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

Andrea SERVIDA
European Commission
Directorate General
Information Society and Media - DG INFSO
Unit A3 – Internet Governance; Network and Information Security
andrea.servida@ec.europa.eu
Network and information security (NIS)


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”
Cyber security: the EU Policy

- Focus on prevention, resilience and preparedness (complementary to fighting cyber crime)
- Take into account the civilian & economic stakeholders’ role and capability (role of private sector & the governance challenge)
- Make security and resilience the frontline of defence
- Adopt an all-hazards approach
- Develop a risk management culture in the EU
- Focus on the role socio-economic incentives
- Promote openness, diversity, interoperability, usability, competition as inherent security safeguards
- Boost a global collaborative policy and operational cooperation across the EU, in particular on CIIP
A Digital Agenda for Europe—COM(2010)245

The Seven Priority areas for action

“Every European Digital”

N. Kroes

1. Creating a Digital Single Market
2. Improving the framework conditions for interoperability between ICT products and services
3. **Boosting internet trust and security**
4. Guaranteeing the provision of much faster internet access
5. Encouraging investment in research and development
6. Enhancing digital literacy, skills and inclusion
7. Applying ICT to address social challenges such as climate change, rising healthcare costs and the ageing population.
• Adopted on **31 March 2011**

• **Takes stock** of results achieved since 2009 CIIP action plan

• **Builds** on existing policy initiatives, in particular **Digital Agenda for Europe, Stockholm Action Plan** and **Internal Security Strategy**

• **Highlights** next steps at **European** and **International** level
• An evolving scenario

• Threats and risks
  – exploitation purposes (e.g. GhostNet, ETS, recent attacks against government systems and EU Institutions)
  – disruption purposes (e.g. Conficker, StuxNet, submarine cable breaks)
  – destruction purposes (fortunately not yet materialised)
• EU and the global context

  - A purely European approach is not sufficient and needs to be embedded into a global coordination strategy

  - The DAE calls for the “cooperation of relevant actors [...] to be organised at global level to be effectively able to fight and mitigate security threats" and sets out the goal to “work with global stakeholders notably to strengthen global risk management in the digital and in the physical sphere and conduct internationally coordinated targeted actions against computer-based crime and security attacks”
“Achievements and next steps: towards global cyber-security”

Reports on the achievements and next steps 5pillars 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
Baseline of capabilities and services for pan-European cooperation

**Achievements**
- 2010: ENISA gave recommendations on baseline capabilities for Nat/Gov CERTs;
- 20 MS with Nat/Gov CERTs in place*.

**Next steps**
- ENISA to continue support MS – towards well-functioning network of CERTs at national level by 2012 (DAE);
- ENISA to cooperate with Nat/Gov CERTs towards EISAS by 2013 (ISS).

* Based on information provided to ENISA by MS
• **European Public-private Partnership for Resilience (EP3R)**

  *Achievements*
  - 2010: ENISA Three WGs launched within EP3R;
  - EP3R to provide sustainable framework for modernised ENISA.

  *Next steps*
  - WGs to deliver first results;
  - EP3R to be leveraged in support of the EU-US WG on Cyber-security and Cyber-crime.
Achievements and next steps: towards global cyber-security

Preparedness and prevention (3/3)

• **European Forum for Member States (EFMS)**

  **Achievements**
  - Progress on ICT criteria for ECIs, identification of priorities for Internet resilience and stability, exchange of policy practises.

  **Next steps**
  - To finalise discussion on ICT criteria for ECIs;
  - To be further involved in discussions on International priorities on security and resilience (e.g. EU-US WG);
  - To focus on CERTs cooperation, security incentives, driving pan-European exercises.
• **European Information Sharing and Alert System (EISAS)**

  **Achievements**
  - FISHAS and NEISAS currently producing results
  - ENISA devised a high-level roadmap for development of EISAS by 2013

  **Next steps**
  - 2011: ENISA to support MS by developing basic services needed for national ISAS
  - 2012: ENISA to develop “interoperability services”
National contingency planning and exercises

Achievements
- To date, 12 MS* have carried out cyber-exercises at national level

Next steps
- **ENISA** to continue support MS in developing national contingency plans

* Based on information provided to ENISA by MS
• Pan-European exercise on large-scale network security incidents

Achievements
- **Cyber Europe 2010** carried out on 4th November 2010

Next steps
- MS to work on future **pan-European exercise to take place in 2012**
- ENISA to work with MS on a **EU cyber-incident contingency plan by 2012**
• Internet resilience and stability

  Achievements
  – European principles and guidelines for Internet resilience and stability developed within EFMS

  Next steps
  – Discuss and promote the principles at the international level – bilaterally and in multilateral fora (G8, OECD, NATO, OSCE, Meridian, ASEAN,...)
Global cyber-incident exercises

Achievements
- 7 EU MS took part in US exercise Cyber Storm III (EC and ENISA observers)

Next steps
- In 2011, EC and US will develop, under EU-US WG on Cyber-security and Cyber-crime, a common programme and roadmap towards joint/synchronised trans-continental cyber exercises in 2012/2013
Achievements and next steps: towards global cyber-security

**ICT sector criteria for ECIs**

- **Sector specific criteria for identifying European Critical Infrastructures in the ICT sector**

  **Achievements**
  - Development within EFMS of draft criteria of fixed/mobile communications and the internet

  **Next steps**
  - EFMS to complete discussions by 2011
  - EC to discuss with MS on ICT-sector elements for review of Directive 2008/114/EC
Security is a shared responsibility

Positive achievements but further efforts are needed and the EC calls upon MS to commit to:

- Enhance EU preparedness by establishing a network of well-functioning National/Governmental CERTs by 2012;

- A European cyber-incident contingency plan and regular National and pan-European cyber exercises by 2012;

- European coordinated efforts in international fora and discussions on enhancing Internet security and resilience.
Global coordination is important and necessary

The Commission will:
- Promote principles for Internet resilience and stability* developed within the EFMS;
- Build strategic international partnerships (e.g. EU-US Working Group on Cyber-security and Cyber-crime) and pursue coordination in International fora
- Develop trust in the cloud

• **CIIP Ministerial Conference** in Balatonfüred (HU), 14-15 April 2011

• **HU Presidency Statement** on the Conference is available

• Political commitment to **more EU cooperation** and to **reinforce coordination and cooperation at the International level**

• **Council Conclusions** planned on 27 May
Thanks!
Web Sites

- EU policy on Critical Information Infrastructure Protection – CIIP

- A Digital Agenda for Europe

- EU policy on promoting a secure Information Society

• European principles and guidelines on Internet resilience and stability

• Digital Agenda for Europe - COM(2010)245 of 19 May 2010