Editorial

Greetings and welcome to a new edition of the Romanian Journal of Cyber Security (ROCYS). This publication is a landmark for the National Institute for Research and Development in Informatics ICI Bucharest, around which we are building a community of interests and of values on cybersecurity that will enable the sharing of important research. As one of the newer publications of ICI Bucharest, we are hard at work indexing it in new databases and building towards inclusion in the most prestigious scientific and academic database, as for our flagship publications like Studies in Informatics and Control and the Romanian Journal of Information Technology and Automatic Control.

On 8-11 April 2025, our Institute organized the second edition of the Digital Innovation Summit Bucharest. This year it included, among staples such as the Critical Infrastructure Protection Forum and the International Conference on Cyber Diplomacy, also a conference on automotive R&D, a roundtable on European defense, and a conference on the security of intellectual property rights. Cybersecurity permeated the discussions, which featured important panels on the regulation of emerging digital technologies, the changes in the security landscape and the normalization of hybrid threats against civilian critical infrastructure systems (especially in the context of the war in Ukraine). Interacting with experts, businesspeople, government representatives, diplomats and other stakeholders continuously reinforces a series of key lessons that we have assimilated at ICI Bucharest: everybody is affected by cybersecurity threats, everybody is too dependent on networked digital systems to "cut the chord", and everybody is anticipating economic growth, new capabilities and strategic enhancements from the implementation of new digital technologies such as AI and blockchain. Therefore, the cybersecurity issue is not going away; in fact, it is gaining in urgency because of increased exposure to the cyber environment and new avenues for infiltration and attacks. Threat actors are standing up and taking notice, eager for financial gain but also to facilitate strategic goals through cyber-mediated actions for hybrid priming, destabilization and coercion.

In the next period, we are looking forward to a concerted effort at sustainable adoption of AI across wide swathes of the economic and social landscape. Sustainable means not just cost, but also security, resilience and ethics. We will need to develop new tools for certifying AI-based systems as trustworthy, as well as new practices, such as the recognition that high-quality datasets used for AI training are a critical national resource which should be valued as such and protected from theft or "data poisoning". And, of course, the companies that will end up dominating the market for critical AI applications will manage to impose their preferred architecture and standards and will become targets for subversion and supply chain disruption from all sorts of cyber threat actors. Secondarily, we anticipate a big push for post-quantum transition practices. The time for it would have been now,

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

but stakeholders have not caught up to the state-of-the-art like the hackers have. “Harvest now, decrypt later” is a reality, and the “later” is not much later, if we look at the rate of development in quantum computing. Journals such as ROCYS and the community that makes it possible, along with the wider academic-industry-governance nexus, play an important role in the important transformations that are needed for the sustainable adoption of new technologies and for us to enjoy the benefits of digitalization while mitigating the new risks, vulnerabilities and threats.

Another issue that we are analyzing and where we anticipate needs-based growth is in the cooperation between civilian and military entities, including cross-border, in order to manage cyber and systemic risks. The defense stakeholders have unique perspectives on the security environment and also their own reliance on civilian owned and operated infrastructures. Digital technology is fundamentally dual-use and resilience issues will also affect military actors, which can bring to the table important contributions in terms of policy innovation, incident preparedness (tabletop exercises) and actual response capabilities. The mainstreaming of emerging digital technologies such as AI and blockchain are a priority area for these kinds of collaborative approaches, but critical infrastructure protection in general should be one of the main fields of engagement.

With this in mind, we have prepared an interesting line-up of article for you in this issue of ROCYS. Two of our articles are focused on ransomware, the first on automotive and the second on e-commerce platforms. I think we will be hearing a lot about the cybersecurity impact of digitalization in the automotive sector pretty soon, as the number of cars that ship without digital systems dwindles to nothing. Digitalization in healthcare is a priority for ICI Bucharest, so we are pleased to host an article on AI-driven data governance issues in healthcare. On the cybersecurity front, we are pleased to host an article on cyber threats in Big Data and on the cybersecurity implications of quantum key distribution. We have not neglected the issue of governance, with a comparative analysis of the cybersecurity frameworks between Romania and Azerbaijan.

Last, but not least, we are continuing our coverage of the space and cybersecurity nexus, which is receiving significant European attention as it pursues strategic and technological autonomy. Our two featured analyses, on the applications of blockchain technology to space and on the cybersecurity profile of space systems, contribute to our understanding of our critical dependence on the space sector.

We hope that you will appreciate the latest edition of the Romanian Journal of Cyber Security and will remain with us for our publication’s journey of growth.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!