enisa
European Network and Information Security Agency

Improving Resilience in Public eCommunication Networks

P. Saragiotis

Key Facts

eEurope 2005 Action Plan → set up in 2004 by EU Regulation

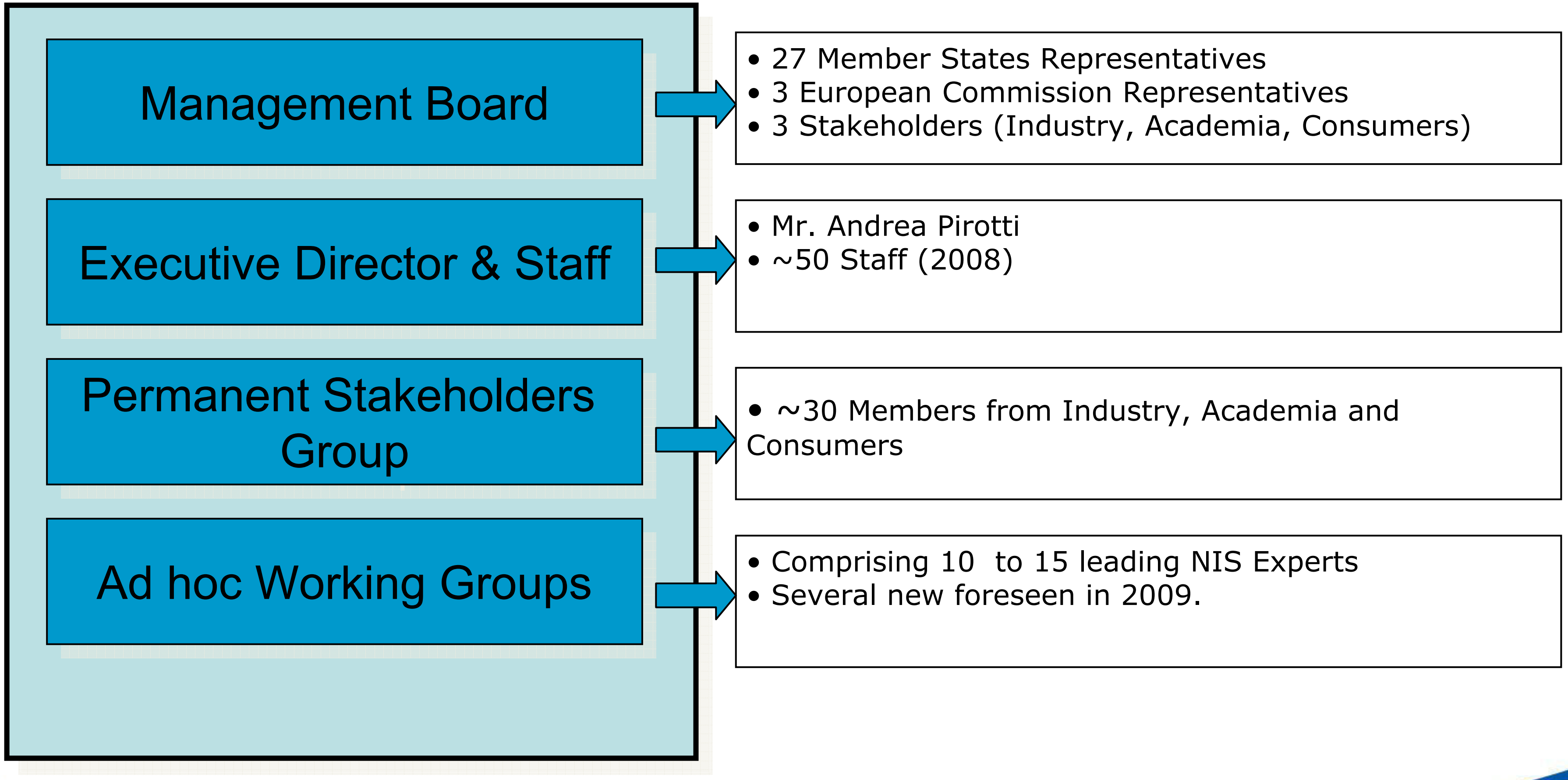
Operational since September 2005 in Heraklion, Greece

~50 Staff

~34.8 M€ for 5 years

ΕΛΛΑΔΑ-ELLADA
Crete

ENISA Structure



Management Board

- 27 Member States Representatives
- 3 European Commission Representatives
- 3 Stakeholders (Industry, Academia, Consumers)

Executive Director & Staff

- Mr. Andrea Pirotti
- ~50 Staff (2008)

Permanent Stakeholders Group

- ~30 Members from Industry, Academia and Consumers

Ad hoc Working Groups

- Comprising 10 to 15 leading NIS Experts
- Several new foreseen in 2009.

ENISA Objectives

To enhance the capability of the Commission, other EU bodies and the Member States to prevent, address and respond to NIS problems

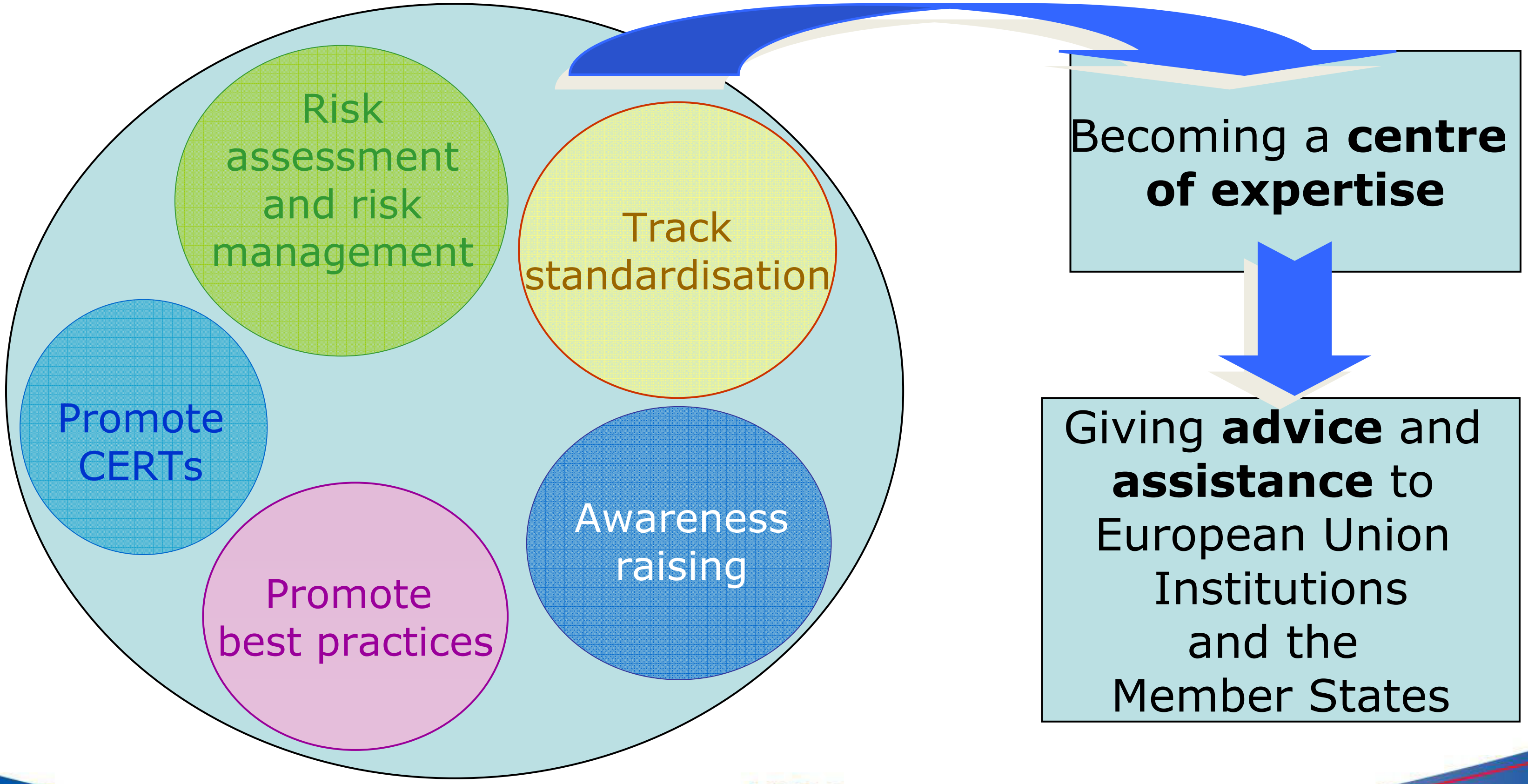
To provide assistance and deliver advice to the Commission and the Member States on issues related to NIS falling within its competencies as set out in its establishing Regulation

To develop a high level of expertise and use this expertise to stimulate broad cooperation between actors from the public and private sectors

To assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of NIS

ENISA’s main tasks

- to promote stakeholder cooperation



Risk assessment and risk management

Track standardisation

Promote CERTs

Awareness raising

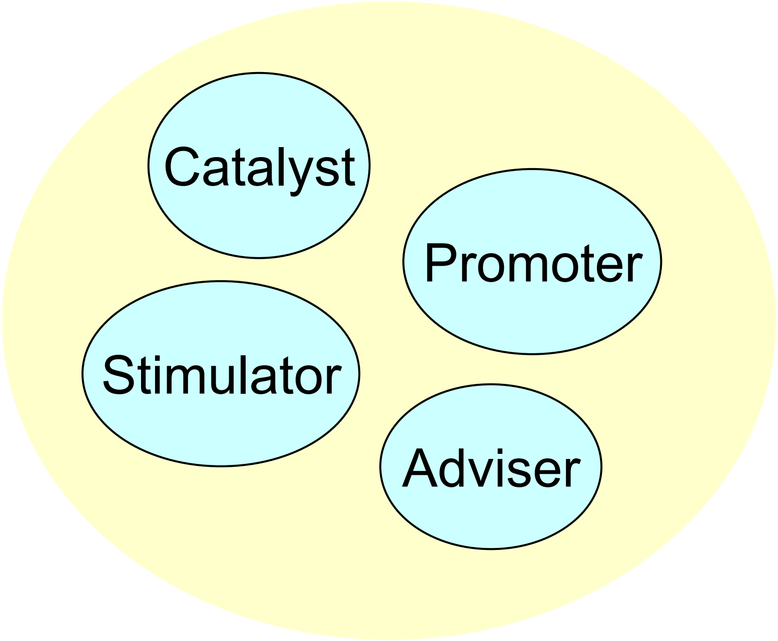
Promote best practices

Becoming a **centre of expertise**

Giving **advice** and **assistance** to European Union Institutions and the Member States

Scope of activities

- to be a…



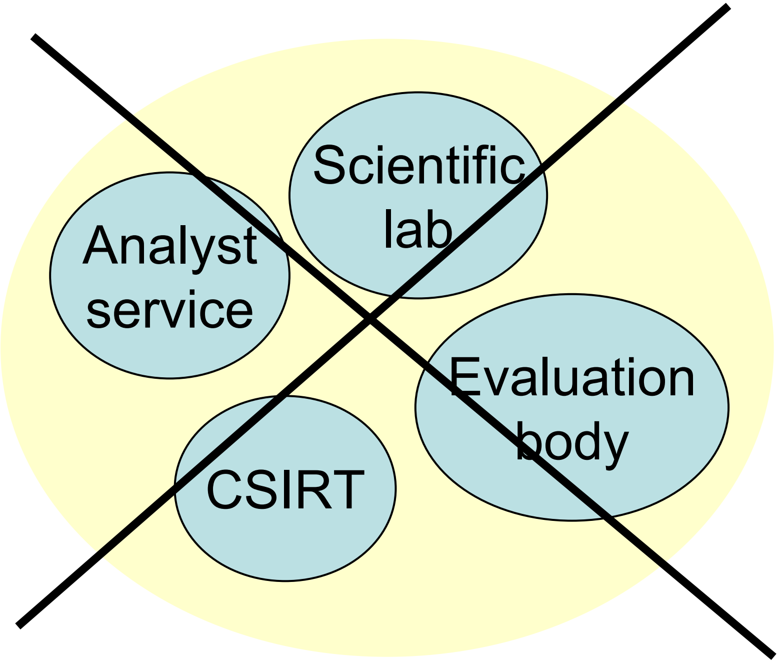
Catalyst

Promoter

Stimulator

Adviser

- and not a…



Scientific lab

Analyst service

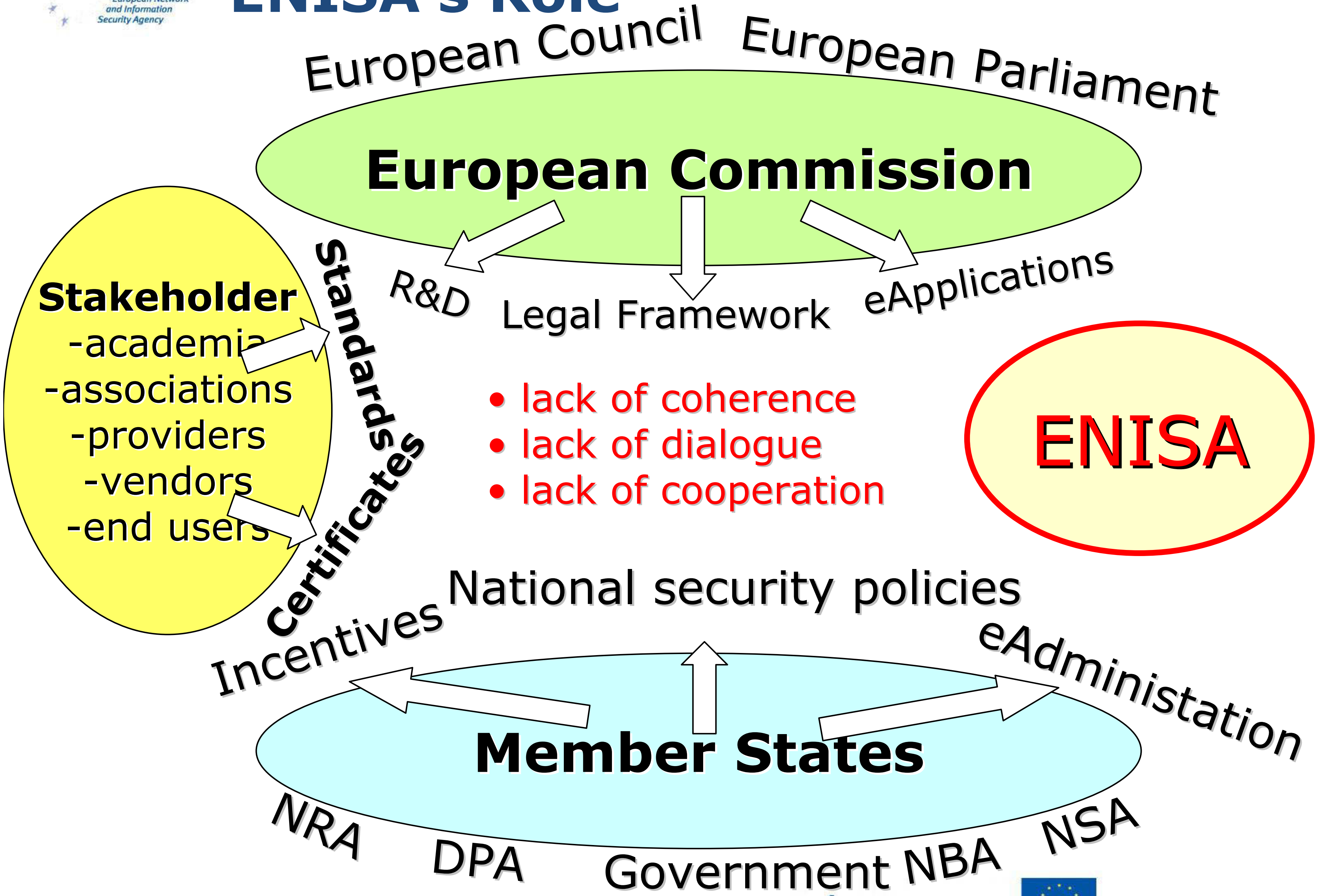
Evaluation body

CSIRT

… maintain internal expertise, at **the disposal for EU and Member State competent bodies**

(respond to Requests and Calls for Assistance)

ENISA's Role



European Council

European Parliament

European Commission

R&D

Legal Framework

eApplications

Stakeholder
-academia
-associations
-providers
-vendors
-end users

Standards

Certificates

- lack of coherence
- lack of dialogue
- lack of cooperation

ENISA

Incentives

National security policies

eAdministation

Member States

NRA

DPA

Government NBA

NSA

Activities for 2008 and beyond

- Multi-annual Thematic Programmes
  - Strategic priorities for ENISA
  - Implemented through a number of Work Packages
- Current focus on:
  - Improving Resilience in European e-Communication Networks
  - Developing and Maintaining co-operation between Member States
  - Identifying Emerging Risks for creating trust and confidence
  - Building information confidence with Micro Enterprises (Preparatory action)

Resilience

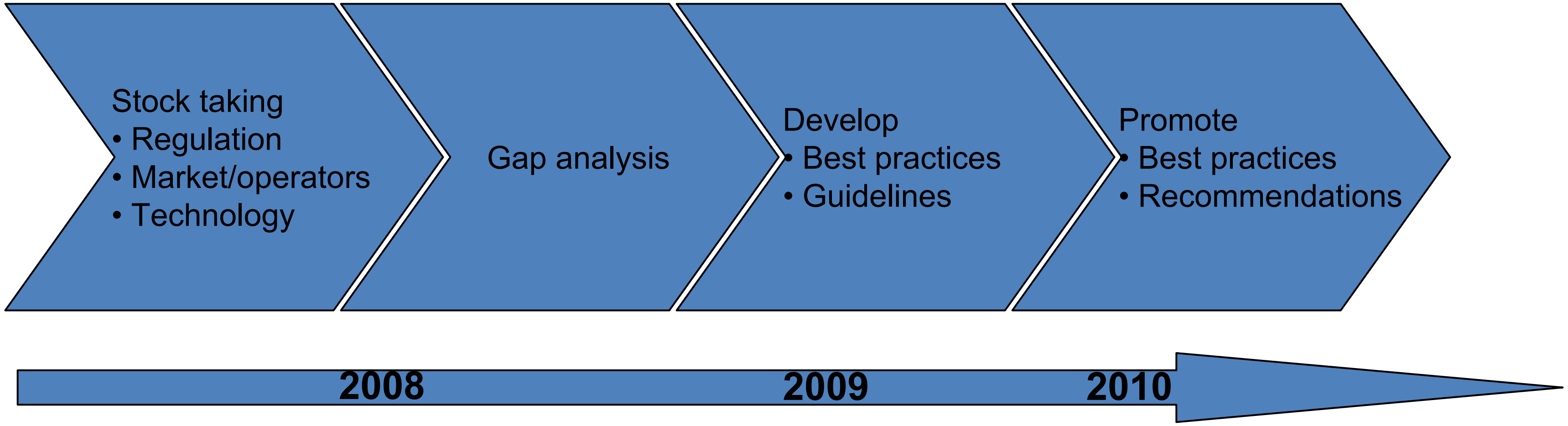
The ability of a system to provide & maintain an **acceptable level of service** in face of faults ***(unintentional, intentional, or naturally caused)*** affecting normal operation

Network resources resilience

- A resilient network design aims to remove single points of failure in switching/routing equipment;
- The main aim of resilience is for fault to be invisible to users;
- Network availability is an issue of risk management and involves technical measures such as:
  - Resilient design;
  - Resilient transmission media;
  - Resilient equipment;

MTP1 - Improving Resilience in European e-Communication networks

Collectively evaluate and improve resilience in European e-Communication networks



Stock taking
- Regulation
- Market/operators
- Technology

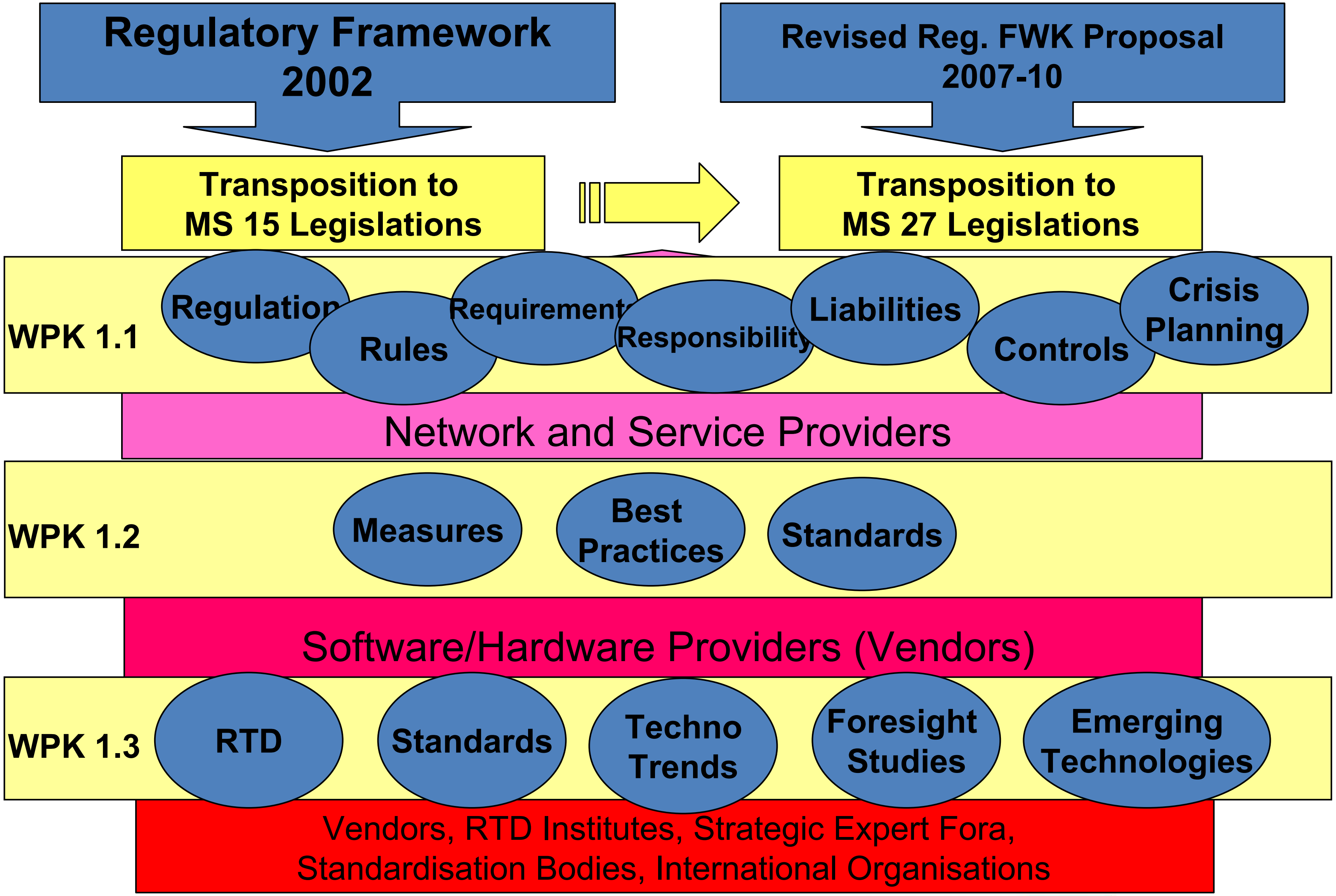
Gap analysis

Develop
- Best practices
- Guidelines

Promote
- Best practices
- Recommendations

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

MTP 1 Overview



Regulatory Framework 2002

Revised Reg. FWK Proposal 2007-10

Transposition to MS 15 Legislations

Transposition to MS 27 Legislations

WPK 1.1

Regulation

Rules

Requirements

Responsibility

Liabilities

Controls

Crisis Planning

Network and Service Providers

WPK 1.2

Measures

Best Practices

Standards

Software/Hardware Providers (Vendors)

WPK 1.3

RTD

Standards

Techno Trends

Foresight Studies

Emerging Technologies

Vendors, RTD Institutes, Strategic Expert Fora, Standardisation Bodies, International Organisations

WPK 1.3 – Background Info

- Objectives
  - Analyze current and emerging technologies used by network and service providers to enhance the resilience of their operations
- Scope
  - IP backbone technologies
- Stakeholders
  - Equipment vendors, network operators, services providers
  - Research institutes and standardization bodies
  - Policy makers
- Target Group
  - Regulators and Policy Makers
  - Operators

Approach - Status

- Selection of topics & stakeholders
  - Consultation workshop, Q1 08, Brussels
- Consultation with stakeholders
  - Interviews, Expert groups (Q3 & Q4 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

Virtual Working Group

- Group of leading experts
- Scope
  - Validate the questionnaire
  - Validate the stock taking and analysis methodology
  - Analyse the received input
  - Draft guidelines
- Deliverables
  - Draft guidelines on the effectiveness of the selected technologies in improving the resilience of public e-Communication networks

Selected Technologies

- IPv6
  - OSI Layer 3 technology replacing IPv4
  - Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe
- MPLS
  - OSI Layer 2.5 technology
  - Used by operators in IP backbones, replacing Frame Relay and ATM
- DNSSec
  - A technology improving the security of Domain Resolution Service

IPv6

- More addresses available
- No need for Network Address Translation
- Site Multihoming
- IP Host Mobility
- IPsec
  - Authentication Header
  - Encapsulating Security Payload

MPLS - Multiprotocol Label Switching

- IP Based networks routing
  - Each node makes its own routing decision
  - Use IP routing protocols to maintain consistent routing tables
  - The per-hop nature of IP routing decisions provides resiliency
- IP routing fundamental constraints
  - Traffic always uses the shortest path to the destination
  - Critical links can get overloaded
  - Convergence time is too long for Real Time Applications

MPLS - Multiprotocol Label Switching

- Provides a Layer 2 connection-oriented transport mode through a Layer 3
- Enables class of service (CoS) tagging and prioritization of network traffic
- Features that enhance Resilience
  - Traffic Engineering (TE)
    - the shortest path with available bandwidth will be chosen
  - TE - Fast Reroute
    - About 50ms
  - MPLS DiffServ - TE

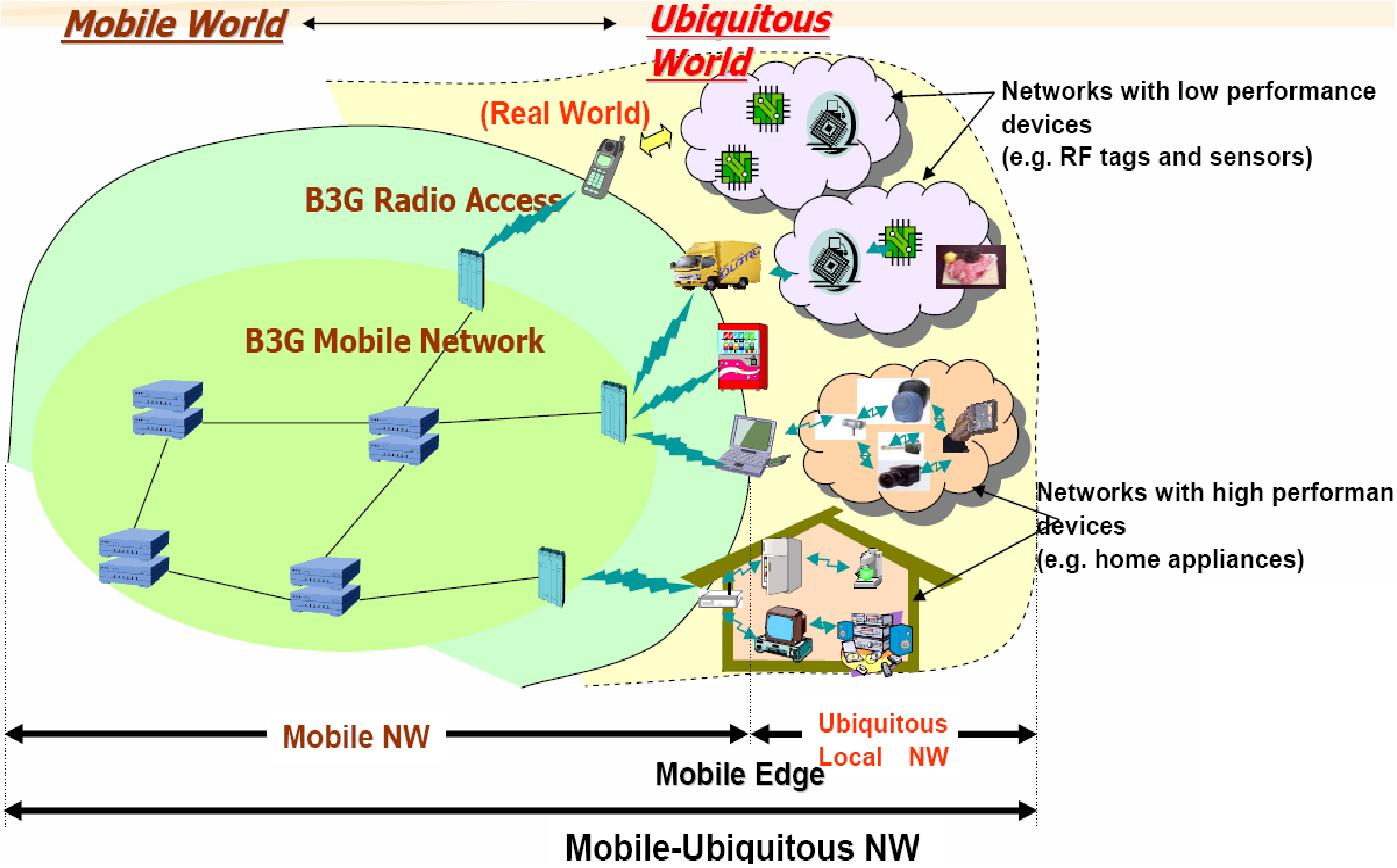
DNSSec

- DNS is a critical service for IP Based Networks
- DNS Known Threats (RFC 3833)
  - Packet Interception - monkey-in-the-middle attacks
  - ID Guessing and Query Prediction
  - Name Chaining - Cache Poisoning
  - Betrayal By Trusted Server
  - Denial of Service
  - Wildcards

DNSSec

- DNSSec resilient features
  - End-to-end data integrity check
  - Use TSIG to ensure the integrity with a recursive name server
- Weaknesses
  - Answer validation increases the resolver's work load
  - Denial of Service
  - Trust model is almost totally hierarchical
  - Key rollover at the root is really hard
  - Betrayal By Trusted Server still exists as threat

Future Networking Trends



MTP1 – Perspectives 2009

- WPK 1.1 : Gap analysis on regulatory measures
  - Analysis of common approaches and gaps
  - Large consultation of stakeholders and authorities
- WPK 1.2 : Gap analysis of implemented measures
  - Clustering of implemented measures and resilience approaches
  - Gaps analysis and best practice identification
- WPK 1.3 : Analysis and recommendations on how to enhance resilience
  - Recommendation on resilience enhancing methods and tools
  - Business impact analysis and incentive proposals
  - Networking trends and impact

Summarizing

- Importance of the Resilience of public eCommunication networks
- ENISA is working with all sector actors
  - Key target audience are Policy Makers, NRAs and Operators
- Technologies benefits are well recognized however the economical / political incentives have to be made

Thank You

Panagiotis SARAGIOTIS,
European Network and Information Security Agency
SN Expert - Security Tools and Architecture

Email: Panagiotis.Saragiotis@enisa.europa.eu
Tel.: (+30) 2810 39 1310

- References
  - http://www.enisa.europa.eu
  - http://www.enisa.europa.eu/pages/resilience.htm