

critical infrastructure PROTECTION AND RESILIENCE EUROPE



3rd-5th October 2023
Prague, Czech Republic
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:



3rd-5th OCT 2023
Prague
Czech Republic



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 a 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!

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 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 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 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.

Attend CIPRE 2023 to learn about the importance of the updated NIS2 Directive...

An important discussion will centre around the EU cybersecurity rules introduced in 2016 and updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

Also learn about the importance of the new directive on the Resilience of Critical Entities...

The Directive on the Resilience of Critical Entities entered into force on 16 January 2023. Member States have until 17 October 2024 to adopt national legislation to transpose the Directive.

The Directive aims to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies.



Follow us:



3rd-5th OCT 2023
Prague
Czech Republic



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.

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), as well as the implementation of the NIS2 and CER Directives.

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
E: neilw@torchmarketing.co.uk

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

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.

Who Should Attend

Critical Infrastructure Protection and Resilience Europe is for:

- National and local government agencies responsible for national security and emergency/contingency planning
- Police and Security Agencies; Policy, Legal and Law Enforcement
- Civil Contingencies, National Security Agencies and Ministry Infrastructure Departments
- CNI Operators (CSO, CISO, Infrastructure Managers, Facilities Managers, Security Officers, Emergency Managers)
- Energy operators, grid, T&D, power generators
- Telecommunications and Mobile Operators
- Water and Utilities Suppliers
- Emergency Services, Emergency Managers and Operators
- Local Government
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- IT, Cyber Security and Information Managers
- Port Security Managers; Airport Security Managers; Transport Security Managers
- Engineers, Architects, Constructors and Landscape Designers; Civil Engineers
- Public Administrators and Managers
- Utility Providers (Energy, Communications, Water and Wastewater)
- Urban Planners and County Commissioners
- Transportation Managers and Planners
- Facility, Data and IT Managers
- Supply Chain Logistic Managers and Operators
- Banking and Financial institutions
- Data Centres
- NATO; Military; Border Officials
- International Corporations



3rd-5th OCT 2023
Prague
Czech Republic

Schedule of Events

Tuesday 3rd October 2023

2.00pm - 3.30pm - Ministerial Opening Keynote

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

4.00pm-5:30pm - Session 1: Interdependencies and Cascading Effects across the CI Communities

5:45pm - Networking Reception

Wednesday 4th October 2023

TRACK ONE

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

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

11:15am - 12:30pm - Session 3a: Power & Energy Sector Symposium

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

2:00pm-3:30pm - Session 4a: Communications Sector Symposium

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

4:15pm - 5:30pm - Session 5a: Transport Sector Symposium

TRACK TWO

9:00am-10:30am - Session 2b: Crisis Management, Coordination & Communication

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

11:15am - 12:30pm - Session 3b: Government, Defence & Space Sector Symposium

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

2:00pm-3:30pm - Session 4b: Information Technology (CIIP) Sector Symposium

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

4:15pm - 5:30pm - Session 5b: CBRNE Sector Symposium

Thursday 5th October 2023

TRACK ONE

9:00am-10:30am - Session 6a: Technologies to Detect and Protect

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

11:15am - 12:30pm - Session 7a: The Insider Threat

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

2pm-3:30pm - Session 8: EU Horizon Projects Overviews

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

TRACK TWO

9:00am-10:30am - Session 6b: Risk Mitigation and Management

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

11:15am - 12:30pm - Session 7b: Business Continuity Management



3rd-5th OCT 2023
Prague
Czech Republic

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 3rd September 2023

Register yourself and your colleagues as conference delegates by 3rd September 2023 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:

- Association of Critical Infrastructure of Czech Republic (AKICR)
- 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

Tuesday 3 rd October	1.00pm to 5.00pm
Wednesday 4 th October	8.30am to 5.00pm
Thursday 5 th October	8.30am to 2.00pm





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.



**International Association of
CIP Professionals**

www.cip-association.org

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 3rd October

Conference Programme

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

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

Ing. Jozef Síkela, Minister of Industry and Trade, Czech Republic

LG Vladimír Váček, General director of the Fire and Rescue System, Prevention and Civil
Emergency Preparedness, Czech Republic

Adrian Victor Vevera, General Director, National Institute for Research and Development,
Informatics ICI Bucharest, Romania

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

4:00pm-5:30pm - Plenary Session 1: Interdependencies and Cascading Effects across the CI Communities

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 should the CI community build situational awareness to mitigate the cascading effect across infrastructures.

Chris Rodriguez, Director of Homeland Security and Emergency Management for Washington DC, USA

Cyber-Physical Security and Critical Infrastructure - Catherine Piana, Secretary General, CoESS

Frederic Petit, Project Officer, European Commission, Joint Research Centre

Update on Directive on the Resilience of Critical Entities - Alessandro Lazari, Senior Key Account Manager, F24

Martin Hromada, Security Research Project Manager, Tomas Bata University, Czech Republic

5:45pm-7:30pm - *Networking Reception*

**invited*



Wednesday 4th October

TRACK ONE

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

The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities and insider threats, and coupled together with the latest challenges with cyber attacks from many directions, creates the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats, both physical and cyber, and how can we identify, monitor and manage their levels of potential damage?

Global threats and local threats to Cis - Lina Kolesnikova, Security Expert

Daniel Golston, Associate Programme Officer, Action Against Terrorism Unit, OSCE

Emerging Cyber Threats - CEO, CyberCX's*

Emerging Threat of Drones - Speaker TBC

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

11:15am - 12:30pm - Session 3a: Power & Energy Sector Symposium

The energy sector has become the most critical of sectors. Without power, driven by oil, gas and renewable energies, all other CI stops. Recent cyber attacks on the energy sector, as well as natural hazards, from hurricanes in the Gulf, or earthquakes in Italy, to fires in California or Greece, gives much room for thought on how we best protect our most vital assets, including IT/OT and SCADA systems. How can we mitigate the impact of an attack or outage on the wider community and society.

Ing. Jindrich Sip MBA, Head of Business Continuity Management, CEZ, Czech Republic

Senior Representative, EUTC*

Senior Representative, EE-ISAC

Modeling resilience of German offshore energy infrastructures - Arto Niemi, Research Team Leader, DLR Institute for the Protection of Maritime Infrastructures

TRACK TWO

9:00am-10:30am - Session 2b: Crisis Management, Coordination & Communication

Planning and preparation is the key to ensuring that CI and venue operators have the right equipment, processes and procedures in place to respond in the event of an emergency. Coordination and information sharing is essential for situational awareness and can improve the planning process. How do we better coordinate and cooperate to enhance protection and resilience.

Chair: Catherine Piana, COESS

Fitting national CIP legislation to new EU CER framework in a view of prospect for better coordination and management - Ivana Cesarec, Head of CI and Cultural Heritage Dept, Civil Protection, Croatia

Building Sustainable and Resilience Communities: The Perspective of The International Emergency Management Society - TIEMS - Harald Drager, President & Jaroslav Pejcoch, Secretary to TIEMS

Javier Larraneta, Secretary General, PESI

Markus Epner, Head of Academy, F24 AG, Germany

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

11:15am - 12:30pm - Session 3b: Government, Defence & Space Sector Symposium

As we rely more and more heavily on satellites for communications, navigation, observation and security/defence, the requirement to ensure that space based systems are both secure and resilient becomes more urgent. Government networks and systems need to lead security and resilience across agencies and departments for confidence throughout the CI sectors and communities. What impact does the Government, Defence and Space based systems have as a growing role in CI resilience.

Chair: John Donlon QPM, FSI

Eugen-Liviu Militaru, Senior Security Officer, Head of the Protective Security and Continuity Sector, eu-LISA

Building the cybersecurity of the eGovernment cloud - Ondrej Nekovar, CISO, Chief Deception Officer, State Treasury Shared Services Centre, the Ministry of Finance

Roya Ayazi, Secretary General, NEREUS

Anita Nikova Bundovski, Country Director, CIDR/North Macedonia, DAI, North Macedonia

12:30pm - Delegate Networking Lunch



Wednesday 4th October

TRACK ONE

2:00pm-3:30pm - Session 4a: Communications Sector Symposium

Communications is key to any community and its infrastructure assets has become increasingly threatened. Without communications, business will be lost, and any emergency coordination would be a disaster. The internet has become a vital part of communications for all. Protection of communication assets and their resilience is vital for businesses, government and all sectors of CI.

Alexandru Georgescu, Scientific Researcher, National Institute for Research & Development in Informatics - ICI Bucharest

Securing postal communications channels at GEOPOST - Jean-Philippe Berillon, Group Chief Security Officer, Geopost, France

Senior Representative, EUTC*

Senior Representative, Vodafone*

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

4:15pm - 5:30pm - Session 5a: Transport Sector Symposium

The movement of goods and people is vital to a local and national thriving economy. Without a safe, secure and resilient transport network, an economy will crumble. The transport network, from rail, road, air and sea, is at threat from cyber attacks, terrorist threats and natural hazards and its protection and resilience is key for communities and countries to maintain their economies.

John Laene, Strategic Advisor, RAILPOL

International cooperation for a better future of transport and traffic - Jana Pelešková, Chief Commissioner, Police Presidium of the Czech Republic, directorate of traffic police

Enhancing Port Security and Resilience: Towards a Holistic Approach for Real-time Performance Monitoring and Threat Mitigation - Babette Tecklenburg, Researcher, Institute for the protection of maritime infrastructures, German Aerospace Center (DLR)

Fusion Threat Intelligence: Concept, Practice, and Future Use in the Transport Sector - Natasia Kalajdziovski, Senior Fusion Threat Intelligence Analyst, SecAlliance

TRACK TWO

2:00pm-3:30pm - Session 4b: Information Technology (CIIP) Sector Symposium

Securing the digital infrastructure. Information technology is responsible for such a large portion of our workforce, business operations and access to information and data, Critical Information Infrastructure Protection (CIIP) through cybersecurity and network security, is vital to protect information assets. Recent ransomware attacks and other threats, such as Malware, Stuxnet, etc and the continued cyber threats and intrusions, means we have to be more vigilant to protect our information assets.

Martin Švéda, Head of the Private Sector Regulation Unit, National Cyber and Information Security Agency (NÚKIB)

Get ready for the transformative effect of blockchain on critical infrastructures - Adrian Victor Vevera, General Director, National Institute for Research and Development, Informatics ICI Bucharest, Romania

Human Factor Control to protect industrial companies against phishing attacks - Mohammed Al-Ghamdi, Information Security Analyst, Saudi Aramco

International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) - Dr. Sandeep Pirbhulal, Senior Research Scientist, Norwegian Computing Centre, Norway

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

4:15pm - 5:30pm - Session 5b: CBRNE Sector Symposium

Sectors such as Chemicals, Nuclear and Water/Wastewater are as much at threat from an attack as a threat they pose that could include CBRNE agents in terrorist attacks against CI. The convergence of biological and cyber sector issues also characterises an evolving frontier in health security, and mitigation of such attacks is as much of a consideration as post attack resilience.

ERNICIP Chemical and Biological (CB) Risks to Drinking Water Thematic Group - Frederic Petit, Project Officer, European Commission, Joint Research Centre

Thomas Fojtik, Director, T.G. Masaryk Water Research Institute, Czech Republic

František Paulus, Director of Population Protection Institute, Czech Republic



Thursday 5th October

TRACK ONE

9:00am-10:30am - Session 6a: Technologies to Detect and Protect

What are some of the latest and future technologies, from ground surveillance, space based or cyber technology, to predict or detect the wide range of potential threats to CNI.

How Unified Physical Security Solutions Help You Thrive in Evolving Times - Jakub Kozak, Regional Sales Manager, Genetec

Seyit Ali Kaya Regional Manager, Eastern Europe, Central Asia, and Türkiye, Iris ID Systems

Communication Systems & Technologies Engineer, European Space Agency*

TBC

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: The Insider Threat

An insider threat is a perceived danger to your company that originates from individuals who work there, such as current or former employees, contractors, or business partners, who have inside knowledge of the company's security procedures, data, and computer systems. The main objectives of malevolent insider threats are espionage, fraud, intellectual property theft, and sabotage, for monetary, private, or malicious purposes, they willfully misuse their privileged access to steal information or damage systems. Here we take a deeper dive into the range of threats and how to mitigate and counter these.

John Donlon, Chairman, International Association of CIP Professionals

Peter Nilsson, Head of AIRPOL

Sarah-Jane Prew, Senior Security Consultant, Arup UK

Catherine Piana, Managing Director, Help2Protect, Belgium

TRACK TWO

9:00am-10:30am - Session 6b: Risk Mitigation and Management

Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure and the broader community, ensuring resilience, safety and security. How can we counter these emerging physical and cyber threats to minimise loss of service and financial impact?

Designing Security for when CNI and Crowded Places meet - Sarah-Jane Prew, Senior Security Consultant, Arup UK

Person-Centric Artificial Intelligence for Critical Infrastructure Surveillance - Amr el Rahwan, Amr el Rahwan, International Security Expert, TPASCO (Terrorism Prevention & Anti Social Crime Organization)

Addressing Consequence within Operational Risk - Ollie Gagnon, Strategic Advisor, Critical Infrastructure Security and Resilience, Idaho National Laboratory, USA

What you don't measure you don't know! - Peter Braun, Sales Manager, Telespazio Germany

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

11:15am - 12:30pm - Session 7b: Business Continuity Management

How to we develop and plan the best resilience strategies within our CI community? Through discipline in information sharing and making infrastructure preparedness personal, we can help to build resilience into our infrastructures that benefit the whole community.

A Serious Game for Coordinated Business Continuity Planning - Boris Petrenj, Senior Researcher, Politecnico di Milano, Italy

Marco Buldrini, Head of Major Risks Unit, NIER Ingegneria S.p.A., Italy

Stefano A. Fulgi, Head of Internal Audit, F.I.S. Fabbrica Italiana Sintetici S.p.A., Italy

TBC

12:30pm - Delegate Networking Lunch



3rd-5th OCT 2023
Prague
Czech Republic

Thursday 5th October

2:00pm-3:30pm - Plenary Session 8: EU Horizon Projects Overviews

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 critical infrastructures and understandings for adapting policies and adopting best practices.

SATIE Project - Tim Stelkens-Kobsch, Project Manager, DLR, Germany

EU-CIP Project - Emilia Gugliandolo, Project Coordinator, ENG, Italy

Sunrise Project - Tomáš Trpišovský, Institut mikroelektronických aplikací s.r.o. (IMA)

CyberSEAS Project - Ilija David, OT Cyber Resilience & Cyber Security Architect, KPCS CZ

PARADeS Project - Roman Schotten, Research Assistant, University of Applied Science Magdeburg Stendal

3.30pm - Conference Close

John Donlon qPM, FSI, Conference Chairman

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

Early Bird Deadline - 3rd September 2023





3rd-5th OCT 2023
Prague
Czech Republic

Networking Reception

Tuesday 3rd October
5.45pm - 7:30pm

In cooperation with the The Ministry of Industry and Trade, Tomas Bata University in Zlin and Technical University of Ostrava, 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 Grandium Hotel, just a few short steps from the Ministry of Trade & Industry Building, Polictal Prisoners 931.

Open to the 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*



Accommodation

Event HQ Hotel

Grandium Hotel
Politických vězňů 913/12 (Political
Prisoners 913/12)
Prague

Critical Infrastructure Protection & Resilience Europe event HQ hotel for the 2023 event is the Grandium Hotel Prague, just 100m from the event venue of the Ministry of Trade & Industry Buildings, Political Prisoners 931.

www.hotel-grandium.cz/en



Additional / Alternative Hotels

Additional hotels all within a 2 minute walk of the venue:

Esplanade Hotel Prague
Washingtonova 1600/19
www.esplanade.cz

Falkensteiner Hotel Prague
Opletalova 1402/21
www.falkensteiner.com/hotel-prague

Occidental Praha Wilson hotel
Václavské nám. 110 00/812/59
www.barcelo.com/en-gb/occidental-praha-wilson

Boutique Hotel Jalta
Václavské náměstí 45/818
www.hoteljalta.com/en



Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience Europe 2023.

Co-Hosted by:



Bronze Sponsor:



Lanyard Sponsor::



Supporting Organisations:



Media Partners:



Media Supporters:





3rd-5th OCT 2023
Prague
Czech Republic

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.

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

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

“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

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

3rd-5th October 2023

Prague, Czech Republic

www.cipre-expo.com

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 3rd September 2023 and save with the Early Bird rate

REGISTRATION IS SIMPLE

1. Register online at www.cipre-expo.com/online
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 3rd October 2023.

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 3rd September 2023. 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 3rd September 2023 €195
 Paid on or after 3rd September 2023 €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 3rd September 2023 €195
 Paid on or after 3rd September 2023 €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 3rd September 2023 €395
 Paid on or after 3rd September 2023 €595

Individual Day Delegate

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

- Paid before 3rd September 2023 €250
 Paid on or after 3rd September 2023 €350
 Attending on: 3rd Oct 4th Oct 5th Oct

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 3rd September 2023 €195
 Paid on or after 3rd September 2023 €295

Student Full Delegate

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

- Paid before 3rd October 2023 €195

PAYMENT DETAILS

(METHOD OF PAYMENT - Conference fees are subject to Czech VAT at 21%.)

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