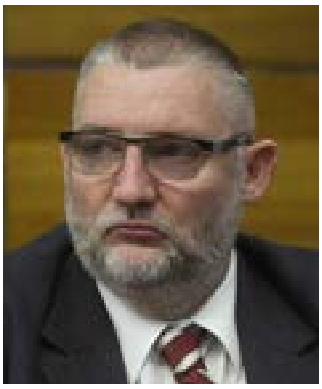
Editorial

On behalf of myself, my colleagues and all of our contributors, I would like to thank our readers for their continuing support for the Romanian Journal of Cyber Security. ROCYS is becoming a valuable product and a flagship for the efforts of ICI Bucharest to contribute to the evolving conversation on cybersecurity that has become a priority for every country in the world.

Contrary to expectations in this period of significant uncertainty and economic and logistic upheaval, cyber-attack frequency has increased, aggravating the impact of the general systemic crisis. This phenomenon also emphasizes the potential that cyber affords adversaries, to heighten and prolong crisis periods through targeted attacks. The increase in cyber-attacks can also be explained through the increased surface contact between the physical, economic, political and social world and the cyber environment. The pandemic has increased the frequency and extent to which we work from home, it has riveted students and teachers in front of the computer screens, but also doctors and patients. Meanwhile, online shopping shatters new records at a regular pace. Since more and more of our lives are mediated by cyber systems, it is to be expected that the frequency and impact of attacks should rise, especially since there is no indication that there has been a commensurate rise in cybersecurity culture, awareness and investment.

The cybersecurity trends, as revealed by industry reports, are taking us into novel, though foreseeable, directions. Remote working was bound to become a headache for security departments all over the world, but now we are witnessing more sophisticated forms of social engineering attacks. Phishing is now done over messaging services (smishing) where (hopefully) ingrained reflexes regarding emails have not reached the same level. There is also a new phenomenon called vishing, where hackers call the customer service representatives of a company and pose as IT staff to obtain access. This happened to Twitter, but it is likely already widespread. The key structural change is the rise in threats to mobile systems, which we do not protect nearly as well as computer systems (even if it is still below what is needed) but which account for more and more of our engagement online, whether working, communicating or shopping. This perennial lag between the depth and breadth of the use of a new medium of communications and the quality of the security attention we invest in it is a permanent source of tensions and vulnerability. Ultimately, it comes down not to technology or even resources, but to



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

behavior or, in a wider sense, to culture. Hopefully, ROCYS will make its own contribution to the expert exchanges that will trickle down towards companies and individuals and ultimately increase general cybersecurity levels.

In this issue, we have an impressive line-up of articles, especially notable for their variety. Foreign contributors have shared with us research on e-policing, on scenario analysis for the impact of digitalization and on the use of blockchain technology for the resilience of disaster aid networks. We are also pleased to be contributing to the multidisciplinary study of cybersecurity through an article on the analysis of emotional states driving phishing susceptibility as measured by physiological indicators. This contribution is part of an emerging body of work on behaviorism that will have an important impact on cybersecurity research and especially on resilience enhancing measures. The selection of articles is rounded up by entries on human-machine interfaces, on mobile forensic tools, on global legislation for cybersecurity and on the storage of claims on blockchain networks.

We hope that you will continue to be alongside us on our journey to develop ROCYS as a quality publication in the region and beyond. We have exciting projects lined up to not only expand the scope and reach of ICI's publications, but also to fully utilize them to build a network of experts and entities that can produce not only valuable research and policy ideas, but also advocacy for more secure systems and networks.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!