



**critical
infrastructure**
PROTECTION AND
RESILIENCE EUROPE

14th-16th June 2022

Bucharest, Romania

www.cipre-expo.com

Securing the Inter-Connected Society

Preliminary Conference Programme

Your invitation and guide to the premier discussion

UN Member States need "to share information [...] to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

Co-Hosted by:



www.cipre-expo.com

*Leading the debate for securing
Europe's critical infrastructure*

Supporting Organisations:

Media Partners:





CIPRE – Where CIIP/Cyber and Physical Security Meet

Attacks on critical infrastructure sites are now a fact of life not simply a potential threat. Power stations, chemical plants, nuclear facilities are routinely targeted by cyber-attacks, the most successful so far being the Ukraine power outage that caused 225,000 customers to lose electricity. Last year an activist landed a UAV carrying small traces of radiation on the roof of the Japanese Premier's office and this year a UAV collided with an aircraft at London's Heathrow airport. And of course the terrible attacks on the metro and airport in Brussels. This is just the start of what we can expect to be the repeated targeting of our critical infrastructure. The potential effects not only in terms of loss of life but also in terms of damage to infrastructure, economic disruption and costs, can be enormous.

Once again widespread flooding across Europe in 2015 caused even bigger outages of power and for longer periods than cyber-attacks and the damage to lives, property and businesses was larger still, emphasising the need for planning and preparation on European scale.

We must be prepared!

The European Commission has adopted a communication on Critical Infrastructure Protection in the fight against terrorism, enhancing European prevention, preparedness and response in the event of terrorist attacks involving critical infrastructures.

The European Programme for Critical Infrastructure Protection (EPCIP) considers measures that will enhance the level of protection of infrastructure against external threats, with the Operator Security Plan for all infrastructures designated as European critical.

The European Union is also developing its policy on critical energy infrastructures in relation to the European Programme for Critical Infrastructure Protection ("EPCIP") which considers measures that will enhance, where necessary, the level of protection of certain infrastructures against external threats.

Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

"The EU Internal Security Strategy highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy."

The integrity of critical infrastructures and their reliable operation are vital for the well-being of the citizens and the functioning of the economy. The implementation of the EPCIP, under Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the need to improve their protection, has not been completely successful.

Why the Need for Such a Discussion?

Article 196 of the Lisbon Treaty enshrines in law that the Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters.

The Union's action shall aim to:

- (a) support and complement Member States' action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union;
- (b) promote swift, effective operational cooperation within the Union between national civil-protection services;
- (c) promote consistency in international civil-protection work.

The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber-attacks, means the need to continually review and update policies, practices and technologies to meet these demands.



Follow us:



Critical Infrastructure Protection & Resilience Europe



Critical Infrastructure Protection / Physical Security

Drone's, Insider threats, Vehicle Borne IED's, Suicide Bombers and Active Shooters are just some of the myriad of known threats facing CNI operators in 2019. Identifying ways of detecting, defeating and mitigating against those threats and building-in resilience are crucial organisation or CNI operator.

Critical Information Infrastructure Protection / Cyber Security

With the ever increasing threat from cyber attacks on critical infrastructure, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber security strategy of an organisation or CNI operator.

Combining CIIP/Cyber and Physical Security into one integrated strategy is not just desirable but crucial!

Why Attend?

Your attendance to Critical Infrastructure Protection and Resilience Europe will ensure you are up-to-date on the latest issues, policies and challenges facing the security of Europe's critical national infrastructure (CNI).

You will also gain an insight in to what the future holds for Europe's, the collaboration and support between member nations required to ensure CNI is protected from future threats and how to better plan, coordinate and manage a disaster.

- High level conference with leading industry speakers and professionals
- Learn from experiences and challenges from the experts
- Gain insight into national and European CIP developments
- Constructive debate, educational opportunities and cooperation advocacy
- Share ideas and facilitate in valuable inter-agency cooperation
- Exhibition showcasing leading technologies and products
- Networking events and opportunities

For further information and details on how to register visit www.cipre-expo.com

For conference or registration queries please contact:
Neil Walker
Events Director
T: +44 (0) 7725 318601 | F: +44 (0) 872 111 3210
E: neilw@torchmarketing.co.uk

Who Should Attend

Critical Infrastructure Protection and Resilience Europe is for:

- Police and Security Agencies
- Emergency Services
- National government agencies responsible for national security and emergency/contingency planning
- Local Government
- CEO/President/COO/VP of Operators of national infrastructure
- Security Directors/Managers of Operators of national infrastructure
- CISO of Operators of national infrastructure
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Event Security Managers
- Architects
- Civil Engineers
- EU
- NATO
- Military
- Border Officials

Join us in Bucharest for Critical Infrastructure Protection and Resilience Europe and join the great debate on securing Europe's critical infrastructure.



Schedule of Events

Tuesday 14th June 2022

11.00am - 12.30pm - Ministerial Opening Keynote

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Opening Keynote Session

3:30pm-4:00pm - Networking Coffee Break

4.00pm-5:30pm - Session 1: Mitigating Major Threats

Tuesday 15th June 2022

CRITICAL INFRASTRUCTURE PROTECTION / PHYSICAL SECURITY TRACK

9:00am-10:30am - Session 2a: Emerging Threats for CI

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3a: Countering the Emerging Threats - Security, Risk & Disaster Mitigation

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4a: PPP & Collaboration in CIP

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5a: Critical Infrastructure Interdependencies - from Risk to Resilience

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION / CYBER SECURITY TRACK

9:00am-10:30am - Session 2b: Cyber Policies, Standards and Best Practice

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3b: Cyber Risks and Resilience

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4b: Cyber Threats and Risk Assessments

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5b: AI, Machine Learning, Automation and Security in the Digitalisation of Critical Infrastructure

5:30pm - Networking Reception

Wednesday 16th June 2022

9:00am-10:30am - Session 6: Overview of European Horizon Europe Programmes

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7: Overview of European Horizon Europe Programmes

12:30pm-2:00pm - Delegate Networking Lunch

2pm-3:30pm - Session 8: Lessons learned from the Pandemic and its affects on CI, Health, Transport and Financial sectors

3:30pm-4:00pm - Review, Discussion and Conference Close



HOW TO REGISTER

1. Online at www.cipre-expo.com.
2. Complete the Registration Form at the back of this booklet and email to: cipre@torchmarketing.co.uk.
3. Complete the Registration Form at the back of this booklet and fax to +44 (0) 872 111 3210.
4. Complete the Registration Form at the back of this booklet and mail to:
CIPRE, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, United Kingdom.

EARLY BIRD DISCOUNT - deadline 14th May 2022

Register yourself and your colleagues as conference delegates by 14th May 2022 and save with the Early Bird Discount.

Discounts for Members of Supporting Associations

If you are a member of one of the following trade associations, supporters of the Critical Infrastructure Protection & Resilience Europe, then you can benefit from a special discount rate:

- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)
- Institute of Engineering & Technology (IET)
- Security Partners Forum (SPF)

Check the Registration Form at the back of this booklet for full details.

On-Site Registration Hours

Monday 14th June	9.00am to 5.00pm
Tuesday 15th June	8.30am to 5.00pm
Wednesday 16th June	8.30am to 2.00pm





International Association of CIP Professionals (IACIPP)

The IACIPP is a global fraternal association of CIP professionals, dedicated to sharing ideas, information, experiences, technology and best practise, with the express purpose of making the world a safer place.

The association is open to critical infrastructure operators and government agencies, including site managers, security officers, government agency officials and policy makers. The purpose is to share ideas, information, experiences, technology and best practise.

The Association, although very young in its journey, is clear in what it is seeking to achieve. The creation of a network of like minded people who have the knowledge, experience, skill and determination to get involved in the development and sharing of good practice and innovation in order to continue to contribute to the reduction of vulnerabilities and seek to increase the resilience of Critical Infrastructure and Information.

A great new website that offers a Members Portal for information sharing, connectivity with like-minded professionals, useful information and discussions forums, with more being developed.

The ever changing and evolving nature of threats, whether natural through climate change or man made through terrorism activities, either physical or cyber, means there is a continual need to review and update policies, practices and technologies to meet these growing and changing demands.

Membership is currently FREE to qualifying individuals - see www.cip-association.org/join for more details.



For further details visit www.cip-association.org or email info@cip-association.org.

The IACIPP initial overall objectives are:

- To develop a wider understanding of the challenges facing both industry and governments
- To facilitate the exchange of appropriate infrastructure & information related information and to maximise networking opportunities
- To promote good practice and innovation
- To facilitate access to experts within the fields of both Infrastructure and Information protection and resilience
- To create a centre of excellence, promoting close co-operation with key international partners
- To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

The Association also aims to:

- Provide proactive thought leadership in the domain of critical infrastructure security and resilience.
- Help set the agenda for discussions in infrastructure security and resilience
- Promote and encourage the sharing of information, knowledge and experience that will enhance security.
- To filter, collect, collate and co-ordinate information and data sharing.
- Identify and promote new technologies that can enhance security and resilience.
- Share information with members about the changing threat landscape
- Share information, ideas and knowledge to promote best practice
- Educate operators and provide industry standards
- Act as a Liaison between operators, government, intergovernmental bodies
- Make available surveys and research
- Provide the mechanism for liaison between operators and industry

Join today at www.cip-association.org/join



Tuesday 14th June

Conference Programme

11:00am-12:30pm - Ministerial Opening Keynote

12:30pm-2:00pm - Networking Delegate Lunch

2:00pm-3:30pm - Opening Keynote

Chair: John Donlon QPM, FSI
International adviser on security intelligence

Victor Vevera, [ICI, Romania CPNI](#)

Jose Luiz Pérez Pajuelo, [Director, Spanish CNPIC](#)

Jakub Boratynski, [Head of Unit for Cybersecurity and Digital Privacy, DG Connect, EC*](#)

Planning for Disaster - Risk Management and Resilience. An EU Perspective - Eugen-Liviu Militaru, [Senior Security Officer, the Head of Protective Security and Continuity Officer, eu-LISA](#)

3:30pm-4:00pm - Networking Coffee Break

4:00pm-5:30pm - Plenary Session 1: Mitigating Major Threats

Being prepared for the changing threat environment, both from a physical and cyber perspective, can benefit greatly in mitigating its impact on infrastructure assets, ensuring resilience, safety and security. What are the latest perspectives of threats/challenges against CI and how can we mitigate these threats and new challenges?

Cyber Terrorism: The Rising Threat in Cyber Kinetic? - Dr Zahri Yunos, COO, Cybersecurity Malaysia & Mustaffa Bin Ahmed, Cybersecurity Malaysia

CIP: coming of age, facing new challenges - Albert Nieuwenhuijs, TNO

The Fifty Shades of Risk Assessment - Simin Nadjm-Tehrani, Professor, Linkoping University, Sweden

Critical Entity Resilience proposal for a new directive - Alessandro Lazari, Regional Director IACIPP

Katri.liekkila, Director, Policy, Planning and Analysis at National Emergency Supply Agency (NESA)*

*invited



Wednesday 15th June

**CRITICAL INFRASTRUCTURE
PROTECTION TRACK**

9:00am-10:30am - Session 2a: Emerging and Future Threats on CNI

The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities and insider threats, means the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats and how can we identify, monitor and manage their levels of potential damage?

Julijus Grubliauskas, Staff Officer, Hybrid Challenges and Energy Security Section, NATO Headquarters, Emerging Security Challenges Division*

Collaborative Research & Book Project of COE-DAT & U.S. Army War College on "Critical Infrastructure Security and Resilience" with a Special Focus on Terrorist Threat - Col. Daniel Stone, Deputy Director, Defense Against Terrorism Center of Excellence (COE-DAT) & Dr Carol Evans, Director of the Strategic Studies Institute and USAWC Press, US Army War College

Electromagnetic pulse attack: a black swan or a grey rhino? - Lina Kolesnikova, Security Consultant

TBC

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3a: Countering the Emerging Threats - Security, Risk & Disaster Mitigation

Understanding the changing threat environment can benefit greatly in mitigating its impact on infrastructure or crowded places, ensuring resilience, safety and security. How can we counter these emerging threats to minimising loss of service and financial impact?

Sendai Framework for Disaster Risk Reduction - Armen Grigoryan, UNDP

Gabriel Badea, President, Federation of Security Services, Romania

Human Assets – Developing Your Team for Effective Critical Infrastructure Protection - Patrick Kane, Atlas Air

Sensor Data Fusion of Multi-Sensor Drone Detection Systems - Peter Braun, Sales & Product Manager Drone Detection, Telespazio Germany GmbH

**CRITICAL INFORMATION INFRASTRUCTURE
PROTECTION / CYBER SECURITY TRACK**

9:00am-10:30am - Session 2b: Cyber Policies, Standards and Best Practice

As the threat of cyber-attacks by state actors grows ever higher and attacks by criminals and malicious rogue players continues unabated the need to put in place robust legislation and standards and best practice becomes all the more urgent.

Senior Representative, European Commission*

NIS Directive - Marnix Dekker, NIS Directive Coordinator, ENISA*

Paolo Grassia, Director of Public Policy for cybersecurity, ETNO*

European UMF Interoperability Standard for Secured Critical Infrastructure - Amr el Rahwan, Sr. Solution Architect, WCC

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3b: Cyber Risks and Resilience

The ability to monitor the cyber threats to Critical Infrastructure can greatly assist the operators and agencies better prepare their defences against cyber attacks on systems and information/data. What are the latest emerging cyber threats and actors and what are the latest strategic perspective on cyber monitoring and cyber defences for enhancing CIIP?

Quo Vadis city dweller? - MIRUNA-MARIA COCOLAN, RASIROM

New Challenges for System Security in the European Power Grid - Options for National Policymakers

- Christoph Mayer, Director, OFFIS - Institute for Information Technology, Germany

Smart Grid Security Using Blockchain - George Suciuc, R&D Innovation Manager, BEIA Consult International, Romania

Cyber resilience at airports - Patrick Mana, Cyber-security Project Manager - EATM-CERT Manager, EUROCONTROL*

12:30pm - Delegate Networking Lunch



Wednesday 15th June

CRITICAL INFRASTRUCTURE PROTECTION TRACK

2:00pm-3:30pm - Session 4a: PPP & Collaboration in CIP

With many critical infrastructures in the hands of private organisations, how does the responsibility of security and resilience lie between government, with public accountability to keep them safe, secure and operational 24/7, and the private operator, with additional responsibilities towards shareholders? How can improving the communication between the public sector and private sector enhance protection and can incentives be employed to better engage private owners into PPP?

CIP From A Law Enforcement Perspective within the Railway Environment - John Laene, Secretary General of RAILPOL and Chief Inspector within the Service of Infrastructure of National Police of The Netherlands

The importance of cooperation in combating crimes in the airport environment - Peter Nilsson, Head of AIRPOL

Improving CIP system in Republic of Croatia: Forming national CI database - Ivana Cesarac, Head of Critical Infrastructure and Cultural Heritage Department at the Civil Protection Directorate, Croatia

The new CEN Standard for Private Security Services in CIP - Catherine Piana, COESS

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5a: Critical Infrastructure Interdependencies - from Risk to Resilience

It is the interoperability between independent critical national infrastructures that is the catalyst for multiple failures in the so called cascade effect. As more infrastructure becomes increasingly interdependent, how do we identify the weaknesses to enhance resilience across industries to prevent and/or mitigate the effects of a natural disaster or man-made attack?

How NOT to conduct a crisis man - Roni Tidhar, IAA

The Importance of Embedding Security into the Design of CNI Facilities - Sarah Jane Prew, Arup

Situational Awareness of Critical Infrastructures at the Local Level – Fostering Resilience Through Accessible Method-based Analysis - Joanna Schroeder / Markus Bresinsky, Ostbayerische Technische Hochschule (OTH) Regensburg

Integrated approach for Risk Management in Critical Infrastructures under Industry 4.0 towards Resilience - Javier Larrañeta, PESI

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION / CYBER SECURITY TRACK

2:00pm-3:30pm - Session 4b: Cyber Threats and Risk Assessments

Critical Infrastructure assets are under increasing cyber attack from unknown threat or malicious actors aiming to disrupt or maim supply and business continuity. How do we identify these threats and assess their risks to ensure resilience against cyber attacks?

The Unknown, Fancy and Misunderstood: Assessing Cyber Risks in Critical Infrastructure - Can Demirel, ICS Cyber Resilience Services Manager, Biznet Bilisim

SCADA/ICS Inherited Insecurity: From Nuclear Power Plants to Oil Rigs - Aleksander Gorkowienko, Spirent Communications

TBC

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5b: AI, Machine Learning, Automation and Security in the Digitalisation of Critical Infrastructure

How can we use AI, quantum computing capabilities, augmented reality and machine learning to create resilience in our infrastructure? How can it affect the environment, transport, smart cities, etc? What are the emerging technologies and how can they assist in disrupting threats?

Dr. Paul Theron, Cyber resilience scientist & advisor- Research on Autonomous Cyber Defence, Thales*

Keys to Resilient Digitalisation in Power Systems: System Knowledge and Flexibility - Dr Davood Babazadeh, Head of R&D Group 'Automation and Control', OFFIS - Institute for Information Technology, Germany

TBC

5:30pm - Networking Reception



Thursday 16th June

9:00am-10:30am - Plenary Session 6: Overview of European Horizon Europe Programmes (Pt1)

A deeper look at the current range of Horizon Europe Critical Infrastructure Protection & Resilience projects and research programmes across Europe that are designed to enhance understandings for adapting policies and adopting best practices.

*Moderator: European Commission**

PHOENIX - Mihai PAUN, Vice-President, Romanian Energy Centre

Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection (PRECINCT) - Konstantinos Loupos, Head of R&D Program, INLECOM Innovation

APPRAISE - Vangelis Sdongos

Security and resilience of EU Ground Segments of Space Systems (7SHIELD) - Ms Eftichia Georgiou, Research Associate, Center for Security Studies - KEMEA

10:30am-11:15am - Networking Coffee Break

11:15am-12:30pm - Plenary Session 7: Overview of European Horizon Europe Programmes (Pt2)

A deeper look at the current range of Horizon Europe Critical Infrastructure Protection & Resilience projects and research programmes across Europe that are designed to enhance understandings for adapting policies and adopting best practices.

*Moderator: European Commission**

PRAETORIAN - Frédéric Guyomard, Project Director and Coordinator*

The Smart Spaces Safety and Security for All Cities project (S4AIICities) - Nikolaos Lalazisis, Research Associate, KEMEA

IMPETUS - Smart City Protection - Joe Gorman, Project Coordinator, SINTEF Digital*

ENSURESEC - Luis Sousa, Project Manager, INOV*

12:30pm-2:00pm - Delegate Networking Lunch



Wednesday 16th June

2:00pm-4:00pm - Plenary Session 8: Lessons learned from the Pandemic and its affects on CI, Health, Transport and Financial sectors

The pandemic has certainly caused a lot of disruption to everyday lives, the economy and provided new challenges for our critical infrastructure to maintain continuous supply of services. Different sectors have managed in different ways, but have there been any outstanding successes. What can we learn from the events of the past 2 years and how can we be better prepared for the next pandemic to minimise impact on the critical infrastructure services, to which life and the economy are so reliant?

Redefining Critical Infrastructure - Lina Kolesnikova, Security Consultant

Advancing critical health infrastructure resilience thinking – insights from a literature study - Nathalie Sanger, Project Associate; Christine Heinzel, Student Assistant; Dr. Simone Sandholz, Academic Officer, Head of Programme, United Nations University - Institute for Environment and Human Security (UNU-EHS)

TBC

Conference Close by John Donlon QPM, FSI, Conference Chairman

Register online at www.cipre-expo.com/onlinereg

Early Bird Deadline - 14th May 2022





critical infrastructure PROTECTION AND RESILIENCE EUROPE



14th-16th JUNE 2022
Bucharest, Romania



The premier conference for securing Europe's critical infrastructure

Networking Reception

**Wednesday 15th June
5.30pm - 7:00pm**

In cooperation with the The National Institute for Research & Development in Informatics (ICI Bucharest), under the coordination of the Ministry of Communications and Information Society, we invite you to joins us at the end of the day for the Networking Reception, which will see the CNI security industry management professionals and delegates gather for a more informal reception.

With the opportunity to meet colleagues and peers you can build relationships with senior government, agency and industry officials in a relaxed and friendly atmosphere.

The Networking Reception is free to attend and will take place in the Palace of Parliament.

Open to industry professionals and delegates of Critical Infrastructure Protection & Resilience Europe.

We look forward to welcoming you.



*Built in security - increasing security without turning
our public buildings and spaces into fortresses*



Bucharest, Romania



Romania's infrastructure is fairly extensive, with 103,671 kilometers of road, 11,385 kilometers of rail, and 3.84 million main telephone lines. But most of it is in a poor state of repair, due to decades of underinvestment. Romania has 6 major ports and investment into Romania's energy sector is also badly needed. The country currently generates 22.6 gigawatts of power from a combination of thermal, hydro-electric, and nuclear power plants. But most of the plants are over 20 years old, and about 60 percent of Romania's power capacity will have to be replaced within the next 10 years.

This is a situation that successive governments have been eager to rectify.

New infrastructure projects worth more than € 1.5 billion are expected to be delivered in the regional cities of Romania this year, while in Bucharest construction works for the new bypass will continue as part of a € 1 billion investment. At the same time, the first new airport in the last decades will start operating in Brasov in the near future, following an investment of approximately 70 million euros, while airports in other cities are included in major modernization programs.

As the capital city of Romania, a beautiful country which is to be found in Eastern Europe, Bucharest has no shortage of striking architecture, historical buildings, and a fantastic foodie scene.

Buchrest is also home to the Palace of the Parliament, the heaviest building in the world and the second largest and most expensive administrative building, after the Pentagon. The Palace was ordered by Nicolae Ceaucescu, the dictator of Communist Romania, and it now houses the Parliament of Romania along with three museums and an international conference centre.

CIPRE is delighted to be invited by ICI Bucharest (The National Institute for Research & Development in Informatics under the coordination of the Ministry of Communications and Information Society) to host the event in the Palace of the Parliament, which offers a magnificent setting and ideal location for the latest round of discussions on protection, security and resilience of critical infrastructure.

We look forward to welcoming you to Bucharest on 14th-16th May 2022.





Accommodation

Event HQ Hotel

JW Marriott Bucharest Grand Hotel
Calea 13 Septembrie 90 Bucharest,
Romania



Critical Infrastructure Protection & Resilience Europe have arranged a Special Rate for accommodation at the JW Marriott Bucharest hotel, the event's HQ hotel for the 2022 event.

Critical Infrastructure Protection & Resilience Europe have arranged a Special Rate for accommodation at the Marriott Bucharest Grand Hotel, the event's HQ hotel for the 2022 event.

A few minutes walk from the Palace of Parliament and located in an area of historic and national interest, JW Marriott Bucharest Grand Hotel in Romania is the only five-star hotel in the district and is in close proximity to the stately Palace of Parliament and People's Salvation Cathedral.

Culturally rich and with a status that befits its quality offering, our luxury hotel provides a restorative setting in Bucharest where its legacy for intuitive service, culinary distinction, and notable grandeur remains unsurpassed.

Its seamless blend of modern luxury and authentic appeal enhances each stay in Bucharest, Romania with a holistic offering, that is both distinctive and deeply enriching.

The JW Marriott Bucharest Grand Hotel in Romania is a premier luxury destination for business and leisure guests, it is just a 30 minutes' drive from Henri Coandă International airport and within walking distance of Old Town, with its diversity of architecture.

The hotel are offering delegates of CIPRE a special rate from RON 550 per night B&B. Ensure you book your room early to avoid disappointment.

Book your accommodation via:
www.cipre-expo.com/accommodation

This offer is only available through CIPRE and www.cipre-expo.com. Critical Infrastructure Protection & Resilience Europe or JW Marriott Bucharest Hotel will NOT phone you to chase your room reservation. Any phone calls you receive from housing management companies are not endorsed or contracted by CIPRE or the event organisers.





Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience Europe 2022.

Co-Hosted by:



Supporting Organisations:



Media Partners:



Media Supporters:





Why participate and be involved?

Critical Infrastructure Protection and Resilience Europe provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection and security policy makers and practitioners.

Your participation will gain access to this key target audience:

- raise your company brand, profile and awareness
- showcase your products and technologies
- explore business opportunities in this dynamic market
- provide a platform to communicate key messages
- gain face-to-face meeting opportunities

Critical Infrastructure Protection and Resilience Europe gives you a great opportunity to meet key decision makers and influencers.

“Although the EC Directive has helped in ‘assessing the need to improve the protection of European critical infrastructures’ in the transport and energy sectors, there is no indication that it has actually improved security in these sectors.”

Why participate and be involved?

Critical Infrastructure Protection and Resilience Europe provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection and security policy makers and practitioners.

Your participation will gain access to this key target audience:

- raise your company brand, profile and awareness
- showcase your products and technologies
- explore business opportunities in this dynamic market
- provide a platform to communicate key messages
- gain face-to-face meeting opportunities

Critical Infrastructure Protection and Resilience Europe gives you a great opportunity to meet key decision makers and influencers.

www.cipre-expo.com

How to Sponsor

Gain access to a key and influential audience with your participation in the limited sponsorship opportunities available at the conference exhibition.

To discuss sponsorship opportunities and your involvement with Critical Infrastructure Protection & Resilience Europe please contact:

Paul Gloc
(UK and Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Sam Most
Mainland Europe & Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

Sponsorship Opportunities

A limited number of opportunities exist to commercial organisations to be involved with the conference and the opportunity to meet and gain maximum exposure to a key and influential audience.

Some of the sponsorship package opportunities are highlighted on the left. Packages can be designed and tailored to meet your budget requirements and objectives.



critical infrastructure

PROTECTION AND RESILIENCE EUROPE

14th-16th June 2022

Bucharest, Romania

www.cipre-expo.com

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 14th May 2022 and save with the Early Bird rate

REGISTRATION IS SIMPLE

1. Register online at www.cipre-expo.com/onlineereg
2. Complete this form and email to: cipre@torchmarketing.co.uk
3. Complete this form and fax to +44 (0) 872 111 3210
4. Complete this form and mail to: CIPRE 2021, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, UK.

DELEGATE DETAILS

(Please print details clearly in English. One delegate per form, please photocopy for additional delegates.)

Title: _____ First Name: _____

Surname: _____

Job Title: _____

Company: _____

E-mail: _____

Address: _____

Street: _____

Town/City: _____

County/State: _____

Post/Zip Code: _____

Country: _____

Direct Tel: (+) _____

Mobile: (+) _____

Passport No (for security clearance) _____

Signature : _____ Date: _____

(I agree to the Terms and Conditions of Booking)

Terms and Conditions of Booking

Payment: Payments must be made with the order. Entry to the conference will not be permitted unless payment has been made in full prior to 14th June 2022.

Substitutions/Name Changes: You can amend/change a delegate prior to the event start by notifying us in writing. Two or more delegates may not 'share' a place at an event. Please ensure separate bookings for each delegate. Torch Marketing Co. Ltd. reserve the right to refuse entry.

Cancellation: If you wish to cancel your attendance to the event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a £100 administration charge, providing that cancellation is made in writing and received before 14th May 2022. Regrettably cancellation after this time cannot be accepted. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.

Alterations: It may become necessary for us to make alterations to the content, speakers or timing of the event compared to the advertised programme.

Data Protection: Torch Marketing Co. Ltd. gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services.

Please tick if you do not wish to be contacted in future by:

- Email Post Phone Fax

PARTICIPATION FEES

GOVERNMENT, MILITARY AND PUBLIC SECTOR/AGENCY

Individual Full Delegate

(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and 2 lunches, plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)

- Paid before 14th May 2022 €195
 Paid on or after 14th May 2022 €295

OPERATORS OF INFRASTRUCTURE

Individual Full Delegate

(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and 2 lunches plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)

- Paid before 14th May 2022 €195
 Paid on or after 14th May 2022 €295

COMMERCIAL ORGANISATIONS

Individual Full Delegate

(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)

- Paid before 14th May 2022 €595
 Paid on or after 14th May 2022 €795

Individual Day Delegate

(includes participation on one day, coffee breaks and lunch on the day plus ONE YEAR BASIC MEMBERSHIP of IACIPP)

- Paid before 14th May 2022 €350
 Paid on or after 14th May 2022 €450
 Attending on: 14th June 15th June 16th June

Sponsor Full Delegate

(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)

- Paid before 14th May 2022 €300
 Paid on or after 14th May 2022 €400

Student Full Delegate

(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch) - Student ID required

- Paid before 14th May 2022 €195

PAYMENT DETAILS

(METHOD OF PAYMENT - Conference fees are subject to Romanian VAT at 19%.)

Wire Transfer (Wire information will be provided on invoice)

Credit Card

Invoice will be supplied for your records on receipt of the order/payment.

Please fill in your credit card details below:

Visa MasterCard

All credit card payments will be subject to standard credit card charges.

Card No: _____

Valid From ____ / ____ Expiry Date ____ / ____

CVV Number ____ (3 digit security on reverse of card)

Cardholder's Name: _____

Signature: _____ Date: _____

I agree to the Terms and Conditions of Booking.

Complete this form and fax to +44 (0) 872 111 3210 or email to cipre@torchmarketing.co.uk