CyberCon Romania 2022 Conference - Welcome Message

Professor Ioan C. Bacivarov, PhD
President of the Romanian Association for Information Security Assurance (RAISA)

Ladies and gentlemen, first of all, I would like to extend to you, as President of the *Romanian* Association for Information Security Assurance, a warm welcome to the *CyberCon Romania 2022 Conference.*

I would like to express our special thanks for the support given in organizing CyberCon Romania to the Embassy of the United States of America in Romania, to the main national bodies involved in the field of cybersecurity, such as the Romanian National Cyber-Security Directorate, the Romanian National Cyberint Center, the Romanian Police, as well as all the other organizations involved in this sensitive and important area, whose names are mentioned on the CyberCon website.

Special thanks are due to all the important experts in the field, who will present their views during the conference and will thus contribute to shaping a realistic picture of the challenges, risks and solutions in the field of cybersecurity, in the very difficult international period we are going through.

The *Romanian Association for Information Security Assurance (RAISA)* **-** the main organizer of this conference - is a professional, nonprofit and public benefit association, founded a decade ago, as an initiative dedicated to disseminating the concept of cybersecurity and fighting against cybercrime.

The vision of RAISA is to promote research and education in information security field, to contribute to the creation and dissemination of knowledge and technology in this domain and to create a strong "cybersecurity culture" at national level.

Among the notable activities developed by *RAISA,* we mention the publishing of *International Journal of Information Security and Cybercrime (IJISC),* a scientific journal indexed in international databases (and I would like to invite the specialists in the field to publish in this journal the results of their researches), awareness websites, workshops, research projects and studies in the field of cybersecurity.

We are aware that the achievement of a strong "cybersecurity culture" at national level can be achieved only through the joint effort of several entities from the public, private and academic sectors.

I am working as a Professor in the field of Quality and Dependability (reliability, security, survivability, resilience a.o.) at the Faculty of Electronics, Telecommunications and Information Technology of the most important Romanian technical university, the University Politehnica of Bucharest. From this position I coordinated several research and educational postgraduate programs in the field, programs in which to cyber-security is given a special position: I want to mention in this regard the Master program *Quality and Dependability in Electronics and Telecommunications*, which has been running

successfully for 25 years. There is a high demand for highly trained cyber-security specialists, and the Master's programs of the type listed can of course help to solve this problem.

As I already mentioned in my previous papers, it is important to underline that while organizations continue to purchase and deploy technical controls, not much has been done to focus on the *human side of cybersecurity* - so named *layer 8*. The term layer 8 is often used by the IT professionals to refer to employees' lack of awareness and a weak overall cybersecurity culture. Today, it is just as important to secure *human assets - layer 8 -* as it to secure layers 1 through 7.

I would like to emphasize that the issue of cybersecurity is very important, at present, for military structures, but also for civilian ones. It is useful to mention that - six years ago NATO recognized the cyberspace as an operational domain. A Cyberspace Operations Centre was created at the heart of the NATO military command structure, too.

Digitalization presents tremendous opportunities for businesses, but also increases cyber risks. I would like to mention the recent series of distributed denial-of-service (DDoS) attacks targeting several public websites managed by the Romanian state entities, claimed by the pro-Russian group calling themselves Killnet. As was mentioned during the recent European Cybersecurity conference, when cyberattacks hit infrastructures that are critical to the functioning of our economies and of our societies, they do not only disrupt our networks; they directly put at risk the lives of the citizens.

All these comes to prove the topicality and importance of cybersecurity in the current period and to highlight the importance of scientific forums in which specialists in the field to debate and seek to find solutions to these pressing problems, as is the CyberCon conference. The conference *CyberCon Romania 2022* aims to raise the level of awareness, embodies the cybersecurity culture, and share best practices in fighting cybercrime.

Finally, we would like to thank all the authors who submitted their work, all experts participating in the panels, and all those who contributed to the Conference with their efforts and support. We hope that the *CyberCon Romania 2022* Conference will be a both stimulating and enjoyable forum in which to share current results and trends in cybersecurity and we wish it every success.

More information about *CyberCon Romania 2022* Conference can be found on the webpage https://cybercon.ro/.