Romanian Association for Information Security Assurance

THE INTERNATIONAL CONFERENCE

CyberCon Romania

2022 EDITION

HIGHLIGHTS

PARTNERS

U.S. Embassy in Romania

Romanian National Cyber Security Directorate

Romanian National Cyberint Center

Romanian Police

Romanian National Institute of Magistracy

Romanian Banking Institute

European Institute of Romania

CyberCon Romania conference focuses on the latest trends, challenges, and future strategic directions related to the cybersecurity field. It brings together relevant experts from public institutions, private companies, universities, and NGOs, for raising awareness level, strengthening the cybersecurity culture, and sharing best practices in fighting cybercrime.

Website: https://www.cybercon.ro

TABLE OF CONTENTS

WELCOME MESSAGE

Ioan C. BACIVAROV
President, Romanian Association for Information Security Assurance (RAISA)
Professor Emeritus, ETTI Faculty, University Politehnica of Bucharest, Romania
https://www.raisa.org

Ladies and gentlemen,

First of all, I would like to extend to you, as President of the *Romanian Association for Information Security Assurance (RAISA)*, a warm welcome to the *Cybercon Romania* conference. I would like to express our special thanks for the support given in organizing *Cybercon Romania 2022* to the *U.S, Embassy in Romania* and to the conference partners, such as the *Romanian National Cyber-Security Directorate, National Cyberint Center, Romanian Police*, as well as all the other organizations involved in this important area, whose names are mentioned on the conference website.

Special thanks are due to all the important experts in the field, who presented their views during the conference and contributed 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. 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.

Digitalization presents tremendous opportunities for businesses, but also increases cyber risks. As was mentioned during the recent European Union cybersecurity conferences, when cyber-attacks 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 Romania* 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 to the scientific side of this conference, all experts that presented in the panels, and all those who contributed to the conference with their efforts and support. We hope that the *Cybercon Romania 2022* online conference was both a stimulating and enjoyable event which provided the latest results and trends in cybersecurity.

SECTION I: DEVELOPING CYBER DEFENCE AND CYBER RESILIENCE

Speakers:

- **Ioan BACIVAROV**, President, Romanian Association for Information Security Assurance (RAISA)
- **Megan BISHOP**, Economic Officer, U.S. Embassy in Romania
- **Anton ROG**, General Director, National Cyberint Center
- **Adrian DUȚĂ**, Vice-President, Euro-Atlantic Centre for Resilience (E-ARC)
- **Liliana MUȘEȚAN**, Head of Cybersecurity Unit, General Secretariat of the European Council
- **Daniel FIOTT**, Security and Defence Editor, EU Institute for Security Studies (EUISS)
- **Horațius GÂRBAN**, Training Manager, European Security and Defence College (ESDC)
- **Florin POPESCU**, Associate Professor, "Carol I" National Defence University (UNAP)

Moderator: **Dan CÎMPEAN**, Director, National Cyber Security Directorate (DNSC)

Dan CÎMPEAN
Director, Romanian National Cyber Security Directorate (DNSC)
https://www.dnsc.ro

MODERATOR

It goes without saying that setting out and implementing a simple and straightforward plan is a cornerstone of cyber resilience and cyber defence at national level. We need a plan to animate and leverage upon a task force of active promoters, thought leaders and experts that shall bring to the attention of policy and decision makers the need for reaching an increased level of cyber education and awareness, for projects to demonstrate and accelerate adoption of good practices, for information sharing and promoting the most successful cyber security initiatives and best practices. Closer cooperation is instrumental, so bringing together key actors from public institutions, private companies and academia is a must for having a strong cyber security ecosystem.

Ioan C. BACIVAROV
President, Romanian Association for Information Security Assurance (RAISA)
https://www.raisa.org

In the current context, 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. Consequently, is of crucial importance for all the countries, professional organizations, and companies to consolidate a powerful "cybersecurity culture". In this context, one of the main objectives of the Romanian Association for Information Security Assurance is to support research and education in the field of cybersecurity in Romania, for a better cyber defence and resilience.

Megan BISHOP
Economic Officer, U.S. Embassy in Romania
https://ro.usembassy.gov/ro/

Megan spoke about major trends in cybersecurity defense and resilience regarding the U.S. and its allies, including NATO and EU countries. She talked about how the U.S. has prioritized its efforts toward an increased level of cybersecurity in the current geopolitical context. Through the creation of the Department of State's Bureau of Cyberspace and Digital Policy (CDP) in April 2022, the Department has elevated cybersecurity as a priority in today's increasingly digitalized environment. Megan also underscored the importance of Romania-U.S. cyber cooperation in the coming years and highlighted that the role of the private sector was key in maintaining security through increased information sharing and cooperation with national governments.

Florin PANĂ
Head of the Analytical Department, National CYBERINT Center
https://www.sri.ro

The National CYBERINT Center (CNC) within SRI works to prevent, detect and mitigate cyber threats against Romania`s national security. These are mainly state sponsored, financially and ideologically motivated cyber-attacks. In the context of the current military conflict, the websites of several private and public entities in Romania faced multiple DDoS attacks. Given their scale, although SRI was not responsible to ensure the cyber security of the websites, CNC fully supported the investigations conducted by the responsible authorities. To raise the national awareness, CNC constantly publishes CYBER Bulletins and public statements regarding cyber-attacks that encourage public-private partnerships and contribute to national cyber educational programs.

Adrian DUȚĂ
Vice-president, Euro-Atlantic Centre for Resilience (E-ARC)
www.e-arc.ro

Cyberspace is an environment characterized by insecurity and asymmetry, and anyone can be a target of a cyber-attack, which is why it is necessary to ensure cyber resilience. But Cyber Resilience is difficult to be achieved because cyber infrastructure is vulnerable to a wide range of threats and vulnerabilities. As an inter-institutional hub supporting and participating directly to the development of concepts, doctrines and analyses in the field of resilience, E-ARC supports the efforts to increase the resilience of population to cyber threats, and assesses that in order to build a cyber-resilient society, nations have to invest in: Human resources, Redundancies, Flexibility, Implement Fail Safe Systems, Rapid Rebound Capabilities and Lessons Learned process.

Liliana MUȘEȚAN
Head of Cybersecurity Unit, General Secretariat of the European Council
www.consilium.europa.eu

In cybersecurity, the time is now. It is imperative that we act given the current geopolitical security context that urges us to rethink how to fend off the cyberattacks. What we need to do is to adapt our approach to overcome these changeable threats. The key is to mobilise our full potential by taking cyber out of its tech silo and putting it at the core of our security and defence. This is what we are doing in the EU today. We are tapping into the immense potential of cybersecurity expertise, knowledge and information across our 27 Member States. Neither the institutions, nor the private sector can defend our core business alone. It is going to be a shared mission to build together our capacity and our skills, to be prepared to deter and respond to cyber and hybrid threats.

Daniel FIOTT
Security and Defence Editor, European Union Institute for Security Studies (EUISS)
https://www.iss.europa.eu

Cyber defence and resilience are an essential part of the way the EU strives for security and defence, and it is a policy and technology domain that crosses the boundaries between internal and external security. The recently endorsed EU Strategic Compass for security and defence stresses the importance of cyber defence and it calls for the Union to build up its cyber defence policy to meet the challenge of global strategic competition. To this end, the EU will lower its technological dependencies and ensure that it frequently conducts cyber exercises as part of its broader preparedness efforts. Through its cyber posture, the Union also recognises that the protection of critical digital infrastructure is a hallmark of power and defence.

Horațius GÂRBAN
Cyber Defence Training Manager, European Security and Defence College (ESDC)
https://esdc.europa.eu

When we are speaking about cooperation in the cyber domain, there are several key aspects to be taken in consideration. None is less important, and cooperation should be developed, understanding the crosscutting interaction with any other domain. Starting from any small organization or company (resilience plans, strong cyber-awareness education on all levels), crossing the governmental sector (good and updated cyber-strategies and policies), and going to international actors (developing strong pools of capabilities in region, trust and stability), cooperation is a must. Another important aspect is the civilian-military cooperation, which should be highlighted especially in crisis and resilience cooperation programmes, continuously trained and maintained.

Florin POPESCU
Associate Professor, “Carol I” National Defense University, Romania
https://www.unap.ro

Today’s culture of security needs a cyber innovation ecosystem. The companies need to get creative about how and where they find the next cyber experts. This could be achieved by partnering with local schools and funding more science, technology, engineering, and mathematics programs, creating more internship opportunities for early talent, or launching a robust upskilling or retraining initiative internally. Cyber innovation ecosystem should involve universities or institutes playing a leadership role in R&D, funded in partnership with the government and/or private industry. Romanian Academia environment should be encouraged to offer these partnerships, a place to convene and experiment in a rich setting with a diversity of technical, business, and advanced technology.

SECTION II: INTERNATIONAL COOPERATION FOR FIGHTING CYBERCRIME

Speakers:

- **Philipp AMANN**, Head of Strategy, EU Agency for Law Enforcement Cooperation (EUROPOL)
- **Ionuț STOICA**, Head of Sector, EU Agency for Law Enforcement Training (CEPOL)
- **Silvia PORTESI**, Cybersecurity Expert, EU Agency for Cybersecurity (ENISA)
- **Yvonne SERRATO**, Cyber Assistant Legal Attaché, Federal Bureau of Investigation (FBI)
- **Cătălin ZETU**, Head of Bureau, Central Cybercrime Unit, Romanian Police
- **Sorin STĂNICĂ**, Head of Bureau, Research and Crime Prevention Institute, Romanian Police
- **Thomas DOUGHERTY,** ICHIP Attorney, U.S. Embassy in Zagreb, Croatia
- **Chris STODDARD**, Expert, National Cyber-Forensics and Training Alliance (NCFTA)

Moderator: **Virgil SPIRIDON**, Head of Operations, Cybercrime Programme Office of the Council of Europe

Virgil SPIRIDON
Head of Operations, Cybercrime Programme Office, Council of Europe
www.coe.int/cybercrime

MODERATOR

Council of Europe has a global action on cybercrime which promotes international legal standards (Budapest Convention-most relevant international treaty on cybercrime and e-evidence) backed up by capacity building support for criminal justice authorities. Moreover, the Cybercrime Convention Committee (T-CY) which is the follow up mechanism on the implementation of the Budapest Convention brings together cybercrime experts from members to the Convention for assessing cybercrime global challenges. As a major highlight, T-CY coordinated for the last four years the negotiations of the Second Additional Protocol to the Budapest Convention, on enhanced cooperation on cybercrime and e-evidence.

Philipp AMANN
Head of Strategy, European Cybercrime Centre, European Union Agency for Law Enforcement Cooperation (EUROPOL)
https://www.europol.europa.eu

Cybercrime remains a top threat within the European Union and beyond, and continues to cause significant damage, disruption and financial losses. With criminals seeking to maximise their illicit gains and operating across borders and from different jurisdictions, a networked response is required based on international cooperation and supported by the necessary legal frameworks. This must include law enforcement, industry, the CSIRT community, academia and public-private-partnerships, such as the *No More Ransom* initiative. The *No More Ransom* is an initiative of law enforcement agencies and cybersecurity companies, with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

Ionuț STOICA
Head of Sector - CEPOL Cyercrime Academy, European Union Agency for Law Enforcement Training (CEPOL)
https://www.cepol.europa.eu

Training and education are important factors in the fight against cybercrime and the approach should be coordinated and sustainable at EU level. The EU Agency for Law Enforcement Training (CEPOL) is providing training to LE agencies across EU and to other framework partners on cybercrime and other thematic areas in line with the training need analyses regarding the beneficiary countries. We should keep in mind that technology is the most rapidly developing area and cyber-criminals are often among the earliest adopters of new technology. Therefore, LE agencies have the obligation to keep the pace with the innovation and in order to encourage the development, the new regulations aim to provide legal certainty, protection and ensure financial stability.

Silvia PORTESI
Cybersecurity Expert, European Union Agency for Cybersecurity (ENISA)
https://www.enisa.europa.eu

During incident handling and cybercrime investigations CSIRTs and Law Enforcement Agencies (LEAs) interact and cooperate. Examples of their synergies are the technical support that CSIRTs can provide to the LEAs or the knowledge on investigative skills that the LEAs can share with the CSIRTs. At national and even more at cross-border level the cooperation can be complex. Appointing liaison officers, sharing methodologies and platforms as well as organizing mutual and joint training facilitate this cooperation. For more information, see: 2021 ENISA Report on CSIRT-Law Enforcement Cooperation, Handbook and the Toolset on CSIRT-LE cooperation or contact CSIRT-LE-cooperation@enisa.europa.eu.

Yvonne K. SERRATO
Cyber Assistant Legal Attaché, Federal Bureau of Investigation (FBI)
https://www.fbi.gov/

There are serious threats to all countries: to personal safety, to the health of world economies and to all countries' national security. Ransomware is currently one of the biggest international threats: transnational cybercriminals use malicious software to hold digital systems hostage and demand a ransom. The cyber-attacks have targeted critical infrastructure, law enforcement agencies, hospitals, schools, municipalities and businesses of all sizes. Addressing cybercrime requires strong and enduring partnerships between public and private sectors: law enforcement, academia, industry, etc., and international counterparts, like the Romanian National Police, specifically the Directorate for Combating Organized Crime.

Cătălin ZETU
Head of Bureau, Central Cybercrime Unit, Romanian Police
https://www.politiaromana.ro

The Romanian Police, through his specialized Central Cybercrime Unit, is working to combat a large number of cybercrime related threats as non cash means of payment and Internet frauds, child sexual exploitation over the Internet and cyber-attacks. Lately, an increase of attacks driven from the military conflict in Ukraine challenges both law enforcement and cyber security sector. Also, a wave of Android Malware campaigns delivered over Short Message Service (SMS) impacted a large number of Romania citizens. Fighting these kinds of threats is only possible through solid cooperation and continuous efforts in specializing the public sector and law enforcement representatives.

Sorin STĂNICĂ
Head of Bureau, Research and Crime Prevention Institute, Romanian Police
https://www.politiaromana.ro

The IT revolution that we are currently experiencing moved a lot of crimes online. But, when we talk about crime prevention, it is not only the cyber space that we have to protect, but the physical one in the same time. In the last years, the Romanian Police tried to mix the classic offline approach with the digital one in the matter of crime prevention. Cybercrime has a very fast rate of development and diversification, and we try to keep our methods updated. Crime prevention represents the most effective tool to tackle cybercrime. Whether we talk about big projects/campaigns, at national, regional or local level, or singular actions, the partnership with governmental and non-governmental organizations or with companies represent a valuable instrument of preventive approach.

Thomas S. DOUGHERTY
International Computer Hacking and Intellectual Property (ICHIP) Attorney for Central, Eastern and Southern Europe at the U.S. Department of Justice (DOJ)
https://hr.usembassy.gov

Mr. Thomas Dougherty, ICHIP Attorney Advisor for Central, Eastern and Southern Europe, provided an overview the U.S. DOJ's Computer Crime and Intellectual Property Section (CCIPS) and ICHIP program's international cybercrime cooperation efforts. The ICHIP program is funded by the U.S. State Department and implemented by the U.S. DOJ and consists of 12 Federal Prosecutors stationed in Europe, Africa, Asia and the Western Hemisphere, 2 digital forensic experts and 1 cyber investigator (FBI Agent) all working together to with prosecutors, judges and investigators to build cybercrime capacity and international cooperation through case-based mentoring, legislative reform and the use of international digital evidence-sharing platforms.

Chris STODDARD
Director of Operations, National Cyber-Forensics and Training Alliance (NCFTA)
https://www.ncfta.net

The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime. NCFTA objectives for information sharing is identifying risk, threats, and threat actors impacting the cyber ecosystem, confirm assumptions, share mitigation strategies to help make everyone more resilient and leverage law enforcement and judicial process to disrupt the miscreants responsible for the criminal activity: disrupt criminal infrastructure and make indictments/arrests.

SECTION III: CYBERSECURITY CHALLENGES AND OPPORTUNITIES

Speakers:

- **Megan BISHOP,** Economic Officer, U.S. Embassy in Romania
- **Adrian DANCIU**, Regional Director, Fortinet
- **Paul MARAVEI**, General Director, Cisco Romania
- **Cătălin COȘOI**, Chief Security Strategist, Bitdefender
- **Magda POPESCU**, Outside Legal Counsel to the Digital Crimes Unit, Microsoft Corporation
- **Adrian IFRIM**, Senior Manager, Deloitte
- **Radu STĂNESCU**, CEO, Sandline
- **Bogdan TOPORAN**, CEO, Best Internet Security

Moderator: **Toma CÎMPEANU**, CEO, National Association for Information Systems Security (ANSSI)

Toma CÎMPEANU
CEO, National Association for Information Systems Security (ANSSI)
www.anssi.ro

MODERATOR

The pandemic brought several new trends, such as the rise of hybrid work and increasing reliance on cloud-based solutions, while the geopolitical tensions in the wake of Ukraine invasion emphasize the importance of cybersecurity. Cybercrime is now the third largest economy, after US and China, and the annual damage costs surpass all natural disasters. Malicious state-backed and non-state actors are reshaping the cyber threat landscape, while existing cybersecurity infrastructures were mostly designed and calibrated for "normal" times. Being part of EU and NATO, Romania is facing the same challenges as our allies and the only logical way to tackle these is through joint efforts and increase cooperation.

Adrian DANCIU
Sr. Regional Director - South Eastern Europe, Fortinet
https://www.fortinet.com

We see a convergence of Networking and Security, as well as the move towards consolidation of security vendors and solutions to reduce complexity and accelerate responsiveness to threats. Today's cyber threat landscape continues to accelerate, both in volume and sophistication, increasing the demand for high levels of automation as well as Artificial Intelligence and Machine Learning models. To address these challenges, Fortinet's Security Fabric delivers a multi-phase approach to cyber security, including the prevention of threats, while continuing to detect intrusion or attack in progress, with a quick response to cyber events coordinated across the cybersecurity mesh. Monitoring is done centrally, providing correlated data and single-pane visibility for an efficient response.

Paul MARAVEI
Country Leader, Cisco Romania
https://www.cisco.com

Most of the cyber-attacks start with some sort of phishing. We have to focus on several aspects regarding cyber security: users' behavioral, skill set and proper tools. In the current geopolitical context, it is imperative for us to find the right mindset, to be cyber-alert, cyber-vigilant. We also need to create more cyber-experts through training activities. The non-IT experts have access to various computer systems, so they need to be trained with basic cybersecurity trainings, to be aware with the common threats from cyberspace. Organizations need to define cyber security policies and find the tools to implement them. Cisco offers training on cybersecurity for government organizations and a broad range of cybersecurity technologies.

Cătălin COȘOI
Chief Security Strategist, Bitdefender
https://www.bitdefender.ro

The Investigation and Forensics Unit within Bitdefender has been created in 2015 with the purpose to help law enforcement or state institutions with their investigation on cyber-attacks. The Unit has been involved in many takedowns of dark markets where criminals sold drugs, weapons or malware. Nowadays, there is a big increase of cyber incidents and attacks, like email scams and phishing, ransomware and social engineering attacks, security incidents with Internet of Things (IoT) devices. With the recent geopolitical events, Bitdefender works together with the National Cyber Security Directorate in supporting Ukraine by providing technical consulting, threat intelligence and cybersecurity technology for people and organizations in Ukraine, NATO and EU countries.

Magda POPESCU
Outside Legal Counsel, Digital Crimes Unit, Microsoft Corporation
https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/

Magda shared Microsoft Digital Crimes Unit's view on challenges and opportunities in tackling cybercrime, as a prerequisite to ensuring cybersecurity – and how such can be seized. Digital Crimes Unit is a complex multinational team of lawyers, analysts, investigators, engineers focused on fighting cybercrime – from Malware to Ransomware, from malicious use of Azure to addressing Business Email Compromise and Tech Support Fraud. The borderless nature of this crime and its use of technical, human, and financial resources across the globe represents a challenge, but at the same time an opportunity for disrupting the criminal infrastructure and dismantling the flows used by cybercriminals in their activity.

Adrian IFRIM
Senior Manager, Deloitte
https://www2.deloitte.com

In managing risks, there are risks that cannot be predicted, due to geopolitical events, technology and natural disruptors. It is important to do research in order to decrees the amount of uncertainty and to share cyber incidents experience for increasing the level of cybersecurity. The emerging topics on cybersecurity are deceptions, behavioral biometrics, post quantum cryptography, awareness, industrial security and Internet of Things (IoT), products/services built on automation. The cybersecurity market is not yet mature in providing tools to respond to these needs. Current infrastructures are built upon years of bad practice, fast workarounds and make it work asap situations.

Radu STĂNESCU
CEO, Sandline
https://sandline.ro

Humans can be hacked: over 75% of successful attacks are due to insider threats. Successful security attacks exploit the human interests, weaknesses, social values, beliefs motivations, behaviors, cognitive biases and errors. In order to deal with these attacks, we have to prevent human profiling, to assess the persons, to identify the human vulnerabilities and remediate them, to train and test people in cybersecurity. It is important to find the balance between flexibility and procedures, to make the cyberspace flexible and responsive. Technology can be used to focus on risk-based vulnerability management, to help the organizations to optimize their vulnerability management, track down the blocking factors and to improve the time to fix the discovered vulnerabilities.

Bogdan TOPORAN
CEO, Best Internet Security (BISS)
www.biss.ro

For me and Best Internet Security (BISS), it was a pleasure and a great occasion to participate and to remind of the constant challenges in Cybersecurity, while emphasizing the issues that have been accelerated by the pandemic and by the realities of cyberwar. We took the opportunity to advise on the countermeasures that are to be taken under such circumstances. Based on our hands-on experience together with our customers, we thought it is important to mention a few technologies that we see fit to be deployed with priority, so we presented a short list. Hopefully it was relevant information for the participants also from our side and I am looking forward to future events organized by RAISA. Thank you!

SECTION IV: RESEARCH AND DEVELOPMENT ON CYBERSECURITY

Speakers:

- **Tuan TRINH**, Director for Eastern Europe, EIT Digital
- **Marcel PATATU**, Expert, EUROPOL Innovation Lab
- **Corina PASCU**, Cybersecurity Expert, EU Agency for Cybersecurity (ENISA)
- **Cristian PAȚACHIA**, Development and Innovation Manager, Orange Romania
- **Andrei AVĂDANEI**, CEO, Bit Sentinel
- **Sorin MIRIȚESCU** & **Olivia COMȘA**, Information Security Managers, Safetech Innovations
- **Dănuț TURCU**, Head of Department, "Carol I" National Defense University (UNAP)
- **Costel CIUCHI**, Associate Professor, University Politehnica of Bucharest (UPB)

Moderator: **Ioan-Cosmin MIHAI**, Vice President, Romanian Association for Information Security Assurance

Ioan-Cosmin MIHAI
Vice President, Romanian Association for Information Security Assurance (RAISA)
https://www.raisa.org

MODERATOR

Research and development (R&D) represent keys component in the successful discovery and development of new cybersecurity technologies and services. Along with creating new cybersecurity products and adding features to old ones, investing in research and development can make the cyberspace safer and more secure. This includes capacity building, proactive and strategic activities, and it is essential for gaining and maintaining a business growth and increased long-term profitability. For obtaining a successful innovation in the cybersecurity field, it is important to have international cooperation among public institutions, private companies, and universities, to share experience, good practices, and tools.

Tuan TRINH
Director for Eastern Europe, EIT Digital
https://www.eitdigital.eu

In the context of its activities in its strategic innovation area Digital Industry, at EIT Digital we believe that research and development as well as innovation activities as well as regulation of modern digital infrastructures and the relation to personal data governance in cybersecurity are crucially important for Europe's sovereignty and economic strength. I also believe that it is crucial to pay a strong attention to important European values, potential for global sovereignty and Europe's economic well-being. Impacts of latest technology such as quantum computing on cybersecurity should be properly dealt with. European cybersecurity startup and innovation ecosystems should be strengthened.

Marcel PATATU
Expert, EU Agency for Law Enforcement Cooperation (EUROPOL) Innovation Lab
https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab

In the last years, criminals are quickly integrating new technologies into their modus operandi or building brand-new business models around them. At the same time, emerging technologies create opportunities for law enforcement to counter these new criminal threats. Thanks to technological innovation, law enforcement authorities can now access an increased number of more suitable tools to fight crime. The Europol Innovation Lab aims to identify, promote and develop concrete innovative solutions in support of the EU Member States' operational work. These will help investigators and analysts to make the most of the opportunities offered by new technologies to avoid duplication of work, create synergies and pool resources.

Corina PASCU
Cybersecurity Expert, European Union Agency for Cybersecurity (ENISA)
https://www.enisa.europa.eu

Cybersecurity research and innovation is in the front row of the digital transformation of the economy and society, by ensuring a trustworthy and reliable digital environment, promoting the European way of life, supporting democracy and values, and protecting its strategic autonomy. In this context, ubiquitous connectivity, datafication of everything and Artificial Intelligence are key trends that will have major implications for the EU's digital ambitions to 2030. However, while the benefits are well known, the challenges and risks are yet to be fully recognised. Cybersecurity is crucial to ensure that EU citizens, businesses and organisations can enjoy the benefits of the digital transformation of the economy and society.

Cristian PAȚACHIA
Development and Innovation Manager, Orange Romania
https://www.orange.ro

A big achievement last year and an ongoing development in terms of partnerships and innovation is the launch of Orange 5G Lab. In partnership with the “CAMPUS” Research Institute within POLITEHNICA University of Bucharest, this is the first 5G laboratory in Romania, which offers companies the chance to develop the technologies of the future together with start-ups and academia. An important activity of the 5G Lab is dedicated to the evaluation and security assessment of the 5G cloud native network applications (NetApps). 5G technology adoption “everywhere”, together with Edge Computing as a key enabler, will become the standard, accelerating the evolution across multiple industry verticals.

Andrei AVĂDANEI
CEO, Bit Sentinel
https://bit-sentinel.com

Cyber-attack vectors are becoming increasingly complex lately and we’ve seen organizations trying to effectively keep up with the ever-changing threat landscape. Under such circumstances, an easy-to-use early warning service is vital to detect the new vulnerabilities that could be camouflaged in your network. CVE Monitor is that specific tool that aggregates and processes social media threat intelligence feeds and other trusted public, commercial and closed sources, and combined with a proprietary system based on ML & AI algorithms scores results faster than other tools available on the market. Moreover, CVE Monitor predicts a vulnerability's severity from low to critical. It can be used, complementary to existing threat intelligence products, by any organization worldwide.

Sorin MIRIȚESCU
Head of Security Architecture and Software Development, Safetech Innovations
https://www.safetech.ro

For most organizations the current approach towards cybersecurity protection is reactive rather than proactive and that's where the need for research and development comes in. However, R&D is not enough. We need execution and doing so in a way that suits an organization's unique needs. The speaker mainly talked about the pivotal role of R&D in cybersecurity, emphasized why academic partnership is important to stay ahead of the game and also presented some of the projects Safetech Innovations carried out in this space, from an integrated software platform for mobile malware analysis to a software solution that the company developed to covers the information security management requirements of an organization.

Dănuț TURCU
Director, Information Systems and Cyber Operations Department, "Carol I" National Defense University, Romania
https://www.unap.ro

Professor Turcu highlighted the importance of research and development in the activities of the Romanian National Defence University "Carol I" but equally important with education and training. The university's programs are in strict accordance with NATO's cyber requirements, accessing both NATO and EU funds through ongoing projects. The university will launch a new master's program in the field of cyber security for critical infrastructure protection in parallel with a new qualification of cyber security expert for critical infrastructures in the national register of qualifications. The university is based on the research and development activity on the collaboration with both research institutes from the country and private entities.

Costel CIUCHI
Associate Professor, University Politehnica of Bucharest (UPB)
https://upb.ro/en/

The success of a national resilience strategy in cybersecurity requires more attention to the field of research and development. The recent developments in the European cyberspace require new strategies and approaches regarding the IT systems. The diversity of current vulnerabilities and cyber threats, doubled by the complexity of the attack vectors, reinforce the need for research and development (R&D), education and awareness, and professional training activities in cybersecurity. Cooperation among academia, public administration, private sector and civil society is important to ensure the implementation of a sustainable research and development ecosystem.

SECTION V: CYBERSECURITY EDUCATION AND CAREER DEVELOPMENT

Speakers:

- **Viorel GAFTEA,** Scientific Secretary, Romanian Academy
- **Richard WHITE**, Research Assistant Professor, University of Colorado
- **Natalia BELL**, Assistant Professor, Marymount University
- **Mircea ȘCHEAU**, Honorary Associate Researcher, University of Craiova
- **Bogdan BANU**, Senior Director, Meridian International Center
- **Nathalie RÉBÉ**, Financial Crime and AML Consultant, PwC Luxembourg
- **Joseph JONES**, CEO, Strategy Nord, OS2INT
- **Tiberiu BOROȘ & Andrei STAN**, Information Security Engineers, Adobe
- **Larisa MUNTEAN**, Data Protection Officer, JS Information Governance

Moderator: **Costel CIUCHI**, Associate Professor, University Politehnica of Bucharest (UPB)

Costel CIUCHI
Associate Professor, University Politehnica of Bucharest (UPB)
https://upb.ro/en/

MODERATOR

Education, lessons learned, share and cooperation represent the keys to succeed in achieving cybersecurity goals, especially for education and career development in the field. Cybersecurity policies, action plans, education and trainings require more attention to lessons learned, sharing data and cooperation between the basic components of society (academia, public administration, the private sector, and civil society) ensure the implementation of a sustainable career development ecosystem. In this context, cooperation between universities to share the results obtained in research activities, complemented by lessons learned from the states agencies, private and civil society should represent the foundation for resilient education and awareness process.

Viorel GAFTEA
Scientific Secretary, Science and Information Technology Section, Romanian Academy
https://acad.ro/institutia/sectia_14.html#sectie

Cyber security is no longer an option, it is a determinant, is a condition in today time and world, in a highly digitalized and computerized society in terms of social, educational, economic, technological, covering the entire age spectrum. The combination of cyber problems and threats in the social and geopolitical field, of security in the fields of social and economic life, of the respective services and activities, require a good knowledge, disaster recovery plans, resilience and constant, modern and effective security preventions in multiple domains. It becomes an imperative at the national educational level in addition to security requirements, to have a much more complex plan form, including aspects on the side of computer systems, electronic and computerized services.

Richard WHITE
Research Assistant Professor, University of Colorado, Colorado Springs
www.uccs.edu

The US has dramatically increased spending in both cybersecurity education and R&D to fend off the threat of domestic catastrophic destruction resulting from cyber attack. Unfortunately, none of these efforts are sufficient to fill the 465,000 jobs waiting in cybersecurity nor make the breakthrough in revolutionary technology that could eliminate the threat from cyber attack. Fortunately, the threat from cyber attack will gradually subside as infrastructure is incrementally upgraded and technology evolves and made less susceptible to catastrophic failure. Given this inevitable outcome, should the US stop funding cybersecurity education and R&D? No, because in either case the future is technological, and US citizens need technological skills to live and thrive in that future.

Natalia BELL
Assistant Professor, Marymount University
https://marymount.edu

Nowadays, the industry is struggling with considerable shortages of cybersecurity professionals and organizations have primarily relied upon colleges and universities to supply the necessary workforce. To align with such demand, educational institutions should adapt their strategies in attracting not only young learners coming from high school, but also towards reskilling and upskilling existing talent like retired military, police officers and career changers. Additionally, the higher education institutions should treat the cybersecurity industry as it is: an interdisciplinary field, by combining not only cybersecurity and computer science and information technology, but also business, data science, business intelligence, artificial intelligence, robotics, etc.

Mircea ȘCHEAU
Honorary Associate Researcher, University of Craiova

Daniel LEU
Threat Researcher, Farscope Information Consulting

The last few years have brought forward a multitude of changes in regards to the methods, motives and capabilities of cyber threat actors, especially those that operate in the gray area between financial motivation and political ideology. The exponential increase in the advancements registered across all sectors of the information technology field gave a new, ever-expanding dimension to the idea of protesting against national governments by introducing activism into cyberspace. Despite the apparent noble objectives, there is a thin line between hacking as a form of protest against the established order and cyber-criminal activity that can cause financial or material prejudice against organizations.

Bogdan BANU
Senior Director, Meridian International Center
https://www.meridian.org

Meridian is an organization that has sixty years' track record of being a trusted partner of the US Department of State and US embassies, by designing, implementing, and stewarding impactful exchanges, training and cultural programs. Meridian has started the first global emerging cyber leadership fellowship, a program that will help building a cohesive group of cyber security leaders from across the globe, who are committed to the framework of responsible state behavior. The purpose of the fellowship is to improve understanding of the framework of responsible behavior and the threat facing cyberspace and to foster collaboration and coordination approach to cybersecurity between US and international cyber security officials from all around the world.

Nathalie RÉBÉ
Financial Crimes and AML Consultant, Luxembourg

As criminals have always been agile in adopting new techniques to circumvent laws, they now take advantage of technological innovation and globalization to further expand their illicit businesses. To comprehend the functioning of online unlawful financial activities, we have discussed how money and assets can be laundered, reviewed cyber-laundering risk factors, suspicious activities, and regulatory loopholes, such as weak or inefficient regulations, privacy concerns, jurisdictional conflicts, or law enforcement issues. As launderers always manage to stay one step ahead of law enforcement using new technologies, only harmonized regulations, international cooperation, and education will prevail in the fight of cyber-laundering.

Joseph JONES
CEO, Strategy Nord and OS2INT
https://strategynord.com

The EU and NATO militaries are facing significant challenges as they seek to maintain information manoeuvre in cyberspace. As militaries face significant challenges in developing operationally-effective cyber defence and offensive cyber operations capabilities, there is an opportunity for EU and NATO members to create interoperable processes in this regard. That said, recruitment and training of cyber personnel within the military domain remains a key issue for many EU / NATO countries. However, there are models – like UK Future Force Concept – which countries can adopt in order create the necessary capacities. Overall, Public-Private Partnerships should play a crucial role in the development of effective strategic and operational capacities across EU and NATO members.

Tiberiu BOROȘ & Andrei STAN
Information Security Engineers, Adobe
https://www.adobe.com/ro

Cybersecurity education became a must in the past years, especially with the increasing numbers of cyberwarfare methods and financially driven threat actors. Therefore, the open-source projects, like *Living off the Land* (*LotL*) *Classifier Open-Source Project*, help professionals and researchers educate on new ways to proactively detect threat actors using machine learning and raise awareness about them. This project is a great starting point for cybersecurity students to understand how technology can be used to boost their career development in this field, as it will provide new skills and push them to apply them in other cybersecurity-related issues, like privacy protection or risk management.

Larisa MUNTEANU
Data Protection Lawyer & Deputy Data Protection Officer, JS Information Governance
https://js-ig.com/

Research is essential in education and career development. During Larisa's presentation, the audience could understand where personal data sits in the ecosystem of cybercrimes and how legal instruments safeguarding personal data and combatting cybercrimes do overlap. Moreover, the misconception that non-complying with personal data protection rules is always sanctioned by fines or warnings was challenged - there are many cases, worldwide, when breaching obligations regarding personal data protection (especially digital data) might lead to imprisonment. This is why, three global models could have been identified within the legal systems that were assessed. These ideas were expanded in the article published by Larisa in the proceedings of the conference.

www.cybercon.ro

CYBERCON ROMANIA 2022 FACTS

CyberCon Romania 2022 brought together 45 internationally recognized experts, from European Union and United States Agencies, international public institutions, private companies, research centers and universities, and non-governmental organizations, with the aim of raising the level of awareness, embodies the cybersecurity culture, and sharing best practices in fighting cybercrime.

The conference had five sections that gave the opportunity to speakers to share knowledge, perspectives, and to highlight synergies between different areas of expertise:

- Developing cyber defence and cyber resilience;
- International cooperation for fighting cybercrime;
- Cybersecurity challenges and opportunities;
- Research and development on cybersecurity;
- Cybersecurity education and career development.

CyberCon Romania 2022 included the presentations from the ninth edition of the scientific **International Conference on Cybersecurity and Cybercrime (IC3)**, organized by the Romanian Association for Information Security Assurance (RAISA). The selected papers were presented by their authors at the "*Cybersecurity education and career development*" section.

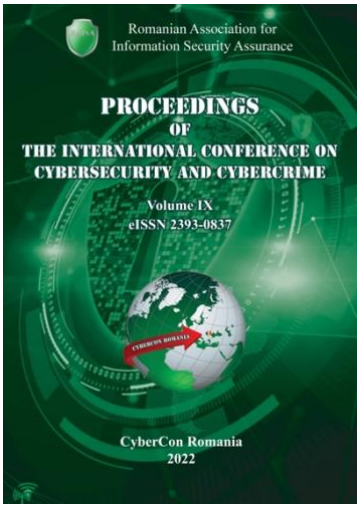
More than **700 persons** have registered to attend CyberCon Romania 2022 online conference, with an average of 200 attendees per section.


WHAT DOES THE COUNCIL OF EUROPE STAND FOR?
Disrupting Criminal Infrastructure
CAPABILITY
INFRASTRUCTURE
VICTIM
Our opportunity
EIT DIGITAL – FOR A STRONG DIGITAL EUROPE
DIGITAL FINANCE
DIGITAL CITIES
DIGITAL INDUSTRY
DIGITAL WELLBEING
DIGITAL TECH
INVESTING IN AREAS STRATEGIC FOR EUROPE
FRONTEX
EU INNOVATION HUB
NVD CVSS
Model Training
Input/Output
Base Score Classifiers
Predictive Model
Impact Score Determination
#BeCyberSmart
security students?
Military and Retired Public Servants
Career Changers!!!
Let's talk about them!

THE SCIENTIFIC SIDE OF CYBERCON ROMANIA

CyberCon Romania includes the **International Conference on Cybersecurity and Cybercrime (IC3),** an annual scientific conference organized by the Romanian Association for Information Security Assurance (RAISA).

The purpose of this scientific conference is to encourage the exchange of ideas about evolution of cyberspace, information security challenges and new facets of the phenomenon of cybercrime. The event started in 2014 as an initiative to provide the appropriate framework for students to present their research in this field.



Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)

Volume IX, Year 2022

Online ISSN: 2393-0837

Print ISSN: 2393-0772

DOI: 10.19107/CYBERCON.2022

Published: 2022-04-30

Website: https://proceedings.cybercon.ro

The Proceedings of the International Conference on Cybersecurity and Cybercrime includes scientific papers reviewed by the *Editorial Board* that consists of experts from academic police structures and university departments, their work taking place under the guidance of the *Advisory Board*, composed of internationally recognized personalities from academic field.

The conference proceedings is an *Open Access Journal* starting with 2022 and it will be indexed in international databases like *EBSCOhost*, *Central and Eastern European Online Library (CEEOL)*, and *Google Scholar*.

The selected papers from the 9th edition of the International Conference on Cybersecurity and Cybercrime were presented during CyberCon Romania 2022 conference, at the "*Cybersecurity education and career development*" section.

CONFERENCE PARTNERS

PRIVATE PARTNERS

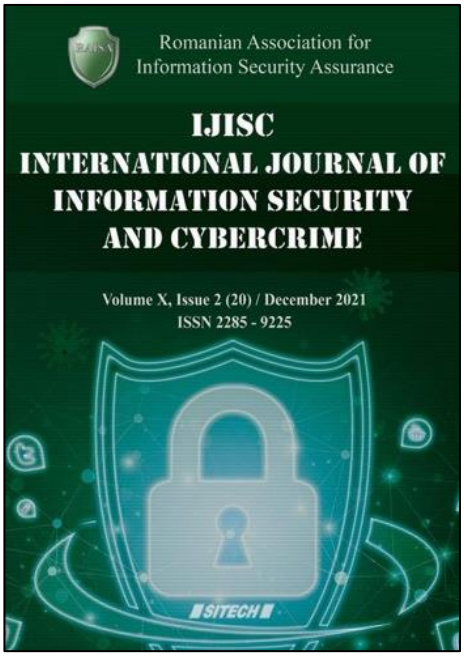
MEDIA PARTNER

ABOUT THE ORGANIZER

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit and public benefit association. Founded in 2012, RAISA started as an initiative dedicated to promote the information security.

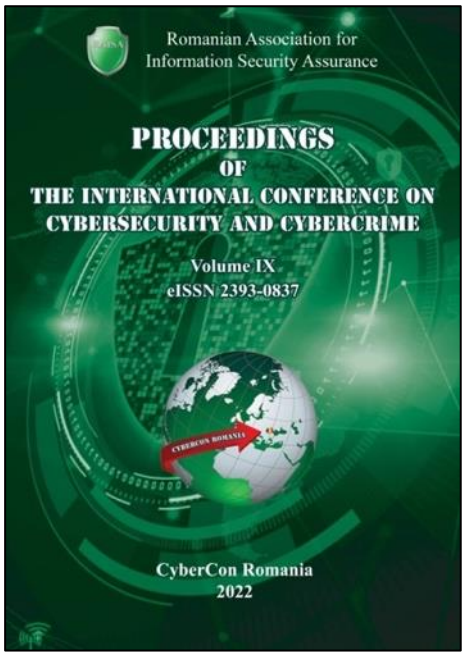
The aim of the Romanian Association for Information Security Assurance (RAISA) is promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment from Romania.

RAISA supports scientific work in the fields of cybersecurity and cybercrime by publishing and promoting books, technical guidelines, and scientific publications like the *International Journal of Information Security and Cybercrime (IJISC)* and the *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)***,** with the purpose of analyzing cybersecurity and identifying new valences of the cybercrime phenomenon.



https://ijisc.com

https://raisa.org/cybersecurity-guide



https://proceedings.cybercon.ro

Knowledge, implemented through common effort, for mutual benefit, is, in the opinion of the Romanian Association for Information Security Assurance, the richest expression in information security education!

Website: www.raisa.org (EN) / www.arasec.ro (RO)

Romanian Association for Information Security Assurance (RAISA)

https://www.raisa.org

2022