critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026

Sheraton Hotel Brussels Airport, Belgium

www.cipre-expo.com

Preliminary Conference Programme Guide

Critical Infrastructure Protection and Resilience events bring together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing the nations critical infrastructure.

Gain greater understanding on the latest challenges, changing regulations and threats against Europe's critical infrastructure and critical entities, from over 50 international expert speakers.

Join us in Brussels, Belgium for CIP Week in Europe
Register online at www.cipre-expo.com/register

Co-Hosted by:

International Association of CIP Professionals

Global Cybersecurity Partner/ Platinum Sponsor:

ESET Cybersecurity Progress. Protected.

Gold Sponsor:

IndraMind

Silver Sponsor:

FORTINET

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS













Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium

International Association of CIP Professionals

The International Association for CIP Professionals (IACIPP) is proud to announce that CIP Week Europe 2026 will take place in Brussels, Belgium, in the heart that shapes policy for CIPR.

As the premier gathering for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together senior representatives from industry, operators, agencies, and governments to advance collaboration and innovation in securing Europe's essential systems and services.

With the ongoing implementation of the Critical Entities Resilience (CER) Directive and the NIS2 Directive, the EU is strengthening its framework for ensuring that vital societal and economic functions remain resilient in the face of evolving threats. These directives establish robust obligations for Member States and operators, including enhanced risk management, stricter reporting and cybersecurity requirements, and comprehensive crisis response planning.

Compliance with the CER and NIS2 Directives is now a key priority for public and private sector organizations across Europe—essential not only for regulatory adherence but also for safeguarding national and cross-border resilience.

Brussels, as the heart of the European Union, offers the perfect setting for this vital dialogue. Home to major EU institutions, international organizations, and a vibrant innovation ecosystem, Brussels provides a unique platform for shaping Europe's critical infrastructure protection strategy at the highest level.

Join us in Brussels, Belgium, for CIP Week Europe 2026 and the 11th edition of Critical Infrastructure Protection and Resilience Europe, as we work together to strengthen the resilience and security of Europe's critical infrastructure for the future.

www.cipre-expo.com

Co-Hosted by:

International Association of CIP Professionals

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Supported by:

CRISR, ASD, CCNE, E.DSO, etis, 2 years PAN EUROPEAN NETWORK OF CITY REGIONS FOR ENERGY AND CLIMATE, African Young People Support Center, EurEau, CoESS, AUTO-ISAC, AVIATION ISAC, Health-ISAC, FS-ISAC, euralarm, SPACE ISAC

Leading the debate for securing Europe's critical infrastructure



critical infrastructure
PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium
www.cipre-expo.com

Cyber and Physical Threats to Critical Infrastructure

Cyberattacks on critical infrastructure have evolved from potential threats to a persistent reality. Power plants, chemical facilities, and nuclear sites are increasingly targeted by malicious actors. A notable example is the 2015 Ukraine power outage, which affected 225,000 customers.

More recent incidents underscore the growing vulnerability of critical infrastructure. In 2023, a significant cyberattack disrupted critical services in a European nation, highlighting the potential for widespread disruption. Additionally, physical threats, such as drone attacks and sabotage, remain a concern.

The potential consequences of these attacks are far-reaching, encompassing loss of life, economic disruption, and significant infrastructure damage. The 2015 European floods serve as a stark reminder that natural disasters can exacerbate the impact of cyber and physical attacks, necessitating robust preparedness and planning at a European scale.

Strengthening European Infrastructure Protection

To address these evolving threats, the European Union has taken significant steps to enhance the protection of critical infrastructure. The European Commission's communication on Critical Infrastructure Protection provides a framework for prevention, preparedness, and response to attacks.

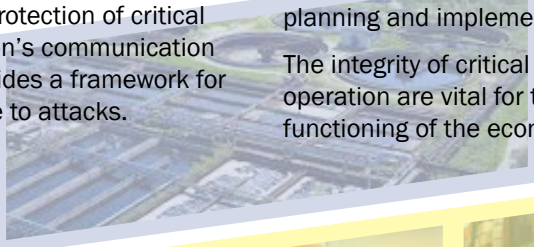
The European Programme for Critical Infrastructure Protection (EPCIP) is a key initiative that mandates Operator Security Plans for all designated European critical infrastructures. This program aims to improve the security posture of these vital assets against external threats.

Furthermore, the EU is developing a comprehensive policy on critical energy infrastructure, aligning with the EPCIP to bolster the resilience of the energy sector.

Given the escalating threat landscape, it is imperative to prioritize the protection of critical infrastructure. By investing in robust cybersecurity measures, fostering international cooperation, and promoting resilience, we can mitigate risks and safeguard the essential services that underpin our societies.

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.




Understanding the Impact of Recent EU Cybersecurity Directives

The European Union has taken significant steps to bolster cybersecurity and critical infrastructure resilience. The Network and Information Systems Directive 2 (NIS2), which entered into force in 2023, updates the 2016 NIS Directive. This updated legislation expands the scope of cybersecurity requirements to new sectors and entities, including key digital service providers.

Key provisions of NIS2 include:

- Enhanced security measures: Businesses designated as operators of essential services must implement robust security measures to protect their systems and data.
- Mandatory incident reporting: Entities must report serious cybersecurity incidents to national authorities.
- Increased accountability: Key digital service providers are subject to specific security and notification obligations.

In addition to NIS2, the Directive on the Resilience of Critical Entities was adopted in 2023 to strengthen the resilience of critical entities against a wide range of threats, such as natural disasters, cyberattacks, and terrorist attacks.

Key provisions of the Resilience of Critical Entities Directive include:

- Identification of critical entities: Member States must identify entities that are critical to society and the economy.
- Risk assessments and mitigation measures: Critical entities must conduct risk assessments and implement measures to enhance their resilience.
- Cross-border cooperation: The EU will facilitate cross-border cooperation and knowledge sharing among Member States and critical entities.

By understanding and complying with these directives, organizations can better protect themselves against cyber threats and contribute to a more resilient European Union.



Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

20th-22nd October 2026 - Brussels, Belgium

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 currently facing CNI operators. 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?

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is organising the 3rd 'Critical Infrastructure Protection Week' in Europe as part of an initiative focused towards enhancing collaboration and cooperation amongst the industry.

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

Join us in Brussels, Belgium, in the heart of EU policy making, for CIP Week, Critical Infrastructure Protection and Resilience Europe and join the great debate on securing Europe's critical infrastructure.

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

HOW TO REGISTER

Online at **www.cipre-expo.com/register**

EARLY BIRD DISCOUNT - deadline 20th September 2026

Register yourself and your colleagues as conference delegates by 20th September 2026 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:

- Europe's Distribution System Operators (E.DSO)
- Auto-ISAC; Health ISAC; Aviation ISAC; Space ISAC
- European Telecommunications ISAC (ETIS-ISAC)
- The European Network of Logistics Competence Centres (OPEN ENLoCC)
- The Centre for Interdisciplinary Research on Critical Infrastructure Security and Resilience (CRISR)
- European water services association (EurEau)
- Crisis Communications Network Europe (CCNE)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)
- European Cluster for Securing Critical Infrastructures (ECSCI)

Check the Registration Fees online at www.cipre-expo.com/conference-fees

On-Site Registration Hours

Tuesday 20th October	1.00pm to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm





Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

20th–22nd October 2026 – Brussels, Belgium

Schedule of Events

Tuesday 20th October 2026

10.30pm-12:30pm - ESET Closed-Door Roundtable (Invitation on

1.30pm - 3.15pm - Joint Opening Keynote

3:15pm-4:00pm - Networking Coffee Break

4.00pm-5:30pm - Session 1: From Definition to Delivery: Governance, Methodology, and Practic

5:30pm - Networking Reception (in exhibition hall)

Wednesday 21st October 2026

7.30pm-8:45pm - IndraMind Breakfast Workshop (Invitation only)

Track One

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

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

11:15am - 12:30pm - Session 3a: Infrastructure Interdependencies and Cascading effects

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

2:00pm-3:30pm - Session 4a: Infrastructure Resilience Under Fire: Ukraine Case Study

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

4:15pm - 5:30pm - Session 5a: Skills Gaps, Fragmentation Capabilities & Public–Private and Cross-Sector Coordination

Track Two

9:00am-10:30am - Session 2b: Power & Energy Sector Symposium

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

11:15am - 12:30pm - Session 3b: Cybersecurity and Cyber Resilience Sector Symposium

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

2:00pm-3:30pm - Session 4b: Transport & Logistics Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Maritime and Subsea Infrastructure Sector Symposium

Thursday 22nd October 2026

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: Drones and UAS

Track Two

9:00am-10:30am - Session 6b: Risk Mitigation, Resilience, Business Continuity Strategies

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

11:15am - 12:30pm - Session 7b: AI and Cyber in CI

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

2pm-3:30pm - Session 8: **Panel Discussion** - Systemic Risk and Uneven Resilience: Confronting Eu

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

critical infrastructure PROTECTION AND RESILIENCE EUROPE

ly)

cal Implementation of NIS2 and CER

Track Three (Workshops)

9:00am-10:30am - Crisis Communications Network Europe (CCNE) Workshop

10:30am-11:00am - Networking Coffee Break

11:00am - 12:30pm - Confederation of European Security Services (CoESS) Workshop

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

2:00pm-3:30pm - AYPSC Africa Workshop

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

4:00pm - 5:30pm - Information Sharing & Analysis Centres (ISACs) Workshop

Track Three (Workshops)

9:00am-10:30am - European Cluster of Securing Critical Infrastructures (ECSCI) Workshop - Resilience Stress Testing

10:30am-11:00am - Networking Coffee Break

11:00am - 1:00pm - ECSCI Workshop (contd.)

urope's Next Critical Infrastructure Shock

e

Partner Conferences / Workshops:

CCNE CRISIS COMMUNICATIONS NETWORK EUROPE

CoESS

AUTO-ISAC

AVIATION ISAC

Health-ISAC

SPACE ISAC

FS-ISAC

African Young People Support Center

etis

Exhibition Opening Hours

Tuesday 20th October	1.00pm to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm

On-Site Registration Hours

Monday 19th October	1.00pm to 5.00pm
Tuesday 20th October	8.30am to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm

critical infrastructure
PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium
www.cipre-expo.com

Registration and Participation Fees

GOVERNMENT, PUBLIC SECTOR AND MILITARY: The Critical Infrastructure Protection & Resilience Europe is open and ideal for members of federal government, emergency management agencies, civil contingencies, emergency response and law enforcement or inter-governmental agencies, Homeland Security & Emergency Management Agencies, Fire, Police, INTERPOL, EUROPOL and associated Agencies and members (public and official) involved in the management and protection of critical national infrastructure.

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE: The Conference is a must attend for direct employees, CSO, CISO's, security management and security personnel of critical infrastructure owner/operators.

COMMERCIAL ORGANIZATIONS: Industry companies, other organizations and research/Universities sending staff members to Critical Infrastructure Protection & Resilience Europe are also invited to purchase a conference pass.

Register online at **www.cipre-expo.com/register**

GOVERNMENT, PUBLIC SECTOR AND MILITARY

Individual Full Delegate

Paid before 20th September 2026 .... €195
Paid on or after 20th September 2026 ..... €295

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE

Individual Full Delegate

Paid before 20th September 2026 .... €195
Paid on or after 20th September 2026 ..... €295

COMMERCIAL ORGANIZATIONS

Individual Full Delegate

Paid before 20th September 2026 .... €495
Paid on or after 20th September 2026 ..... €695

Sponsor/Exhibitor Full Delegate).

Paid before 20th September 2026 .... €295
Paid on or after 20th September 2026 ..... €395

Student/University/Research Full Delegate

Student ID will be required to be shown on collection of pass €295

Delegate Fees include: 3 day participation, conference proceedings, keynote, workshops, networking reception, coffee breaks and 2 lunches. Also includes One Year Membership of International Association of CIP Professionals (IACIPP).

Tuesday 20th October

Conference Programme

1:30pm-3:15pm - Joint Opening Keynote

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

Floriana Sipala, Director for Internal Security (Directorate D) and Counter-Terrorism Coordinator, DG Home

Dr Oleksandr Sukhodolia, Head of Dept of CI, Energy & Envisonrmental Security, National Institute for Strategic Studies & Lead Consultant, Dept of CIP, SSCIP, Ukraine *(representing Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection)*

Ricardo De Sousa Figueiredo, Cybersecurity Expert – Resilience of Critical Sectors Unit, ENISA

Habtamu Abie, Chairman, ECSCI Cluster

3:15pm-4:00pm - Networking Coffee Break

4:00pm-5:30pm - Plenary Session 1: From Definition to Delivery: Governance, Methodology, and Practical Implementation of NIS2 and CER

This session explores how the translation of policy into practice has developed under NIS2 and CER. There still appears to be a lack of understanding around who is responsible for identifying critical infrastructures in a transnational setting, who is responsible for its security and resilience and which actors are required to report incidents, particularly under the evolving NIS-2 and the CER Directive regimes. We will examine governance models, definitions, and practical methodologies for risk assessment, compliance, and reporting.
Chair: John Donlon QPM, FSyI

When 'Critical' Depends on Where You Stand: Infrastructure Governance Across Borders - Flavio Häner, Critical Infrastructure Protection, Canton Basel-Stadt, Government

Chasing Ghosts, Missing Threats: Securing Critical Entities in the Era of Hybrid Warfare - Alessandro Lazari, Fellow and Lecturer, University of Salento - Department of Engineering for Innovation

Compliant on Paper. Ready in Practice? - Catherine Piana, Director General, Confederation of European Security Services (CoESS)

Enhancing the resilience of critical entities - the need for integrated and systemic risk management - Fred Petit, Project Officer, European Commission JRC

Critical Infrastructure Governance and Protection: Perspectives from Across the OSCE Area - Daniel Golston, Associate Programme Officer, OSCE

5:30pm-7:30pm - Networking Reception (in Exhibition Hall)

**invited*

Wednesday 21st October

Track One

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

Critical infrastructure faces increasingly complex and evolving threats. Cyberattacks are growing more sophisticated, terrorism remains a concern, and climate change is making natural disasters more unpredictable. New dangers such as drone attacks, misuse of artificial intelligence, evolving hybrid threats and state sponsored attacks further complicate the landscape. A key challenge is how to effectively identify, monitor, and understand these diverse and emerging threats.
Chair: John Donlon QPM, FSyI

Detecting Hybrid Campaigns Against Critical Infrastructure: A Cybersecurity-Informed Framework for Early Warning - Jonas Schmänk, Policy Assistant / Doctoral Researcher, European Commission, Joint Research Centre (JRC)

Changing Threats of Terrorism Against CI - Lina Kolesnikova, Director of European & International Affairs/Fellow, ICPEM

Emerging Threats, Enduring Weaknesses: Why Threat Intelligence Should Become a Leadership Capability for Critical Infrastructure Resilience - Paulina Rafalak-Lamparska, Threat Intelligence Manager, ESET

Tracking the Typhoons: China's Cyber Operations Against Critical Infrastructure - Eugenio Benincasa, Senior Cybersecurity Researcher, Center for Security Studies (CSS) at ETH Zurich

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

11:15am - 12:30pm - Session 3a: Infrastructure Interdependencies and Cascading effects

Modern critical infrastructure is deeply interconnected, making it increasingly vulnerable to cascading failures. Disruptions in one sector—such as energy, transport, or communications—can rapidly propagate across systems, amplifying impacts and complicating response efforts. Understanding these interdependencies is essential for effective protection and resilience. This session explores how to identify systemic risks, model cascading effects, and strengthen cross-sector coordination to mitigate disruptions, enhance situational awareness, and ensure continuity of essential services in an increasingly complex threat landscape.
Chair: Alessandro Lazari

Resilient Critical Infrastructure Governance in Climate-Induced Urban Crises: Lessons from Dubai's Adaptive Model - Prof. Ehab Elhegawy, Head of the Department of Security Crisis Management, Dubai Police Acadamy

From Compliance to Consequence: Engineering "Even If" Resilience for Europe's Energy Systems - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory)

Understanding Systemic Risk in Critical Infrastructures: A Semantic Approach to Cross-Sector Resilience - Antonella Calo, Expert Consultant, European Commission - Joint Research **Centre**

Know Your Adversary: Sharing Threat Actor Insights to Secure Telecom Infrastructure - Andrija Višić, Senior Community & Programme Manager, ETIS – European Telecommunications ISAC

Track Two

9:00am-10:30am - Session 2b: Power & Energy Sector Symposium

Europe's power and energy sector—spanning oil, gas, and rapidly expanding renewables—remains fundamental to all critical infrastructure. In today's security climate, it faces escalating cyber and hybrid threats targeting IT, OT, and SCADA systems, alongside intensifying climate-driven disruptions. Ensuring resilience means anticipating attacks, reducing the impact of outages, and safeguarding interconnected grids. Strengthening Europe's energy networks is now a strategic priority to maintain stability, security, and continuity across essential services and economies.
Chair: Charles Esser, EDSO

Black Start Resilience - Energy Operator*

Maximilian Urban, Information Security Officer at E.DSO member Netz Niederösterreich and Chair of the E.DSO 'Cybersecurity' Task Force

Martin Hromada, Vice Dean for International Relations / Researcher, Tomas Bata University in Zlín, Czech Republic

Beyond Prevention: Engineering Cyber Resilience for Europe's Energy Infrastructure - Antoine d'Haussy, VP OT Security Practice Lead International, Fortinet

Agahro Ono, Chief Executive Officer, ASCANO Integrated Services

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

11:15am - 12:30pm - Session 3b: Cybersecurity and Cyber Resilience Sector Symposium

Cybersecurity for critical infrastructure has shifted from prevention alone to a broader focus on resilience. While strong defenses, threat detection, and response remain essential, today's threat landscape demands the ability to withstand, adapt to, and rapidly recover from cyber incidents. This session explores the nature of increasingly sophisticated and disruptive cyber threats to proactive strategies for ensuring business continuity, disaster recovery, and operational integrity, enabling vital services to remain secure, reliable, and functional, to meet NIS2 and DORA regulations.
Chair: John Donlon QPM, FSyI

Dr Victor Vevera, General Director, National Institute for Research and Development in Informatics, ICI Bucharest

Mitigating Cybersecurity Risks in Legacy Healthcare Systems: Policy, Technology, and Response Strategies for Critical Infrastructure - Angela Wells, Professor/Technologist, City U Seattle Washington

The Human Factor: Cyber Security Culture in European Critical Infrastructure - Laith Shahin, CEO & Founder, Secolve

Critical infrastructure under pressure in an evolving threat landscape - Andrew Lee, Vice President of Government Affairs, ESET

12:30pm - Delegate Networking Lunch

Wednesday 21st October

Track One

2:00pm-3:30pm - Session 4a: Infrastructure Resilience Under Fire: Ukraine Case Study

Lessons learned from Ukraine - the most advanced real-world laboratory for modern critical infrastructure resilience under sustained attack - where the country is witnessing constant coordinated attacks. Listen to Ukraine's experts tasked with keeping the lights on and goods moving. It's the only large-scale, prolonged test of critical infrastructure under continuous cyberattacks, physical strikes (from missiles and drones) and hybrid warfare.
Chair: John Donlon QPM, FSyI

Critical Infrastructure Protection in Wartime: Ukraine's Approach to Integrated Protection and Defence - Vasyl Ananyev, Head of Unit, Dept of CIP, SSCIP, Ukraine

Energy Infrastructure & Energy Supply Resilience: War-time Lesson - Dr Oleksandr Sukhodolia, Head of Dept of CI, Energy & Environmental Security, National Institute for Strategic Studies & Lead Consultant, Dept of CIP, SSCIP, Ukraine

Implementation of the State Concept of Engineering Protection of CI Facilities 'Fortress Country' - Artem Bilyk, Assistant Professor, Research Institute of Military Intelligence, Ukraine

Establishment and Development of a System for the Deployment of Interceptor Drones - Tymur Khromaiev, Deputy Commander of Separate Special Purpose Center, Armed Forces of Ukraine

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

4:15pm - 5:30pm - Session 5a: Skills Gaps, Fragmentation Capabilities & Public–Private and Cross-Sector Coordination

Critical infrastructure resilience is increasingly constrained by workforce shortages and fragmented capabilities across sectors and borders. This session explores how skills gaps in cybersecurity, OT, and crisis management limit preparedness, and siloed operations hinder effective response. It will examine the urgent need for cross-sector coordination, improved information sharing, and aligned capability development. Attendees will gain practical insights into building a more integrated, skilled, and collaborative resilience ecosystem.
Chair: John Donlon QPM, FSyI

Maj. Gen. Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection (SSCIP)

Pressuring the chain: a live tabletop exercise for stress-testing the Gold–Silver–Bronze command - Kim Covent, Advisor, Ghent Local Police

Next-Generation Models for Cross-Sector Coordination: Building an Operational Ecosystem for Infrastructure Resilience - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory)

A Strategic Framework for National and Critical Infrastructure Resilience in the Hybrid Threats Era - Abraham (Avi) Bachar, CEO, IsraTeam 98 Ltd

Track Two

2:00pm-3:30pm - Session 4b: Transport & Logistics Sector Symposium

The transport (road, rail, air) and logistics sector is a cornerstone of critical infrastructure, enabling the movement of people, goods, and essential services. Increasing interconnectivity, digitalisation, and reliance on complex supply chains expose it to cyber, physical and hybrid threats. This session examines strategies to enhance resilience, protect key assets, and ensure continuity, focusing on risk management, cross-border coordination, and safeguarding operations against evolving threats in a dynamic global environment.
Chair: Catherine Piana

Developing Governance to Manage Security in Infrastructure Design Projects at Airports: Heathrow Case Study - Sarah Prew, Arup UK

David Nieto, VP Member Success, Aviation ISAC

Faye Francy, Executive Director, Auto-ISAC

Railway resilience – impact of an infrastructure manager - Peter Driessens, Head of Safety, Infrabel

Philip Van den Bosch, Senior Supply Chain Strategist and Rail Freight Expert, Lineas

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

4:15pm - 5:30pm - Session 5b: Maritime and Subsea Infrastructure Sector Symposium

Maritime and subsea infrastructure now face an intensified threat landscape, from hybrid and cyber attacks on ports, vessels, and undersea cables to rising geopolitical tensions and sabotage risks. As digitalisation expands vulnerabilities, protecting this sector requires integrated resilience strategies, including integrating physical security, cybersecurity, and operational continuity, alongside stronger international collaboration to protect global trade and connectivity.
Chair: Lina Kolesnikova

Resilience of the Maritime Critical Infrastructure in Belgium - Eric Rummens, Advisor, Service Public Federal Mobilité et Transport (DG Navigation), Belgium

SAFEDigimar: Strengthening cybersecurity to build a more resilient port ecosystem - Maarten Boot, Policy Advisor, FEPORT - Federation of European Private Port Companies and Terminals

SIDMETICS: The Mediterranean Hub for the Protection of Submarine Critical Infrastructures - Francisco Luis De Andrés Pérez, CEO, Ciso.es

Underwater Threats – CIP Water Frontier Expansion - Simon Goldsworthy, Global Business Development Manager, Forcys

critical infrastructure
PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium
www.cipre-expo.com

Thursday 22nd October

Track One

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

The latest technologies for detecting and predicting threats to critical national infrastructure span ground, land, underwater, space-based, and cyber domains, supported by advanced sensors and access control systems. Artificial intelligence increasingly enhances these capabilities by improving speed, accuracy, and cross-domain analysis of threat signals. New, developing systems and solutions enable earlier detection, better prediction, and stronger situational awareness across interconnected infrastructure systems.
Chair: Martin Hromada

Cryptographic Keys in Access Control Systems for Critical Infrastructure - Harish Rasiah, Sales Support Manager (Speaker will be Head of Sales or Product Manager), LEGIC Identsystems

Jose Ruiz Cristina, IndraMind Security Business Development Director Indra Group, Spain, IndraMind

From Drone Detection to Defensible Decisions: Lessons from Protecting Belgium's Critical Infrastructure - Gerrit Van Kerckhoven, Key Account Manager, Skeydrone

Resilience by Design: how fire and security technologies protect critical infrastructure - Christian Grossenbacher, Senior Director, Honeywell, Switzerland

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: Drones and UAS

Drones present a growing threat to critical infrastructure due to their accessibility, manoeuvrability, and payload capabilities, enabling surveillance, disruption, or delivery of explosives. However, they can also support infrastructure protection through monitoring and response applications. This session examines the evolving drone threat landscape, available countermeasures, and the dual-use role of drones in both challenging and enhancing critical infrastructure security and resilience.
Chair: Catherine Piana

Clogged Skies, Clogged Feeds: Drone Sightings and the Weaponisation of Information Disorder - Natasia Kalajdziovski, Senior Fusion Threat Intelligence Analyst, SecAlliance

Drones for Resilience & Surveillance - Ievgen Romanov, CEO, SkyDock

The Convergence of Physical and Aerial Threats: Protecting Critical Infrastructure from Drone-Delivered Attacks - Hollice Stone, President, Stone Security Engineering

Adapting to Drone Threats: Scalable Non-Disruptive, Non-Kinetic Counter-UAS Strategies for Critical Infrastructure Protection - Marco Harder, Sales Director, Benelux and Scandinavia, D-Fend Solutions

Track Two

9:00am-10:30am - Session 6b: Risk Mitigation, Resilience, Business Continuity Strategies

Developing effective resilience strategies across the critical infrastructure community requires disciplined information sharing, strong preparedness, and robust risk mitigation and management. This session explores how organisations can identify, assess, and prioritise risks in a structured way, while reducing vulnerabilities and strengthening overall system resilience. It also examines how to embed continuity planning for potential disruptions or disasters, ensuring coordinated responses and support long-term operational stability across interconnected infrastructure systems.
Chair: John Donlon QPM, FSyl

Bridging Public Warning Systems and Critical Get risk wrong, get the response wrong - Chris Needham-Benne, Managing Director and Visiting Professor University College London, Needams1834

Risk Mitigation, Resilience, Business Continuity Strategies - Hugo Marynissen, Managing Partner,/Co-holder Chair of Crisis Governance, PM/Risk Crisis Change, University of Antwerp

Insider Risk Management in Critical Infrastructure: A Path to Resilience and Compliance - Dennis Bijker, CEO and Enrico Henriksson, Senior Risk Adviser , SignPost Six

The development of an effective PNT test framework to measure resilience in critical infrastructure - Eleftherios (Akis) Drosinos, PNT Solutions Architect, Keysight

How Europe's consulting engineering community supports infrastructure reduce risk across the infrastructure lifecycle - Sue Arundal, Director General, EFCA

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

11:15am - 12:30pm - Session 7b: AI and Cyber in CI

AI plays a dual role in critical infrastructure cybersecurity, acting as both a defensive tool and a potential threat. It strengthens protection by improving threat detection, automating responses, and predicting attacks through advanced data analysis and anomaly detection. However, malicious actors can also exploit AI to develop more sophisticated attacks. We investigate how effective defence requires harnessing AI's benefits while managing its risks through strong security controls and continuous adaptation.
Chair: Alessandro Lazari

AI-driven cybersecurity for critical private wireless networks - Filippo Gaggioli, Head of Security Product Introduction, Nokia Cloud and Network Services

Safety by Design: AI-Assisted Threat Detection That Protects Industrial Operations - Ali Mohammed, Senior OT/ICS Cybersecurity Engineer, Resilience

Alexandru Georgescu, ICI Bucharest, Romania

Isolated AI Systems and Secure Orchestration Strategies for Strengthening Critical Infrastructure Protection and Resilience - Roger Sanz Gonzalez, European Projects Manager. R&D, UI1 University

12:30pm - Delegate Networking Lunch

Thursday 22nd October

2:00pm-3:30pm - Plenary Session 8:
PANEL DISCUSSION - Systemic Risk and Uneven Resilience: Confronting Europe's Next Critical Infrastructure Shock

In this panel discussion, we will examine Europe's current preparedness for systemic infrastructure disruption, exploring the persistent resilience gaps across Member States and critical entities, and its fragmented capabilities against the evolving hybrid threat landscape. In this engaging discussion, we will assess how current NIS2 and CER implementation is addressing these challenges, where governments and operators are succeeding and falling short, and what must change to influence future frameworks such as NIS3 and CER2, ensuring more consistent, cross-border, and operationally effective resilience across Europe.

Moderator: John Donlon QPM, FSyI,

Sebastian Serwiak, Policy Officer, European Commission

Catherine Piana, Secretary General, CoESS

Vasyl Ananyev, Head of Unit, Dept of CIP, SSCIP, Ukraine

Esmeralda Kazia, Chief Technology Officer, Albanian Power Corporation

Ricardo De Sousa Figueiredo, Cybersecurity Expert – Resilience of Critical Sectors Unit, ENISA

Vasileios Mingos, European Operations Director, Health-ISAC

3.30pm - Conference Close
John Donlon QPM, FSyI, Conference Chairman

Register online at www.cipre-expo.com/register
Early Bird Deadline - 20th September 2026





Crisis Communications Network Europe (CCNE) Workshop

CCNE
CRISIS COMMUNICATIONS NETWORK EUROPE

Workshop: From Incident to Communication: Crisis Communications for Critical Infrastructure

Wednesday 21st October - 9.00am-10.30am

Effective crisis communications are an essential part of organisational resilience and crisis management, as recognised by the Critical Entities Resilience (CER) Directive. In this interactive workshop, the Crisis Communications Network Europe (CCNE) will explore how communications support the response to incidents affecting critical infrastructure, from tactical communications in the field to strategic engagement with stakeholders, authorities, and the public. Working through a realistic scenario, participants will examine challenges, exchange experiences, and explore practical methodologies, best practices, and lessons learned. The session is intended for anyone responsible for, or interested in, crisis communications and resilience, and aims to provide practical insights that can be applied across a wide range of organisations and sectors.

Speakers:

- Stijn Pieters, Managing Partner PM • Risk Crisis Change
- Robbert Meulemeester, Senior Advisor & Trainer PM • Risk Crisis Change

Register online at **www.cipre-expo.com/register**

CoESS

Confederation of European Security Services (CoESS) Workshop

Workshop: The Role of Private Security in Safeguarding Critical Infrastructure in the Context of Europe's Preparedness Union

Wednesday 21st October - 11.00am-12.30pm

Europe has entered a new era of preparedness. As the threat environment becomes more complex, the challenge is no longer simply whether Europe has the capabilities to protect its critical infrastructure, but whether those capabilities can be effectively organised and mobilised when they are needed most. This session will explore what we call the Preparedness Gap: the gap between the capabilities and experience that already exist across society and those that are effectively recognised, connected and integrated into preparedness planning before a crisis occurs.

Private security provides a compelling illustration. Every day, private security professionals protect critical infrastructure and essential services, monitor sensitive sites, assess and respond to incidents, support business continuity and contribute to situational awareness. Yet these capabilities are not always systematically embedded in emergency planning, information-sharing arrangements, joint exercises and crisis governance. How can Europe move from ad hoc cooperation during crises towards Preparedness by Design, where roles, relationships and operational interfaces are established beforehand?

Co-hosted by the Confederation of European Security Services (CoESS), the session will bring together European policymakers, corporate security leaders and private security practitioners to examine how existing capabilities can be better recognised, integrated and governed as part of Europe's preparedness architecture.

Hans-Ulrich Goessl - Head of Unit B2 – Civil Protection Policy at DG ECHO, European Commission, will open the session with a keynote, followed by Marc Léoutre, Deputy Head of Unit at DG HOME D2. The panel discussion will bring together Jean-Philippe Bérillon, Chairman of the CoESS Critical Infrastructure Protection Committee and Member of the CoESS Board of Directors; Yvan De Mesmaeker, Secretary General of the European Corporate Security Association (ECSA); and Karolien Verbeiren, Country President of Securitas Belgium NV.

Together, they will consider a central question: how do we ensure that the capabilities Europe already possesses become part of preparedness before, not during, the next crisis? The session will be moderated by Catherine Piana, Director General of CoESS."

Speakers:

- Catherine Piana, Director General, CoESS Confederation of European Security Services, Belgium
- Hans-Ulrich Goessl, Head of Unit, DG ECHO, European Commission
- Marc Leoutre, Deputy Head of Unit DG HOME - Unit D2 Unit D2: Counter-Terrorism, Anti-Radicalisation, Critical Infrastructure
- Jean-Philippe Bérillon, Chair of the CoESS Critical Infrastructure Protection Committee
- Yvan De Mesmaeker, Director General of ECSA (European Corporate Security Association)
- Karolien Verbeiren, Country President of Securitas, Belgium

Register online at **www.cipre-expo.com/register**



African Young People Support Center

AFRICAN SMART CITIES INNOVATION FOUNDATION

African Young People Support Centre / African Smart Cities Innovation Foundation Workshop

Workshop: Africa–Europe Cooperation for Critical Infrastructure Resilience

Nigeria at the Forefront: Emerging Voices, Rising Together Youth Powering Regional Infrastructure Protection

Wednesday 21st October - 2.00pm-3.30pm

As the international communities continue to confront diverse threats to critical infrastructure—from cyber disruptions and climate shocks to energy insecurity and health crises—a more inclusive and collaborative response is urgently needed. Historically under-represented, Africa's young people are now stepping into leadership roles, developing innovative solutions, and advocating for more secure, inclusive systems.

Nigeria, as Africa's most populous country and economic powerhouse, is uniquely positioned to lead on young people-driven resilience efforts. This side event, held on the margins of Critical Infrastructure Protection & Resilience Europe (CIPRE), offers a platform to elevate African young people voices and foster cross-continental dialogue and cooperation with European counterparts.

Objectives

* To highlight Nigeria's role as a leader in young people engagement on critical infrastructure protection in Africa.
* To facilitate dialogue between African and European people and institutional stakeholders on resilience-building.
* To share real-life young people-led innovations and approaches from Nigeria and other African countries.
* To lay the groundwork for a formal young people platform focused on infrastructure protection cooperation between Africa and Europe.

Target Participants

* African and European young people and industry leaders and innovators
* Policymakers and government officials from both continents
* Infrastructure and cybersecurity professionals
* Representatives of the AU, EU, UN, and development partners
* Academic and civil society actors

AGENDA

Opening Session : Welcome address & keynote: "From Abuja to Brussels: Why Young People Must Lead the Next Era of Infrastructure Resilience"

Part 1 : "Young People at the Crossroads: Africa–Europe Partnerships for Infrastructure Resilience" Panel discussion highlighting opportunities, challenges, and success stories.

Part 2 : "Nigeria at the Forefront: Young People Powering Regional Infrastructure Protection" Dialogue on Nigeria's national leadership, innovation, and young people participation in resilience planning.

Part 3 : "NextGen Solutions: Young People Innovations for Critical Infrastructure" Young people-led pitches and showcases of real-world projects.

Part 4 : "Co-Designing Young People-Led Africa–Europe Resilience Platforms" Interactive roundtable generating practical recommendations and frameworks.

Closing Remarks : Summarising outcomes and proposing the launch of the Young People for Infrastructure Resilience Africa–Europe Network (YIR-AEN).

Expected Outcomes

* Strategic recommendations for enhancing young people roles in transnational infrastructure security
* Strengthened Africa–Europe partnerships focused on inclusive resilience planning
* Visibility for Nigerian young people leadership in global policy circles
* Momentum for establishing a permanent young people dialogue platform

Participation in this Workshop is complimentary and open for delegates to CIP Week and CIPRE.

SPEAKERS:

- Aigbe Osagie Daniel, Systems Security Engineer, Major Solar
- How aviation, immigration, and tourism infrastructure across Africa intersect with critical infrastructure protection - Omotola James, Travel, Tourism & Immigration Advisory Specialist
- Paul Igbinere, Executive Director, African Young People Support Centre
- Ehimwenma Idemudia, IT Specialist & Data Science & Analytics Professional, iChase Outsourcing
- Harrison Efe Ogiemwanre, Chief Executive Officer, SEF

Register online at **www.cipre-expo.com/register**



Information Sharing & Analysis Centres (ISACs) Workshop

Workshop: Cyber Resilience Without Borders: Lessons from the ISAC Community in Collective Defense

Wednesday 21st October - 4.00pm-5.30pm

Cyber resilience depends on trusted collaboration that transcends organizational, sector, and national boundaries. Information Sharing and Analysis Centers (ISACs) have become a cornerstone of collective defense by enabling members to exchange timely threat intelligence, operational experiences, vulnerabilities, mitigation strategies, and lessons learned within trusted communities.

This interactive session brings together leaders from multiple sector-specific ISACs—including automotive, aviation, financial services, healthcare, and space—to explore how trusted information sharing strengthens resilience across Europe's critical infrastructure. Participants will gain insight into the origins and evolution of the global ISAC model, the role of the European Council of ISACs in fostering cross-sector collaboration, and the current cyber threat landscape impacting European critical infrastructure.

The session will conclude with a discussion on the essential partnerships between ISACs and public-sector organizations, including ENISA and the European Commission, highlighting how industry and government work together to enhance situational awareness, improve coordinated response, and advance collective cyber defense across Europe.

Speakers:

- Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)
- David Nieto, VP Member Success, Aviation ISAC
- Rebecca Huffee, Senior Consultant Secure Space Systems, CGI, UK
- Vasileios Mingos, European Operations Director Health-ISAC
- Andrija Višić, Senior Community & Programme Manager, ETIS – European Telecommunications ISAC
- Kai Jensen-Kusk, Director of EMEA Strategic Partnerships, FS-ISAC

Register online at **www.cipre-expo.com/register**







International Association for Resilience Analysis

European Cluster for Securing Criticl Infrastructures (ECSCI) Workshop - Resilience Stress Testing

Workshop: Resilience Stress Testing as a Critical Element of Implementation of the European Directive on Critical Entity Resilience (CER Directive)

Thursday 22nd October - 9.00am-10.30pm

The European Directive on Critical Entity Resilience (CER Directive), has entered into force in 2023, became mandatory in the EU in 2024, and, by now, widely adopted as national law and included in national strategies for enhancing resilience of critical entities/infrastructures (CIs). Out of estimated more than 15,000 CIs concerned by CER Directive, several hundred of them are assumed to involve possible cross-border impacts. These cross-border cases will certainly increase the need for resilience benchmarking and stress testing, as metrics and processes for quantifying cross-functional and cross-border interdependencies still need to be developed and be agreed upon.

The workshop will, therefore, focus on ongoing efforts to develop the relevant, consensus-based guidelines, including those related to the common stress testing framework, agreed stress testing procedures, resilience measurement and its use in stress testing, and providing and promoting samples of good stress testing practice in the relevant stress testing application cases/scenarios.

Examples of the real-life scenarios are abundantly provided in the current geopolitical and economic risk landscape, such as extreme threats (XTs), polycrises and issues related to the critical supply chains. Networks and associations can and should play a pivotal role in both the co-development and acceptance of the above guidelines. The workshop will, therefore, explore practical approaches for co-designing, agreeing upon and aligning of the common resilience stress testing guidelines, focussing on the EU level, where the European Cluster for Securing Critical Infrastructures (ECSCI, https://www.ecsci.eu), which brings together 71 projects focused on critical infrastructure resilience, has already established itself as a key stakeholder actor in this context. This workshop will be part of and contribute to this broader ECSCI context.

The Workshop is organized in cooperation with IARA – International Association for Resilience Analysis.

Tentative list of topics to be considered for the short presentations & and the panel:

1. EU: Current status and scientific and technical challenges of the CER implementation
2. Implementation at the National level (Germany, France, Italy...)
3. Role of cluster, networks and associations at the EU level
4. How the EU resilience strass testing setup could look like (ENISA, NIS2, CER, DRS ...)?
5. Relevant international efforts (ISO, OECD, IARA, UK, USA, Australia, China, Canada...)
6. Discussion
   - How to ensure that all the eleven CER sectors of the CIs achieve the same maturity as the cyber/IT sector?
   - What kind of support (actions, supporting documents, events...) is needed for successful resilience stress testing?
   - What kind of interaction is needed? Interaction with the Commission? What kind interaction with regulatory and implementation authorities (e.g., the CER Competent Authorities in the EU)?
   - What can be shared as good practice internationally (US, Canada, Australia...)?
   - Relevant issues for particular stakeholders' groups? Insurance? PPP?
   - Other relevant issues?

Organizers:

- Prof. Aleksandar JOVANOVIC, CEO, Steinbeis European Risk & Resilience Institute (EU-VRi), Germany
- Dr. Habtamu ABIE, ECSCI Chair, Chief Research Scientist, Norwegian Computing Center (NRS), Norway
- Prof. Igor LINKOV, Founding President, International Association for Resilience Analysis (IARA), USA

Register online at **www.cipre-expo.com/register**



Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

20th-22nd October 2026 - Brussels, Belgium



Networking Reception

Tuesday 20th October
5.30pm - 7:30pm

We invite you to join 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 Exhibition Hall at CIP Week / CIPRE.

Open to the delegates of Critical Infrastructure Protection & Resilience Europe and CIP Week.

We look forward to welcoming you.





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

Event Venue & Accommodation

Sheraton Brussels Airport Hotel

Brussels National Airport
Brussels, 1930
Belgium
www.marriott.com/en-us/hotels/brusi-sheraton-brussels-airport-hotel/overview/

For more details visit:
www.cipre-expo.com/venue



Steps away from the main gate at Brussels Airport, the Sheraton offers sound-proofed rooms with flat-screen TV. The hotel includes a gym, 24-hour room service and a lobby computer terminal. Guests can benefit from the Sheraton Club Lounge experience. The design guest rooms at Sheraton Brussels Airport Hotel & Conference Center have Sheraton Sleep Experience Bed. Each of the air-conditioned rooms also benefit from a mini-bar. Brussels Express Train Station is located underneath the hotel and offers direct links into the center of Brussels. The Atomium is a 15-minute car journey from the hotel and the NATO Headquarters are only 5 minutes away by car. Gullivers Restaurant serves anything from a breakfast buffet to a chic à-la-carte dinner and cocktails. Guests can also enjoy a traditional Belgian beer at the bar.

Accommodation Information and Booking link can be found at www.cipre-expo.com/accommodation

Direct hotel booking link: www.cipre-expo.com/hotel-booking



Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium

International Association of CIP Professionals

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



Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to CIP Week and Critical Infrastructure Protection & Resilience Europe 2026.

Co-Hosted by:

International Association of CIP Professionals

Global Cybersecurity Partner / Platinum Sponsor:

ESET Digital Security Progress. Protected.

Gold Sponsor:

IndraMind

Silver Sponsor:

FORTINET

CIP Week Event Partners:

CCNE Crisis Communications Network Europe · CoESS · African Young People Support Center · AUTO-ISAC · Health-ISAC · Aviation ISAC · FS-ISAC · Etis · Space ISAC

Executive Sponsors:

ASD · E.DSO · CRISR · EurEau · ENLCC · euralarm

Supporting Organisations:

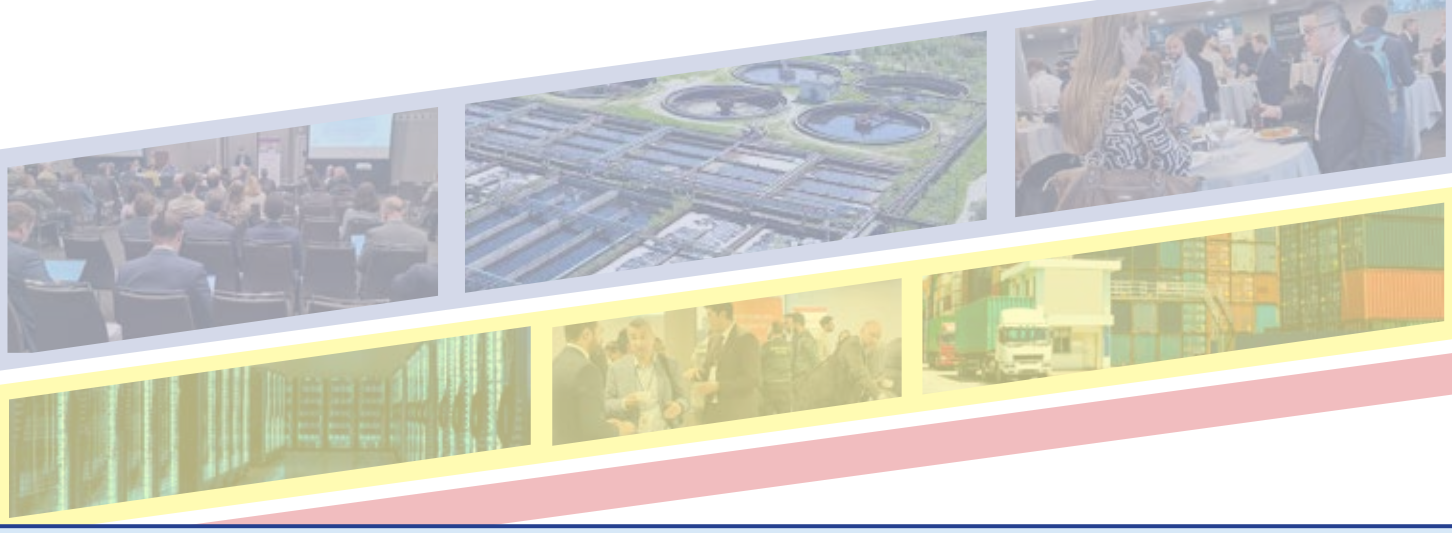
International Association for Resilience Analysis · African Smart Cities Innovation Foundation · Help2Protect · NS&RC

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporters:

Cyber Security Review · Biometric Update.com · govCIO Outlook · CIO Review Europe



We look forward to welcoming you to Brussels, Belgium for the next gathering of the international critical infrastructure protection and resilience community.

critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium

www.cipre-expo.com

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

Early Bird Deadline - 20th September 2026