Editorial

Welcome to a new edition of the Romanian Cyber Security Journal (vol. 5, issue 1/2023). ROCYS is one of ICI Bucharest's newer products, but is also entering its fifth year of publication. The quality of our publication has risen continuously, and we look forward towards indexing it in increasingly more important databases, thereby providing more exposure to our featured research and raising the profile of Romanian scientific publishing.

Cyber security is intimately linked with the "permacrisis" of recent years. From the pandemic to the war in Ukraine, the cyber environment has continuously acted as a medium for the transmission of risks, for the cultivation of vulnerabilities and for the propagation of disruption. Bad actors, from lone wolves to organized crime and state-sponsored entities have attempted to advance agendas, to generate profit or to destabilize adversaries by attacking critical cyber systems linked to critical infrastructures. We have seen it in energy, in public administration, in supply chains and even in hospitals, the latter being especially relevant given the stresses of the pandemic. The cyber threats have evolved in line with the priorities of the perpetrators and in response to system shifts and defense measures implemented by the potential victims, who are increasingly coordinating to achieve a better response and to share best practices. Trends include a rise in ransomware, more attacks on supply chains, broken access control pathways, crime-as-a-service and more. Stakeholders are responding by increasing investment and committing to processes that increase security and resilience in enterprise systems and in public administration. As ever, the initiative is with the attackers, not the defenders. Concepts such as "zero trust" are meant to stir efforts at reforming organization-based approaches towards cybersecurity, but more is needed, including an exploration of the security consequences of remote work, as well as means to avoid turning actions such as penetration testing into box checking for the sake of compliance with a security audit. Getting safely past the tumultuous period of digitalization and widespread implementation of emerging technologies will require, from a critical infrastructure perspective, not only an "all hazards" approach, but also an "all hands on deck" approach.

This issue of the Romanian Journal Cyber Security has a diverse roster of contributions, possibly the most diverse we have ever had. They explore different facets of the cyber security conundrum. Topics include emerging digital ecosystems and applications for institutional non-fungible tokens, applications of data management plans in the healthcare sector, a comparative analysis of EU and US cyber

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

diplomacy approaches and the issue of cyber security in the energy sector. We would note that contributors also approach sensitive topics such as the issue of values in strategic frameworks for cyber security, as well as the cyber security of space infrastructures. The former is a necessity in our race to harmonize our new technological capabilities with our values, culture and expectations regarding privacy, personal safety and the prevention of abuse. The latter is an exciting new frontier on which every state, whether it is spacefaring or not, must set its eyes given our reliance on space infrastructures for a wide variety of critical services. We continue our exploration of technical issues through contributions on ransomware applied to MacOS devices and on AI for enhanced email security.

As you can see, we are striving to increase quality and to make ROCYS a mainstay of ICI Bucharest's effort at developing and promoting a community of cyber policy, expertise and capability, composed of publications, products, networks and events. With this in mind, we are pleased to remind our readers that, on the 25th of April, ICI Bucharest will organize a new edition of the International Conference on Cyber Diplomacy at the Romanian Palace of Parliament, while 26 and 27 April will be dedicated to the Critical Infrastructure Protection Forum, organized with IDEA Factory and wide institutional support, including from the Romanian Parliament. These two events, which we intend on holding each year, give continuity to our contacts and efforts in two key interests of ICI Bucharest, for which we are also developing products and centers – critical infrastructure protection and cyber diplomacy. The CIP Forum is in its sixth year of organization, and has become the most important event of its kind in South Eastern Europe and a relevant forum for discussion on pressing issues related to resilience. The International Conference on Cyber Diplomacy is in its third year, but we plan on supporting it for a long time and building a community of interest on this critical topic.

That being said, we want to thank you for being part of our community and for reading the Romanian Journal Cyber Security. We hope that you find the contributions useful and that you continue being a member of our growing community.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!