Editorial

Welcome to the new issue of the Romanian Cyber Security Journal. Our journal is in its fourth year and is well on its way to becoming a flagship product for ICI Bucharest, tying together an ever wider community of research and policy expertise with the purpose of exploring the fascinating and rapid evolutions in the cyber threat environment in the context of the rapidly digitalizing world. The pandemic has accelerated trends in the digitalization of public administration, education and labor which had been evolving steadily for years, and the gradual shift away from the pandemic in the public consciousness does not detract from the significant transformations which have already taken place. Cybersecurity is more important than ever, and our knowledge, training, resources and innovation capacity must keep pace with the cyber threat environment.

This is our second issue since the Russian invasion of Ukraine upended expectations that large-scale conventional warfare was a thing of the past, at least in Europe. However, as we know also from evolutions within NATO, with its declaration of cyber and space as operational domains, the resurgence of conventional and attritional warfare does not invalidate our fears of increasing cyber threats. Rather, it accelerates them, as adversaries focus multiple "streams of fire", including cyber, onto the battlefield. They spill also beyond, as parties not engaged in the hostilities are nevertheless targeted for their positions on sanctions and other issues. While we have and will see physical attacks against infrastructures, the best cost to benefit ratio for attacks on our critical infrastructures are still afforded by cyber-attacks. These attacks will come not only from state actors and state-sponsored proxies, but also from ideological groups, lone wolves and organized crime groups with a profit motive. The boost to digitalization that I have previously mentioned also served as a boost for the surface contact between key infrastructures, institutions, systems and an increasingly perilous and chaotic online environment. If anything, I would posit that all of these attackers feed off each other, since there is a vicious feedback loop between increasingly frail systems and opportunistic actors undermining them even more. Along with these systems, we also see the undermining of trust in state institution and state and private companies.

The good guys are not standing still, however, though we can always complain about the pace of progress. Since last we spoke, we have obtained a political agreement in the EU on the NIS 2 Directive, whose initial draft had been published in December 2020. Along with the Critical Entities Resilience Directive, with which it shares a domain list for critical entities in energy, finance, health and others (proving that

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

cyber is truly ubiquitous), they provide a welcome enlargement of the EU framework on increasing our security from cyber-attacks and other threats while also underscoring the cross-border interdependencies that heighten and lengthen crises.

We have a stellar line-up of articles for this issue, on a wide variety of subject, as befits the digitalization of everything and everyone. Topics of significant interest are pursued, such as the issue of AI applications for increasing the capacity of 5G communication systems, investigation tools for Software-as-a-Service and the investigation of alerts in digital enterprises. This issue of ROCYS also includes reviews of cybersecurity in railway systems and of the European High Performance Computing landscape. Continuing the enduring interest on the part of ICI Bucharest in approaching issues related to cultural infrastructure, we are hosting an article on on innovative system for preservation and valorization of the Romanian Literary Heritage. Of the remaining articles, we would also highlight one with a focus on governance and policy issues, regarding the introduction of the profession of Cybersecurity Specialist for automated command-and-control systems in the Romanian Classification of Occupations. This is very important, since the authorities in any country can be either a great help in advancing cybersecurity or a great hindrance, and they themselves are an important source and destination for cybersecurity products, services and expertise. Making sure that the institutional, administrative and legislative frameworks of the state are keeping pace with the rapidly developing needs of the digitalized society is a constant preoccupation, and introducing such a profession will ultimately allow for increased standards, greater professionalization and the encouragement of continuing education of cadres in this field of maximum importance. Coming back to our discussions of the grave threats we face, industrial control systems will emerge as a favored target for actors seeking to sow maximum disruption, to generate economic damage or worse and to demoralize our societies.

I urge to read these articles and all of the others included in this edition of the Romanian Cyber Security Journal and to consider interacting with us to develop this publication further with presentations of your research and with your involvement in ICI Bucharest's significant line-up of publications and events that all point towards a single goal – greater national and collective security in an ever more challenging world.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!