Editorial

We are pleased to welcome you to a new edition of the Romanian Cyber Security Journal. This is a high-quality product of ICI that we are developing with the support of a growing community of contributors to advance discussions on cybersecurity and to integrate Romanian expertise with the global community of academics and experts. Cyber issues are global, and we can no longer persist in parochial modes of organization and information exchange, with only cursory contacts with the evolving global conversation on these issues. Romania's roles as regional leader in ICT-related economic sectors must be balanced by a corresponding weight of effort in the cybersecurity realm, or else the digitalization of processes and systems and the digitization of data will lead to an unmanageable increase in risks, vulnerabilities and threats.

This is all too pertinent, because this is the 4th Volume (1st issue) of ROCYS, but the first in the new world of the return to conventional warfare in Europe, right on Romania's doorstep, through the war of aggression waged by the Russian Federation in Ukraine. While rockets and tanks take center stage in news media, we know very well that no war is purely conventional anymore and that, in the backstage of the armies and only seldom glimpsed in the media, and then only on the surface level, there is a ferocious cyber war that targets not only Ukraine, but also NATO and EU countries, both to disrupt capabilities, but also to deter increased assistance to Ukraine. Cybersecurity matters more than ever before, and this is a power law of the rate of digitalization in society. It will matter even more tomorrow and so on, for the foreseeable future. One thing that is not discussed publicly, or not yet at least, is how inter-state conflict also breeds the proper environment for the manifestation of a wider variety of threats. It is the same in cyberspace, where non-state actors are increasingly being felt, as hacktivists, transborder organized crime groups, lone wolves, some of them acting as state proxies, and empowered by the disruption of hostile state actors. We may eventually see a global cyber escalation, encompassing not only the West, but also the states on the sidelines of the conflict in Ukraine, such as those in Asia, Africa and Latin America.

We must not only research cybersecurity as a reactive measure, but also as an element of the design of the new digital systems, and especially of cyber-physical systems, which soon enough will also include household appliances for the average family and supporting systems for our daily lives, all the way down to the most mundane and yet potentially disruptive.

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

It is for this reason that we have mobilized a truly interesting selection of blind peer reviewed articles, featuring a mix of strategic, technical and policy-oriented materials. We would point out an article on industrial traffic control systems and communication protocols, that is surely a timely addition to the discussions on logistics and the strain on transborder critical infrastructure systems, especially with the lingering effects of the pandemic.

Continuing our series of analyses on malicious actions, we feature an article on watering hole attacks. Romanian cyber strategic thought is also analyzed, which is of immense importance given the speed with which the security environment is changing, proving that policymakers need not only to update their mental models but also work to keep the structural foundations of state-determined cybersecurity abreast with the new demands of the cyberspace threat complex. Cryptography is an area of especial interest, both for confidentiality and also for security from malicious actors, and we feature an interesting article that advances our journal's growing relevance in this field.

Moving forward, we anticipate a full schedule of events at ICI Bucharest pertaining to cybersecurity, allowing us to keep in touch with and expand our community of individual and institutional partners. Our publications are an integral element of this approach. In the very next period, we will be organizing two courses for experts from European and national institutions under the aegis of the European Security and Defence College, one on Cyber Diplomacy in May and one on Critical Infrastructure Protection in June, featuring tabletop exercises and the latter also benefiting from a partnership with the European Union's Joint Research Centre. Needless to say, cybersecurity is an integral part of both of these courses. We will be organizing a conference on Cyber Diplomacy in May and, after a long pandemic-induced pause, we will resume the Critical Infrastructure Protection Forum with high level international attendance, to be organized in June at the Palace of Parliament.

Extraordinary times call for extraordinary efforts and cybersecurity is no exception. Yet, we must be prepared to accept that this is the new normal and adapt the tempo of our efforts to this new reality, striving for cooperation, research, perspective sharing and, ultimately, coordinating collective action through a wide array of stakeholders, from industry and academia, to civil society, diplomacy and even educational institutions for our children.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!