Editorial

It is my pleasure to welcome you to a new edition of the Romanian Journal of Cyber Security. For those who are reading us for the first time, ROCYS is a flagship publication project of the National Institute for Research and Development in Informatics ICI Bucharest, which is the oldest and most important civilian research institute on cyber issues in Romania. With the trust placed in us by our contributors who deliver exciting and substantial reports of their research, we can look forward to a day soon enough when ROCYS will have joined the academic publication elite and be indexed in the most prestigious database, alongside two other journals of ICI Bucharest, Studies in Informatics and Control and Romanian Journal of Information Technology and Automatic Control. Even without such inclusion yet, we have noticed a significant uptick in the amount of interest ROCYS is shown, the readership that the open access model affords us and the quantity and quality of submissions.

It is also helped that, being very close to the core competency and responsibility of ICI Bucharest, ROCYS is the indirect beneficiary of the large number of specialty events that ICI Bucharest organizes and participates in, especially its flagship international event, the Digital Innovation Summit Bucharest, with its numerous component events on critical infrastructure protection, cyber diplomacy, tabletop exercises, hackathons, business expos and more.

Cybersecurity is, of course, on everybody's lips. This is the result, on the one hand, of the global elections year and the undoubted evidence of attempts by malicious actors to target election infrastructure and to use disinformation and fake news to sow doubt and discord. The upcoming US elections are an especially hard fought battleground for cybersecurity, but also the referendum and elections in the Republic of Moldova and in Georgia (which recently digitalized its voting process to boot). This is also the result, on the other hand, of the relentless wave of digitalization in society, economy, the media and in politics.

We are not just exposed to malicious actors motivated by profit, ideology or reasons of state, but also at the whim of vast digitized systems that are mostly automated, and we suffer keenly from a loss of control and agency over our data, our digital identity and our livelihoods. Responding to this anxiety is an important step in regulating cybersecurity effectively, especially when it comes to the emerging digital technologies, otherwise we risk not just failing to improve our security, but also killing the goose that lays the golden eggs by deterring innovation, digital investment, and business. This is what some consider is happening now in the EU, which will affect its capacity to be a normative superpower and export its values and preferred governance approaches to the rest of the world.

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

While such instances of regulatory overreach can be found, especially when prodded by interested stakeholders that want to maintain the status quo (in blockchain for instance), I have reserves against emitting blanket judgements. In the next period, with the adoption by EU MS of legislation derived from the CER and NIS 2 Directives (the deadline being the 17th of October 2024, though most will miss it), as well as the entry into force in 2024 of the Markets in Crypto-Assets Regulation (MiCA) and the Cyber Resilience Act (whose main impact will be seen at the level of SMEs), we will have plenty of opportunity to evaluate the effectiveness and wisdom of EU regulatory approaches.

We have a stellar lineup of articles for this issue of ROCYS. For myself, I am always interested in reading up on emerging digital technologies, and so we have articles on Artificial Intelligence and OSINT, the acceptance of extended reality (XR) technologies, the cybersecurity of quantum networks and using neural networks to identify deviant personality traits in cyber threat detection. For topical issues, ROCYS offers an article on e-governance, one on cybersecurity for space systems, cybersecurity for healthcare systems and cybersecurity in IoT systems. Lastly, we have an article on the contribution of the R&D processes in the military domain to regional economic growth.

We thank you once again for being with us and look forward to our continuing conversation with you as readers, contributors and fellow researchers.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!