Resilient eCommunications Networks

Dr. Vangelis OUZOUNIS

Dr. Demosthenes IKONOMOU

Pascal MANZANO

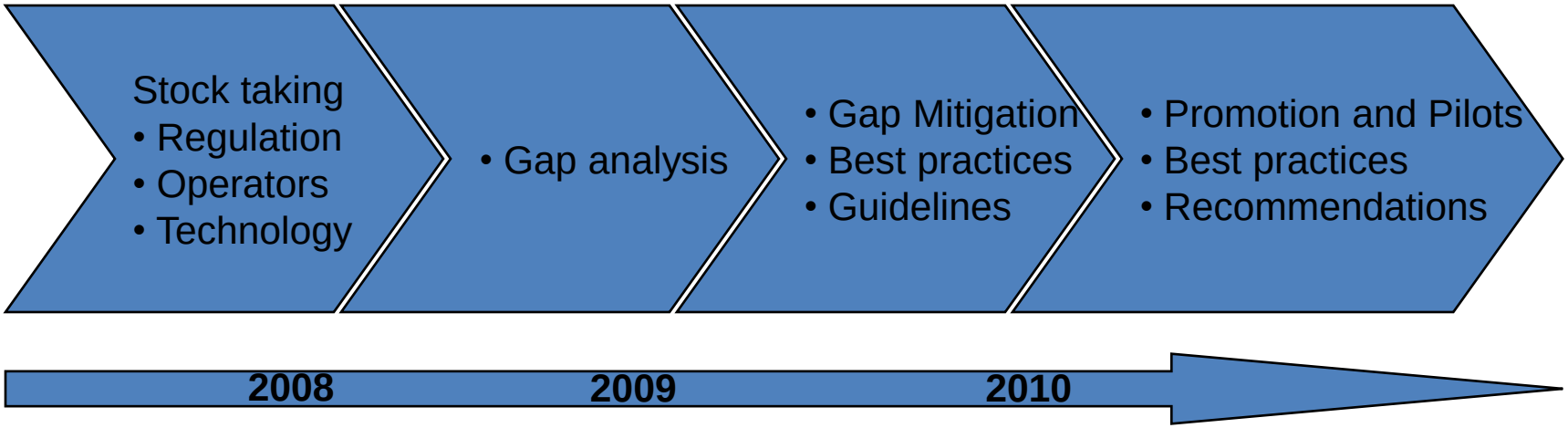
ENISA - Technical Department

Outline

- ENISA's Resilience Program
  - Overview
  - Structure
  - Scope and Progress
  - Future actions
- ENISA's Role
- Conclusions
- Open Consultation

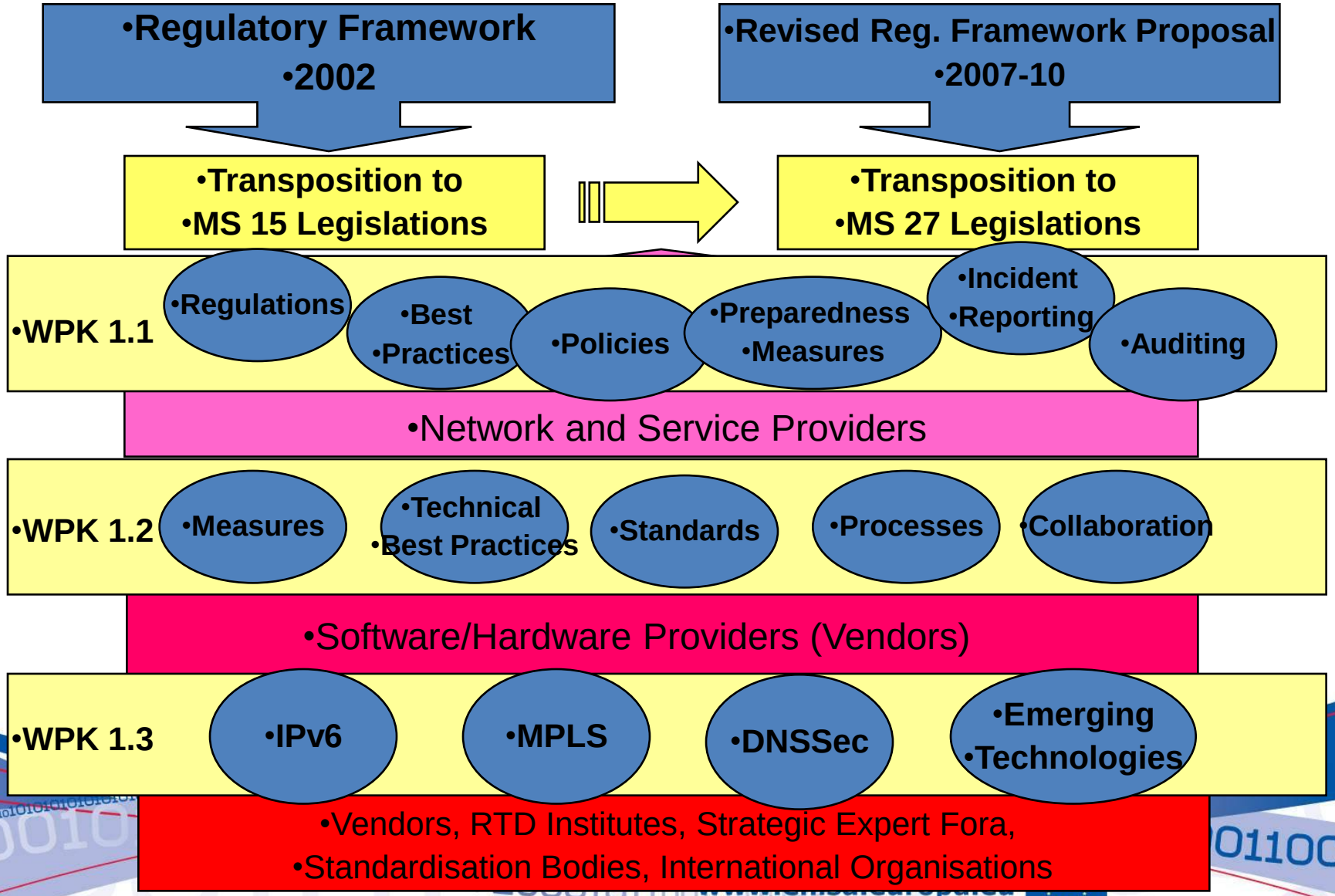
MTP1: Resilience

Collectively evaluate and improve resilience of European public eCommunications Networks



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

MPT 1 Structure



Challenges

- resilience of public eComs networks is a complex issue
  - technical, organisational, policy, physical, etc.
  - difficult to regulate due to evolving risk and threat profiles
- eComs network providers
  - already invest a lot, in their business interests to do more
  - consolidated market, easy to meet, discuss, decide, develop partnerships
  - natural strong interdependencies among providers, already working together (e.g. co-location)
- diversity of standards and technologies
- interplay of existing and emerging technologies
- Not always a technology problems but business/market related decisions

MTP 1 – Roadmap

Scoping & stakeholders identification (Q1 08)	Workshop with stakeholders (7.03 Brussels)	expression of interest	identification of stakeholders
questionnaires (Q2 08)	consultation process with stakeholders	questionnaires development and validation	
data collection & analysis (Q2-3-4 08)	interactive interviews with stakeholders	validation of stock taking findings	publication of stock taking findings (WPK 1.1)
consultation on findings & future orientations (Q4 08)	analysis of stock taking findings (WPK 1.1)	consultation on stock taking findings - future orientations	publication of stock taking and analysis findings

WPK 1.1 – Stock Taking

Governance

- authorities,
- legal mandates
- regulatory measures, guidelines
- existing co-operation models and initiatives
  - partnerships between authorities and providers
  - partnerships among providers

Co-operation Models and Exchange of Information

- typical tasks of authorities
- information exchange mechanisms between authorities and providers
- reporting of incidents (e.g. outages, breaches, etc.)
- audit mechanisms
- enforcement actions

Preparedness and Recovery Measures

- national risk management processes
- preparedness and recovery measures
- incident response capabilities
- good practices development
- guidelines or policies affecting public procurements

WPK 1.1 in 2009

- Develop best practices in three policy areas
- Possible topics
  - Partnerships among authorities and providers,
  - reporting & analysis of incidents through information exchanges (e.g. security breaches, network failures, service interruptions),
  - National risk management processes
  - national preparedness & recovery measures (e.g. restoring priority communications),
  - monitoring and auditing mechanisms
  - .....
- How
  - organise thematic workshops,
  - form a group of experts from public and private stakeholders
  - perform targeted interviews and discussions with experts,
  - assess similar cases of non EU countries (e.g. OECD countries).
  - develop realistic and implementable guidelines
  - pilot them in real working environments in 2010

WPK 1.2 – Scope

- Objectives
  - Analyze measures deployed by network and service providers to enhance the resilience of public communication networks;
- Scope
  - Providers' Core Network;
  - Get feedback from diverse kind of providers:
    - Geographically
    - Size
    - Coverage
- Stakeholders
  - Equipment vendors, network operators, services providers, Internet Exchange points, operators associations
- Target Group
  - Regulators and Policy Makers;
  - Operators and vendors;

WPK 1.2 in 2009

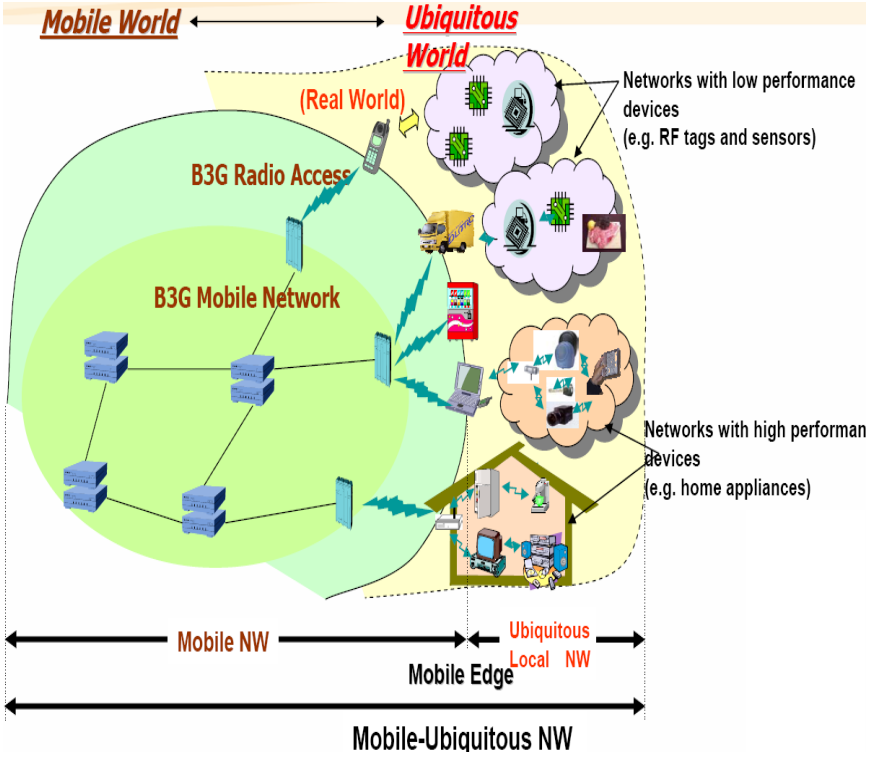
- Assess the gaps based on the analysis of the information collected in 2008
- Identify measures and appropriate implementation strategies that could potentially fill in these gaps by
  - Analyse existing practices
  - Organise a workshop with stakeholders to debate about possible measures that could be used to improve the situation
- Based on this input, Guidelines addressing the identified gaps will be drafted and challenged via an open consultation process

WPK 1.3 – Scope

- Objectives
  - Analyze current and emerging technologies used by network and service providers to enhance the resilience of their operations;
- Scope
  - IP backbone technologies;
  - **IPv6:** A technology replacing IPv4, the internet protocol;
  - **DNSSEC:** Security extensions improving the security of Domain Resolution System;
  - **MPLS:** A protocol used by operators in IP backbones, replacing Frame Relay and ATM;
- Stakeholders
  - Equipment vendors, network operators, services providers
  - Research institutes and standardization bodies
- Target Group
  - Regulators and Policy Makers;
  - Operators and vendors;

WPK 1.3 in 2009

- Finalise the activities of 2008 by elaborating the definition of guidelines about innovative actions to enhance the resilience of public eCommunication networks;
- Moreover, assess the impact of the evolution of networking technologies in terms of resilience, for example:
  - edge networking;
  - Machine to machine communications,
  - Personal and Body Area Networks (PAN, BAN);
  - Sensor networks;
- The results of the latter activity are expected to form contributions to the preparation of the Framework Programs of EU funded R&D through the identification of research priorities in the areas of networking resilience as well as network and information security.



ENISA's Role

- emerging centre of excellence on security and resilience issues
- trusted body, politically accountable to EU Parliament and Council
-
- at the disposal of MSs and EU bodies to analyse policy and regulatory issues
- at constant consultation with public and private stakeholders

Conclusions

- Regulatory & Policy initiatives at early stages
- Variety of policies, strategies, regulatory provisions, measures and operation capabilities of MS'
- Different maturity levels, but big interest and commitment by all to improve
- Partnerships among public and private entities are important
- Providers invest a lot, in their interest to do more (if there is a business case or relevant incentives)
- This is a journey, not an one off activity; strong commitment and leadership is needed
- Co-operation among Member States (and other key countries) is essential

Public Consultation

- Commission organises an public consultation on Network and Information Security in Europe
- Consultation is open to both citizens and organisations
- Objectives
  - gather information on the challenges in network and information security,
  - identify priorities of a strengthened network and information security policy
  - propose means and strategies needed to achieve them
- http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=InfsoNis