity and artificial intelligence (AI). Accelerated digitalisation, the operational deployment of advanced AI systems, and the intensification of geopolitical tensions collectively reshaped the contemporary threat environment. Cybersecurity in 2025 can no longer be conceptualised solely through the prism of technical vulnerabilities. It increasingly reflects systemic risk emerging from the convergence of AI autonomy, information manipulation, supply chain fragility, and regulatory asymmetry. This evolution underscores the growing need to analyse cybersecurity as a multidimensional phenomenon situated at the intersection of technological, social, political, and legal domains.

At the global level, the proliferation of AI-enabled threats altered both scale and velocity of cyber incidents. Automated vulnerability discovery, adaptive malware, and AI-assisted intrusion campaigns reduced the threshold for executing sophisticated attacks while simultaneously challenging conventional detection and response mechanisms. In parallel, disinformation operations amplified by generative AI evolved into persistent instruments of strategic influence, targeting democratic processes, critical infrastructure debates, and social cohesion. These dynamics reinforced the interdependence between cybersecurity and information security, a relationship that gained increasing prominence across academic, policy, and operational communities.

The operational threat landscape in 2025 was characterised by persistent ransomware campaigns, supply-chain intrusions, and state-linked activity exploiting geopolitical tensions. Particularly significant were coordinated attacks on cloud service integrations and software-as-a-service ecosystems, demonstrating the systemic propagation of risk through digital supply chains. Disruptive ransomware incidents affecting aviation management systems and municipal administrations illustrated the continued vulnerability of essential services to financially motivated cybercrime. Concurrently, politically motivated hacktivist campaigns and state-aligned influence operations targeted governmental networks and public information systems, reinforcing the strategic role of cyberspace in contemporary conflict environments.

From the European Union (EU) perspective, 2025 was defined by the transition from regulatory design to regulatory enforcement. The implementation phases of the Network and Information Security 2 (NIS2) Directive, the Cyber Resilience Act, and the Critical Entities Resilience framework signalled a shift towards systemic risk governance, extending responsibility beyond operators to vendors, integrators, and supply chains. Analyses published by the European Union Agency for Cybersecurity (ENISA) throughout the year consistently highlighted that while regulatory coherence improved, capacity gaps persisted, particularly in coordinated vulnerability disclosure, AI risk governance, and cross-border incident response [1]. The European approach increasingly recognises that resilience must be socio-technical, integrating legal, organisational, and cognitive dimensions alongside technical safeguards.

National experiences further illustrate these challenges. In Poland, where the publisher of this journal, the NASK–National Research Institute, operates as a core component of the national cybersecurity system through the Computer Emergency Response Team (CERT) Polska, 2025 recorded an unprecedented number of reported computer security incidents, exceeding 260,783 cases. Compared to 2024, this represents an increase of approximately 135%. Computer fraud, including phishing campaigns and fraudulent investment schemes, accounted for more than 250,000 incidents, representing approximately 96% of all recorded cases in 2025. This growth was driven not only by intensified malicious activity but also by enhanced detection capabilities, expanded reporting obligations, and improved situational awareness across the national cybersecurity ecosystem. The Polish case exemplifies a broader European trend: rising incident statistics reflect both escalating threat pressure and the maturation of institutional monitoring and response frameworks.

Disinformation and cognitive influence operations emerged as particularly salient risks in 2025. AI-driven content generation blurred the boundaries between authentic discourse and synthetic manipulation, complicating attribution and response. These dynamics were evident in the contexts related to energy security, armed conflict, and technological sovereignty. As argued in *Humans in the Cyber Loop: Perspectives on Social* Cybersecurity [2], contemporary cybersecurity challenges cannot be effectively addressed through technological solutions alone, as human agency, social structures, and political contexts remain integral components of cyber risk and resilience. Consequently, technological approaches to cybersecurity should be systematically complemented by insights from the social sciences, particularly in the analysis of behaviour, power relations, governance mechanisms, and trust in digital environments [2]. Cybersecurity, therefore, increasingly intersects with questions of governance, trust, and democratic resilience, demanding interdisciplinary analytical tools and policy responses.

From the perspective of international governance, 2025 was also notable for the consolidation of global cyber norms. The adoption of the United Nations Convention against Cybercrime represented the first multilateral treaty establishing shared procedures for cross-border digital evidence exchange and coordinated cybercrime prosecution [3]. Simultaneously, several states introduced accelerated incident-reporting obligations for critical network operators, reflecting a broader shift towards state-level operational oversight of cyberspace. NATO and partner countries expanded large-scale cyber defence exercises in 2025, testing collective responses to simulated attacks on civilian critical infrastructure and further institutionalising cyber resilience as a dimension of collective security. This was demonstrated by Locked Shields 2025 (Tallinn, Estonia, 27 April–10 May 2025), Crossed Swords 2025 (Tallinn, early November 2025), and NATO’s Cyber Coalition 2025 (Tallinn, 28 November–4 December 2025), which collectively advanced multinational interoperability and coordinated defence of national and Alliance networks [4].

The contributions assembled in Volume 4 (No. 1) directly engage with these developments. The articles explore AI-powered pervasive computing and its threat models; principles for building trustworthy autonomous AI; transnational digital repression; and social cybersecurity frameworks addressing AI-driven information manipulation. Further contributions analyse vulnerability coordination under the Cyber Resilience Act, AI risk governance for critical infrastructure under NIS2 and CER, and threat mapping in the energy sector. Methodological advances in intrusion detection, DevSecOps decision-making, intelligence transformation, data governance, and critical theoretical perspectives on cybersecurity and AI governance collectively reflect the expanding scope of the field.

Collectively, the articles in this volume respond to a defining characteristic of 2025: cybersecurity has become an arena in which technology, law, geopolitics, and society converge. The *Applied Cybersecurity & Internet Governance* (*ACIG*) is intended to foster scholarly reflection and informed practice in a context where resilience increasingly depends on critical understanding and responsible governance grounded in interdisciplinary cooperation, as much as on technological innovation.

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

References

[1] European Union Agency for Cybersecurity (ENISA). (2025). “ENISA threat landscape 2025.” [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025. [Accessed: Dec. 31, 2025].

[2] D. Domalewska, A. Gasztold, A. Wrońska, *Humans in the cyber loop: Perspectives on social cybersecurity* Studies in critical social sciences, vol. 317. Leiden: Brill, 2023.

[3] United Nations Office on Drugs and Crime (UNODC). (2025). “United Nations convention against cybercrime.” [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html. [Accessed: Dec. 31, 2025].

[4] NATO Allied Command Transformation. (2025). “Cyber coalition 2025.” [Online]. Available: https://www.act.nato.int/article/cyber-coalition-2025/. [Accessed: Dec. 31, 2025].