Towards a modernised NIS policy in the Europe

Andrea Servida

European Commission

DG INFSO-A3

Andrea.Servida@ec.europa.eu

NIS has never been so high on the EU political agenda

President Barroso "Political guidelines for the next Commission", 3 September 2009

"*The next Commission will develop a **European Digital Agenda** (accompanied by a targeted legislative programme) to tackle the main obstacles to a genuine digital single market, promote investment in high-speed Internet and avert an unacceptable digital divide.* ***Because of the increasing dependence of our economies and societies on the Internet, a major initiative to boost network security will also be proposed.***"

HOW DID WE GET HERE?

NIS : a cross-cutting issue @ EC

DG INFSO

- NIS policy
- CIIP
- e-Signature & eID
- e-privacy
- SPAM
- harmful content
- FP7 ICT theme
- IPv6
- …

DG MARKT

- e-payment
- e-frauds
- …

DG JLS

- Cyber crime
- EPCIP & support programme
- Data protection
- Data retention
- Travel documents
- Identity theft
- …

DG ENTR

- SME's & NIS
- standards
- FP7 Security theme
- …

DG JRC

- Support to policy DG
- Specific R&D
- ERN for CIP
- …

DGIT/ADMIN-DS

- e-Commission
- IDABC
- Internal security policy/rules
- …

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"

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 policy
  - importance of "resilience" strategy for CIIP, i.e. the ability to deal with unexpected events

- **Council Resolution 2007/C 68/01 on a Strategy for a Secure Information Society in Europe of 22 March 2007**
  - Endorses the key elements of the strategy, including the focus on resilience and the key role of ENISA

- **Other policy 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 security breach notifications**
      - **significant impact on operations (Art 13 FWD)**
      - **personal data compromised (Art 4 e-privacy D)**
  - **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**
  - **A clear role for ENISA (FW D & e-privacy D)**

ENISA

- **European Network and Information Security Agency (ENISA)**
  - **Established** in March 2004 for 5 years
  - **Main objective:** assist the Commission and the MS, and in consequence cooperate with the business community, in order to help them to meet the requirements of NIS
  - **Key tasks:** collect information, risk analysis; develop 'common methodologies'; contribute to raising awareness; promote 'best practices' and 'methods of alert'; enhance cooperation between stakeholders; assist Commission and MS in dialogue with industry; contribute to international cooperation
  - **Mid term evaluation** in 2006 + public consultation in 2007 [COM(2007) 285]
  - **Extension** for 3 ys [EP and Council Regulation n. 1007/2008 of 24/09/2008]

A EU Policy initiative on CIIP

Motivation

- **CIIs 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 the primary responsibility of Governments**
  → *governance*
- **CIIs stretch out well beyond national borders**
  → *globalisation*
- **The level of security and resilience in any country depends on the level of security outside the national borders**
  → *sovereignty*
- **National Governments face very similar issues and challenges**
  → *scale*
- **The private sector is calling for harmonised rules for security**
  → *market and economic dimension*

COM(2009)149 final of 30.3.2009
{SEC(2009) 399} - {SEC(2009)400}

Communication from the Commission to the European Parliament and the Council

on Critical Information Infrastructure Protection

"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

Communication on CIIP COM(2009)149
The scope

- **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 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**
  - Focus on tactical/operational activities to stimulate and support EU wide collaboration on strategic planning and actions
- **Governing principles**
  - Build on national and private sector initiatives
  - Engage public and private sectors
  - Adopt an all-hazards approach
  - Be multilateral, open and all inclusive

Communication on CIIP COM(2009)149
The Action Plan

The five pillars of the CIIP Action Plan:

1. **Preparedness and prevention**
2. **Detection and response**
3. **Mitigation and recovery**
4. **International Cooperation**
5. **Criteria for European Critical Infrastructures in the ICT sector**

The CIIP Action Plan

1. Preparedness and prevention

- **Baseline of capabilities and services for pan-European cooperation between National/Governmental CERTs**

  Target: ***End of 2010*** *for agreeing on minimum standards*
  End of 2011 *for well functioning National/Gov CERTs in all Member States*

- **European Public Private Partnership for Resilience (EP3R)**

  Target: ***End of 2009*** *for a roadmap and plan for EP3R*
  Mid of 2010 *for establishing EP3R*
  End of 2010 *for the first results*

- **European Forum for information sharing between Member States**

  Target: ***End of 2009*** *for launching the Forum*
  End of 2010 *for delivering the first results*

With the support of ENISA and building upon its activities

European Commission
Information Society and Media

The CIIP Action Plan
2. Detection and response

- **Development and deployment of European Information Sharing and Alert System (EISAS)**
  - **The Commission financially supports two complementary prototyping projects**
  - **ENISA is called upon to take stock of results and produce a roadmap to further develop and deploy EISAS**

Target: ***End of 2010*** *for completing the prototyping projects*
End of 2010 *for the roadmap*

The CIIP Action Plan
3. Mitigation and recovery

- **National contingency planning and exercises**
  - **National/Governmental CERTs/CSIRTs to take the lead in national contingency planning exercises and testing**

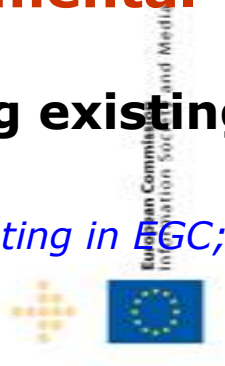
    Target: End of 2010 *for running a national exercise in every MS*

- **Pan-European exercises on large-scale network security incidents**
  - **EC provide some financial support in 2009**

    Target: ***End of 2010*** *for first pan-European exercise*
    End of 2010 *for EU participation in international exercises*

- **Reinforced cooperation between National/Governmental CERTs**
  - **Support pan European cooperation also by expanding existing cooperation schemes (like EGC)**

    Target: ***End of 2010*** *for doubling the number of national bodies participating in EGC;*
    End of 2010 *for ENISA to develop reference materials*



The CIIP Action Plan
4. International Cooperation

- **Internet resilience and stability**
  - **Define European priorities on long term Internet resilience and stability**

    Target: ***End of 2010*** *for EU priorities*
  - **Define principles and guidelines for Internet resilience and stability at the European level** *("focusing inter alia on regional 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")*

    Target: End of 2009 *for a roadmap towards the principles & guidelines*
    Target: End of 2010 *for agreeing on first drafts*
  - **Promote the principles and guidelines for Internet resilience and stability at global level** *("strategic cooperation with third countries will be developed, notably in Information Society dialogues, as a vehicle to build global consensus")*

    Target: Beginning of 2010 *for a roadmap for international cooperation*
    Target: End of 2010 *for first drafts of international principles & guidelines*

The CIIP Action Plan
4. International Cooperation (2)

- **Global co-operation on exercises on large-scale Internet incidents**
  - **Practical way to extend at the global level National and pan-European exercises and to build upon regional contingency plans and capabilities**

    Target: end of 2010 for the Commission to propose a framework and a roadmap to support the European involvement and participation in global exercises on recovery and mitigation of large-scale Internet incidents

The CIIP Action Plan
5. ICT Criteria to identify ECI

- **Continue to develop the criteria for identifying European Critical Infrastructures (ECI) for the ICT sector**
  - **Process conducted in cooperation with Member States and all relevant stakeholders**
  - **A 9-month study was launched in June 2009 to support the process**
  - **Staff Working Paper on criteria is under development**

Target: ***First half of 2010*** *to define the criteria*

The CIIP Action Plan
The role of ENISA (1)

- ENISA is called to
  - **Support the process of defining and agreeing** on a baseline of capabilities and services for national/Governmental CERTs in support to pan-European cooperation
  - **Take stock of the results** of the projects aiming the prototyping of EISAS and other national initiatives **and produce a roadmap** to further progress in the development and deployment of EISAS
  - **Support the exchange of good practices** between Member States on national contingency planning and exercises
  - **Stimulate and support** pan-European cooperation between National/Governmental CERTs and develop reference materials
- Both EP3R and EFMS would greatly benefit from and build upon ENISA's activities

Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) – Presidency conclusions

"There is an urgent need for Member States and all stakeholders to commit themselves to swift action in order to enhance the level of preparedness, security and resilience of Critical Information Infrastructures throughout the European Union."

"The Communication by the European Commission on Critical Information Infrastructure Protection furnishes a solid basis for taking such urgent action as is necessary"

Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) - Presidency conclusions

"It is necessary to stimulate the dialogue between public authorities and the private sector to ensure that the responsibilities of Member States to protect their citizens as well as the practical constraints faced by businesses – which own or operate most Critical Information Infrastructures – are well understood by all parties. The public and private sectors should be engaged at the EU level in developing an appropriate policy, economic framework and the incentives to support the uptake of security and resilience measures. At the same time, an instrument serving to facilitate the sharing of information and the dissemination of good practices between Member States would help to maximise the overall capability and level of expertise across the European Union"

Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) – Presidency conclusions

"Flexible arrangements – for example, in the form of Public-Private Partnerships or a Forum of Member States – are essential to ensure that such understanding and information exchange is followed by concrete action at the strategic and tactical levels "

"The responsibility of ensuring that the level of preparedness, security and resilience of Critical Information Infrastructures in the European Union, as is more generally the case for creating a secure Information Society, is a shared one. Everyone – EU bodies, Member States, the private sector, citizens – must play their part in achieving this objective"

Ministerial Conference on CIIP 27-28 April 2009, Tallinn (Estonia) – Presidency conclusions

"A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan. This joint endeavour would be the first tangible step towards a strong coordination and cooperation among Member States as well as help identify areas requiring immediate actions "

Conference web site http://www.tallinnciip.eu/

TTE Council – 11 June 2009

Ministers expressed full support to the objective and action plan of the Commission's Communication on critical information infrastructure protection (CIIP) as well as to the conclusions of the Ministerial Conference on CIIP held in Tallinn.

The CIIP Action plan – implementation

31 March 2009	**Workshop on EU policy dimension of vulnerability management and disclosure process (report available)**
16 June 2009	**Workshop on EFMS**
17 June 2009	**Workshop EP3R (report available)**
June – Sept 2009	**Informal consultation with MS on EU principles for Internet resilience & stability**
Sept – Oct 2009	**Informal consultation with private sector on EP3R and EU principles**
12-13 Nov 2009	**Follow-up Workshops on EFMS and EP3R**
On-going	**Studies & projects**
On-going	**ENISA activities in support to the Commission policy and Action Plan**

WHERE ARE WE GOING ON NIS?

Public debate on the future of 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 in creased 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**

Public Consultation "Towards a Strengthened NIS Policy in Europe"

- **The Commission launched an on-line public consultation (07/11/08 – 09/12/08)**
  - **challenges and priorities of a modernised NIS policy**
  - **means needed to address the challenges**

- **Report on the results is now public available**
  - **~ 600 contributions, from MS authorities, private sector, academics and individuals**
  - **Key issues: globalisations of threats, global interdependencies, convergence of technologies, lack of minimum NIS standards, quality of security in HW and SW, etc.**
  - **Key areas: cooperation between national/Gov CERTs/CSIRTs, information sharing between MS, building trust between stakeholders (PPP), International cooperation, etc.**

Future of NIS policy in Europe

11 June 2009
Meeting of the Telecom Council

The discussion highlighted the importance and the global dimension of network and information security (NIS) challenges and the **need for a pan European approach to cross border issues as an effective way to increase security and resilience in the EU. A long term EU policy on NIS is needed.** Risk management should be at the heart of any future initiative

Policy on CIIP and the future of NIS: *next steps*

On-going

- **Commission – Impact Assessment on option for future ENISA**

4-5 November 2009

- **Swedish Presidency Conference – "Resilient Electronic Communications - A Multi-stakeholder Challenge"**

17-18 December 2009

- **TTE Council - Council Resolution on future NIS policy in the EU**

December 2009

- **EESC – Opinion on the CIIP communication**

1st half 2010

- **Commission - Proposal for a modernized NIS Policy in the EU**

End of 2010

- **Commission - Stock-taking exercise to evaluate the first phase of actions and to identify and propose further measures**

Web Sites

CIIP related activities and CIIP Communication

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

Presidency Conclusions of the Ministerial Conference on CIIP Tallinn (EE), 27-28 April 2009

http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

Web Sites

EU policy on secure Information Society

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

Report on the public consultation "Towards a Strengthened Network and Information Security Policy in Europe"

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