

Security and resilience in Information Society

*The European initiative on Critical
Information Infrastructure protection*

**Achilleas Kemos
Policy Officer
European Commission
DG INFSO-A3**

Achilleas.Kemos@ec.europa.eu



ICT : The Paradigm Shift

- State monopolies →
 - privatisation, deregulation
- Security Maximisation →
 - Optimisation
- New Role for
 - Governments
 - Industry
 - Users



Network and Information Security The key objectives of the strategy

... to revitalise the EC strategy set out in 2001

- By reviewing the NIS situation and challenges posed by convergence of technologies, media and markets
- By building better coordination between the various EC policy initiatives (e.g. spam, **Reg. Framework Review, CIIP, cyber crime**, RFID, etc)
- By mobilising all stakeholders to strengthen the cooperation in the EU

... to adapt the EU approach to future challenges

- **By strengthening the role of ENISA**
- **By emphasising the value and benefits of measuring and learning**
- **By launching few actions to stimulate the exchange of good policy practice across the EU**



NIS in the Information Society Holistic View on Security

TECHNICAL dimension

SOCIAL dimension



ECONOMIC dimension

LEGAL dimension



The key principles ...

... to improve and develop a culture of NIS

- **Technical**
 - Promote **diversity, usability openness and interoperability** as integral components of security
- **Economic**
 - Present NIS as a virtue and an opportunity
- **Social**
 - **Individual users need to understand that their home systems are critical for the overall security chain**
- **Legal**
 - **Security and privacy are a prerequisite for guaranteeing fundamental rights on-line**



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



The challenges for stakeholders ...

... to take responsibility for their respective roles

- **Public Administrations**
 - to address the security of their own networks and **serve as an example of best practice** for other players
- **Private sector enterprises**
 - to **address NIS as an asset and an element of competitive advantage** and not as a “negative” cost
- **Individual users**
 - to **understand that their home-personal domain systems are critical** for the overall “security chain”



European Commission
Information Society and Media

Dialogue

- **“Benchmarking” national NIS-related policies**
 - Comparing to learn and to transfer **best practices to improve awareness** among SMEs & individual users to
 - public administrations shall act **as ‘intelligent’ users and serve as an example for best practice** drivers (-> eID)

Structured multi-stakeholder dialogue

- **where to strike the balance between security and the protection of fundamental rights**
- develop a **sector-specific policy for the ICT** sector to enhance the security and the resilience of information and communication networks (-> CIIP)



European Commission
Information Society and Media

Partnership

- **Improve knowledge of the problem**
 - **ENISA** is asked to develop a **trusted partnership with Member States and stakeholders** to create a data collection framework to collect EU-wide data on security incidents and consumer confidence
- **Understand the ICT security sector and market in the EU**
 - **fostering a strategic relationship between governments, businesses and research community** to deliver data on trends in ICT security
- **Support response capability**
 - ENISA is asked to **examine the feasibility** of a European information sharing and alert system (including a multi-lingual security portal)



EMPOWERMENT *NIS in the new package (1)*

- **Security and integrity**
 - **Current framework (Art 23 Univ. Service Directive)**
 - telephone network / fixed location
 - **New proposal (Art 13 FW D)**
 - level of security appropriate to risks
 - prevent or minimise impact of security incidents on users and interconnected networks
 - focus on continuity of supply of services



EMPOWERMENT

NIS in the new package (2)

- **Responsibilities of operators**
 - **stronger obligations to ensure security and integrity (art 13 FWD)**
 - **Mandatory breach notification**
 - to NRA (art 13 FWD): significant impact on operation
 - to consumers and NRA (art 4 e-privacy D): personal data compromised



Empowerment: *invite Member States*

- **Proactively participate in the proposed benchmarking exercise of national NIS policies;**
- Promote, in close cooperation with ENISA, **awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies**, practices and behaviour;
- Leverage the roll-out of e-government services to **communicate and promote good security practices** that could then be extended to other sectors;
- Stimulate the development of **network and information security programmes** as part of higher education curricula.



Empowerment: *invite private sector*

- Promote **diversity, openness, interoperability, usability and competition** as key drivers for security as well as stimulate the **deployment of security-enhancing** products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks.
- **Disseminate good security practices** for network operators, service providers and SMEs **as baseline levels for security and business continuity**.
- Promote **training programmes in the business sector**, in particular for SMEs, to provide employees with the knowledge and skills necessary to effectively implement security practices.
- **Work towards affordable security certification schemes** for products, processes and services that will address EU-specific needs (in particular with respect to **privacy**).



Empowerment: *invite private sector*

- Develop an appropriate **definition of responsibilities for software producers and Internet service providers** in relation to the provision of adequate and auditable levels of security. Here, **support for standardised processes** that would meet commonly agreed security standards and best practice rules is needed.
- Involve the **insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management** in organisations and business (in particular in SMEs).



C(I)IP – European Context

- European **NIS strategy**
- Because of their horizontal nature with inter-linkages into many other critical infrastructures, **the protection of communication and information infrastructure is a priority**
- A major **policy initiative on CIIP** will be launched in 2008



CIP – European Context

- In June 2004, the **European Council** asked for an overall strategy to protect critical infrastructures
- On 17 November 2005, the Commission adopted a **Green Paper** on the policy options for a **European Programme on Critical Infrastructure Protection (COM(2005)576)**
 - Contributions from **22 Member States** and over **100 private companies and industry associations**
 - need for action at the European level to **enhance the protection and resilience of critical infrastructures**
- **In December 2006** the Commission adopted
 - a **communication and**
 - a **proposal for a directive on the identification and designation of European Critical Infrastructure**



Scope of the directive

To establish a common procedure concerning:

- the **identification** of European Critical Infrastructure (ECI)
 - 11 sectors + interdependencies (horizontal)
 - **Priority sectors**
- the **designation** of ECI
- the assessment of the **need to improve the protection** of European Critical Infrastructure



Identification of ECI

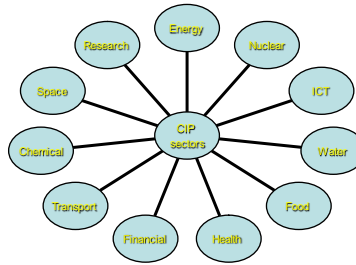
- Based on a three step process:
 - The development and adoption of **cross-cutting** and **sectoral** criteria to identify ECI
 - The **identification by each Member State** of those infrastructures which satisfy the criteria
 - The **notification to the Commission** of the critical infrastructures which satisfy the established criteria



Identification of ECI

Criteria development

- sectoral criteria:
 - to be adopted for priority sectors
 - should take into account the characteristics of individual critical infrastructure sectors
 - their development should involve relevant stakeholders
 - To be adopted through the comitology regulatory procedure for each priority sector at the latest one year following the designation as a priority sector



The multi-stakeholder dialogue on CIIP

- Public Private Partnership
 - Government – stakeholders
 - Information sharing
- Between government bodies
- Intergovernmental
- NEED FOR
 - **network of trust**
 - **Honest Broker - Mediator**



CIIP - Preparatory study in 2006

“Availability and Robustness of Electronic Communications Infrastructures”

- Aimed at identifying the threats and vulnerabilities in next generation 3G mobile and Internet core networks
- developed 10 recommendations to MS, EU institutions and private sector to avoid or reduce their potential impact on the European Critical Infrastructure;
- Ended February 2007 - the contractor is Alcatel-Lucent;
- validation Workshop held in January 2007
- Comments invited until mid May 2007
- Final report available

http://ec.europa.eu/information_society/newsroom/cf/itemdetails.cfm?item_id=3334



CIIP – Initial discussions

“Informal meeting of National experts on CIIP – Brussels, 19 January 2007”

- Aimed informally discuss the outcomes Alcatel-Lucent study as well as exchange views on the CIIP component of EPCIP;
- The Focus was on
 - the needs, challenges and opportunities for an EU dialogue on CIIP;
 - How a EU dialogue could add value to the National initiatives;
 - Who should be part of such a dialogue;
 - How to engage the public and the private sector;
 - What are the main issues to address



CIIP – Initial discussions (2)

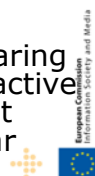
“Joint Member States and private sector meeting – Brussels, 18 June 2007”

- To debate the policy options for the EU;
- Exchange views on how resilience and robustness are approached and tackled in the EU;
- Focus on identifying:
 - The policy options for an EU dialogue on CIIP;
 - The roadmap for an EU initiative;
 - The role of stakeholders;
 - The mechanisms for an EU multi-stakeholder dialogue



Challenges of the CIIP dialogue

- **Organisational:** to build trusted relationships and motivate the stakeholders (in particular the private sector)
- **Policy orientations:** to achieve a better understanding and clarity on the guiding policy principles
- **Issues:** National vs. European Infrastructures; 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.



CIIP - Preparatory study in 2007

“Study on critical dependencies of energy, finance and transport infrastructures on ICT infrastructures”

- Examine what are the critical ICT based dependencies in the sectors under consideration;
- Identify and assess existing (cross-sector) early warning systems and protection strategies;
- Identify existing (cross-sector) best practices where available to counter or mitigate cyber vulnerabilities and threats.

**Call for tender 165210 - 2007/S 135/2007
deadline for submission 5 October 2007**



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-hazards**
 - **Strengthen** the synergies between 1st and 3rd pillar measures



CIIP initiative Flagship actions

- **Defining Criteria for European CII**
- **Bridging gaps between national CIIP policies**
 - identifying and transferring good CIIP policy practices.
- **European Resilience Council,**
 - good practices to be followed, in terms of industrial deployment, in order to ensure resilience.
- **European Information Sharing and Alert System**
 - Member States to establish governmental Computer Emergency Response Teams (CERTs).
- **Internet:** Member States and all relevant stakeholders to agree
 - **priorities for Internet security and resilience**
 - **a unified European voice and strategy** in international discussions and fora.



Web Sites

A Strategy for a secure Information Society – “Dialogue, Partnership and empowerment” COM(2006) 251

http://ec.europa.eu/governance/impact/docs/ia_2006/com_2006_0251_en.pdf

Commission Staff Working Document – Impact Assessment SEC(2006) 656

http://ec.europa.eu/governance/impact/docs/ia_2006/sec_2006_0656_en.pdf

Background information (including the COM in all languages)

http://europa.eu.int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2766

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT>

