Security of Critical Infrastructures – Consequences for Enterprises?

Dr. Stephan Lechner

Director of the Institute for Protection and Security of the Citizen, IPSC
Joint Research Center (JRC), European Commission

A bit of recent history

17./18.06.2004	Council request to European Commission for an overall CIP strategy
22.10.2004	European Commission Communication "CIP in the Fight against Terrorism", 13979/04, COM (2004) 702
17.11.2005	Green Paper on a European Programme for CIP (COM (2005) 576 final)
26.10.2006	Decision (C/2006/5025) on the financing of a Pilot Project (prep. actions)
12.12.2006	Communication – general EPCIP policy (CIWIN, work-streams to develop EPCIP, sectoral interdependencies, annual work planning and the residual work on National Critical Infrastructure)
	Directive - designation of critical infrastructure of a European dimension

The European Programme for CIP

Countering threats from terrorism is a priority, but the programme encompass an all hazards approach (i.e. terrorist attacks and natural disasters alike) Protection measures should be:
Affordable; Sustainable; Reliable; Proportionate; interoperable and take into account privacy concerns

- **Measures designed to facilitate the implementation of EPCIP**
  - **EPCIP Action Plan**
  - **Critical Infrastructure Warning Information Network (CIWIN)**
  - **CIP expert groups**
  - **CIP information sharing**
  - **identification and analysis of interdependencies**
- **Support for Member States concerning National Critical Infrastructures (NCI)**
- **Contingency planning**
- **External dimension**
- **Accompanying financial measures**
  - **EU programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013**
- **Directive concerning European Critical Infrastructure (ECI)**
  - **A procedure for the identification and designation of ECI**
  - **A common approach to the assessment of the needs to improve the protection of such infrastructures**

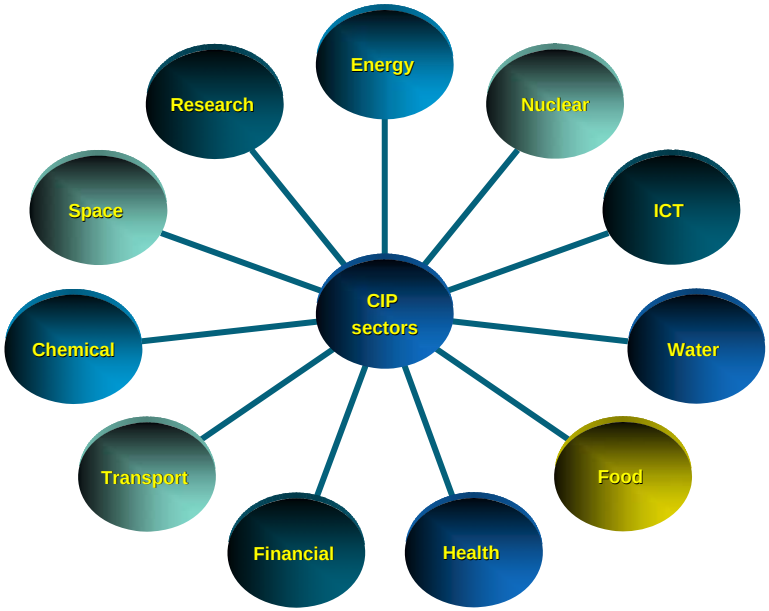
CIP Sectors and Subsectors

CI SECTOR		SUB-SECTOR	
I	Energy	1	Electricity Infrastructure and facilities for generation and transmission of electricity in respect of supply electricity.
		2	Oil production, refining, treatment, storage and transmission by pipelines
		3	Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
II	Nuclear industry	4	Production and storage/processing of nuclear substances
III	ICT	5	European Information systems
		6	Internet
		7	Provision of fixed telecommunications
		8	Provision of mobile telecommunications
		9	Radio communication and navigation
		10	Satellite communication
		11	Broadcasting
IV	Water	12	Provision of drinking water
		13	Control of water quality
		14	Stemming and control of water quantity including dams
V	Food	15	Provision of food and safeguarding food safety and security
VI	Health	16	Medical and hospital care
		17	Medicines, serums, vaccines and pharmaceuticals
		18	Bio-laboratories and bio-agents
VII	Financial	19	Trading, payment and settlement infrastructures and systems for financial instruments
VIII	Transport	20	Road transport
		21	Rail transport
		22	Air transport
		23	Inland waterways transport
		24	Ocean and short-sea shipping and ports
IX	Chemical industry	25	Production and storage/processing of chemical substances
		26	Pipelines of dangerous substances
X	Space	27	Space

Scope of the Directive

- The Directive establishes a common procedure for the identification and designation of European Critical Infrastructure (ECI)

- ECI is defined as critical infrastructure located in the EU Member States, the disruption or destruction of which would have a significant impact on at least two Member States of the EU



Identification of ECI

The Directive requires each EU Member State to apply sectoral criteria followed by the application of cross-cutting criteria, in order to identify those infrastructures which may be designated as ECI

SECTORAL CRITERIA

- **Are adopted for each sector**
- **Take into account the characteristics of individual critical infrastructure sectors**
- **Will be developed, as appropriate, involving the stakeholders**

CROSS-CUTTING CRITERIA

- **are characterized by their horizontal application to all critical infrastructure sectors**
- **Take into account the availability of alternatives and the duration of disruption/recovery**
- **are developed based on the severity of the effects**

Identification of ECI

The identification and designation process takes place through a cooperative effort between the relevant EU Member States and the Commission. No EU-wide lists of European Critical Infrastructure will be created – the identity of the designated ECIs will be known only to those Member States which may be affected by them.

Step 1 Are the Sectorial Criteria met?

Step 2 Is the Infrastructure critical?

Step 3 Is there a trans-boundary impact?

Step 4 Are the Cross-Cutting criteria met?

Sanity check

If accepted by the relevant EU Member State, the CI is designated as an ECI

Member States Involvement

- Member States report to the Commission on the types of threats, vulnerabilities and risks identified in each sub-sector
- Member States designate a formal European Critical Infrastructure Protection Contact Point
- Based on the information gathered through the ECI process, the Commission and the Member States perform an assessment of whether further measures are needed concerning the protection of ECI
- Review after three years – new sectors to be included

Industry obligations

There will be **two basic obligations** for ECI owners / operators

- To establish an **Operator Security Plan** (OSP)
- To designate a **Security Liaison Officer** (LSO)

- Sectors that meet the equivalent of having already designated an OSP can be **exempted**.
- Compliance with relevant Community measures **can also satisfy** the requirement for an OSP

The Operator Security Plan

The OSP (one for each ECI) should identify the assests of an individual European Critical Infrastructure and establish relevant security solutions for their protection. The basic contents should include:

- Identification of important assets
- A risk based analysis on major threat scenarios, vulnerability of each asset and potential impact
- Identification, selection and prioritisation of countermeasures

Sector specific requirements for OSPs can be adopted

The Security Liaison Officer

- **Point of contact for security related issues between the owner or operator of ECI and the relevant CIP authorities in the Member States**

- **The SLO receives information from the member states concerning identified risks and threats**

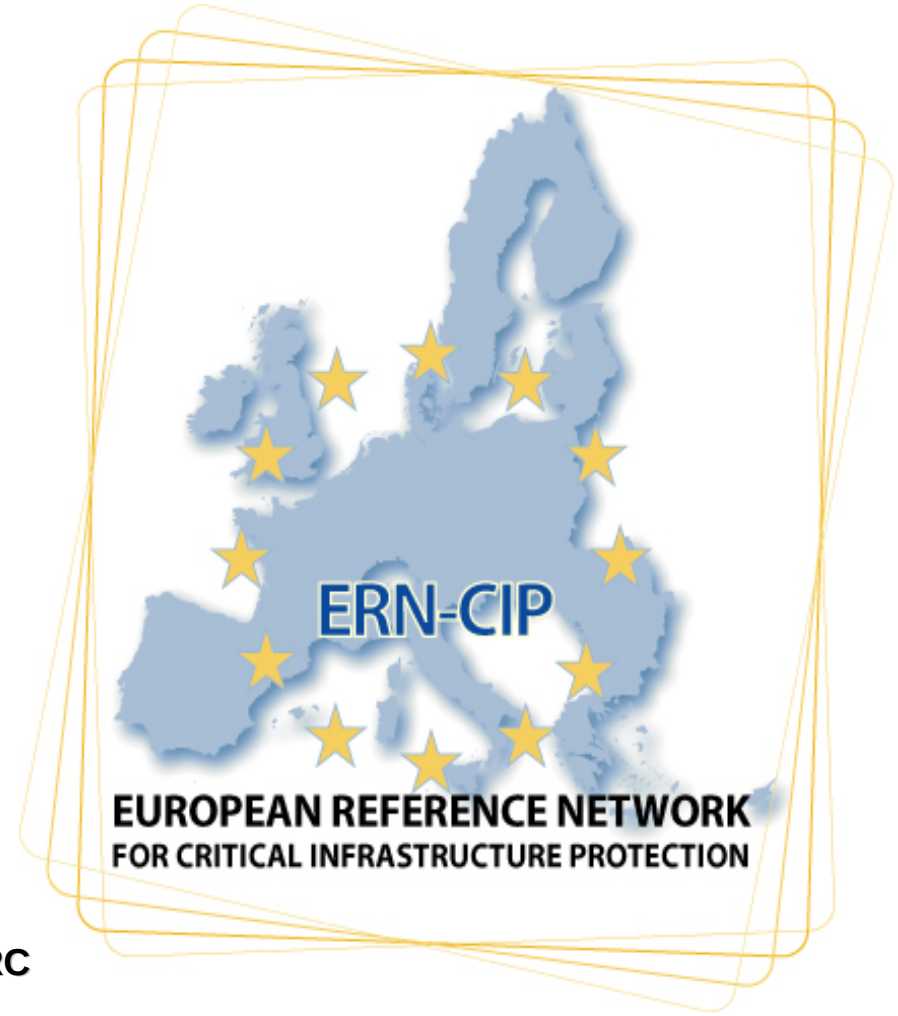
CIP Stakeholders Involvement

CIP Expert Groups will facilitate the EPCIP process

- Assist in identifying vulnerabilities, interdependencies and sectoral best practices;
- Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;
- Provide sector-specific expertise and advice on subjects such as research and development.
- Facilitating CIP information-sharing, training and building trust;
- Develop and promote “business cases” to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;

CIP Research Needs

European Reference Network for Critical Infrastructure Protection



What shall it become?

- **A Reference Network of European dimension**
  - **–Partnership of EC with authorities, industry, manufacturers, etc.**
  - **–Networking between national initiatives, with JRC participation**
  - **–Making use of existing facilities and setting up new unique facilities as required**

CIP Research Needs

Efforts should be made to launch a **„European Security Tool-Pool“** initiative

- Appraisal and testing by authorities of other Member States
- When useful, support to mutual deployment

Carring out CIP relevant security **experiments**

- Vulnerabilities, threats, attack means
- resilience, countermeasures
- practices, policies, scenarios
- technolgies, architectures, systems
- interdependencies

CIP Research Goals

Gathering CIP security knowledge

- vulnerabilities, threats, attack methods, countermeasures
- real world events
- R&D results
- defining experimental programmes

Generating security data

- preparing and running the experiments
- following standard procedures
- observing and measuring

Analysing security data

- aggregating and evaluating experimental results
- linking to technology watch activities

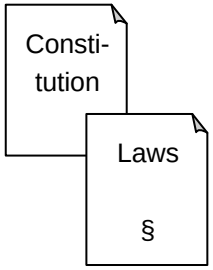
Distributing security data

- organising data repositories
- producing reports

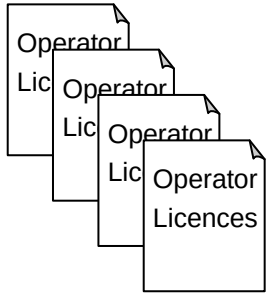
Enterprise Responsibility

Market de-regulation has created a split in Responsibilities

Government



Industry



Public Service Alignment → Professional Service Offer

Infrastructure availability →

Internal Security → ✗

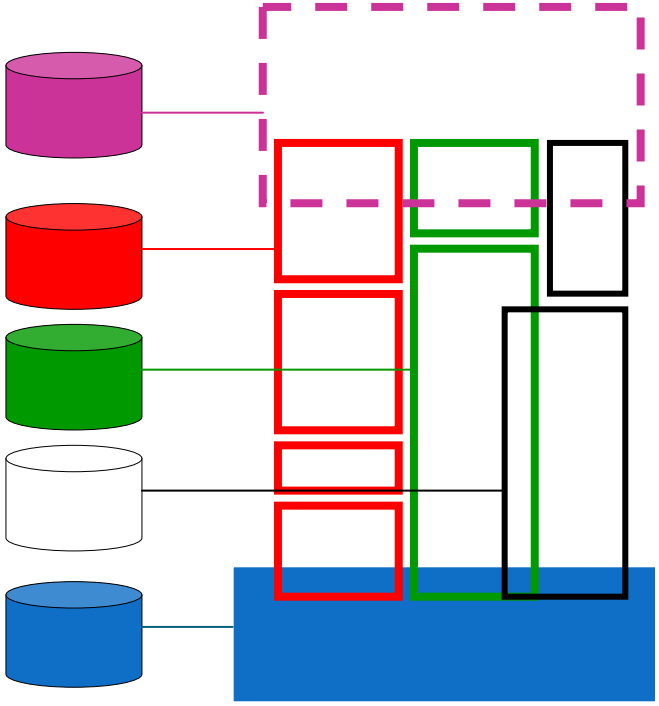
There are many Infrastructure “Owner” Concepts

Telecommunications

Customers

Databases

Virtual Networks &
Service Providers

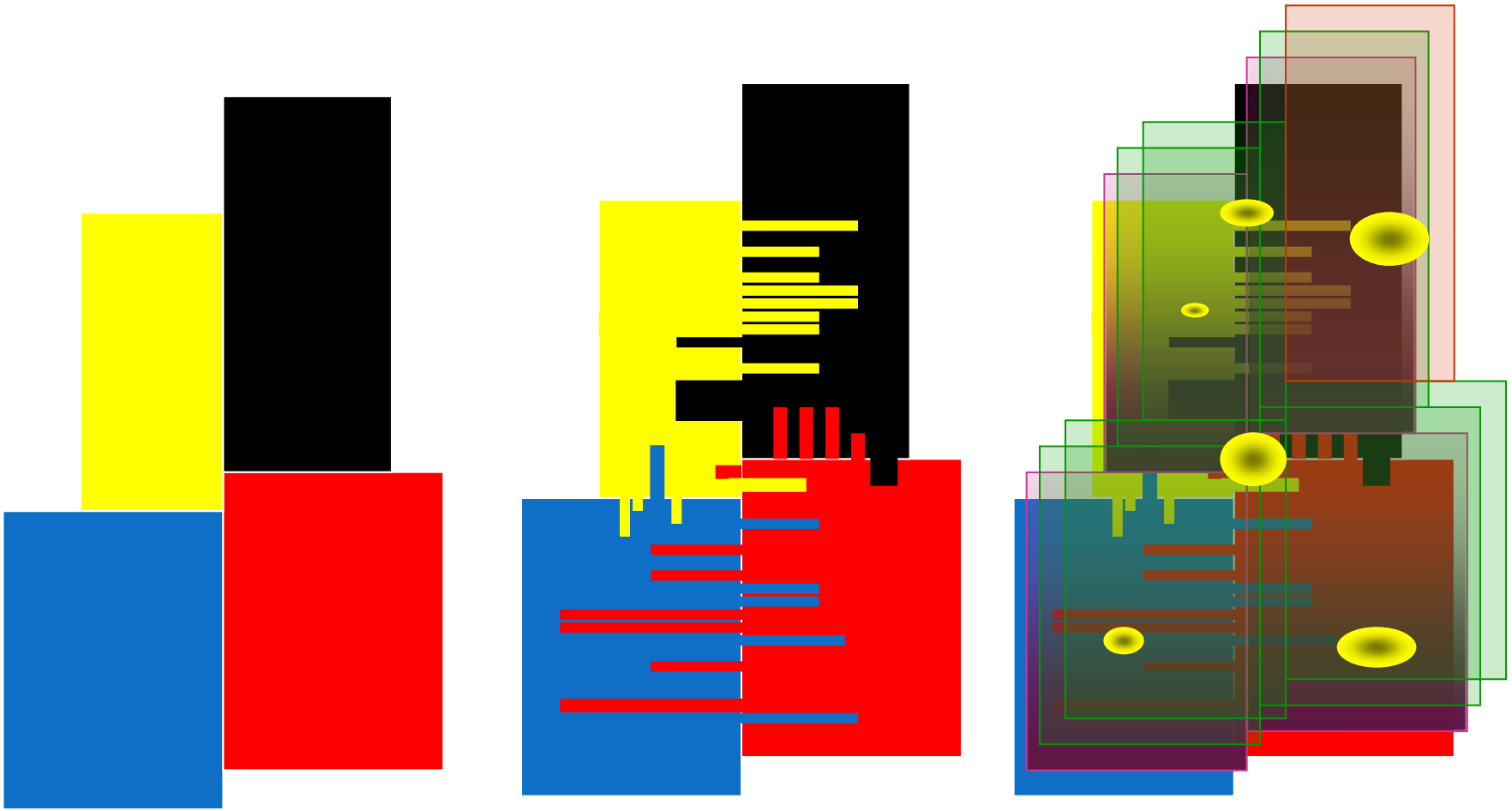


Cellular Networks

Fixed Network Incumbant

Interdependencies

Power



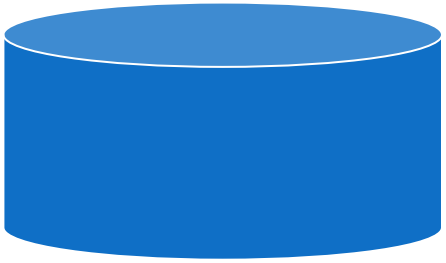
Regional Concept

Leased Lines

Service Providers

Data Provision

- Network Structure is specific: Milano does not match Munich
- Network Structure is heterogeneous : Multiple vendor formats
- Data are sensitive: Competitive advantage
- Incident Reporting is a hot issue: Not everything can to be told!



SME structures

Limited dimensions in

- Security Expertise
- Implementation Funds
- Legal Expert Advice
- Operational coverage
- Lobbying
- Company impact

applies to

Regional or local operators in all CI sectors

Virtual owners of CI (if any)

Overall situation

	Business interest	Big player capabilities	SME capabilities
Protecting the company business	**very high**	**very high**	**limited**
Protecting the sector (partners)	**reasonable**	**limited**	**limited**
Protecting the sector (competitors)	**negative**	**limited**	**limited**
Intersector protection	**non existing**	**none**	**none**

Operator Mandate

EPCIP needs

CI Vendors

- need to prepare for some years ahead
- deliver to all operators
- interested in standardisation
- good customer relations

Vendors are key stakeholders in sustainable CIP!

Recommendations

Set up security structures (if not done yet)

=> ability to participate in the discussion.

Join the dialogue

=> know what to do

Use your Industry associations

=> make yourself heard

Do not implement proactively !!!

Conclusions

Do not assume other stakeholders as hostile by nature!

EPCIP is important to all of us…

… but by our mandates we have different stakes in it!

Reluctance can create unnecessary pressure…

… from both sides.

There will be changes ahead …

… but it is us to influence them together.