Security and resilience in the Information Society: *the role of CERTs/CSIRTs in the context of the EU CIIP policy*

Andrea Glorioso

European Commission

DG INFSO-A3

Andrea.Glorioso@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]**

- Proposed package to **reform the Regulatory Framework for e-communications** [COM(2007)697, COM(2007)698, COM(2007) 699]

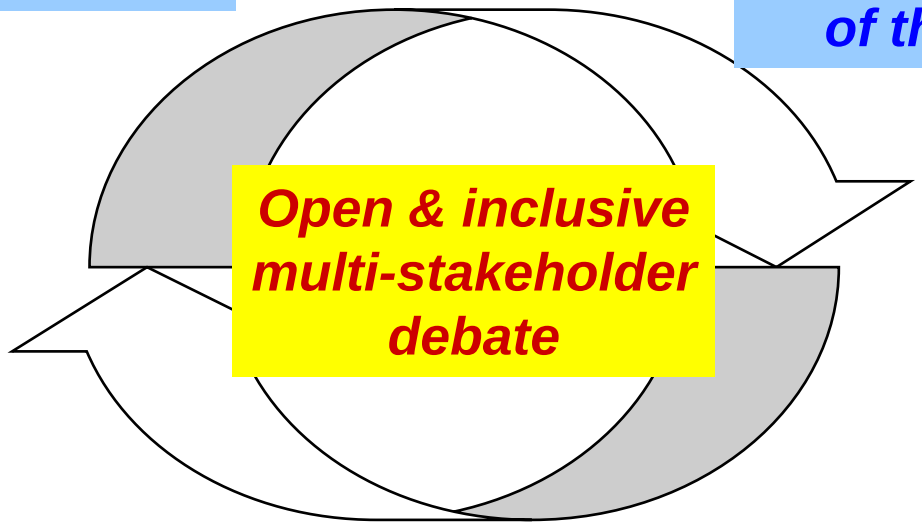
- **European Network and Information Security Agency**, (ENISA) established in 2004

- **A policy initiative on CIIP is announced** in the CLWP 2008 [COM(2007) 640]

Towards a secure Information Society

DIALOGUE
structured and multi-stakeholder

PARTNERSHIP
greater awareness & better understanding of the challenges



EMPOWERMENT
commitment to responsibilities of all actors involved

European Commission
Information Society and Media

Dialogue & Partnership: *CLWP 2008 Policy initiative on CIIP*

- **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**

- **Approach**
  - **Build on national and private sector initiatives**
  - **Engage relevant public and private stakeholders**
  - **Adopt "all-hazard" approach**
  - **Strengthen the synergies between 1st and 3rd pillar measures**

Dialogue & Partnership: *Challenges for CIIP*

- **Organisational:** build trusted relationships and engage the stakeholders at the EU level
- **Policy orientations:** achieve a better understanding and clarity on the guiding policy principles
- **Issues:**
  - National vs. European information infrastructures (criteria);
  - long-term Internet stability & resilience;
  - preventive, detection/early warning & reaction measures;
  - recovery and continuity strategies;
  - sharing knowledge and good practices;
  - cross-sector proactive information assurance methods;
  - risk management approach and tools;
  - inter-dependencies, in particular across heterogeneous infrastructures;

CIIP - Preparatory activities (1)

- **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**
  - **Study on "Critical dependencies of energy, finance and transport infrastructures on ICT infrastructures"**

CIIP - Preparatory activities (2)

- **2008**
  - **Workshop on "Learning from large scale attacks on the Internet: policy implications"**, Brussels, 17 January 2008;
  - **Meeting with MS on the criteria to identify European Critical Infrastructures in the ICT sector**, Brussels, 5 February 2008;
  - **Planned studies and projects** funded under EPCIP financial scheme: "*Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks*";

CIIP - Preparatory activities (3)

- **2008 (cont.)**
  - **Meeting on "Sectoral criteria for the identification of European Critical Infrastructures in the ICT sector"**, Brussels, 29 May 2008;
  - **Workshop on "The role of the private sector for Critical Information Infrastructure Protection"**, Brussels, 25 June 2008;

CIIP - Preparatory activities (4)

- **2008 (cont.)**
  - **Workshop on "Learning from large scale attacks on the Internet: policy implications"**, Brussels, 17 January 2008;
  - **Lessons learned?**

Lessons learned
the way forward (1/3)

- **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)
- **Response preparedness**
  - National contingency plan for the Internet
  - Cyber exercises at 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
  - Computers at the edges could be leveraged to build collective intelligence

Lessons learned
the way forward (2/3)

- **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

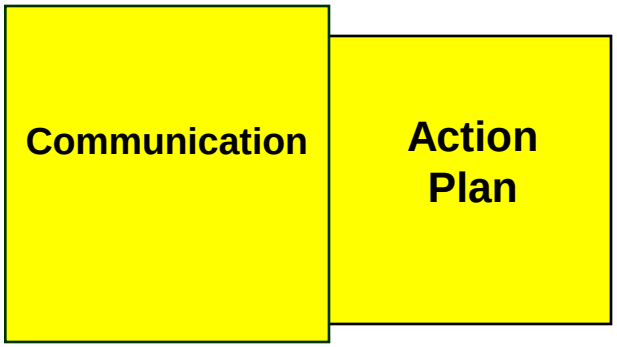
Lessons learned
the way forward (3/3)

- **Agree on responsibility's allocation**

- **Information and best practices sharing**
  → importance of trust
  - *EISAS (European Information Sharing an Alert System) feasibility study* (ENISA)
  - Call for "proof of concept" implementation of an EISAS (closed on May 15)

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

CIIP – Flowchart (tentative)



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)

Strengthening the incident response capability for Europe by creating:

1. **National CERTs** in all Member States
2. **EISAS** – multi-lingual **European Information Sharing and Alert System**

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

International dimension: creating a **unified European security voice and strategy** in international discussions and fora (in particular for the Internet).

Global security dialogue post-WSIS to create **guidelines on risk preparedness and response**

European Commission
Information Society and Media

Food for thought

- What are the (new) areas CERTs/CSIRTs should focus on?
  - Mobile networks?
  - Satellite networks?
  - SCADA?

- What is the role of CERTs/CSIRTs in:
  - Strengthening national response capability
  - Strengthening the EU response capability
    - Sharing of continuity plans?
    - European Cyberstorm?

Food for thought

- What are the minimal (baseline) services and functions for national CERTs as pillar for national incident response capability and as a basis for structured and effective European and international cooperation?

- What should be the scope of the constituency of a national CERT/CSIRT?
  - Should the principle of subsidiarity – entities operating as close as possible to the relevant constituency – be applied to CERTs/CSIRTs?
  - In such a case, how should such entities be coordinated to ensure that all citizens are covered and can benefit to the utmost from synergies between entities?

- Can/should CERTs/CSIRTs play more than an operational role in order to enhance security and resilience of the Information Society in the EU? Are they already doing it?

Web Sites

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

http://ec.europa.eu/information_society/policy/nis/index_en.htm

Page on CIIP

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

THANK YOU

QUESTIONS/COMMENTS:

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