

EU policy on Network and Information Security and Critical Information Infrastructure Protection

Andrea Glorioso
European Commission
DG INFSO-A3

Andrea.Glorioso@ec.europa.eu



Network and information security (NIS)

- **COM(2001) 298 final - Network and Information Security: Proposal for A European Policy Approach**

Network and information security is defined as “*the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems*”



A Policy initiative on CIIP

- **“ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)”** (Green Paper on a European Programme for Critical Infrastructure Protection)
- **“Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy”** (OECD)



A Policy initiative on CIIP

- There are **differences**, in national and international policy contexts, in how Critical Information Infrastructures (CIIs) are defined/identified.
- BUT the notion of CII is conducive to a **holistic policy perspective** on the secure and continuous functioning of ICT systems, services, networks and infrastructures **of which the Internet is a very important component**, due to its widespread diffusion and the process of technological convergence.



Motivation

- **CII 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 governments' primary responsibility → *governance***
- **CII stretch out well beyond national borders → *globalisation***
- **The level of security 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 → *market dimension***



What is at stake

- **The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately \$250 billion**
- **The US Business Roundtable in 2007 suggested that the economic costs of a month-long Internet disruption to the United States alone could be more than \$200 billion.**
- **According to OECD report on “Malicious software”, the estimated annual loss to United States businesses caused by malware is USD 67.2 billion**
- **The macroeconomic costs of a major disruption to Switzerland, having an annual GDP of CHF 482 billion are estimated at CHF 6 billion, i.e. 1.2% of GDP**



Reality beyond fiction?

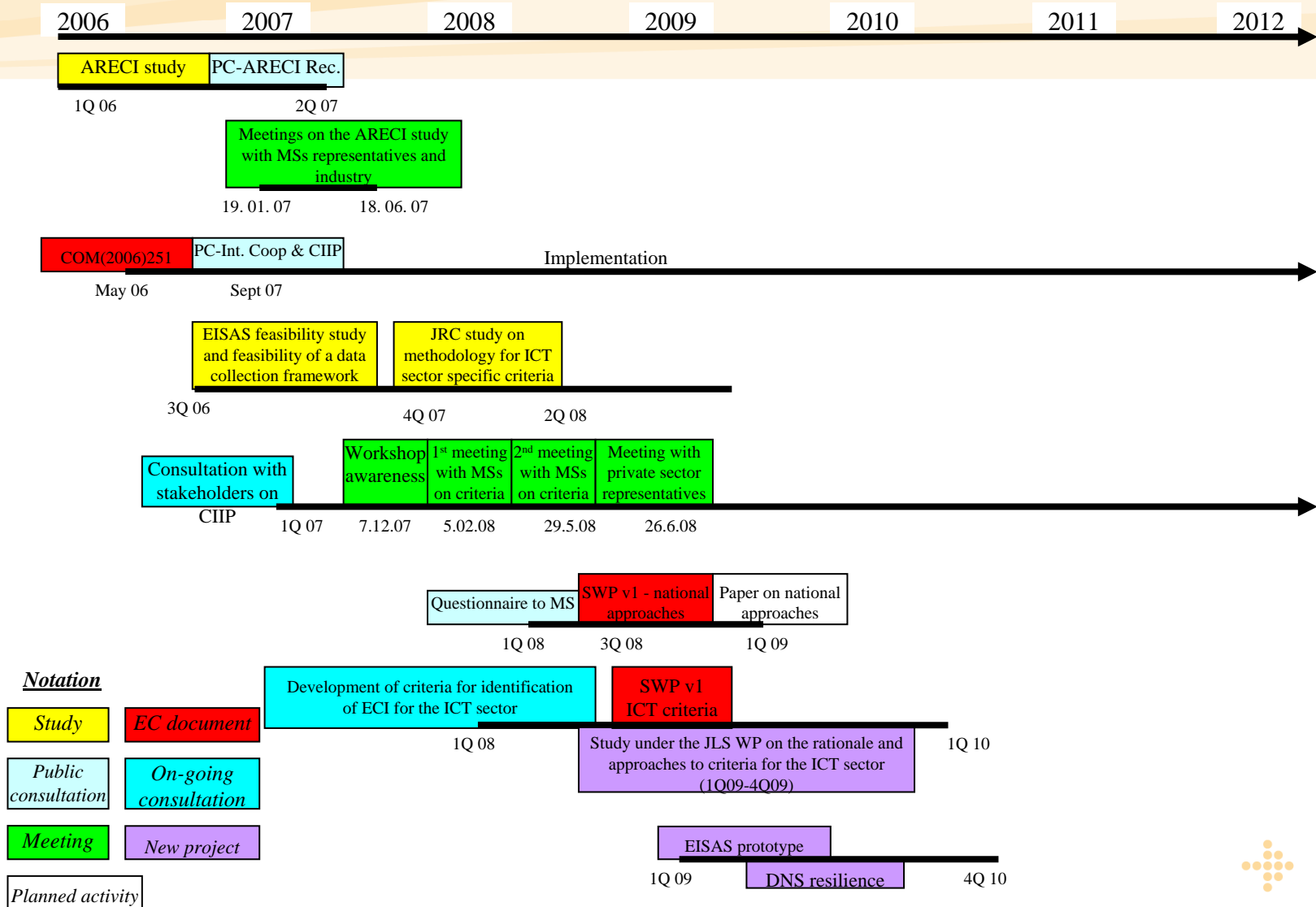
Few recent large scale events

- **DDoS attacks on Estonian networks (April-May 2007)**
- **Defacement attacks on more than 300 private and official sites in Lithuania (June-July 2008)**
- **Three major cables cuts in the Mediterranean (January, February and December 2008)**

Lowering entry barriers for malicious attackers

- **According to UK House of Lords report on Personal Internet Security, the “competition” to supply botnets has decreased the cost of renting a platform for spamming to around 3-7 US cents per zombie per week**
- **One report averaged the weekly rental rate for a botnet at USD 50 – 60 per 1 000 – 2 000 bots.**

Timeline of the CIIP initiative: *preparatory activities*



Communication on Critical Information Infrastructure Protection Protecting Europe from large-scale cyber-attacks and disruptions – enhancing preparedness, security and resilience

- **Goal**

- Protect Europe from large scale cyber attacks and disruptions
- Promote security and resilience culture (*first line of defense*) & strategy
- Tackle cyber attacks and disruptions with 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** all-hazards
- **Be** multilateral, open and all inclusive



Policy initiative on CIIP *Actions*

- **Preparedness and prevention**
 - **European Public Private Partnership on Resilience**
 - **Baseline of capabilities and services for National/Gov CERTs for pan-European cooperation**
 - **European Forum for Member States to exchange good policy practices**
- **Detection and response**
 - **Prototyping a European Information sharing and alert system**



Policy initiative on CIIP *Actions*

- **Mitigation and recovery**
 - **Cooperation between European National/Gov CERTs**
 - Support pan European cooperation also by expanding existing cooperation schemes (like EGC)
 - **Promote national contingency planning for incident response and disaster recovery**
 - National/Governmental CERTs/CSIRTs to take the lead in national contingency planning exercises and testing
 - **Promote pan European exercises on simulated large-scale public network security incidents**
 - EC provide some financial support in 2009



Policy initiative on CIIP Actions

- **International Cooperation**
 - **Internet long term resilience and stability**
 - EU priorities on security and resilience of critical components (i.e. DHCP, DNS, MPLS)
 - Principles and guidelines for Internet resilience and stability (*focus on remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data*)
 - **Global co-operation on exercises on large-scale network security incidents exercise**



Policy initiative on CIIP *Actions*

- **ICT sector specific criteria**
 - **continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria**
 - **A study is being launched**
 - **Staff Working Paper on criteria**



Policy initiative on CIIP *Actions*

- The action plan identifies a number of priorities from now until 2011
- It is clear that we must act **now**
- In addition, we must prepare our longer-term strategy for the future



Web Sites

EU policy on secure Information Society

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

Page on CIIP activities

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

Page on ARECI study

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

Page on the workshop on large scale attacks

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

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

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

<http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=Infsolis>



Public debate on NIS policy

- **Calls were made both in EP and Council** for a debate on the future of ENISA and on the *“general direction of the European efforts towards an increased network and information security”*
- **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**
- **The aim of the public debate:**
 - Possible **objectives** for a modernised and reinforced NIS policy at EU level, and the **means** to achieve those objectives

