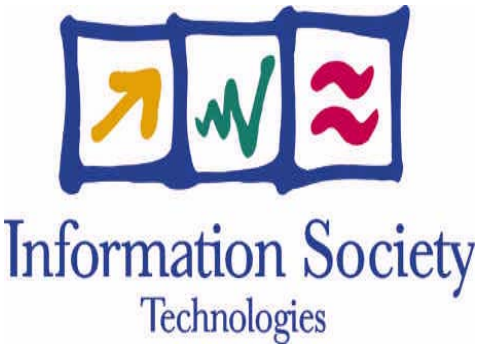
# Security and resilience in Information Society: *the European approach*

Andrea Servida
Deputy Head of Unit
European Commission
DG INFSO-A3
Andrea.servida@ec.europa.eu.

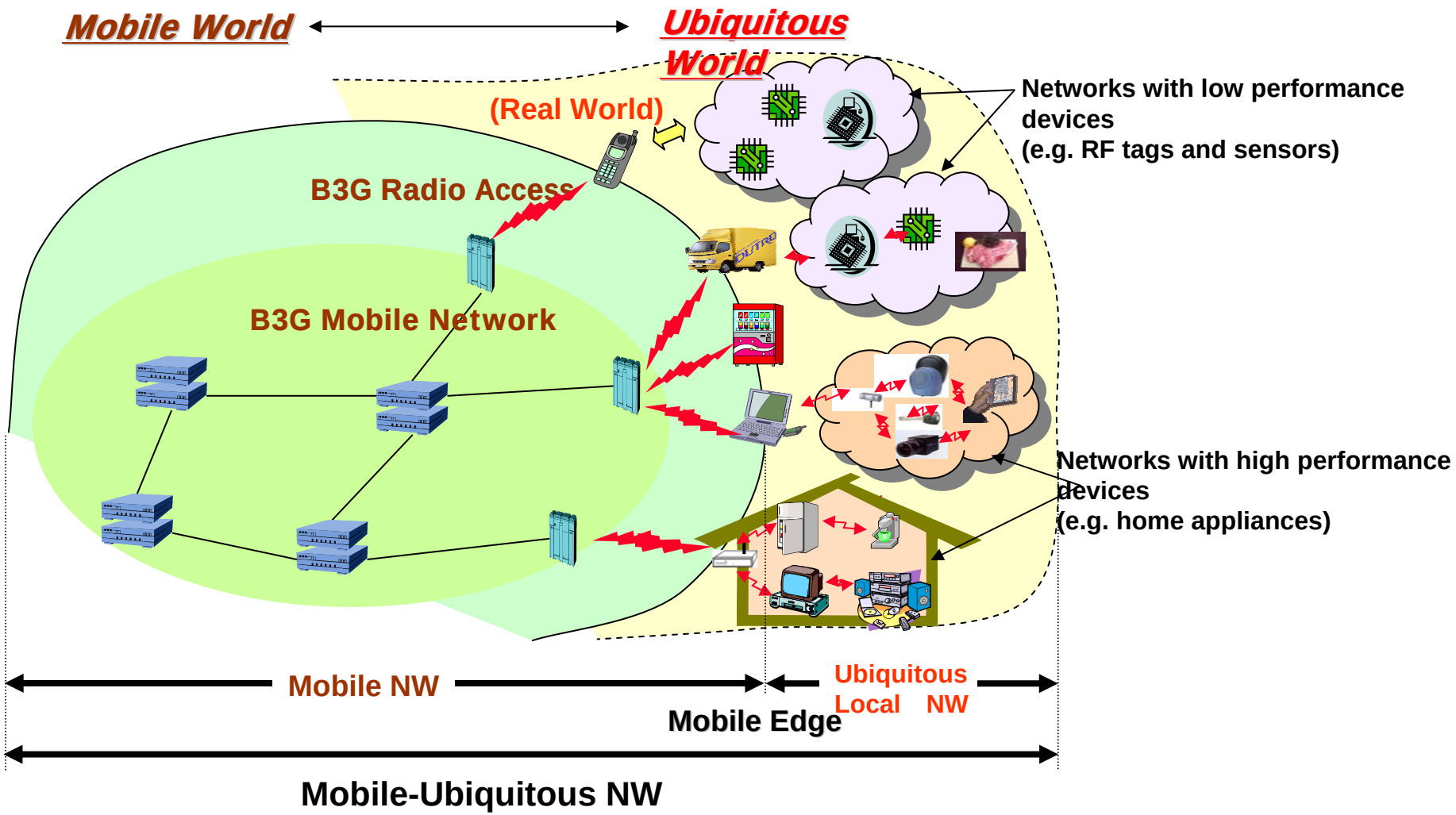


# OUTLINE

- **NIS policy: the background and the new strategy**
- **CIIP plans & challenges**
- **The role of EU R&D on security & dependability**
- **Where we stand in FP6 on CIIP-related research**
- **The future & FP7: towards resilience and plasticity**

# What's ahead: mobile ubiquitous environments

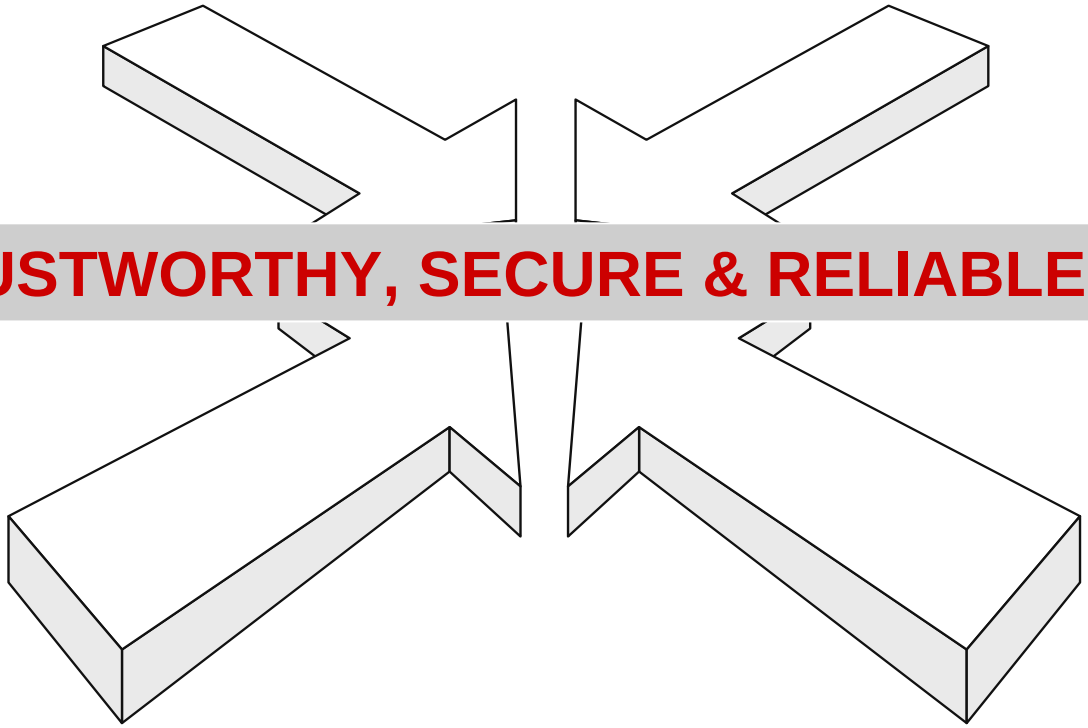
*Broaden communication parties, networking, and business opportunities*



# NIS in the Information Society

TECHNICAL dimension

SOCIAL dimension




ECONOMIC dimension

LEGAL dimension

# The technical dimension & challenges

- Threat landscape changes
- Convergence of digital services
- COTS products and systems
- Interdependent devices and applications
- Pervasiveness of ICT

# The economic dimension & challenges

- **Lack of user confidence**
- **Make the EU ICT industry a competitive supplier**
- **Private and public sectors as demanding users**
- **NIS industry to become a strategic sector for EU**
- **Financial loss due to poor risk preparedness**

# The social dimension & challenges

- **Citizens & consumers may become “vehicles” of attacks**
- **Societal dependence on ICT (→CIIP)**
- **Protection of fundamental rights as a prerequisite for democracy**
- **Balance between NIS policies and civil liberties**

# The legal dimension & challenges

- **A substantial body of legislation relevant to NIS exists**
- **Need for new legal and/or regulatory measures**
- **New regulatory measures, if needed, as result of the 2006 Review of the Regulatory Framework for eCommunications**
- **Proportionality & enforceability of laws**

# The key principles …

*… to improve and develop a culture of NIS*

- **Technical**
  - Promote diversity, openness and interoperability as integral components of security
- **Economic**
  - Present NIS as a virtue and an opportunity
- **Social**
  - Individual users need to understand that their home systems are critical for the overall security chain
- **Legal**
  - Privacy and security are a prerequisite for guaranteeing fundamental rights on-line

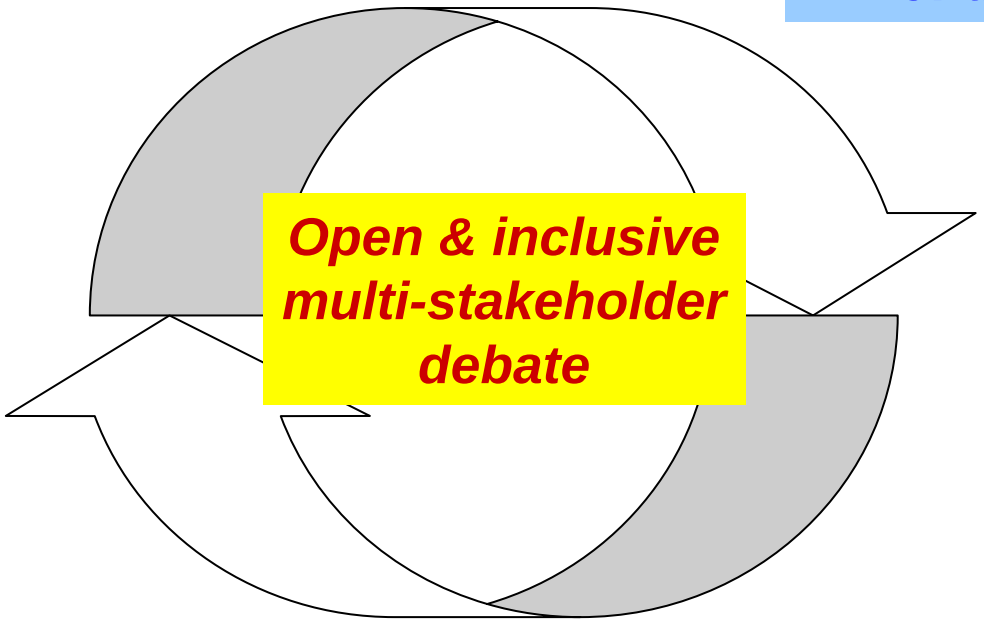
# The challenges for stakeholders

- **Public Administrations**
  - to address the security of their own networks and **serve as an example of best practice** for other players
- **Private sector enterprises**
  - to **address NIS as an asset and an element of competitive advantage** an not as a “negative” cost
- **Individual users**
  - to understand that **their home systems are critical** for the overall “security chain”

# Towards a secure Information Society

**DIALOGUE**
*structured and multi-stakeholder*

**PARTNERSHIP**
*greater awareness & better understanding of the challenges*




**EMPOWERMENT**
*commitment to responsibilities of all actors involved*

# Dialogue

- **Benchmark national NIS-related policies**
- **Address SMEs as well as individual users**
- **Structured multi-stakeholder dialogue**
  - How to exploit existing regulatory instruments to strike a balance between security and the protection of fundamental rights
  - **Develop a sector-specific policy for the ICT sector to enhance the security and the resilience of networks (->CIIP)**
- **A Business Summit**
- **A Seminar for end-users**

# Partnership

- **Improve knowledge of the problem**
- **Establish strategic platform**
- **Support response capability**

# Empowerment

- **Invite Member States to:**
  - **Participate in the benchmarking exercise**
  - **Promote awareness campaigns on virtues and benefits of NIS**
  - **Promote good security practices to other sectors**
  - **Reinforce higher education curricula in NIS**

# Empowerment (2)

- **Invite private sector stakeholders to take initiatives to:**
  - **Tackle the issue of responsibilities for software producers and Internet service providers**
  - **Promote diversity, openness, interoperability, usability and competition**
  - **Disseminate good security practices**
  - **Promote training programmes in the business sector**
  - **Work towards affordable security certification schemes**
  - **Involve the insurance sector in risk management tools and methods**

# To complete the picture

- **Two forthcoming Communications on spam, spyware and malware & on cybercrime**
- **Follow up to the Green Paper on Critical Infrastructure Protection (→CIIP)**
- **2006 Review of the Regulatory Framework**
- **International cooperation- promoting global cooperation on NIS (e.g. WSIS follow-up)**
- **eCommission**
- **FP7 …**

# Plans on CI IP

- In June 2004, the **European Council** asked for an overall strategy to protect critical infrastructures
- On 17 November 2005, the Commission adopted **a Green Paper** on the policy options for a **European Programme on Critical Infrastructure Protection (COM(2005)576)**
- Contributions were received from **22 Member States** and over **100 private companies and industry associations**
- Contributions confirm the need for action at the European level to **enhance the protection and resilience of critical infrastructures**
- Because of their horizontal nature with inter-linkages into many other critical infrastructures, **the protection of communication and information infrastructure is mentioned as a priority**
- We intend to launch a **Europe-wide dialogue on CIIP with public and private stakeholders in the fall**

# Challenges of the CIIP dialogue

- **Organisational: to build trusted relationships and motivate private sector**
- **Policy orientations: to achieve a better understanding and clarity on the guiding policy principles**
- **Issues: preventive, detection/early warning & responsive measures; cross-sectors proactive information assurance methods; share knowledge and best practices; inter-dependencies; long-term Internet stability & security; recovery and continuity strategies; etc.**

# Preparatory studies on CIIP

- ***Availability and Robustness of Electronic Communications Infrastructures***
  - aims at identifying the threats and vulnerabilities in next generation 3G mobile and Internet core networks, with the goal of developing recommendations to avoid or reduce their potential impact on the European Critical Infrastructure
  - started in Jan 2006, duration is 14 months and the contractor is Lucent Technologies

- ***Strengthening the protection of European critical communication and information infrastructures***
  - Call for tenders closed
  - Evaluation in on-going

# The role of EU R&D in ICT trust & security


**R&D shall lead to**

**Develop knowledge & technology - understanding implications and benefits**

**secure, dependable, acceptable & respectful (of human rights and dignity) systems/applications**

**proper assessment and evaluation**

# Resilience of ICT infrastructures & interdependencies

## IP - IRRIIS

- Novel and advanced model and simulation tools in synthetic environment
- MIT components for preventing & limiting cascading effects and support automated recovery and service continuity

## STREP- CRUTIAL

- modelling approaches for understanding and mastering interdependencies
- fault-tolerant architectural configurations and models enabling dependable control and management

## CA - GRID

- Methods to assess reliability, security and risks
- Management, control and protection schemes including architectures and devices

# Security & Resilience in mobile environments

## STREP- UBISEC&SENS

- a security and reliability architecture for wireless sensor networks
- medium and large scale networks

## STREP - HIDENETS

- develop end-to-end resilience solutions in wireless networks
- assuming highly dynamic, unreliable communication infrastructures

## NoE - RESIST

- resilience and survivability of the future ubiquitous computing systems
- to support and provide Ambient Intelligence

# Resilience of ICT infrastructures: technologies

## IP - DESEREC

- innovative approaches and tools to design and model infrastructures resilience
- mechanisms for fast detection of complex incidents
- framework for computer-aided counter-measures to respond and mitigate the threats to dependability

## IP - SERENITY

- S&D patterns and integration schemes including behavioural description and trust mechanisms
- computer aided run-time pro-active and reactive support for identification of potential threats and attacks of implemented security solutions

# Immunity of mobile networks

## *Secure execution of mobile applications*

### STREP - PEPERS

- development of applications from toolbox (framework)
- verification at loading and execution time
- mobile applications in mobile peer-to-peer architectures

### STREP - S3MS

- design of applications by “contract”
- verification at loading and execution time
- mobile applications in mobile networks on Java and Windows platforms

### IP - SERENITY

- development of applications from toolbox (framework) based on security and dependability patterns and Integration Schemes
- verification at loading and execution time
- not limited to mobile applications

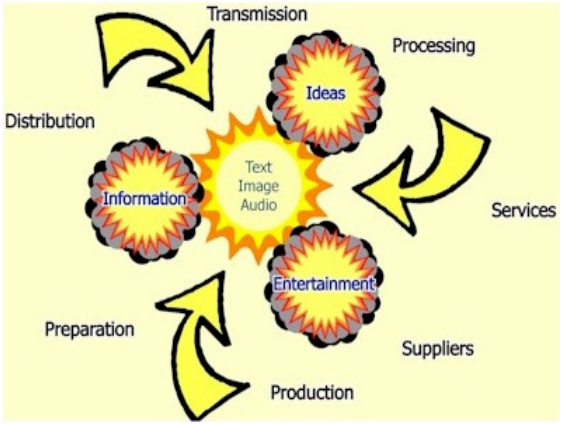
### IP - OPEN_TC

- focuses on open and interoperable trusted computing
- secure execution based on trusted platforms
- not limited to mobile platforms

# What's driving the future?

## CONVERGENCE OF:

MEDIA




PROCESSES

IP & NETWORKS

# From dependability to resilience …

- **Dependability – a system property**
  - **"the trustworthiness of a system that allows reliance to be justifiably placed on the service it delivers"**
- **Survivability – a system capability**
  - **"the capacity of a system to fulfil its mission, in a timely manner, in presence of attacks, failures and accidents"**

- **Resilience – a "system quality"**
  - embraces both **dependability and survivability** as it captures the **property and capacity** of a system to (**ideally**) **autonomously and gracefully tackle, adapt, response, recover, self-heal, reconfigure,** etc., and, in a sense, to be **"flexible enough"** to accommodate & tolerate upsets/disruptions/failures/attacks

# … and plasticity

- **Plasticity**
  - **embraces the properties and capabilities** that would make digital environments and systems to be able to **dynamically adapt and evolve** (both with respect to **time and technological innovations and cycles**) securing the **seamless control and use** of data, information, knowledge and, more in general, intangible asset, etc.

# ICT in FP7: the approach

## Reinforce leadership and open new fields

**Reinforce areas where Europe has recognized strengths**

**Build capacity to seize new opportunities as they emerge**

## Mainstream ICT and Push the limits of technology

**Boost innovation from ICT use and new forms of content**

**Widen the performance and functionality of technology**

**Combination of market or applications-pull and technology and science-push**

## Balance between basic and applied research

**Flow of ideas from theory to practice and from academia to markets**

# FP7: structure & budget

**"Cooperation"** — *44735 m€ (61%)*

**Predefined themes, refined FP6 instruments**

"Ideas" — *11942 m€ (16%)*

Frontier research, competition, individual grants

"People" — *7178 m€ (10%)*

Human potential, mobility

"Capacities" — *7536 m€ (10%)*

Infrastructure, SMEs, science and society,

Joint Research Center – non-nuclear — *1824 m€ (3%)*

\+ EURATOM

**Note: financial figures from Commission proposal 6/04/05**

# ICT in FP7: Main Themes and Activities

## Future and Emerging Technologies

**supporting research at the frontiers of knowledge**

## ICT Technology Pillars

**pushing the limits of performance, usability, dependability, cost-efficiency**

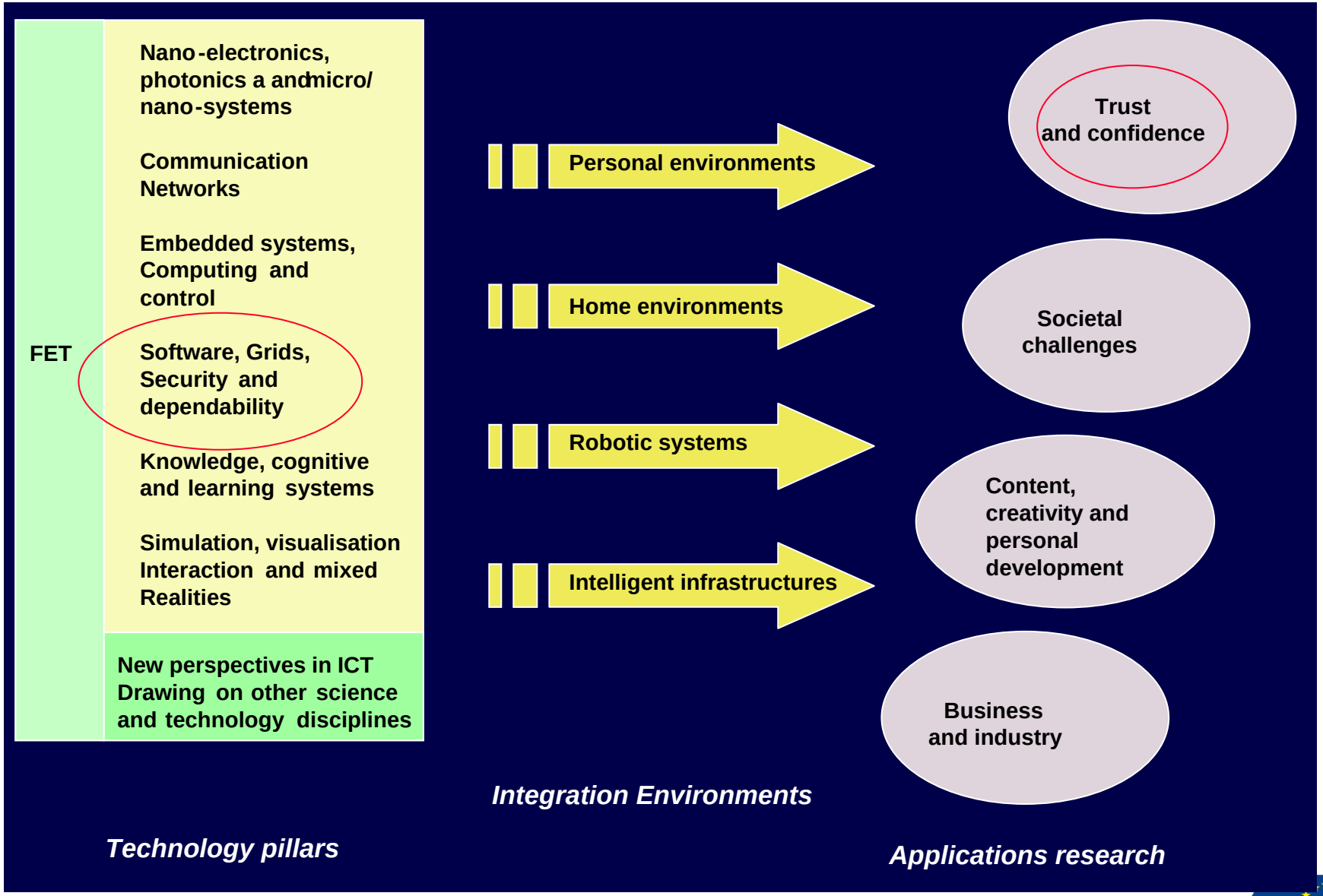
## Integration of Technologies

**integrating multi-technology sets that underlie new functionalities, services and applications**

## Applications Research

**providing the knowledge and the means to develop a wide range of ICT-based services and applications**

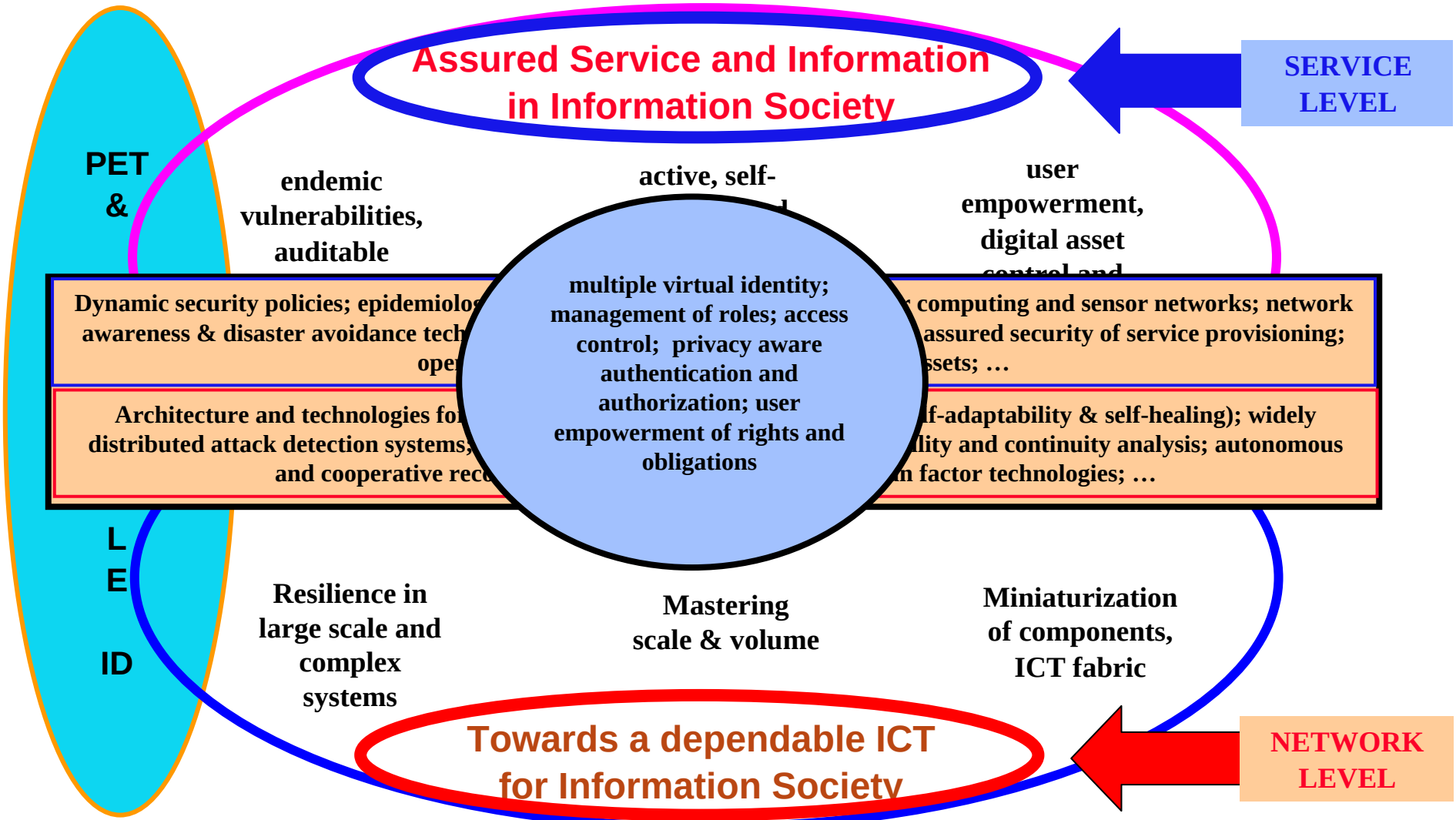
# ICT in FP7 (2007-2013)



# FP7 "Cooperation" – Collaborative Research

1. Health
2. Food, Agri, Biotech
3. **Information and Communication Technologies**
   **Technology Pillar**: **Software, Grids, Security and Dependability**
   ***dynamic, adaptive, dependable and trusted software and services, and new processing architectures, including their provision as a utility***
   **Application Research**: **ICT for Trust and Confidence**
   ***identity management; authentication; privacy enhancing technologies; asset management; protection against cyber threats***
4. Nano, Materials, Production
5. Energy
6. Environment
7. Transport (including Aeronautics)
8. Socio-econ
9. **Security**: ***Interdisciplinary, solution oriented research for civil security; anti-terrorism; CIP; border control, interoperability for first responders; …***
10. Space

# Resilience and plasticity in a complex world



# ICT-FP7: State of Play

**Work programmes under FP7**

- Orientations, objectives and structure
- Budgets and mechanisms within each priority research topic
- **Drafting first Work Programme texts** — End JUL
- Consolidation & improvement
- Opinion by IST-C and adoption by Commission — End OCT
- First Calls for proposals — DEC?

**Operational Issues**

- Model contracts and procedures
- Guidance for proposers and evaluators
- Development/adaptation of IT tools
- Information and communication actions

# Web Sites

**COM(2006) 251 “A Strategy for a secure Information Society – Dialogue, Partnership and empowerment”**

**http://ec.europa.eu/information_society/doc/com2006251.pdf**

**SEC(2006) 656 “Commission Staff Working Document – Impact Assessment”**

**http://ec.europa.eu/information_society/doc/com2006251.pdf**


**IST helpdesk**
**Fax : +32 2 296 83 88**
**E-Mail : ist@cec.eu.int**


**IST Programme**

**http://cordis.europa.eu.int/ist**

**ICT for Trust & Security**

**http://cordis.europa.eu.int/ist/trust-security/index.html**