Security and resilience in the Information Society: towards a CIIP policy in the EU

Valérie Andrianavalaly
European Commission
DG INFSO-A3
valerie.andrianavalaly@ec.europa.eu
Network and information security: The European Context

- **Strategy for a Secure Information Society** [COM(2006)251]

- Policy initiatives on:
  - fighting against spam, spyware and malware [COM(2006)688]
  - promoting data protection by PET [COM(2007)228]
  - fighting against cyber crime [COM(2007)267]


- **European Network and Information Security Agency**, (ENISA) established in 2004

- **A policy initiative on CIIP** to be adopted by early 2009 – under the general framework of the European Programme on Critical Infrastructure Protection
Towards a secure Information Society

**DIALOGUE**
structured and multi-stakeholder

**PARTNERSHIP**
greater awareness & better understanding of the challenges

Open & inclusive multi-stakeholder debate

**EMPOWERMENT**
commitment to responsibilities of all actors involved
Policy initiative on CIIP – Q1 2009: The issues at stake / Rationale

- CII are the nervous system of the Information Society
- Liberalisation, deregulation and convergence → complexity / multiplicity of players
- Infrastructures are privately owned and operated
- Ensuring the stability of society and economy is governments’ responsibility
- CII stretch out well beyond national borders
- The level of security in any country depends on the level of security put in place outside the national borders
- National governments face very similar issues and challenges
- The private sector is calling for harmonised rules

→ A more integrated and co-ordinated approach to complement and add value to the national programmes
→ Contribute to reinforce the EU wealth creation capabilities
Policy initiative on CIIP – Q1 2009: Dialogue & Partnership

• Objectives
  – Enhance the level of CIIP preparedness and response across the EU
  – Ensure that adequate and consistent levels of preventive, detection, emergency and recovery measures are put in operation

• Policy orientations
  – Achieve a better understanding and clarity on the guiding policy principles

• Approach
  – Build on national and private sector initiatives
  – Engage relevant public and private stakeholders
  – Adopt All-hazards
Policy initiative on CIIP – Q1 2009: Preparatory activities (1/2)

• 2006:
  – **Study** on “Availability and Robustness of Electronic Communications Infrastructures” (ARECI)

• 2007
  – Informal **meeting** of National experts on CIIP – Brussels, 19 January 2007
  – Public **consultation** on the final ARECI report drafted by Alcatel-Lucent - April 2007
  – Member States and private sector **meeting** on the outcomes of the public consultation– Brussels, 18 June 2007”
  – **Workshop** on “cc TLD’s Contingency practices”, 19/09/2007
  – **Workshop** on challenges for awareness raising, 07/12/2007
• 2008

– 2 Meetings with MS on the criteria to identify European Critical Infrastructures in the ICT sector, Brussels, 5 February & 29 May 2008;
– Workshop on “The role of the private sector for Critical Information Infrastructure Protection”, Brussels, 26 June 2008;
– Questionnaire sent to Member States
Policy initiative on CIIP:
Next steps - Short term

- **Q4 2008**
  - Completion of the survey on MS policy approaches on CIIP
    - Focus on i) definitions/criteria; ii) risk assessment activities; iii) incident response capability; iv) Public Private Partnership; v) International dimension
  - Analysis of inputs

- **Q1 2009**
  - Adoption of Commission policy on CIIP + Action Plan
Policy initiative on CIIP – Q1 2009: The main areas for action

• Process to **define the ICT criteria** to identify the European critical infrastructures
• **Improvement of the incident response capability** at national and European level
• **Development of a trusted public-private partnership** at the European Union level on security and resilience to support sharing of information and good practices
• **Bridging gaps on national CIIP policies** across Europe - Reinforcing the cooperation and the information exchange between Member States
• **International dimension** of CIIP to reinforce co-operation on global issues, in particular the **security and the robustness of the Internet**

→ A significant step forward in the implementation of the Commission's strategy for a Secure Information Society
Policy initiative on CIIP – Q1 2009

Tentative Flowchart

Implementation for the ICT sector* of the European Programme on Critical Infrastructures Protection framework (EPCIP) by defining the criteria for identification of European Critical Information Infrastructures (ECIIs)**

Tool: Staff Working Paper & Study to be launched by the end of 2008

Strengthening the incident response capability for Europe by creating:
1. Governmental CERTs in all Member States
2. EISAS – multi-lingual European information Sharing and Alert System
   - Tool: 1. Obligation/Recommendation for Member States
   - Tool: 2. Development of prototype tool (to be funded under the EU Programme on "Prevention, Preparedness and Consequences Management of Terrorism and other security related risks")

Creation of a strong and trusted EU Public-Private Partnership determining the good practices to be followed, in terms of:
- Industrial deployment
- Public policy practices
Tool: Public Private Partnership for European Resilience

International dimension – Creating a unified European security voice and strategy in international discussions and fora (in particular for Internet)
Tool: Global security dialogue following WSIS with aim to create guidelines on risk preparedness and response
Policy initiative on CIIP: 
Next steps - Medium term

2009

- A study on dependencies on ICTs of finance, energy and transport sectors*
- Prototype of a European multilingual information sharing and alert system to provide appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices*
- A project on DNS security*

Call just closed:
- A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet*
- A study to support the process to define sectoral criteria to identify European Critical Infrastructures in the ICT sector focusing on the sub-sectors of Internet, fixed and mobile telecommunications*

* Projects and studies funded under EPCIP financial scheme: "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"
Web Sites

DG INFSO Web site on the EU policy on secure Information Society

Page on CIIP

Page on ARECI study

Page on the workshop on large scale attacks
• **Strategy for a Secure Information Society [COM(2006)251]**
  

• **Fighting spam, spyware and malicious software [COM(2006)688]**
  

• **Promoting data protection by Privacy Enhancing Technologies (PETs) [COM(2007)228]**
  

• **Towards a general policy on the fight against cyber crime [COM(2007)267]**
  

  
• European Programme for Critical Infrastructure Protection [COM(2006) 786]

• Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection


• EPCIP financial scheme: "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks"

  Call for proposals [http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm]

  Call for tenders [http://ec.europa.eu/justice_home/funding/tenders/funding_calls_en.htm]

  Call for expression of interest (looking for external experts) [http://ec.europa.eu/justice_home/funding/tenders/funding_interest_en.htm]
• **Key findings & way forward**
of the workshop on
“Learning from large scale
attacks on the Internet:
policy implications”
(17.01.2008)
Workshop on “Learning from large scale attacks on the Internet: policy implications”

Key findings & way forward (1/4)

- **Build resilience / Harden the infrastructure**
  - Servers and links redundancy, Anycast
  - Security of routing protocol / traffic exchange
  - Security of DNS service

- **Profiling attackers and understanding their objectives (know your enemies)**
Workshop on “Learning from large scale attacks on the Internet: policy implications”
Key findings & way forward (2/4)

- **Response preparedness**
  - National contingency plan for the Internet
  - Cyber exercises on National/international level are crucial
  - Strengthen multinational cooperation for rapid response (formal rather than informal)
  - Importance of CERTs/CSIRTs and their role for national and international cooperation

- **Measurement - monitoring** of traffic to understand what is going on
  - Computers at the edges could be leveraged to build collective intelligence
Workshop on “Learning from large scale attacks on the Internet: policy implications”

Key findings & way forward (3/4)

– Technology will not be sufficient

– Study the economics of security and cyber crime
  • R. Anderson (et al) report on “Security Economics and the Internal Market” (ENISA)

– Set-up Public Private Partnership (PPP)
  • Importance of the role of government, which is to coordinate and be a good user

– Develop cross-sector and cross-organisational cooperation on national, EU and international levels
Workshop on “Learning from large scale attacks on the Internet: policy implications”

Key findings & way forward (4/4)

- Agree on responsibility’s allocation

- Information and best practices sharing
  → importance of trust
  - *EISAS (European Information Sharing an Alert System) feasibility study* (ENISA)
  - Funding for “proof of concept” implementation of an EISAS

- Raising awareness and education of individuals, public bodies, corporate users and service providers