

ENISA

Mission & Current Activities

Steve Purser

Head of Technical Competence Department

4 November 2009



Agenda



Who are we?

Activities



Multi-Annual Thematic Programs

- ★ ENISA's work plan is based around a number of **Multi-Annual Thematic Programs (MTPs)**.
 - ★ The current set of MTPs was launched in 2008. They cover the following areas:
 - ★ Improving resilience in European networks.
 - ★ Developing and maintaining cooperation models.
 - ★ Identifying emerging risks
 - ★ These MTPs are scheduled to complete in 2010.
 - ★ We are currently finalising the strategy for the next three years.
- 




Resilience

- ★ Goal : To 'Improve Resilience in European eCommunications Networks & Services.'
- ★ This work consists of three phases:
 - ★ Stock-taking of regulatory/policy environments and provider measures.
 - ★ Identification of good practices and gap analysis.
 - ★ Support for deployment.
- ★ The scope of the work covers:
 - ★ Policy issues.
 - ★ Deployment issues.
 - ★ Technical issues (e.g. DNSSEC).



Maintaining Co-operation Models

- ★ Goal : 'Increasing cooperation between Member States to reduce differences in capability between Member States in the area of NIS'.
 - ★ ENISA develops and supports cooperation models in pre-defined areas.
 - ★ Currently, these areas are:
 - ★ Awareness Raising.
 - ★ Supporting the CERT community.
 - ★ European NIS good practice brokerage.
- 
- A photograph showing several hands of different skin tones stacked together in a circle, with fingers pointing towards the center. This gesture is commonly used to represent teamwork, unity, and collective effort. The hands are positioned in a way that they form a solid, circular base.



Emerging Risks

- ★ Goal: To enable stakeholders to better identify and understand Emerging and Future Risks in the area of NIS.
 - ★ Scenarios submitted by public sector and private sector stakeholders.
 - ★ Expert groups are used to validate and analyse submitted scenarios from a risk standpoint.
 - ★ Will be supplemented by the creation of an EFR Knowledge Base.
- 
- A man in a dark suit and red tie is walking a tightrope. He is holding a brown briefcase in his right hand. The tightrope is stretched over a cityscape made of many small, light-colored cubes. The background is a bright blue sky with white clouds.





The Commission CIIP Communication

- ★ “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” – published 30 March.
- ★ Strengthens the role of ENISA.
- ★ Activities within the scope of the European Program for Critical Infrastructure protection (EPCIP).
- ★ Proposes five areas, or ‘pillars’, of action.
- ★ ENISA is explicitly called upon to contribute to three of these areas.



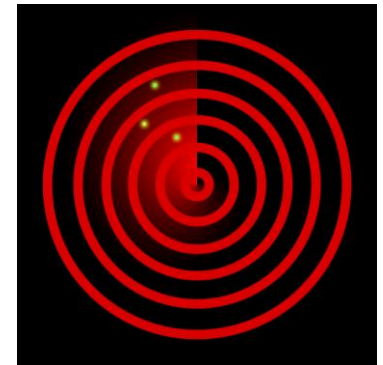
Preparedness & Preparation

- ★ **Baseline Capabilities of National CERTs.**
 - ★ Inventory of baseline services produced in 2009.
 - ★ The inventory will be refined and updated on a periodic basis.
- ★ **Strategic pan European PPP for Resilience.**
 - ★ ENISA proposes to support the Commission and the Member States in establishing and running this forum.
- ★ **European Forum for information sharing.**
 - ★ ENISA will support by offering expertise on policy and operational aspects.
 - ★ Provision of good practice guides as a starting point.



Detection & Response

- ★ European Information Sharing & Alert System (EISAS).
- ★ The Commission will financially support two prototyping projects.
- ★ ENISA can support the Member States by playing the roles of collector and custodian of good information sharing practices.
- ★ ENISA will closely follow the pilot projects, report on the results and produce a roadmap for further EISAS deployment.



Mitigation & Recovery

- ★ National Contingency Plans & Exercises.
 - ★ ENISA has already developed exercises for national CERTs.
 - ★ Currently in the pilot phase.
- ★ Pan-European Exercises on Large-Scale Network Security Incidents.
 - ★ Using lessons learned through the stock-taking exercises, ENISA will help Member states identify the content of such exercises.
- ★ Reinforced Cooperation Between National/Governmental CERTs.
 - ★ Emphasis on analysing standards and obstacles to share information.

