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

Andrea Servida

European Commission

DG INFSO-A3

Andrea.servida@ec.europa.eu

NIS Policy and related Regulations (1)

- **Strategy for a Secure Information Society [COM(2006)251]**
  - **holistic approach for a comprehensive EU-wide strategy across "pillars", related policy and regulatory initiatives**
  - **"voluntary" activities stakeholders via dialogue, partnership and empowerment**
  - **reinforce ENISA's role in implementing the EC policy**
  - **importance of "resilience" strategy for CIIP, i.e. the ability to deal with unexpected events**

- **Other initiatives related to NIS**
  - **fighting against spam, spyware and malware [COM(2006)688]**
  - ***promoting data protection by PET [COM(2007)228]***
  - ***fighting against cyber crime [COM(2007)267]***
  - **new Safer Internet Programme [COM(2008) 106]**

NIS policy and related Regulations (2)

- **NIS in the eCommunications Review**
  - **Security and integrity (Art 13 FW D)**
    - **level of security appropriate to risks**
    - **prevent/minimise impact of security incidents on users and interconnected networks**
    - **focus on continuity of supply of services**
  - **Responsibilities of operators**
    - **stronger obligations to ensure security and integrity (Art 13 FW D)**
    - **mandatory breach notifications**
      - **to NRA (Art 13 FWD): significant impact on operations**
      - **to consumers and NRA (Art 4 e-privacy D): personal data compromised**
  - **Technical measures (Art 13 FW D)**
    - **The Commission ("... *taking the utmost account of the opinion ...")* may adopt appropriate technical implementing measures with a view to harmonising**

NIS policy and related Regulations (3)

- **European Network and Information Security Agency (ENISA)**
  - **Established in March 2004 with a 5 ys mandate**
  - **Mid term evaluation in 2006 followed by a public consultation in 2007 [COM(2007) 285]**
  - **Extension of the mandate for 3 ys formally adopted in September**

- **What's ahead?**
  - **A public debate on the long terms goals for a reinforced European policy on NIS and the most adequate means to achieve them**
  - **A policy initiative on Critical Information Infrastructure Protection (CIIP)**
  - **Recommendations on security and privacy of RFID**

Public debate on NIS policy

- **Broader thinking** on NIS is essential
- **Commissioner Reding** called on EP and Council to **open an intense debate on Europe's approach to network security** and on how to deal with cyber-attacks
- **Calls were made both in EP and Council** for a debate on further discussion **on the future of ENISA and on the general direction of the European efforts** towards an in creased network and information security
- **Aim and Scope:**
  - objectives of a modernised NIS policy at EU level, and the means to achieve those objectives

Public Consultation "Towards a Strengthened NIS Policy in Europe"

- **The Commission has just launched a public consultation**
- **Focus on:**
  - **challenges to NIS**
  - **priorities of a modernised NIS policy**
  - **means needed to address the challenges**
- **Timing: 7 Nov 08 – 9 Jan 09**

http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4464

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

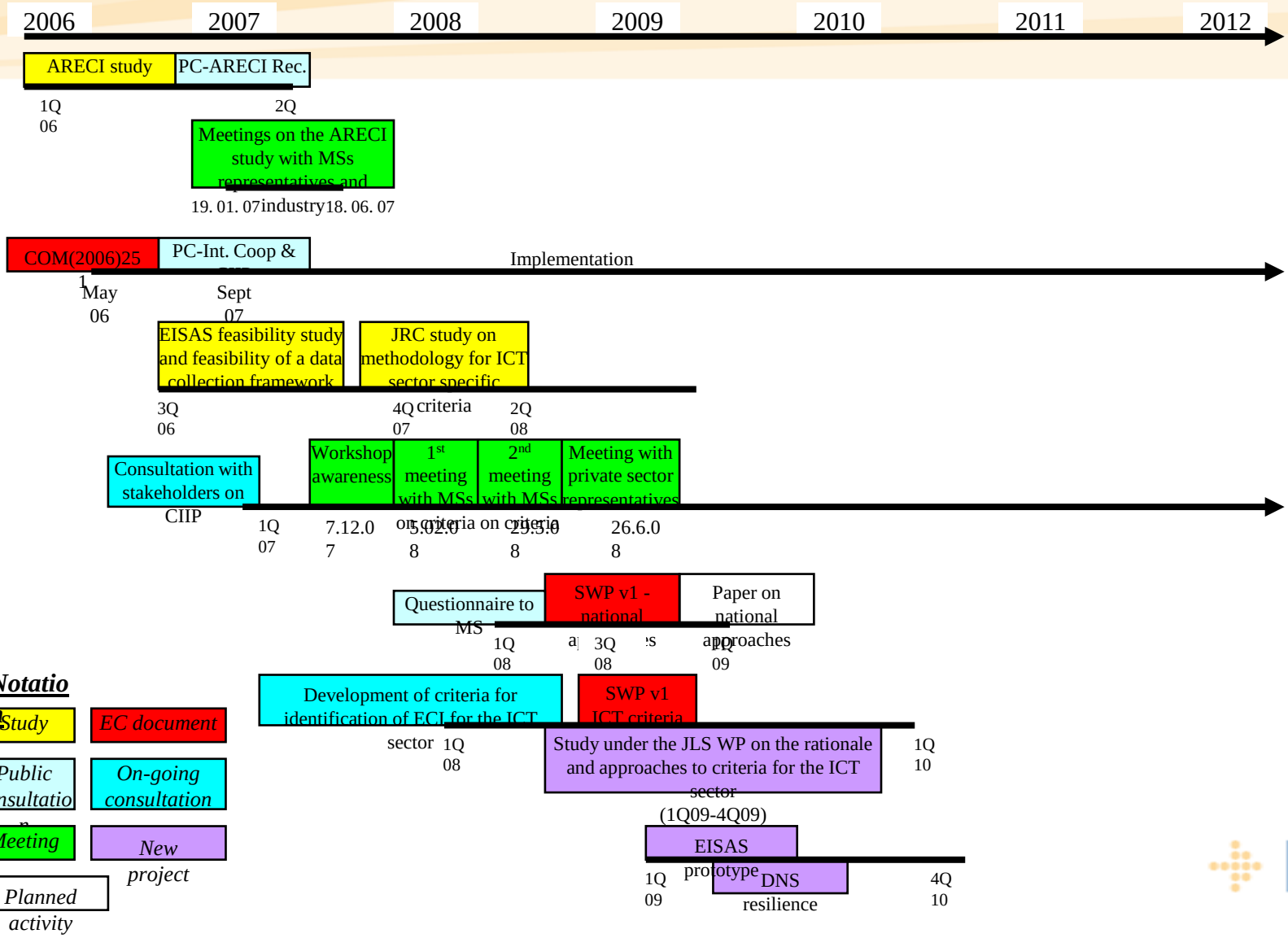
→ A more integrated and co-ordinated approach to complement and add value to the national programmes

→ Contribute to reinforce the EU wealth creation capabilities

Challenges of an EU policy on 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 & responsive measures;
  - recovery and continuity strategies;
  - sharing knowledge and good practices;
  - cross-sectors proactive information assurance methods;
  - risk management culture and tools;
  - inter-dependencies, in particular across heterogeneous infrastructures; etc.

TIMELINE OF THE CIIP INITIATIVE: *preparatory activities*



Planned policy on CIIP

- **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 an ecosystem 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 all-hazards**
  - **Be multilateral, open and all inclusive**

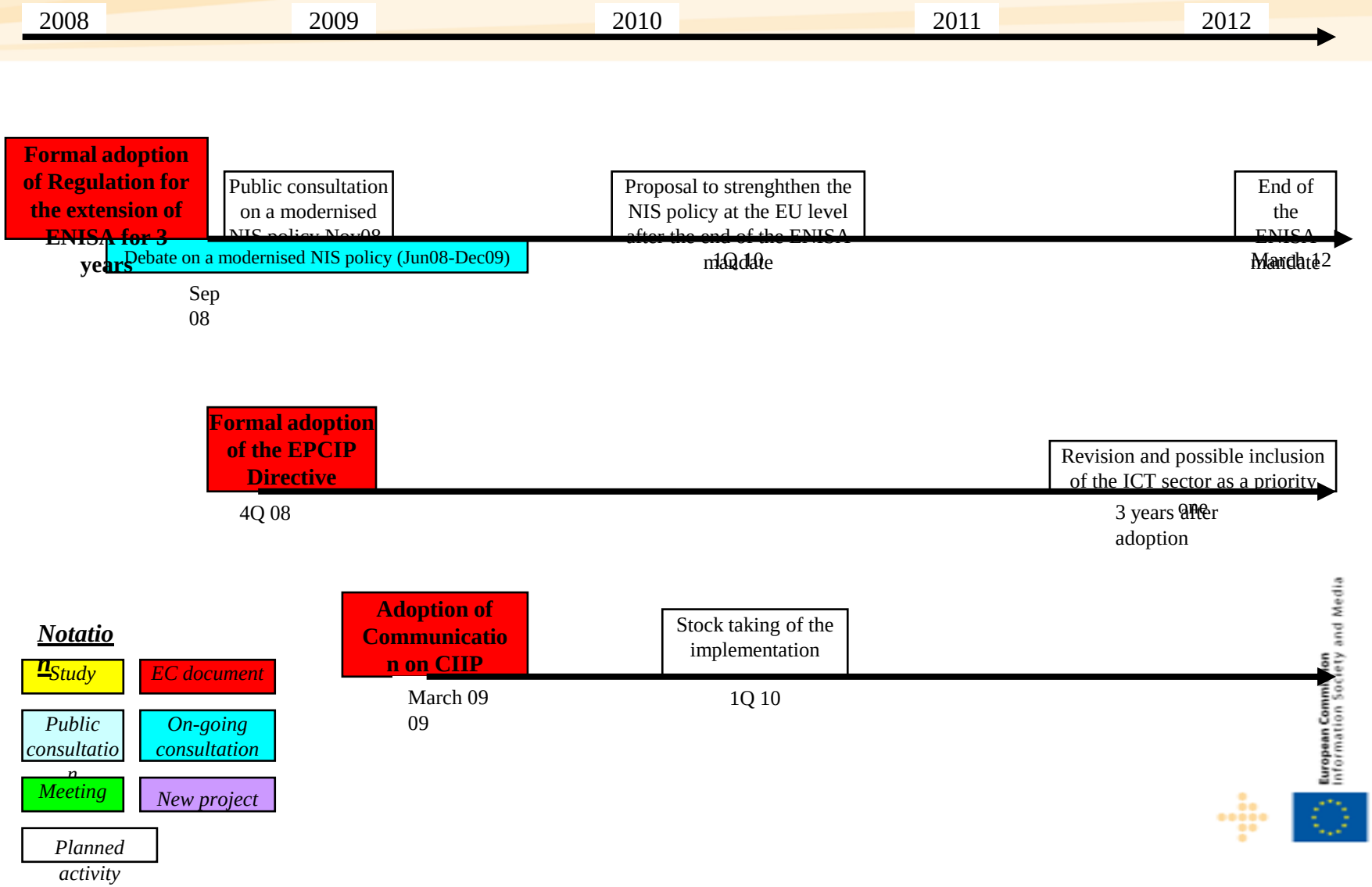
Planned policy on CIIP *priority areas (1)*

- **Preparing**
  - European Public Private Partnership on resilience
  - National preparedness capability - information sharing, planning, coordination and response
- **Early Warning**
  - Prototyping a European Information sharing and alert system
- **Defending**
  - Cooperation between European GovCERTs
  - Promote national contingency planning for incident response and disaster recovery
  - Promote pan European exercises on simulated large-scale public network security incidents

Planned policy initiative on CIIP *priority areas (2)*

- **Cooperating (*internationally*)**
  - **Internet long term stability and resilience**
    - **security and resilience of critical components (i.e. DHCP, DNS, MPLS)**
    - **remedial, mutual assistance and recovery strategies**
  - **Exchange of policy principles & good practices (i.e. OECD)**
  - **Global co-operation on exercises on simulated large-scale network security incidents exercise**

TIMELINE OF THE CIIP INITIATIVE: *implementation activities*



Policy initiative on CIIP: *Next steps - Short term*

- **Q3-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**
  - **Impact Assessment**
- **Q1 2009**
  - **Adoption of Commission policy on CIIP + Action Plan**

Web Sites

EU policy on secure Information Society

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

CIIP activities

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

Public consultation "Towards a Strengthened Network and Information Security Policy in Europe"

http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4464

http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=nfsoNis