Improving Resilience in European e-Communication networks MTP 1

Dr. Vangelis OUZOUNIS
Senior Expert – Security Policies
Technical Department
ENISA

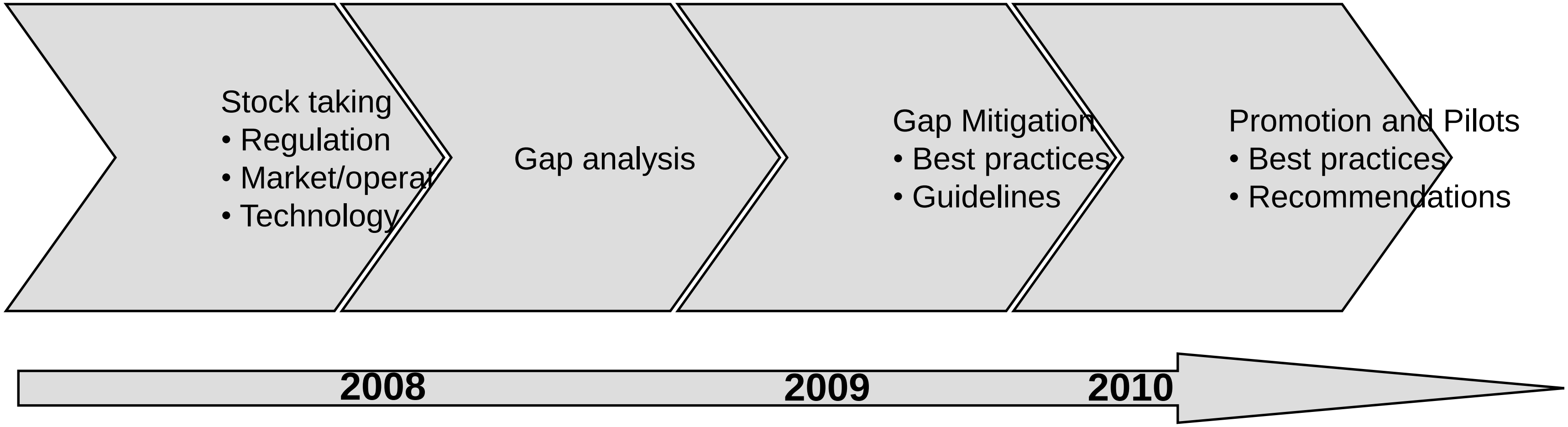
29th of May, Athens

Outline

- ENISA’s MTP 1 Work Programme
  - Work Packages
  - Challenges
- Challenges
- Expression of Interest
- Conclusions

MTP1: Resilience

Collectively evaluate and improve resilience in European e-Communication networks



Stock taking
- Regulation
- Market/operat
- Technology

Gap analysis

Gap Mitigation
- Best practices
- Guidelines

Promotion and Pilots
- Best practices
- Recommendations

2008 **2009** **2010**

By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process

enisa
European Network
and Information
Security Agency

Work Package 1.1

- Objectives
  - analyse existing regulatory measures and requirements put in place by Member States on network and service providers regarding resilience of their operations
- Scope (indicative)
  - identifying authorities in MS and their tasks (e.g. audits, information collection),
  - analysing existing regulatory measures (regulations, recommendations, guidelines)
  - analysing preparedness and recovery measures (e.g. specification, testing, restoration, repair and recovery plans of priority communications)
  - analysing incident response capabilities
  - data exchange among providers, mutual co-operation
  - overall risk assessment measures
- Stakeholders
  - regulators (e.g. ERG and IRG) and National Agencies/Authorities
  - sector associations (e.g. EICTA, ETNO, EUROISPA, national ISP associations, …)
  - pan European Telcos, ISPs, Service Providers, …
  - domain experts and specialised companies
- Approach
  - scoping of topics & identification of stakeholders (workshop Q1 08, Brussels)
  - workshop on questionnaire and stock taking (16.06, Brussels)
  - data collection through targeted interviews of MS representatives (Q2+3 08)
  - analysis of collected data (Q3+4 08)
  - validation of findings with experts and stakeholders (consultation Workshop, Q4 08)
  - Publication of stock taking results

http://www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf

Work Package 1.2

- Objectives
  - analyse approaches, methods, measures and strategies deployed by Network Providers to maintain an acceptable level of operational service
- Scope
  - preparedness and protection measures (e.g. contingency and business continuity plans, priority communications, critical communication paths, ….
- Stakeholders
  - Network and Service Providers, ISPs, ESPs, cc-TLDs,
  - sector associations (e.g. EICTA, ETNO, EUROISPA, GSM Association, National and Regional ISP associations, …)
  - domain experts and specialised companies in resilience services/products
- Approach
  - identification of topics and stakeholders (workshop Q1 08, Brussels)
  - data collection through an online survey (Q2+3 08)
  - analysis of collected data and measures (Q3+4 08)
  - validation of findings with experts and stakeholders (consultation workshop Q4/08 to Q1/09)

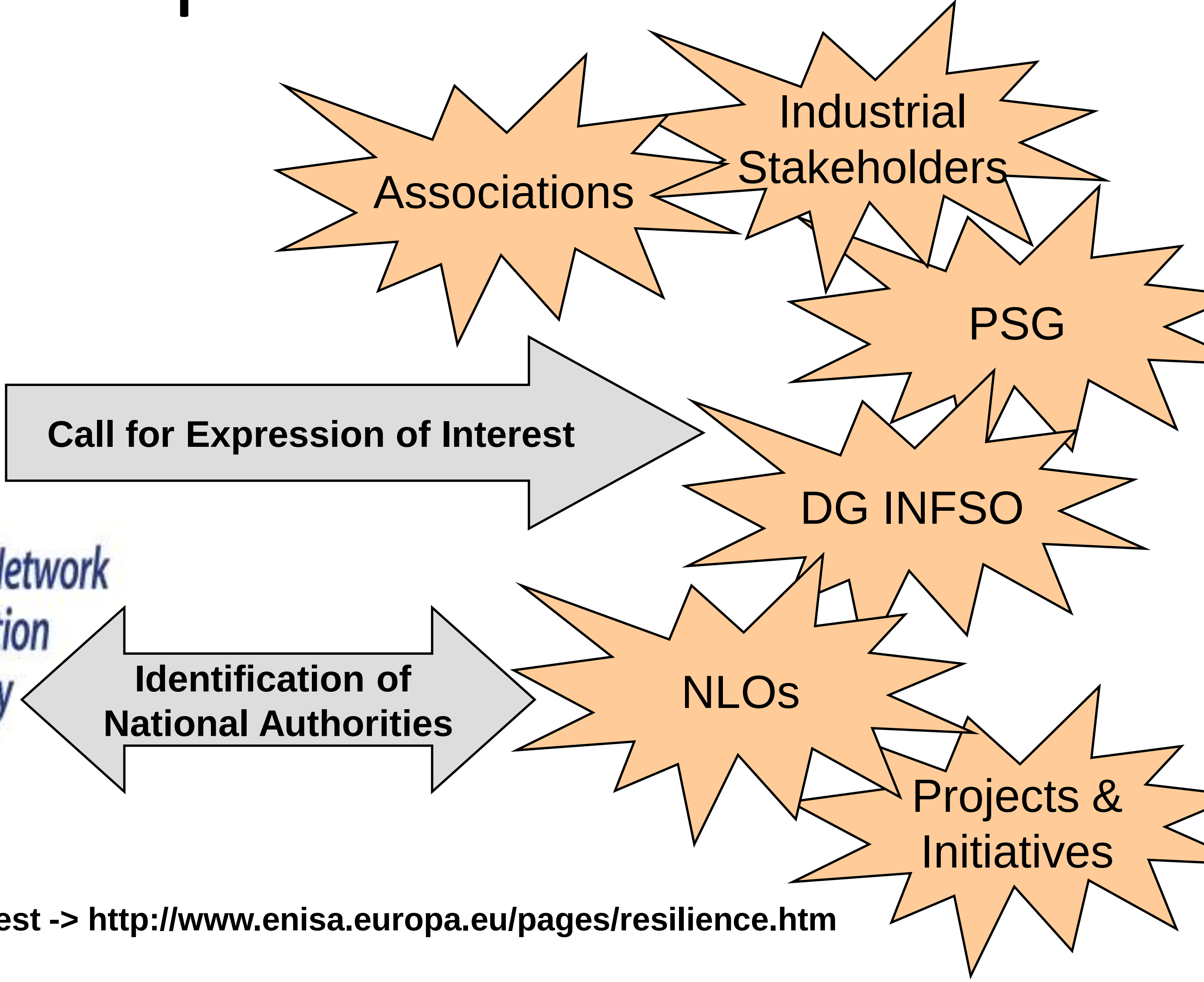
Work Package 1.3

- Objectives
  - analyse current and emerging technologies used by network and service providers to enhance the resilience of their operations
- Scope
  - Internet backbone technologies, DNSEC, security in BGP, IPv6 deployment, …
- Stakeholders
  - network equipment providers, software providers, service developers, outsourcing service providers, …
  - domain experts and specialised companies in resilience service products
  - Research institutes and standardisation bodies
- Approach
  - selection of topics & stakeholders (consultation workshop, Q1 08, Brussels)
  - consultation with stakeholders through seminars, studies, interviews, expert groups (Q2+3 08)
  - analysis of resilience enhancement of existing and emerging technologies (Q4 08)
  - validation of findings with experts and stakeholders (consultation workshop Q4 08 to Q1 09)

Challenges

- complexity (overlapping, conflicting) regulations and measures in MS
- multiplicity of owners and point of references
- diversity of requirements from different sectors
- variety of expectations from different sectors
- emerging topic, only a few pan European specialised professional bodies
- existing stakeholder groups just started developing capabilities
- standards and technologies in progress

Call for Expression of Interest



Call for Expression of Interest

Identification of National Authorities

Call for Expression of Interest -> http://www.enisa.europa.eu/pages/resilience.htm

Identification of National Authorities

- **Who**
  - defines security measures at national level for public communication networks and services
- **Which**
  - security measures were defined
- **How**
  - companies ensure compliance with measures
  - compliance is ensured
  - breaches or deviations from security measures are dealt by both companies & authorities
  - regulation influences security threats
  - can we improve our measures (best practices)?
- **Which is the status so far (lessons learned, way forward)**

- **Response (ENISA's National Liaison Officers)**
  - Austria, Cyprus, Estonia, Finland, Germany, Greece, Iceland, Ireland, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Norway, Portugal, Sweden, UK

Conclusions