Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

CYBER RESILIENCE ACT
OSCRAT SEMINAR

Digital Innovation Hub
Trakia

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

OSCRAT
Open-Source Cyber Resilience Act Tools

About the Lecturer

- Lead Auditor for Management Systems (information security, services, quality, and more).
- Chairman of the **Institute for Artificial Intelligence**.
- Deputy Manager of the **Bulgarian Union of Standardizers**.
- Active participant in numerous European and national cybersecurity projects.
- Assistant Professor at **UniBIT**:
  - Cybersecurity Standards
  - Cybersecurity Management
  - Cryptography
  - Zero Trust Architectures

Seminar Structure

01

From September 2025 to April 2026.

02

First **four sessions** (Sep–Dec 2025): *theoretical foundations*.

03

Next **four workshops** (Jan–Apr 2026): *hands-on training and case studies with OCSRAT*.

04

Goal: build both **strategic understanding** and **practical skills** to apply the Cyber Resilience Act.

08.09.2025 Summary Key Points

•**Motivation:** Rising cyber incidents and fragmented national rules led to the need for a single EU framework ensuring “secure-by-design” products and trust across the Digital Single Market.
•**Scope:** Applies to *products with digital elements* — IoT devices, software, embedded hardware.
•**Structure:** Defines essential cybersecurity requirements, roles of manufacturers, importers & distributors, conformity assessment, CE marking, and declarations of conformity.
•**Regulatory Ecosystem:** Complements DORA, NIS2 & GDPR — together forming the EU digital resilience framework.
•**Implementation Status (2025):**
– European Vulnerability Database operational.
– Standards mapping by ENISA and JRC under way.
– Delegated acts and Single Reporting Platform pending.
– Full application by December 2027.
•**Core Message:** CRA is not just law but a strategic shift toward proactive cyber resilience in the EU.

Today’s Agenda

01

Which products are covered: IoT, software, embedded hardware.

02

Roles & responsibilities: manufacturers, importers, distributors.

03

EUCS (Cloud Services Scheme) – regulating cloud providers.

04

CRA impact on IoT manufacturers.

05

Obligations: declarations of conformity, vulnerability reporting.

06

Sanctions and consequences of non-compliance.

Q&A

- **How to ask:** Post questions in the **chat window**
- **When answered**
    - End of the current session
    - Beginning of the next session
- **Special cases**
    - Some questions may require deeper research
    - Answers may be provided later via **email**
- **Future opportunities**
    - Dedicated discussion slots in next sessions
    - Interactive Q&A during the workshops

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitev@dihtrakia.org