



Targeted actions for enhancing the protection of national characterized European critical infrastructure

Ilias Gkotsis

Associate Researcher

KE.ME.A.

Pantelis Themelis

Police Major

KE.ME.A.

3rd IMPROVER/ERNICIP Operators Workshop on Resilience for Critical Infrastructures - Lisbon (Portugal) - 23-24 May 2018



Legal framework for CIP in Greece

- **8th December 2008: 2008/114EC Directive of the European Council**



- ✓ A procedure for the identification and the designation of European Cis and a common approach to assess the need of improving the protection of these infrastructures
- ✓ Regular review of the list of designated European Cis
- ✓ Priority in the energy and transport sectors.

- **6th May 2011: Harmonisation of the Greek legislation with the Council Directive (Presidential Decree No 39/2011)**

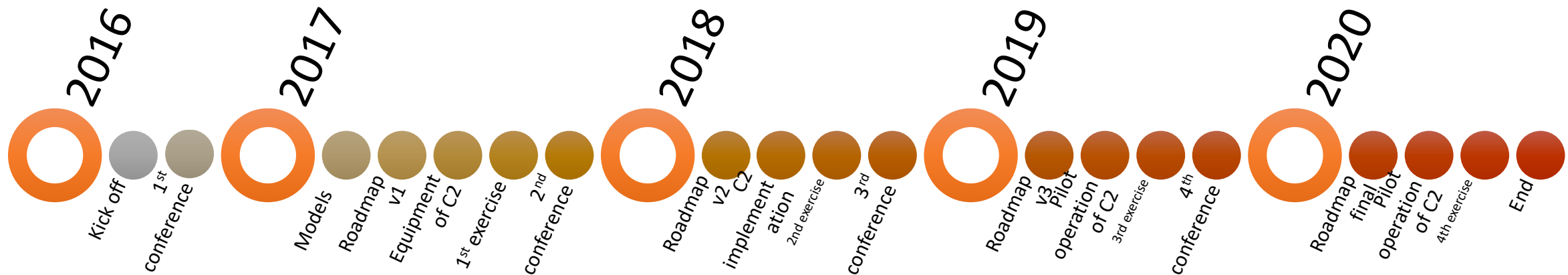


- ✓ KEMEA was appointed as the “**National Contact Point**” for the protection of European Critical infrastructures (ECIs) in context of the European Program of CIP - “EPCIP contact point” – aiming to implement the EC Directive 114/2008 “regarding the definition and designation of the European Critical infrastructures and the assessment of the need to improve the protection of such infrastructures”



Targeted actions for enhancing the protection of national characterized European critical infrastructures

- A series of actions designed to develop and establish a commonly accepted level of security and protection in Critical Infrastructures
- Objectives of these actions: Road Map for CIP, Model OSP, Pilot CIP Coordination Center, Preparedness Joint Exercises, CIP Networking and Synergies (Public and Private Sector)
- Project funded by the European Internal Security Fund / Police Cooperation Section





Roadmap for the protection of Critical Infrastructures

Policy document including background information and recommendations for CI and ECI protection:

- Identification of critical sectors and infrastructures and their characteristics
- Registration of CIs and ECIs
- Legal and institutional framework (national and EU)
- Challenges of CIP in Greece
- Technology and operational security capabilities
- Funding opportunities and instruments for CIP
- Role of KEMEA in the protection of ECIs



CIP OSP model

- Reference Models for the design of Operator Security Plans that include suggestions and guidance for the:
 - Structure
 - Contents
 - Methodology, Guidelines and instructions to deploy and apply security plans
 - Reporting templates
 - Monitoring and validation indicators
- Model OSP is structured in 5 Parts (Risk, Vulnerability, Operational Security, Emergency/Incident Response, Business Continuity)
- It will be provided as a guide to CI Managers and Operators for developing OSP



Parts of Model OSP for CIP

- Risk modeling part, based on all hazard approach
- Vulnerability modeling part, based on a common approach to identifying vulnerabilities of the infrastructure
- Physical Security modeling part, aiming to serve as a guide to improve the security and resilience of facilities
- Emergency/Incident Response modeling part, which will be a guide to deal with emergencies against a variety of risks
- Business Continuity modeling part, to guide restoration of the CI operation back to acceptable elementary levels of service following a disruption of disaster.



National CIP Coordination Center

- Development of a pilot (though operational) Coordination Center
- Video wall, teleconference, ICT facilities
- Database with national infrastructures
- Spatial DB (thematic maps) of natural hazards and threats (static / dynamic)
- Risk assessment software (according to the respective plan model)
- On-line available risk / threat maps with CI assets overlay (accessible only from the corresponding infrastructures)
- Incident reporting software (from the Infrastructures to the C2)
- Repository of CIP information (legislation, standards, model OSP, security plans etc) to be accessed by authorized users (operators and managers of CI/ECIs)



Preparedness exercises

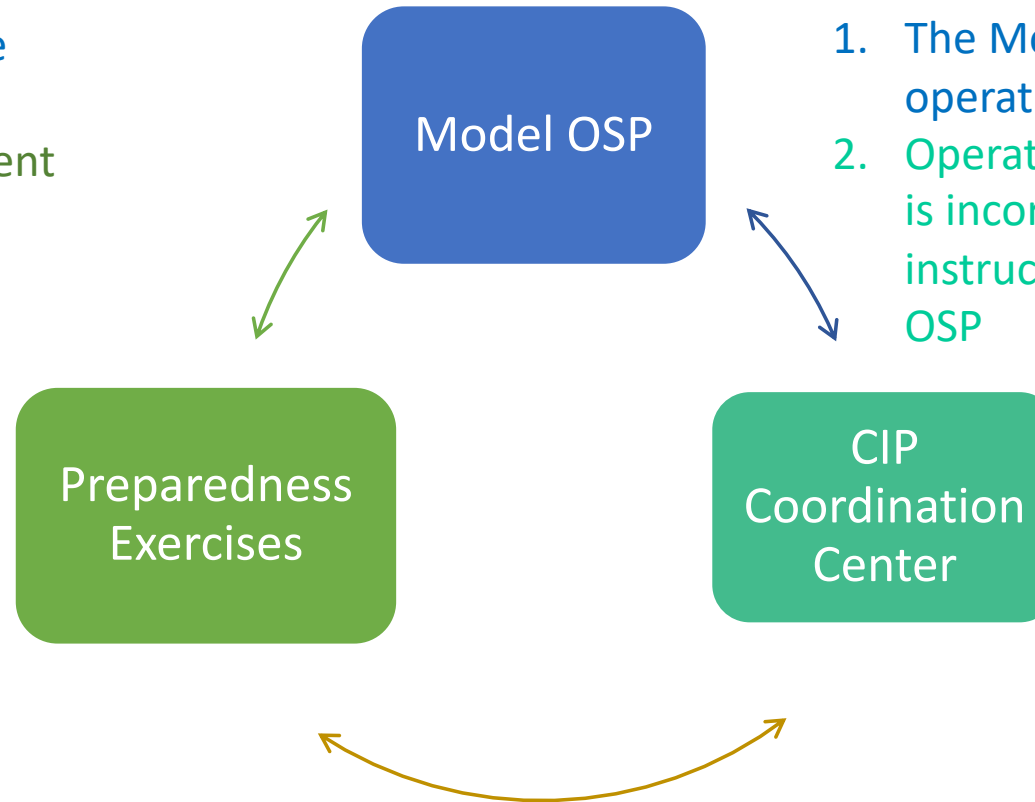


- Annually organized table-top exercises (preparedness) for different types of critical infrastructures using relevant scalable risk / threat scenarios
- Focus on the Energy and Transport sectors
- Involvement of security managers and infrastructure operators, public bodies and services



Holistic approach towards CIP at national and EU level

1. The Model OSP is related to the scenarios of the exercises
2. Exercises assist on the assessment of the Model OSP



1. The Model OSP is incorporated in the operation of the Coordination Center
2. Operation of the Coordination Center is incorporated in the instructions/guidelines of the Model OSP

1. Operation of the CIP Coordination Center is incorporated in the scenarios of the exercises



Thank you for your attention...

Ilias Gkotsis

Email: i.gkotsis@kemea-research.gr

Tel: +302107710805 ext. 333

Pantelis Themelis

Email: pthemelis@kemea.gr

Tel: +302107710805 ext. 344

www.kemea.gr