Editorial

Welcome to a new edition of the Romanian Journal of Cyber Security ROCYS continues to grow as both a scientific publication and a focal point for the community of researchers, practitioners and policymakers that ICI Bucharest is building around some of the most pressing issues of our time. Cybersecurity is one of those fields where the pace of change makes it impossible to stand still, and this issue is no exception to the tradition of bringing together diverse, high-quality contributions that reflect both the breadth of the field and the depth of expertise in our community.

The world in which we are publishing this issue is one defined by accelerating technological change and a security environment that has not grown more benign. The geopolitical tensions that have marked the past several years remain in full force, and cyberspace continues to serve as a primary medium for hybrid operations, economic espionage and the coercion of states and institutions. The war in Ukraine has made plain what many analysts had long argued: that cyber operations are not a standalone domain of conflict but are deeply interwoven with kinetic, informational and economic instruments of statecraft. Ransomware groups, some operating with the tacit tolerance of state sponsors, have continued to target critical infrastructure across the energy, water, health and transport sectors. The SolarWinds and MOVEit intrusions remain instructive case studies, but the attack surface has only grown since then. Supply chain security, which was once the concern of a specialized minority, is now a central preoccupation of governments and companies alike, and rightfully so, since the interdependencies of modern digital ecosystems mean that a compromise of a single node can propagate across entire sectors. The European Union has responded with an ambitious regulatory agenda, with NIS 2 now being transposed into national law across Member States and CER bringing critical entities into a more comprehensive resilience framework. But legislation, however well-crafted, is only as effective as its implementation, and the gap between regulatory intent and operational reality remains one of the defining challenges of the current period.

Artificial intelligence has moved from a background concern to a front-and-center issue for cybersecurity in a remarkably short time. On the offensive side, AI is lowering the barrier to entry for social engineering, phishing and the generation of disinformation at scale. On the defensive side, it is offering new capabilities for anomaly detection, threat intelligence and incident response. Neither side has achieved a decisive advantage, and the race is genuinely open. What is clear is that the governance of AI, both within organizations and across borders, has become a cybersecurity matter of the first order. The question is no longer whether AI will be integrated into critical systems, but how quickly and with what safeguards. For countries in our region, the imperative is to build indigenous capacity and expertise, to avoid a situation in which our critical systems are secured by tools and

Adrian Victor VEVERA
Founding Editor in Chief,
General Director,
ICI Bucharest

architectures whose inner workings we do not fully understand and cannot fully audit. ICI Bucharest is contributing to this effort through the RO AI Factory and through the research and community-building activities that make publications such as ROCYS possible.

This issue of the Romanian Journal of Cyber Security brings together a roster of contributions that reflects the complexity of the current security landscape. The role of AI in combating cyber threats is addressed directly, providing a timely overview of where machine learning and AI-based tools are making a practical difference in defensive operations. On the technical frontier, we feature a study on repetitive high-voltage pulse generators based on thermally depolarized ferroelectrics, and an article on server-authoritative and OIDC approaches for secure player authentication in immersive digital environments, which speaks to the growing importance of security in extended reality and gaming platforms. The security of mechatronic control modules in the context of current cyber threats brings us into the domain of operational technology, where the convergence of IT and OT systems is creating new vulnerabilities that traditional cybersecurity approaches are not fully equipped to address. Intrusion detection in intelligent energy prediction systems for non-residential buildings connects two of the most important policy priorities of our time: energy security and cybersecurity, and the article makes a valuable contribution to understanding how to protect the data-driven systems that are becoming central to building management and energy efficiency. The issue of pattern recognition in cybersecurity and information science is covered in a conceptual review that maps the state of the art and the open challenges in this foundational area. For practitioners, the article on operationalizing NIS2 compliance through SIEM-driven alert and incident management provides concrete guidance at a moment when organizations across the EU are working out what the new regulatory requirements mean for their day-to-day operations. We are also pleased to include an article examining the intersection of ESG considerations and cybersecurity from the perspective of firm value, which speaks to the growing integration of cybersecurity into corporate governance and investment analysis. A systemic analysis of internet domain vulnerabilities and multi-layered mitigation strategies rounds out the more technical contributions. Finally, the issue closes with an article on forest management as a critical infrastructure and key asset challenge, exploring how satellite imagery, AI, drones and private blockchain-based decision support systems can be integrated into a coherent governance framework for this often-overlooked sector.

As you can see, the range of topics covered reflects our conviction that cybersecurity cannot be understood or addressed in isolation. It reaches into energy, built environments, digital identity, financial markets, natural resource management, regulatory compliance and emerging technologies. ROCYS is committed to providing a venue that does justice to this breadth while maintaining the scientific rigor that our readers and contributors rightly expect.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!