

# **EU policy on Critical Information Infrastructure Protection**

**Andrea Servida  
European Commission  
DG INFSO-A3  
Andrea.Servida@ec.europa.eu**



# A EU Policy initiative on CIIP

## *Motivation*

- CIIIs are the nervous system of the Information Society
  - *economic and societal dimension*
- Liberalisation, deregulation and convergence
  - *complexity / multiplicity of players*
- Infrastructures are privately owned and operated
  - *accountability vs. control*
- Ensuring the stability of society and economy is the primary responsibility of Governments
  - *governance*
- CIIIs stretch out well beyond national borders
  - *globalisation*
- The level of security and resilience in any country depends on the level of security put in place outside the national borders
  - *sovereignty*
- National Governments face very similar issues and challenges
  - *scale*
- The private sector is calling for harmonised rules for security
  - *market and economic dimension*

# Communication on CIIP COM(2009)149

## *The scope*

### • Goal

- Protect Europe from large scale cyber attacks and disruptions
- Promote security and resilience culture (*first line of defense*) & strategy
- Tackle cyber attacks & disruptions from a systemic perspective

### • Aims

- Enhance the CIIP preparedness and response capability in EU
- Promote the adoption of adequate and consistent levels of preventive, detection, emergency and recovery measures
- Foster International cooperation, in particular on Internet stability and resilience

### • Approach

- **Build** on national and private sector initiatives
- **Engage** public and private sectors
- **Adopt** an all-hazards approach
- **Be** multilateral, open and all inclusive

# The CIIP Action Plan

## 1. Preparedness and prevention

- **Baseline of capabilities and services for pan-European cooperation between National/Governmental CERTs**  
*Target: End of 2010 for agreeing on minimum standards*  
*End of 2011 for well functioning National/Gov CERTs in all Member States*
- **European Public Private Partnership for Resilience (EP3R)**  
*Target: End of 2009 for a roadmap and plan for EP3R*  
*Mid of 2010 for establishing EP3R*  
*End of 2010 for the first results*
- **European Forum for information sharing between Member States**  
*Target: End of 2009 for launching the Forum*  
*End of 2010 for delivering the first results*

***With the support of ENISA and building upon its activities***

# The CIIP Action Plan

## 2. *Detection and response*

- **Development and deployment of European Information Sharing and Alert System (EISAS)**
  - The Commission financially supports two complementary prototyping projects
  - ENISA is called upon to take stock of results and produce a roadmap to further develop and deploy EISAS

**Target:** *End of 2010 for completing the prototyping projects*  
*End of 2010 for the roadmap*



# The CIIP Action Plan

## 3. Mitigation and recovery

- **National contingency planning and exercises**
  - National/Governmental CERTs/CSIRTs to take the lead in national contingency planning exercises and testing
    - Target: End of 2010 for running a national exercise in every MS*
- **Pan-European exercises on large-scale network security incidents**
  - EC provide some financial support in 2009
    - Target: End of 2010 for first pan-European exercise*
    - End of 2010 for EU participation in international exercises*
- **Reinforced cooperation between National/Governmental CERTs**
  - Support pan European cooperation also by expanding existing cooperation schemes (like EGC)
    - Target: End of 2010 for doubling the number of national bodies participating in EGC;*
    - End of 2010 for ENISA to develop reference materials*



# The CIIP Action Plan

## 4. *International Cooperation*

- **Internet resilience and stability**

- Define European priorities on long term Internet resilience and stability

*Target: End of 2010 for EU priorities*

- Define principles and guidelines for Internet resilience and stability at the European level

*Target: End of 2009 for a roadmap towards the principles & guidelines*

*Target: End of 2010 for agreeing on first drafts*

- Promote the principles and guidelines for Internet resilience and stability at global level

*Target: Beginning of 2010 for a roadmap for international cooperation*

*Target: End of 2010 for first drafts of international principles & guidelines*

- **Global co-operation on exercises on large-scale Internet incidents**

*Target: End of 2010 to propose a framework and a roadmap*



# The CIIP Action Plan

## 5. ICT Criteria to identify ECI

- **Continue to develop the criteria for identifying European Critical Infrastructures (ECI) for the ICT sector**
  - Process conducted in cooperation with Member States and all relevant stakeholders
  - A 9-month study was launched in June 2009 to support the process
  - Staff Working Paper on criteria is under development

*Target: First half of 2010 to define the criteria*

# The CIIP Action Plan

## *The role of ENISA (1)*

- ENISA is called to
  - **Support the process of defining and agreeing** on a baseline of capabilities and services for national/Governmental CERTs in support to pan-European cooperation
  - **Take stock of the results** of the projects aiming the prototyping of EISAS and other national initiatives **and produce a roadmap** to further progress in the development and deployment of EISAS
  - **Support the exchange of good practices** between Member States on national contingency planning and exercises
  - **Stimulate and support** pan-European cooperation between National/Governmental CERTs and develop reference materials
- Both EP3R and EFMS would greatly benefit from and build upon ENISA's activities

# Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) - Presidency conclusions

“It is necessary to stimulate the dialogue between public authorities and the private sector to ensure that the responsibilities of Member States to protect their citizens as well as the practical constraints faced by businesses – which own or operate most Critical Information Infrastructures – are well understood by all parties. **The public and private sectors should be engaged at the EU level in developing an appropriate policy, economic framework and the incentives to support the uptake of security and resilience measures.** At the same time, an instrument serving to facilitate the sharing of information and the dissemination of good practices between Member States would help to maximise the overall capability and level of expertise across the European Union”



# Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) – Presidency conclusions

“**Flexible arrangements** – for example, in the form of Public-Private Partnerships or a Forum of Member States – **are essential** to ensure that such understanding and information exchange is followed by concrete action at the strategic and tactical levels ”

“**The responsibility** of ensuring that the level of preparedness, security and resilience of Critical Information Infrastructures in the European Union, as is more generally the case for creating a secure Information Society, **is a shared one. Everyone – EU bodies, Member States, the private sector, citizens – must play their part in achieving this objective”**



# European Public Private Partnership for Resilience (EP3R)

- **What's the need**
  - To provide a European-wide governance framework to involve all stakeholders, in particular the private sector in defining:
    - Strategic public policy objectives
    - Operational/tactical priority and measures (e.g. industrial deployment)



# European Public Private Partnership for Resilience (EP3R)

- **Objectives of partnering with the private sector (1)**
  - At the strategic/policy level:
    - To discuss and identify the needed for EU policy measures and deepen the knowledge of policy makers on the security and resilience of CIIs (i.e. it includes the analysis of risks at EU level and the planning of measures)
    - To foster the exchange on national policies and measures (good policy practices)
    - To define and steer the policy frameworks that would be needed for the operational/tactical level

# European Public Private Partnership for Resilience (EP3R)

- **Objectives of partnering with the private sector (2)**
  - At the operational/tactical level:
    - To discuss the practical implementing steps to enhance operational cooperation to prepare and respond to security incidents
    - To foster, at EU level, the operational information exchange on current and emerging incidents, vulnerabilities and threats as well as good practices
    - To identify good baseline practices and agree on common guidelines and standards for the security and resilience of CIIs

# European Public Private Partnership for Resilience (EP3R)

- **Key principles**

- **Complementary**: It should **build upon and complement** both existing national initiatives as well as the work conducted by ENISA. It should **fully respect both the national and the private sector responsibility**, without duplicating efforts or putting unnecessary burden or responsibility to participating parties
- **Trust**: It should provide the **structure, processes and environment for "trusted collaboration"**, including the protection of information from disclosure
- **Value**: It should set emphasis on **bi-directional exchanges** between the public and private participants and provide **value for both governments and industry**. Industry and government requirements, priorities and objectives should be aligned
- **No competition**: **Security and resilience of CIIs are NOT issues for competition**

# European Public Private Partnership for Resilience (EP3R)

- **Possible topics**

- Process for vulnerability disclosures
- Practices for threat identification
- Methodologies for risk management
- Common terminology and procedures for the collection and the dissemination of information on economic impacts of security incidents
- Workable frameworks and practices to support the exchange of sensitive information
- recovery and continuity strategies
- ...



# The CIIP Action plan – implementation

<b>31 March 2009</b>	<b>Workshop on EU policy dimension of vulnerability management and disclosure process (report available)</b>
<b>16 June 2009</b>	<b>Workshop on EFMS</b>
<b>17 June 2009</b>	<b>Workshop EP3R (report available)</b>
<b>June – Sept 2009</b>	<b>Informal consultation with MS on EU principles for Internet resilience &amp; stability</b>
<b>Sept – Oct 2009</b>	<b>Informal consultation with private sector on EP3R and EU principles</b>
<b>12-13 Nov 2009</b>	<b>Follow-up Workshops on EFMS and EP3R</b>
<b>On-going</b>	<b>Studies &amp; projects</b>
<b>On-going</b>	<b>ENISA activities in support to the Commission policy and Action Plan</b>

# NIS has never been so high on the EU political agenda

President Barroso "Political guidelines for the next Commission", 3 September 2009

*"The next Commission will develop a **European Digital Agenda** (accompanied by a targeted legislative programme) to tackle the main obstacles to a genuine digital single market, promote investment in high-speed Internet and avert an unacceptable digital divide. **Because of the increasing dependence of our economies and societies on the Internet, a major initiative to boost network security will also be proposed.**"*



# CIIP related activities and CIIP Communication

[http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm)

## Presidency Conclusions of the Ministerial Conference on CIIP Tallinn (EE), 27-28 April 2009

[http://www.tallinnciip.eu/doc/EU\\_Presidency\\_Conclusions\\_Tallinn\\_CIIP\\_Conference.pdf](http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf)