Editorial

Welcome to the second issue of the eighth volume of the Romanian Cyber Security Journal. This issue brings together contributors from universities, research teams and industry, writing from Romania and abroad. We thank our authors, reviewers and readers for helping ICI Bucharest build ROCYS into a place where engineering practice and academic research can speak to each other, in support of our work on cybersecurity and the protection of critical infrastructure.

From 10 to 12 March 2026, the Palace of Parliament hosted the Digital Innovation Summit Bucharest, organized by ICI Bucharest under the high patronage of the President of the Chamber of Deputies and the Government of Romania. It combined the ninth Critical Infrastructure Protection Forum, dedicated this year to dual-use innovation for resilient critical infrastructure, with the fifth International Conference on Cyber Diplomacy and the second Blockchain Intelligence Forum on the final day. Several questions raised there, from the use of artificial intelligence in defending infrastructure to the security of energy systems, return in the articles below.

As we write, administrators around the world are still patching PHP. On 21 October the PHP project released fixes for two critical flaws, CVE-2026-109618 and CVE-2026-109619, each rated 9.2 on the CVSS 4.0 scale and each allowing an unauthenticated remote attacker to run code on a server. The first corrupts memory when a request exceeds the memory limit during form parsing, and the second lets state left over from a failed request leak into the next one. The exploit chain, named PHP2Shell and credited by the PHP Foundation to Calif and other teams, two of which said they used AI models, has been demonstrated against WordPress, Drupal, Joomla and Magento. Amazon saw an exploitation attempt on 17 October, four days before disclosure, and on 26 October the US Cybersecurity and Infrastructure Security Agency added both flaws to its Known Exploited Vulnerabilities catalog. Researchers at Delft University have since counted more than 50,000 exploitation requests from over 600 addresses in 70 countries. Some early reports of intrusions were withdrawn, but one researcher's rough estimate of 1.3 million potentially vulnerable internet-facing hosts explains the urgency.

PHP2Shell arrived in a month crowded with supply-chain incidents. A hijacked release pipeline put a credential-stealing version of the LiteLLM package on PyPI on 21 October. Abused application credentials of ConnectWise's cloud backup service were used in automated scripts, beyond the reach of multifactor authentication, against Microsoft 365 tenants, and one security vendor alone found at least 162 compromised tenants among those it monitors. A BeyondTrust Remote Support zero-day, reportedly exploited since August, entered the CISA catalog on 16 October. They also follow 11 September, when the Cyber Resilience Act began to require manufacturers to notify actively exploited vulnerabilities and severe incidents, starting with an early warning within 24 hours through the single reporting platform that ENISA has launched. How that mechanism copes with a



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

flaw such as PHP2Shell, whose component is embedded in products maintained by others, will become clear soon.

Closer to home, Romania has had its own reminders. On 14 July the e-Terra application of the National Agency for Cadastre and Land Registration went offline in a cyberattack that a threat actor claimed involved ransomware, halting property transactions, and it began returning to service in stages on 11 August, first for agency staff, land registry offices and public notaries. In the wider region, on 13 July the United Kingdom and the European Union formally attributed to Russia's Federal Security Service the December 2025 attack on Poland's power grid, in which the DynoWiper malware failed, although officials said success could have left about half a million people without power in midwinter. For a country on NATO's Black Sea flank, four weeks before a single registry began returning to service and a failed attack on a neighbor's grid suggest that recovery capacity deserves as much attention as prevention, and the article below on SIEM-driven incident management addresses part of that question.

The contributions reflect this range. Three address detection and artificial intelligence. One article examines the role of AI in combating cyber threats, another presents intrusion detection in intelligent energy prediction systems for non-residential buildings, and a review of pattern recognition in cybersecurity and information science sets out its issues and challenges. Read beside the researchers' statements that AI models helped them build the PHP2Shell exploit, they show both sides of the technology in one volume.

A second group looks at the systems beneath everyday services. One article treats the security of mechatronic control modules in the context of current cyber threats, another discusses server-authoritative and OpenID Connect approaches to secure player authentication in immersive Unity environments, and a third applies a critical infrastructure and key asset approach to forest management, combining satellite observation, artificial intelligence, drones and private blockchain-based decision support. From the engineering side, a contribution on a repetitive high-voltage pulse generator based on thermally depolarized ferroelectrics extends the issue toward hardware.

Governance and compliance form a third group. One article shows how compliance with the NIS2 Directive can be put into operation through alert and incident management driven by security information and event management (SIEM) systems, which links directly to the reporting duties described above. Another asks what matters for firm value in the relationship between ESG and cybersecurity, and a systemic analysis of internet domain vulnerabilities considers multi-layered mitigation strategies.

We hope you will keep reading and engaging with us. We invite you to publish your research with ROCYS and to join the next events organized by ICI Bucharest, including DISB 2027 on 20-21 April 2027.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!