

# Towards a European Union Policy on Critical Information Infrastructure Protection

Protecting Europe from large scale cyber-attacks and disruptions:  
enhancing preparedness, security and resilience - the European  
Commission action plan for the protection of Critical Information  
Infrastructures

CCD-COE Conference on Cyber-warfare

Tallin, 17-19 June 2009

Andrea Glorioso

European Commission

DG Information Society and Media

Andrea.Glorioso@ec.europa.eu

On 30 March 2009, the European Commission adopted a Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region, entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"<sup>1</sup> ("CIIP Communication" from now on).

The CIIP Communication represents an important element of the Commission's strategy in the field of Network and Information Security. It addresses the commonly perceived need to raise the level of preparedness and resilience of critical ICT infrastructures across the European Union, as the first line of defence against cyber-threats – complementarily to the policies for fighting cyber-crime and cyber-terrorism and in coherence with international efforts in this area.

Recognising the extremely important role of ICT infrastructures for economic growth and societal cohesion and development on the one hand,<sup>2</sup> and on the other the growing impact of cyber-threats – whether caused by natural disasters or human activity – the Commission proposes a number of immediate actions (running from now until 2011) that Member States, the private sector and all concerned stakeholders should contribute to, in order to enhance the level of preparedness, security and resilience against current and future threats throughout Europe.

In particular, the Commission proposed to focus European efforts on:

- **Preparedness and prevention:** to ensure preparedness by defining a baseline of capabilities and services of national/governmental Computer Emergency Response Teams, creating a European Public-Private Partnership for Resilience and a European Forum of Member States to share information and good policy and operational practices.

---

<sup>1</sup> COM(2009) 149. See also [http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/).

<sup>2</sup> See *inter alia* COM(2008) 199 final (Communication on i2010 mid-term review), the 2006 Aho Group report "Creating an Innovative Europe", the EU Economy 2007 review, the OECD 2008 report "Shaping Policies for the Future of the Internet Economy".

- **Detection and response:** to provide adequate early warning mechanisms, by supporting the development and deployment of a European Information Sharing and Alert System, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems.
- **Mitigation and recovery:** to reinforce EU defence mechanisms for CII, via the development by Member States of national contingency plans and the organisation of regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination, and by strengthening the cooperation between national/governmental Computer Emergency Response Teams.
- **International and EU wide cooperation:** to promote EU priorities internationally, by driving a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet, by working with Member States to define guidelines for the resilience and stability of the Internet and by working on a roadmap to promote principles and guidelines at the global level, possibly leveraging strategic cooperation with third countries.
- **Criteria for the ICT sector:** to support future implementation of EPCIP, by continuing to develop, in cooperation with Member States and all relevant stakeholders, the criteria to identify the European critical infrastructures in the ICT sector.

The results and lessons learned from the implementation of these immediate actions will feed into the ongoing debate on the future of network and information security policy in Europe after 2012.