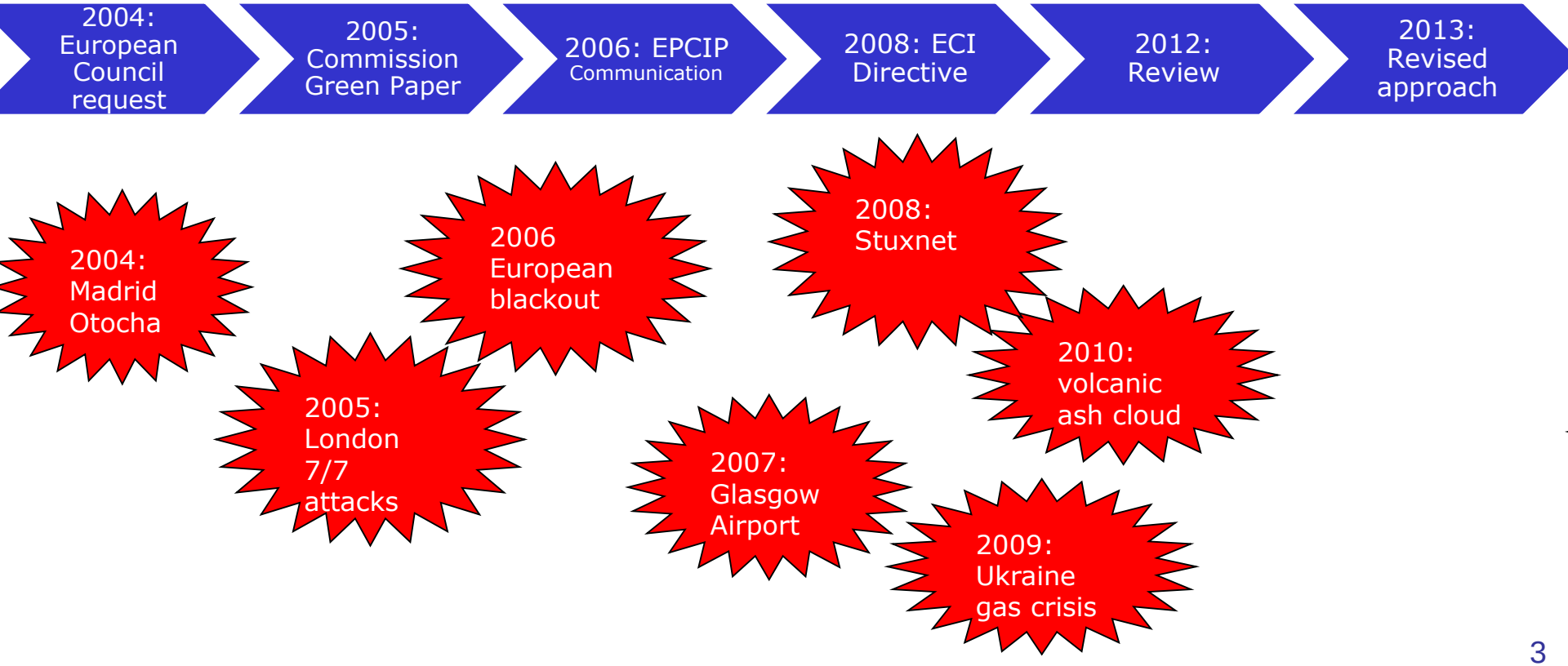
The European Programme for Critical Infrastructure Protection (EPCIP)

European Commission
DG Migration & Home Affairs

Overview

- **Introduction to the EPCIP**
- **New approach to implementing the EPCIP**
- **Current focus / future considerations**

History of EPCIP



The European Programme for Critical Infrastructure Protection (EPCIP)

Directive 2008/114/EC 8 December 2008

A procedure for the identification and designation of European Critical Infrastructures (ECI)

Measures designed to facilitate the implementation of EPCIP

- **CIWIN**
- **CIP expert groups**
- **CIP information sharing**
- **identification and analysis of interdependencies**
- **ERNCIP**

Accompanying financial measures

EU programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013

(CIPS)

Support for Member States concerning National Critical Infrastructure

Contingency planning

External dimension

Directive 2008/114/EC

European Critical Infrastructure (ECI)

- Means critical infrastructure located in Member States, the destruction or disruption of which would have a significant impact on at least two Member States

- Sectoral scope: energy and transport sectors.
- Sets out a 4 step approach to identify ECIs based on specific criteria
  - Cross-cutting criteria: casualties, economic effects, public effects
  - Sectoral Criteria established for Transport and Energy sectors

- Security Liaison Officer / Operator Security Plan

CIPS

- **Objective: to fund CIP-related measures and projects**
- **EUR 140 million for the period 2007-13 allocated for operational cooperation and coordination actions**
- **Since 2007, 125 projects funded, including:**
  - Methodologies for risk analysis
  - Analyses of dependencies and interdependencies
  - Exercises
  - Studies

CIWIN

- **Internet-based protected information and communication system**
- **Objective: to exchange CIP-related information, studies and good practices among the EU CIP community**
- **Operational since January 2013**
- **Plans in the context of new approach to EPCIP:**
  - CIP Toolbox, comprising risk assessment methodologies and the tools (e.g. templates), research results
  - Host platform for several national CIP areas in EU MS

External Dimension

- Perceived as important to CIP by EU MS, because of impact of disrupted third country critical infrastructure on EU and vice-versa
- Currently focused on exchange of best practices and exchange of information
- 2011 Council Conclusions on the development of the external dimension of EPCIP invited MS to step up cooperation with 3rd countries
- USA since 2010, USA & Canada since 2012. Neighbouring Countries from Eastern Europe and Western Balkans since March 2017

Review of EPCIP & Directive 2008/114/EC

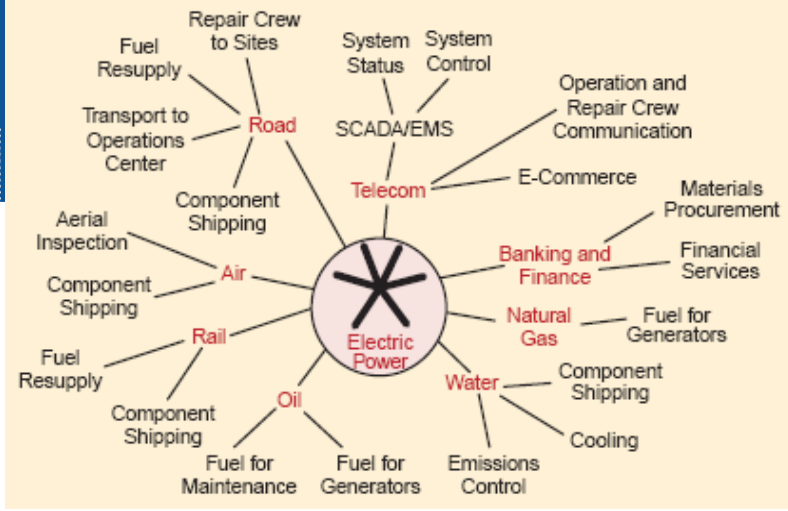
- **Implemented by all EU MS**

- **Review results (2012 COM SWD):**
  - General CIP awareness has increased, particularly in the energy and transport sectors.
  - Until 2012 only 20 ECIs designated (currently 89)
  - The sector-focused approach of the Directive presents challenges
  - Bilateral cooperation rather than a real European forum
  - Need for change:

From Sectoral Expansion

Towards systems and risk based approaches

New approach to EPCIP



- **Presented in 2013 COM SWD**
- **Objective: to provide a reshaped EU CIP approach, based on the practical implementation of activities**
- **Main features:**
  - Looking at interdependencies
  - A step by step practical approach, based on 3 main pillars: *Prevention, Preparedness, Response*
  - Pilot with four critical infrastructures of European dimension: Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network

Aims and future possibilities:

- **Roadmap (SWD(2013) 318 Annex V):**

➢ Action 1: Design of an EU approach for CI protection and resilience

➢ Action 2: Broaden the implementation of the EU approach

- Other possible pan-European infrastructures?
- Regional implementation?
- Funding: large cross-border projects*?*

Recent incidents - 1

2014: German steel mill
20.10.2014 Bank of England computer glitch
12.12.2014 NATS computer glitch
27.03.2015 Netherlands power failure
30.03.2015 Turkey power failure - nationwide power outage
01.04.2015 Rome / Lazio region power outage
07.04.2015 Washington DC power failure
09.04.2015 TV5Monde hack
27.05.2015 Brussels ATC failure
22.06.2015 LOT computer failure / cyber attack
08.07.2015 NYSE / United Airlines / Washington Post computer problems

Cyberattack (confirmed)

Recent incidents - 2

2014/2015: Drones above nuclear power plants in France

Emerging technology challenge

Summer 2014: DOEL-4 nuclear plant shut down

April 2015: Germanwings crash

Insider threat

Jun/Jul 2015: St. Quentin Fallavier gas plant.

July 2015: Berre-l'Etang – refinery tanks blown up.

Aug 2015: Thalys gunman

Oct 2015: AVE sabotage Catalonia

Soft targets vs CI

Recent incidents - 3

March 2016 – two suicide bombings at Airport in Zaventem, and one at Maalbeek metro station. 32 people and three suicide bombers were killed, 340 were injured. A major CI (Zaventem) was also temporarily closed.

April 2017 - a suicide bombing in the St Petersburg Metro. 15 people were killed (plus the bomber), 64 were injured.

June 2017 – at Brussels Central Station a terrorist was shot after trying to detonate a bomb. As the main charge malfunctioned, no other people were injured.

Current focus - 1

Cyber security – after incidents in 2014-2015 (including use of HAVEX and "Black Energy" malware), cyberattacks were recognized a major threat to CIs. EU answered with the Directive on security of network and information systems (NIS Directive) of 6 July 2016. The NIS Directive ensures:

- Member States' preparedness by requiring them to create a Computer Security Incident Response Team (CSIRT), a competent national NIS authority and a single contact point for coordination of international cooperation;
- cooperation among the MS by setting up a Cooperation Group, to support the exchange of information. There is also the obligation to create the CSIRT Network to promote multi-state operational cooperation on specific cybersecurity incidents.

Current focus - 2

I**nsider threats** by infiltrated hostile operators or radicalized individuals. Some are extremely deadly like destruction of Airbus A-321 of Russian company Metrojet on 31 October 2015 in Egypt (224 victims). Mostly however linked to cyber security; in USA a 2016 study for Homeland Security found that 55% of all cyber-attacks in all sectors of industry were the work of insiders. Not all had malicious intentions – some were victims of their own carelessness, using unverified software of dubious provenance in their work place, but the results were usually as damaging as if they acted on purpose. As far as EPCIP is concerned the answer on insider threats includes improved information sharing and support to develop harmonized procedures for vetting.

Current focus - 3

Hybrid Threats: mixture of coercive and subversive activity by conventional and unconventional methods used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of warfare. The issue was addressed by the Joint Communication to the European Parliament and the Council on the Joint Framework on countering hybrid threats from 6 April 2016. It contains 22 actions, including creation of coordination organ (EU Hybrid Fusion Cell) within the existing EU INTCEN structure. DG HOME and JRC are currently working on Action 5: "The Commission, in cooperation with Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors."

Current focus 4

Drones - are a new vector of attack which raises more and more alarms. The illegal overflights of French nuclear plants by drones of unknown provenience in 2014, although harmless, were the first signal, that terrorist menace to CIs can now also be airborne. It was confirmed even more in 2016 with the operational use of drones carrying explosives by ISIS during the battle of Mosul, and in January 2018, with the coordinated UAV attack on Russian base at Hmeimim in Syria.

The future of the Directive 2008/114

2012 options

- *insist on a better application of its mechanism, with insistence on acceleration of work on designation of ECIs*
- *repeal the directive and rely on unilateral action of MS; that would eliminate the only EU level legal text in CIP field*
- *maintain the directive but add accompanying voluntary measures*
- *repeal the directive and replace it with voluntary measures as above*
- *replace the directive with a new legislative instrument,*
- *replace the directive with a new legislative instrument, with added voluntary measures*

The future of the Directive 2008/114

2018 Evaluation. Updated options of future action must be identified – based on them an Impact Assessment should be made in 2019 with the possibility of a new instrument for 2020.

Consultations in 2017, both with MS and the operators of CIs.

- to reduce the complexity of procedures of designation of ECIs

- to shift the focus from identification of ECIs to their protection, unlike in the current instrument

- to give the same attention to resilience, including damage control, backups and recovery, as is given currently to protection

- to consider as priority the maintain of essential services, rather than the protection of infrastructures themselves

Thank you for your attention!

HOME-EPCIP@ec.europa.eu