Editorial

I would like to express our gratitude to our community of contributors and readers for making the Romanian Journal of Cyber Security (ROCYS) an ongoing success story. Having entered our sixth year of publication, we can state that journal's visibility is growing and this is reflected in the success of our efforts to have it indexed in as many reputable databases as possible. The quality of the article we publish issue after issue requires us to do no less than to ensure that ROCYS is visible at the highest level, just like the legacy publications of ICI Bucharest such as RRIA and SIC. With your help, through your continued engagement with our publication, we can make ROCYS into a landmark journal for the region and a contributor to the growing academic excellence of Romania in the ITC sector.

2024 will be a landmark year, the year of democracy. The ten most populous countries in the world will have elections this year, including India, the US, Pakistan (which has already had its elections) and more. 2024 is not just an election year. It is perhaps THE election year. Globally, more voters than ever in history will head to the polls as at least 64 countries (plus the European Union)—representing a combined population of about 49% of the people in the world—are meant to hold national elections, the results of which, for many, will prove consequential for years to come.

Elections include national, European, legislative, executive, federal and provincial. As we have seen in Taiwan, elections can truly mark a particular course for a nation. For others, such as Russia, the results seem pre-ordained. At the moment of the writing of this editorial, Romania, which is the home of ICI Bucharest, is headed towards its busiest electoral year in history, with absolutely every possible election taking place in 2024.

What is certain is that elections and cybersecurity are indelibly linked. Many countries now use voting machines, some sort of networked collation of votes, digital databases of voters, digital verification of registration and ID and many more examples of digital electoral infrastructures. Despite the risks, the use of such solutions is set to grow because of transparency and lower costs, as well as added security for non-cyber risks such as fraud. However, these systems are more and more under attack by hackers and other malign actors trying to either sway elections or simply delegitimize them in the eyes of the respective populations and the world. At the same time, malign actors are using the Internet to increase polarization, to push fake news, misinformation, and disinformation. The results are obvious and are not confined to developing nations. The US has seen accusations of hacked voting machines ever since their introduction, garnering

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

greater visibility in the contested 2016 and 2020 elections (and likely the 2024 ones too). The fear that Russia may have "hacked" the 2016 elections, whether directly or through disinformation, has poisoned the political well for a generation in the US and led to a significant decrease in trust in the political system.

This cannot be allowed to happen in other countries or to continue in the US, where it ultimately affects not just its internal politics, but also its capacity for foreign policy. Decision makers must establish trust in voting solution vendors, in collation systems, in digital voter rolls and in the voting process itself. To do anything is to submit to certain upheaval. This year, we see whether we can truly master digitalization or if it will put the bridle on us, along with every malign actors looking for profit, disruption or geopolitical gain.

We have an exceptional line-up of articles in this issue. As usual, we have a significant variety of topics. Members of our community are aware of ICI Bucharest's strong interest in blockchain – we have three papers on this topic, one on smart contract vulnerabilities, one on hybrid smart contracts with decentralized oracles and the last on data privacy and data security. We continue our exploration of AI and machine learning with papers on vulnerability analysis for AI proposed random number generators and on trojan detection through deep learning techniques. Cybersecurity in space is another topic that will become more and more salient to the wider public in the future. Having discussed the issue of disinformation and polarization swaying elections, we have to mention this issue's papers on textual deepfakes and on digital technologies to combat disinformation and fake news.

Also relevant for the election year is the paper on the use of open-source intelligence in penetration testing. Lastly, we have a profile on a new project that empowers national cybersecurity, a project which ICI Bucharest is also a part of.

Once again, thank you for being with us issue after issue. Paraphrasing the German philosopher Oswald Spengler said, in his work on the effects of technology on man, optimism is cowardice when it comes to cybersecurity. What is needed is a clear head, clear eyes and the will to persevere in the realms of technology, finance, culture and policy. As seen in the recently concluded Digital Innovation Summit Bucharest, our largest event yet, ICI Bucharest is firmly planted on the road towards resilience and security. Stick with us.

ENJOY THIS JOURNAL

WE HOPE IT WILL MAKE A DIFFERENCE TO YOU!