



# Editorial

Welcome to a new edition of the Romanian Journal for Cybersecurity. This is a part of ICI Bucharest's extensive offerings in the area of academic publishing. With your help, we are steadily growing ROCYS into a well indexed purveyor of quality research in support of our extensive community of experts who are not just readers, but also partners and maybe even future contributors.

It is already a cliché to speak of the importance of cybersecurity. The war in Ukraine and the constant hybrid warfare throughout the world prove that cybersecurity threats are omnipresent and constantly evolving. We must evolve with them or risk getting left behind and suffering massive disruptions to our critical infrastructures, in addition to loss of confidence, and interruption to business continuity and falling quality of life. The new issue of ROCYS has an impressive line-up of articles, analyzing everything from “electronic trench warfare” in Ukraine and the Romanian cybersecurity posture, to the security of Metaverse applications and of eHealth services. I want to briefly pause on the former term, as it was new even for us. Electronic trench warfare is a new concept expressing the constant battlefield innovation in terms of cyber and electronic warfare, both in defense and in offense, in which not necessarily expert practitioners engage using commercially available and sourced hardware and software. This constant striving for advantage is a part of warfare, including of the static combat which we seem to be headed towards in Ukraine. However, the knowledge base gained in this way can easily pass the gulf from armed forces to criminal organizations and terrorist groups. We might, in a few years, recognize that this development was ushering in a new age for electromagnetic spectrum threats to critical infrastructures from irregular forces, and also to individuals and general society. The loss of communications for coordination and systems' data exchanges, especially for industrial control systems, can be devastating. I, for one, wish to see this concept explored further.

The main topic for a larger number of our articles in this new issue of ROCYS focuses on security issues for blockchain applications, from the security of smart contracts to that of consensus mechanisms in networks, the establishment of a national data analysis platform to ensure financial stability and national security, as well as account abstraction on the Ethereum network. We never tire of reminding people that blockchain goes beyond cryptocurrencies and financial speculations. Even if the market for these is in a downturn, blockchain continues to insert itself seamlessly into our lives, through key applications related to data access management, logistics tracing and more.



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



As a technical solution to the age-old problem of concentration and costly intermediaries, we have not yet begun to scratch what we can do with distributed ledger technology. The cybersecurity issues are real and go beyond financial fraud, reaching into the area of systemic disruptions of critical infrastructures. We must strive to understand the impact that blockchain technology has on our critical infrastructure systems, especially on industrial control systems and SCADA, wherever the application is feasible to use. And whatever vulnerabilities we find must be addressed before significant changes to infrastructures are made that will compound the risks facing our societies.

ICI Bucharest is especially interested in the topic as, through its Blockchain Software Development Laboratory, its Blockchain Executive Laboratory and its European Center for Excellence in Blockchain, our Institute is becoming immersed in the blockchain industry, not just as a dispassionate academic observer, but also as a player trying to provide key products and services, especially to state actors. Our commitment was proven by the inauguration of the first working European Blockchain Services Infrastructure (EBSI) node in Romania at ICI Bucharest. Our latest development is ICI D|Services, an institutional NFT (non-fungible token) marketplace which already has NFTs from the Romanian Post Office, the Romanian Olympic Committee, museums, and various other cultural bodies. However, and we hope we do not jinx it, the underlying infrastructure can also be adapted for governance use, with land deeds, birth certificates and more, once the competent state institutions move past their conservatism and decide to at least keep up with our European partners.

Lastly, we round out our roster of materials with an article on quantum key distribution applications and on the new ICI Bucharest platform for fostering disruptive emerging technology exploration and use.

We hope you enjoy this new issue of our academic journal and look forward to meeting you at various events and receiving your own research results to publish in ROCYS or other ICI Bucharest publications.

**ENJOY THIS JOURNAL**  
**WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!**