Coordinated by
I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by
DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICĂ

GUVERNUL
ROMÂNIEI

CRA EUROPE 2026 – CYBER RESILIENCE IN ACTION, CYBERFORT Conference

CYBERSECURITY INTERNATIONAL CONFERENCE EVENT

Supported by The Romanian National Cyber Security Directorate (DNSC)

4 March 2026, 09:00 – 17:00 EET (08.00 – 16:00 CET)
Location: Romanian Parliament, Bucharest
Access LINK for Speakers

AGENDA

Time	Topic	Speaker
8:00– 09:00	**Registration & Welcome Coffee**	
09:00 – 09:10	**Opening Remarks: Conference and CYBEFORT Project Main Objectives**	**Mihai PĂUN** *Founder I-ENERGYLINK* *CYBERFORT Consortium Coordinator*
09:10 – 09:20	**The Role of the Commission for Industries and Services for Digitalization and Society's Progress and Economic Security**	**Cristina-Madalina PRUNA** *Vice-President Commission for Industries and Services* *Romanian Parliament*
Session 1 – Setting the CRA Compliance Framework for SMEs		
09:20 – 10:15	**Executive Panel - Setting the Strategic Vision for CRA Compliance**	**Moderator: Radu PUCHIU**, *Director - Technology & Society Program* *ASPEN Institute Romania* **Dan CÎMPEAN**, *The Director of DNSC** **Rodica TIRTEA,** *Senior Policy Officer ECCC* **Dragoș-Cristian VLAD,** *The President of The Authority for the Digitalization of Romania* **Ana Maria BUȘONIU**, *Head of NCC-RO* **Alexandru CHIRIȚĂ**, *CEO Electrica* **Sterică FUDULEA**, *Secretary General SMEs Romania* **Nikos KEKATOS**, *R&D Coordinator CLONE SYSTEMS*
10:15 – 10:30	**The Role of Standardisation in CRA**	**Iuliana CHILEA**, *Director General, Romanian Standardization Association ASRO, VP CEN-CENELEC*
10:30 – 11:00	**Coffee Break & Networking**	

Coordinated by

I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICĂ

Session 2 - Cybersecurity Projects, CRA Compliance, and European Policy Perspectives

		Moderator: Vasilis PSYRAS, *Advocate, Elias Neocleous*
11:00 – 12:00	**High-Level Discussion** **Implementation Perspectives**	**Perit KIRKMANN-RAAVE**, *Seconded National Expert (MTPS unit) at the European Union Agency for Cybersecurity ENISA**
		Claudia LASCATEU, *Legal Expert DNSC*
		Radu VASILE, *CEO Eximprod Engineering*
		Mihai CHIHAIA, *CIO DVLOPER*
		Michael IOANNOU, *CEO BOLTON TECHNOLOGIES LTD*
		Orsolya BAKO, *Vice-President Women4Cyber*
12:00 – 12:10	**Keynote Speech:** **Turning CRA into Reality:** **Implementation Roadmap**	**Tjabbe BOS**, *Policy Officer Cybersecurity European Commission, DG CONNECT**
12:10 – 12:25	**CYBERFORT Project Objectives and Preliminary Outcomes**	**Paul LACATUS**, *Deputy Project Manager CYBERFORT / I-ENERGYLINK &* **Nikos KEKATOS**, *R&D Coordinator CLONE SYSTEMS*
12:25 – 12:45	**Platform Presentation: CYBERFORT in Action -** *Live Demo*	**Nikos KEKATOS,** *R&D Coordinator CLONE SYSTEMS*
12:45 – 13:45	***LUNCH BREAK***	
		Moderator: Mihaela CURCA, *Project Manager DNSC*
13:45 – 14:35	**Pilot Use Cases Showcase – CRA Compliance in Action**	**Project Partners leading CYBERFORT Pilots – Practical Experiences and Lessons learned:**
		Paul LACATUS, *Deputy Project Manager CYBERFORT I-ENERGYLINK*
		Marios IOANNOU, *COLUMBIA (**Maritime**)*
		Daniel AVRAAM, *DEALIO (**Finance**)*
		Angelos FOUNTOULAKIS, *EPG (**Energy**)*
		Giorgos KOUTIDIS, *CLONE SYSTEMS (**Cybersecurity SMEs**)*
14:35 – 15:25	**Panel Discussion: Building a CRA Support Ecosystem**	**Moderator: Sebastian NASTE**, *DNSC - CRA Group*
		Alexandru SUDITU, *Managing Director & Co-founder, SentryOT*
		Rita JONUSAITE, *Government Affairs & Public Policy Manager Google***
		Octavian POPA, *Manager Deloitte*
		Gabriel RAICU, *Rector Constanta Maritime University******
		Emilios CHARALAMBOUS, *Associate, Elias Neocleous*
		Marius ROȘU, *CISO PPC Romania*
15:25 – 15:50	**Coffee Break Networking**	

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Coordinated by

I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Session 3 - From Compliance to Capability: Building Sustainable CRA Readiness for SMEs

15:50 - 16:05	**CYBERSTAND Project - CRA Cluster**	**Nicholas FERGUSON,** *TRUST-IT SERVICES – CYBERSTAND Project**
16:05 – 16:50	**Synergies: What's Next for SMEs post CRA – ECCC co-funded Projects References**	**Moderator: Angelos FOUNTOULAKIS**, *Project Manager, Eximprod Engineering* **Elena COSMA,** *NCC-RO – CRACY Project* **Daniela TAPI,** *DNSC - CRA-AI Project* **Mirabela SAVULESCU,** *DNSC - CONFIRMATE Project* **Michael IOANNOU,** *BOLTON Technologies - SECUR-EU Project* **Marios IOANNOU,** *COLUMBIA Group – CYBERGUARD Project* **Giorgos KOUTIDIS,** *CLONE SYSTEMS – INTERSOC Project* **Paul MUNTEANU,** *I-ENERGYLINK – CYBER-BRIDGE Project*
16:50 – 17:00	**Closing Remarks**	

NOTE: **Confirmed On-Line ***

Coordinated by

I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICĂ

Event Information

Introduction

CRA EUROPE 2026 – Cyber Resilience in Action is a high-level European cybersecurity conference focused on the operational implementation of the **Cyber Resilience Act (CRA)**. The event examines how CRA requirements translate into concrete obligations and practical adjustments for SMEs, public authorities, manufacturers, integrators, and operators in critical sectors.

Organised with the support of the **Romanian National Cyber Security Directorate (DNSC)** and the **CYBERFORT consortium**, the conference convenes European and national decision-makers, regulators, supervisory authorities, industry executives, cybersecurity experts, technology providers, and academic representatives. The objective is to move from regulatory interpretation to structured, actionable compliance models.

The conference provides a platform for aligning European policy direction with national implementation frameworks and project-driven instruments. Through executive panels, high-level discussions, pilot demonstrations, and practical case studies, CRA EUROPE 2026 highlights how legislative requirements, supervisory expectations, and technical capabilities converge in real operational environments.

By hosting this event in Bucharest, Romania reinforces its role as an active contributor to the European CRA ecosystem and as a regional anchor for SME-focused cyber resilience initiatives. The conference demonstrates how coordinated policy, national governance mechanisms, and EU-funded cybersecurity projects can deliver measurable impact and sustainable compliance capacity across the European market.

Objective

The main objective of CRA EUROPE 2026 is to transform the requirements of the Cyber Resilience Act into clear, practical guidance for SMEs and key stakeholders. The conference connects European and national policy perspectives with operational implementation models and real pilot experiences developed within the CYBERFORT project. CRA EUROPE 2026 is designed to:

- Provide clarity on CRA obligations, implementation timelines, and enforcement expectations.
- Demonstrate how compliance looks in real product development environments, particularly for SME product and engineering teams.
- Present practical tools, methodologies, training formats, and services that support structured CRA readiness.
- Facilitate direct connections between SMEs and national or European support mechanisms, including helpdesks, projects, and supervisory authorities.
- Strengthen cooperation between regulators, industry leaders, technology providers, consultants, academia, and cybersecurity authorities in order to build a coordinated and sustainable CRA support ecosystem.
- The conference moves beyond theory and regulatory summaries. It focuses on realistic implementation pathways and long-term compliance capability.

Coordinated by

I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by

DIRECTORATUL NATIONAL
DE SECURITATE CIBERNETICĂ

Session 1 – Objective

Cybersecurity Projects, CRA Compliance, and European Policy Perspectives

Session 1 delivers a strategic and regulatory overview of how the Cyber Resilience Act is being implemented within the broader European cybersecurity architecture.

This session places CRA in context. It explains how the regulation interacts with NIS2, the Cybersecurity Act, certification schemes, and EU funding instruments. It clarifies institutional roles and highlights what national authorities and European bodies are expected to deliver. The discussion concentrates on:

- National and European implementation approaches.
- The alignment between CRA, NIS2 obligations, certification mechanisms, and EU support frameworks.
- The contribution of cybersecurity projects, including CYBERFORT, to practical compliance enablement.
- Concrete national implementation tools such as official guidance, helpdesks, supervisory models, market surveillance approaches, and SME support mechanisms.

Through executive panels, high-level exchanges, platform presentations, and pilot use cases, Session 1 demonstrates how policy direction, regulatory structure, and operational deployment intersect. The objective is to provide clarity, reduce ambiguity, and show how institutional frameworks translate into tangible compliance pathways for SMEs across different sectors.

Session 2 - Objectives

From Compliance to Capability: Building Sustainable CRA Readiness for SMEs

Session 2 moves from regulatory understanding to operational endurance. It focuses on what happens after the Cyber Resilience Act starts to apply and how SMEs can maintain compliance in a structured and sustainable way. This session is project-driven and impact-oriented. It addresses implementation at product and organisational level, with emphasis on:

- Practical application of CRA requirements in development cycles and internal processes.
- Vulnerability handling procedures, incident reporting obligations, and documentation required to support CE marking.
- Mechanisms that ensure continuity of compliance beyond isolated projects or short-term initiatives.
- Synergies between CYBERFORT, CRA-AI, CONFIRMATE, and future DNSC services.
- Coordination among CSIRTs, consultants, academia, and technology providers to create a coherent support environment.

The session demonstrates how CYBERFORT functions as a foundational layer within a broader national and European CRA support ecosystem. SMEs are presented with:

- Structured and ongoing guidance.
- Access to training programmes and helpdesk services.
- Practical assessment methodologies and compliance support tools.
- Clear and realistic pathways to scale cybersecurity maturity over time.

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Coordinated by

I-ENERGYLINK

CYBERFORT
RESILIENT EUROPE

Supported by

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Session 2 concludes the conference by shifting the perspective from understanding regulatory obligations to building durable capability. The focus is not only on achieving compliance, but on maintaining it through coordinated institutional and ecosystem support.

Session 3 - Objective

From National Strategy to Market Transformation: Scaling CRA Implementation

Session 3 brings the discussion to the strategic and economic level. After clarifying obligations and presenting practical tools, this session focuses on long-term positioning: how Romania and its partners can transform CRA compliance into a competitive advantage.

Led by DNSC and I-ENERGYLINK, the session explores how regulatory alignment can evolve into structured market capability, innovation opportunities, and regional leadership in cybersecurity. The session addresses:

- *How national authorities can institutionalise CRA support beyond project cycles.*
- *How public-private partnerships can accelerate secure product development.*
- *How Romanian SMEs can leverage compliance to access new European markets.*
- *How investment, energy, digitalisation, and industrial sectors can align around secure-by-design principles.*

The objective is to move from compliance as an obligation to compliance as strategic positioning. Session 3 closes the event by articulating a forward-looking vision: a coordinated national ecosystem where policy, industry, and innovation converge to strengthen resilience, competitiveness, and trust in the European digital market.

This Project has received funding from the European Union's Cybersecurity and Trust Programme and Digital Europe Programme under Grant Agreement no. 101190281.

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Page 6