Trust and Security in the Ambient Intelligence Space

Andrea SERVIDA

Head of Sector

European Commission
DG Information Society - Unit D/4
B-1049 BRUSSELS
andrea.servida@cec.eu.int

OUTLINE

- EU activities in information security
- The Policy context for the EU R&D
- Ambient Intelligence & security
- Trust and security in FP6

EU Activities on Information and Network Security

Regulatory Framework

- **Electronic Signature Directive**
- **Data protection in electronic communications**
- **Council Resolution on Information & network security**
  - coordination CERTs
  - CSTF
  - Int. Co. on dependency on electronic networks
- **Council Resolution on EU approach to a culture of security**
- **Framework Decision on attacks against information systems**
- **Framework Decision on combating terrorism**

R&D Activities

- **Trust & Security:** 75 R&D projects (~80 M€)
- **Dependability:**
  - 16 R&D projects (~28 M€)
  - Joint EU-US task force on R&D for CIP
- **R&D in information security key in FP6**

Policy

- **eEurope 2005**
  - Cybersecurity Task Force
  - 'Culture of security'
- **JAI initiative on secure VISA**
  - use of biometrics
  - smart travel documents
- **International Fora**
  - OECD
  - GBDe,
  - CoE,
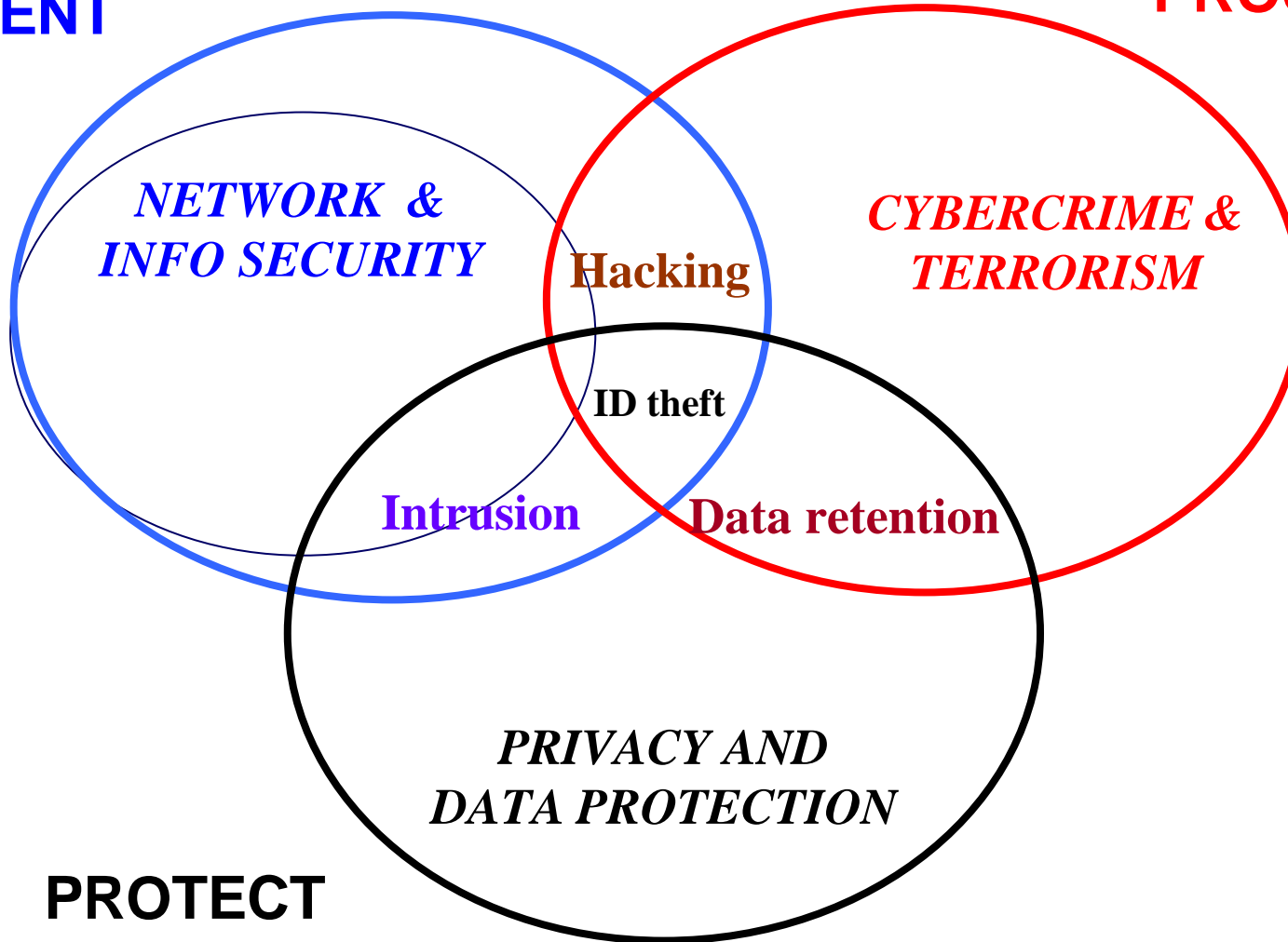 - G8
  - …

Three angles for actions on security Policy

PREVENT

PROSECUTE

NETWORK & INFO SECURITY

Hacking

CYBERCRIME & TERRORISM

ID theft

Intrusion

Data retention

PRIVACY AND DATA PROTECTION

PROTECT

Policy Context for the EU R&D

Information Society Technologies

ERA: European Research Area

FP6, Eureka, COST, National RTD Programmes

... towards a Single Market for Research

Lisbon Strategy

Enlargement

The candidate countries are full partners in FP5.

"EU: Largest knowledge-based economy by 2010"

*e*Europe

Broadband access, e-business, e-government, **security**, skills, e-health, ...

Other policies

Single Market, Single Currency, Security of Europeans, Sustainable Development, ...

The 6th Framework Programme

INTEGRATING EUROPEAN RESEARCH		
PRIORITY THEMATIC AREAS	**ANTICIPATING S/T NEEDS**	
Genomic and biotechnology for health · Information society technologies · Nanotechnologies, intelligent mat., new production processes · Aeronautics and space · Food safety and health risks · Sustainable development and global change · Citizens and governance in the knowledge society	Research for policy support	Frontier research, unexpected developments
	Specific SME activities	
	Specific international cooperation activities	
	JRC activities	

STRUCTURING THE ERA			
Research and innovation	Human resources & mobility	Research infrastructures	Science and society

STRENGTHENING THE FOUNDATIONS OF ERA	
Coordination of research activities	Development of research/ innovation policies

FP6 Budget breakdown

- **Focussing and Integrating**
  - Genomics   2255 M€
  - **Information Society Technologies   3625 M€** ⟶ ~100M€ for GEANT/GRID
  - Nanotechnologies, int..   1300 M€
  - Aeronautics and space   1075 M€
  - Food quality and safety   685 M€
  - Sustainable development   2120 M€
  - Citizens and governance ..   225 M€
  - Anticipation of S&T needs
    - Anticipating needs   555 M€
    - SMEs   430 M€
    - Specific INCO   315 M€
- **Strengthening ERA foundations   320M€**
- **Structuring ERA**
  - Research and Innovation   290 M€
  - Human resources   1580 M€
  - Research Infrastructures   655 M€ ⟶ ~200M€ for GEANT/GRID
  - Science/Society   80 M€
- **Joint Research Centre   760M€**

16270 M€

Around us ...

Micro-capsule

**Products and equipment
at the service of individuals**

… inside us ?
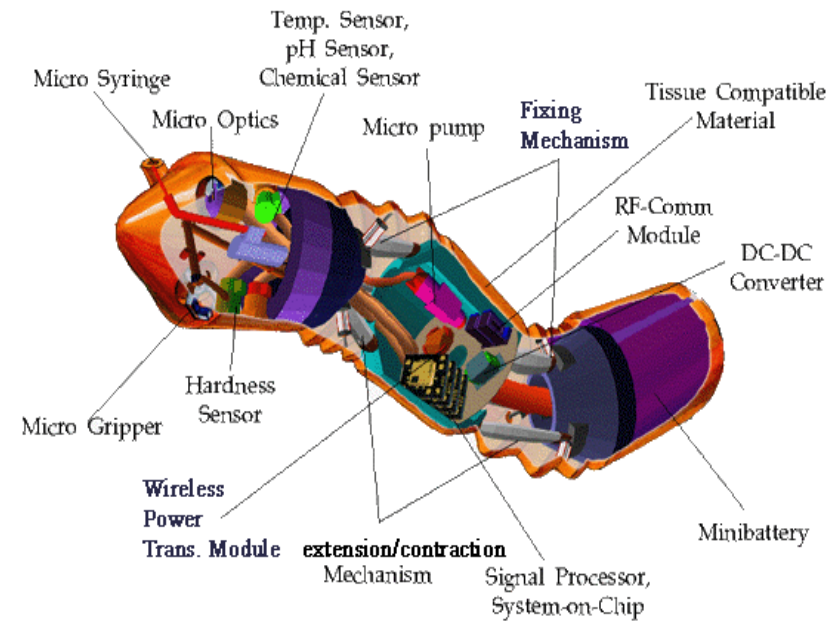
Micro Syringe
Temp. Sensor, pH Sensor, Chemical Sensor
Micro Optics
Micro pump
Fixing Mechanism
Tissue Compatible Material
RF-Comm Module
DC-DC Converter
Hardness Sensor
Micro Gripper
Wireless Power Trans. Module
extension/contraction Mechanism
Signal Processor, System-on-Chip
Minibattery

Today issues

Pervasiveness, interdependencies and intrusiveness

Influencing factors

- **Little attention to compatibility between** technology and human systems

- **Little thinking in terms of** privacy respecting Society

- **Little co-ordinated effort to address** dependability of **information and communication infrastructures**

- **Unforeseeable R&D development**

Future objectives

Develop a "respectful", **productive, innovative and** secure **IS**

How to go about it

- **Foster a global dialogue on an IS respecting** the personal sphere, safeguarding resilience **of systems & infrastructures**, encouraging innovation, **enabling productivity**

- **Promote the** understanding of interdependencies

- **Share vision on** how to depend on technology

- **Innovative R&D**

Ethics in the Information Society

Today issues

Poor understanding and awareness of risks to privacy
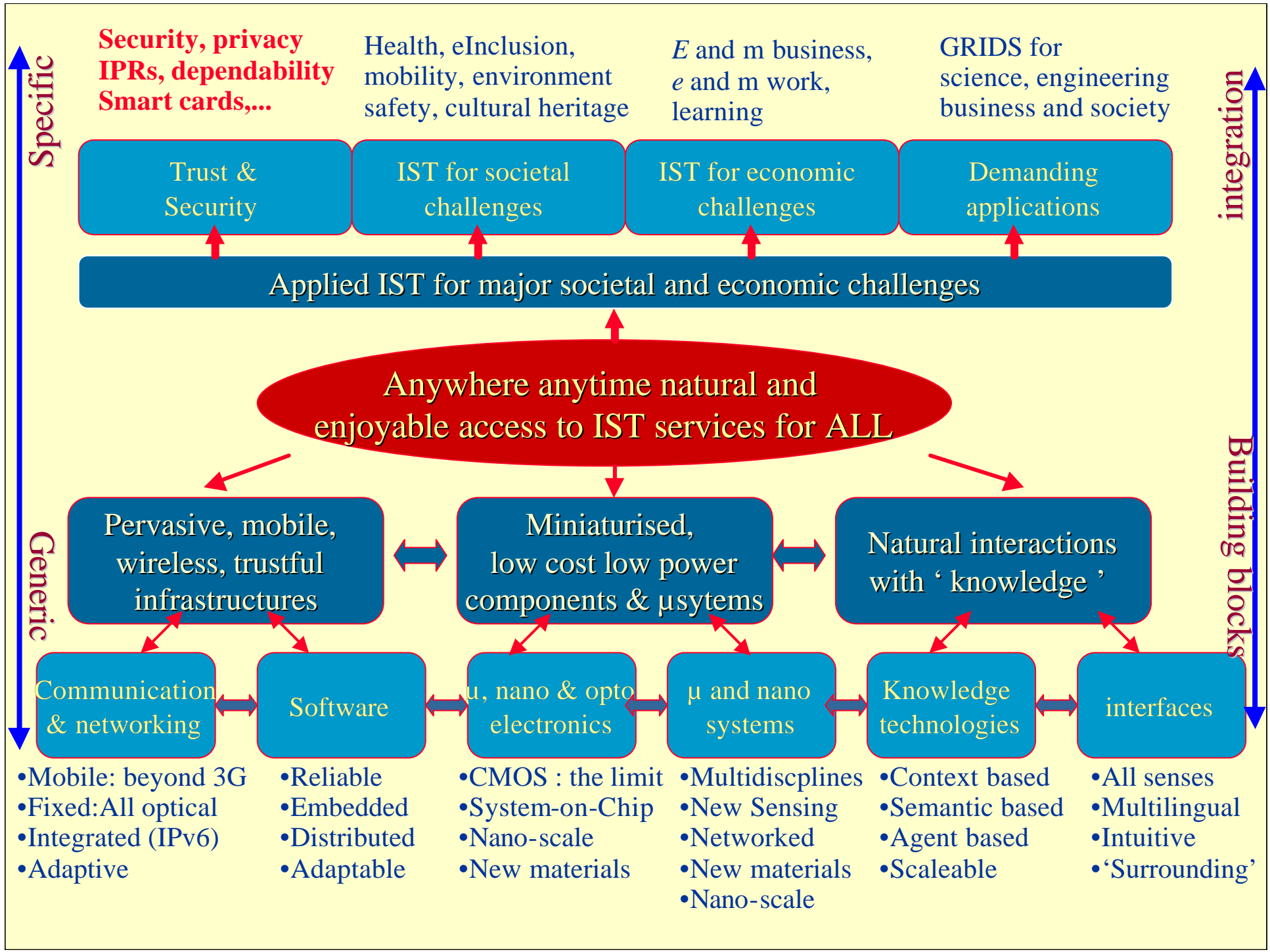
Influencing factors

- **Globalisation**
- Growing **interconnectedness**
- Increasing **educated consumer**
- Growing **business interest** on **knowing more** about customers
- Increasing use of **digital identities**, **virtual persona**, etc.
- **Inefficient enforceability** of privacy law

Future objectives

Ethics of privacy as a key element of the **Information Society**
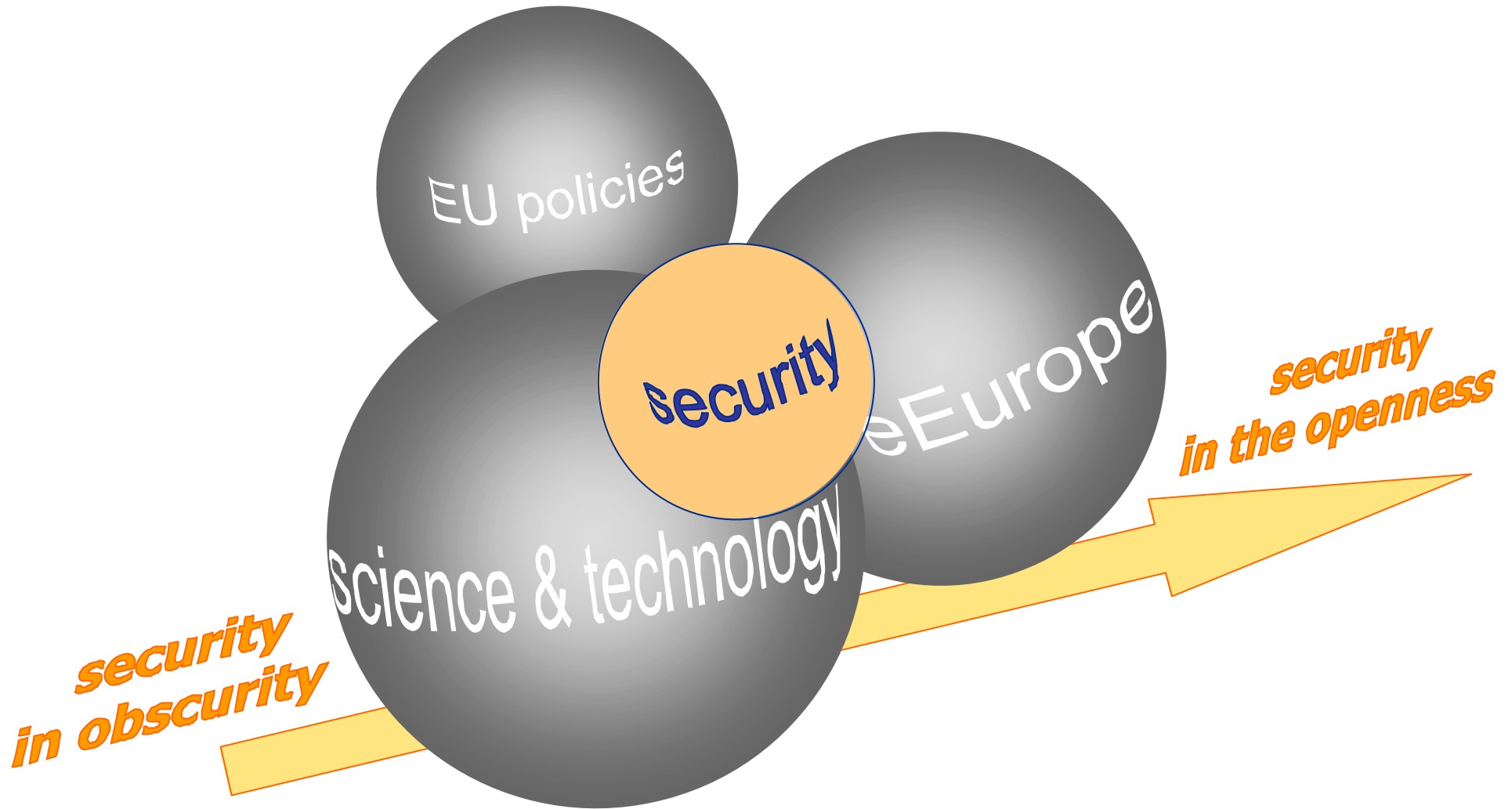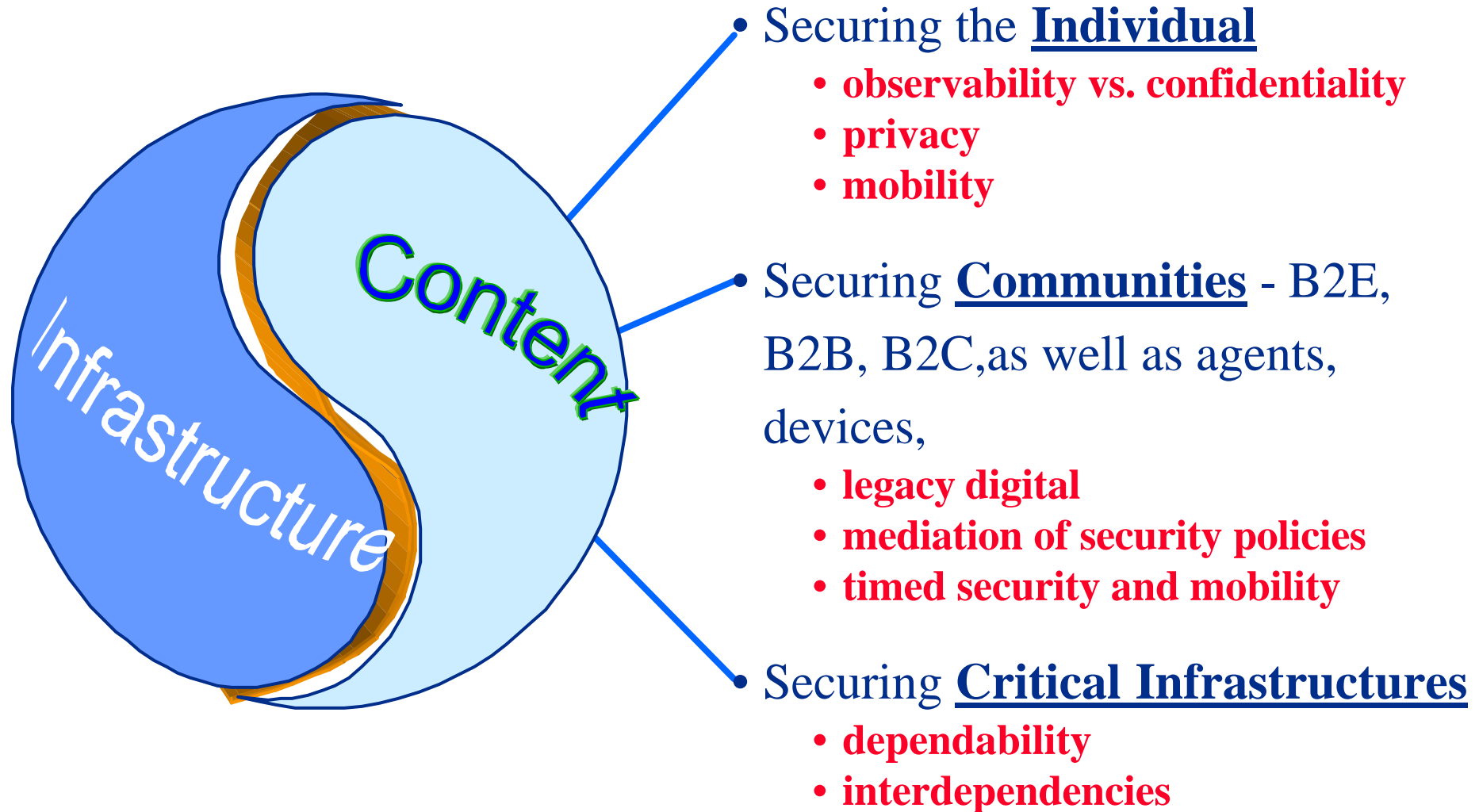
How to go about it

- Make privacy part of **education**, **training** and **public debate**.
- Socioeconomic research **into privacy** in the Information Society.
- Privacy compatible **processes, products and systems**.
- Build-in **privacy enhancing** mechanisms to **ease enforceability**
- Innovative R&D to **ensure personal control of privacy**.

Infrastructure

Content

- Securing the **Individual**
  - **observability vs. confidentiality**
  - **privacy**
  - **mobility**

- Securing **Communities** - B2E, B2B, B2C,as well as agents, devices,
  - **legacy digital**
  - **mediation of security policies**
  - **timed security and mobility**

- Securing **Critical Infrastructures**
  - **dependability**
  - **interdependencies**

Objective: To **strengthen security and enhance dependability** of **information and communication systems and infrastructures** and to ensure trust and confidence in the use of IST by addressing **new security and dependability challenges**. These are resulting from **higher complexity, ubiquity of computing and communications, mobility, and increased dynamicity of content**. **Integrated and comprehensive approaches** involving all relevant stakeholders of the value chain should address security and dependability **at different levels and from different perspectives**.

2.3.1.5 Towards a global dependability and security framework

- **Focus is on:**
  - Development of integrated approaches, architectures and technologies for **security and mobility, virtual identity management, privacy enhancing both at application level and at infrastructure level**. Aspects of usability as well as socio-economic and regulatory issues would have to be taken into account.
  - Development of integrated **interdisciplinary approaches and ensuing technologies for the provision of dependable network and information systems that underpin our economy and our society**
  - Development of modelling-, and **simulation-based management decision support tools for critical infrastructure protection** addressing ICT-related interdependencies of critical infrastructures and aiming at prevention of threats and reduction of vulnerabilities

2.3.1.5 Towards a global dependability and security framework

- Development, testing and verification of underlying and novel **crypto technologies** for a wide spectrum of applications. Development, testing and verification of technologies for protecting, securing and trustable distribution of digital assets. Due consideration should be given to implementation and standardisation issues and to security policy development and consensus building among the relevant key players

- Research, development, testing and certification on **next generation secure smart devices (e.g. smart cards) and their components**. This includes design, production and automated verification of smart devices.

- Multidisciplinary research on **biometrics** and its applications with due consideration also of the social and operational issues. Strengthening European competence on security certification leading to mutual recognition as well as **network and computing forensic technologies to combat cyber-crime**

Work should link to Member State research initiatives and policies. Related to **dependability and critical infrastructure protection, targeted international collaboration** with complementary research communities and programmes should be fostered

1-Strategic Objectives	Budget
Pushing the limits of CMOS, preparing for post-CMOS	75
Micro and nano systems	85
Broadband for all	60
Mobile and wireless systems beyond 3G	90
Towards a global dependability and security framework	**55**
Multimodal Interfaces	65
Semantic-based knowledge systems	55
Networked audio-visual systems and home platforms	60
Networked businesses and governments	75
eSafety of road and air transport	65
eHealth	70
Technology-enhanced learning and access to cultural heritage	65
2- Future and emerging Technologies	
Proactive initiatives: (i) Beyond robotics (ii) Complex systems, (iii) Disappearing Computer	40
3- General accompanying actions	8

Planning over 4 years

Year	2003	2004	2005	2006
Indicative Budget	835,000	891,000	935,000	964,000
Calls per year	Two calls drawing on 2003 and 2004 budgets	One call drawing on 2005 budget	Second WP (covers also all topics of SP) with updated focus	

First WP covers all topics of the SP

Constituency

Building

Derive

Research

Roadmaps

DDSI	WG-ALPINE
Dependability policy support	**Active Loss Prevention**

AMSD : Overall Dependability

e-business   embedded   CIP   privacy

PAMPAS	AMSD	ACIP	RAPID	RESET	BVN	STORK
mobile privacy & security	**dependable embedded systems**	**critical infrastruct. protection**	**Privacy / Identity Mgmt**	**Smart Cards**	**Biometrics**	**Crypto**

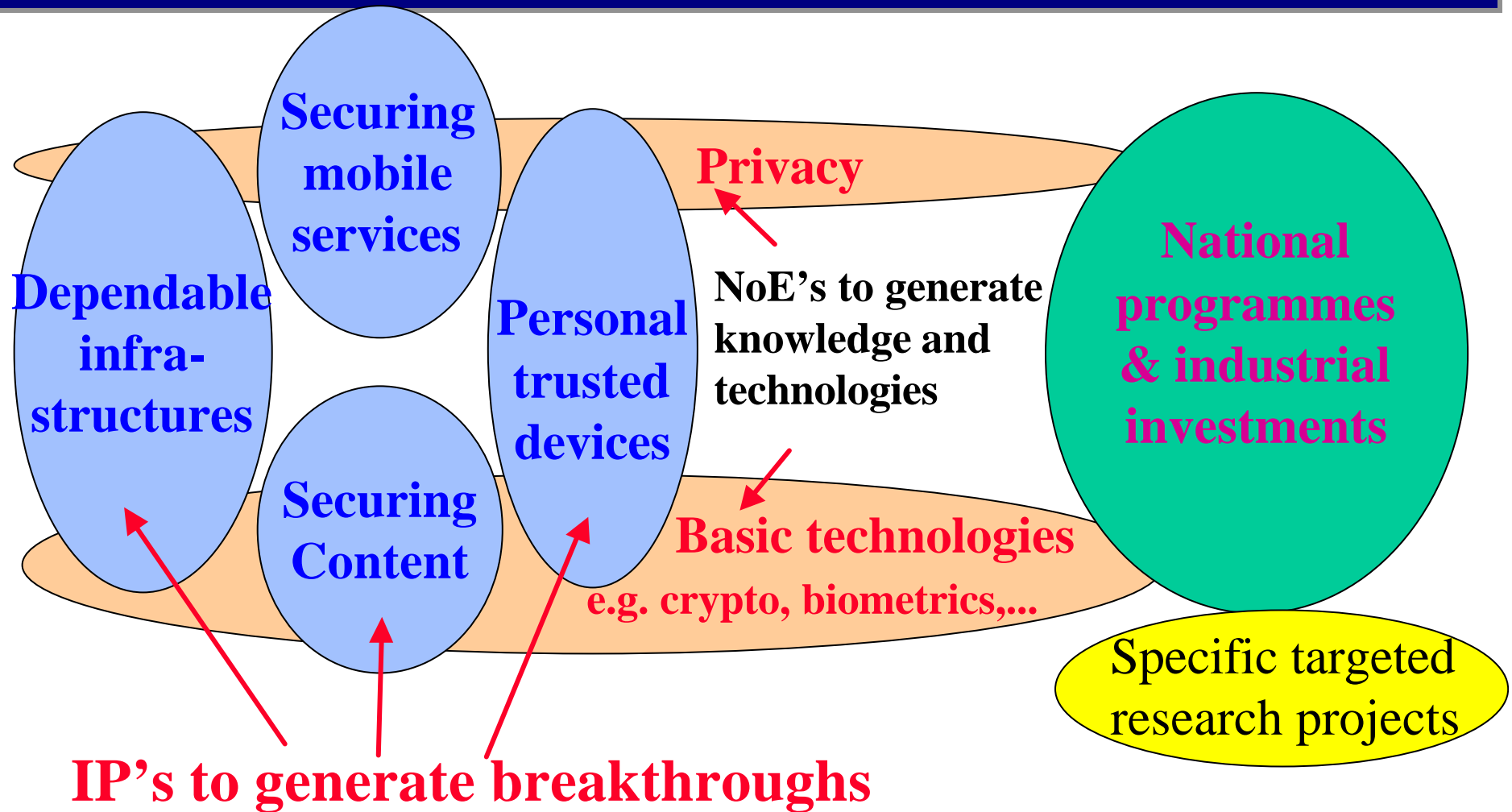**Identify stakeholders & derive Research Roadmap**

OPEN discussion

Dissemination

April 2002 Closure Call 1-FP6

1 June 2002

1 Jan. 2003

Example of potential co-ordinated actions in security

Securing mobile services

Dependable infra-structures

Privacy

Personal trusted devices

NoE's to generate knowledge and technologies

National programmes & industrial investments

Securing Content

Basic technologies
e.g. crypto, biometrics,...

IP's to generate breakthroughs

Specific targeted research projects

EU-US co-operation on R&D

- **FP6 as the framework for EU/US partnership on R&D**
  - detailed Joint R&D agenda to be drafted (Workshop in Leesburg in Sept 2002):
    - **information assurance and survivability**
    - **secure networked embedded systems**
    - **modelling and simulation of critical interdependent systems**
  - contacts with funding agencies established
  - co-ordination with State Department and OSTP
- **Leverage the EU roadmap projects to develop a joint R&D agenda**
  - a Workshop is being planned
  - investigate the needs and options for joint teams on dependability of global critical infrastructures

- US proposal for an initiative on "Perspectives on the Future of Science and technologies"
  - develop common scientific understanding of future policy issues (among which is **cyber security**)
  - provide policy makers with description of foreseeable development in S&T
  - identify future research needs and opportunities for joint collaboration
- Co-operation would contribute to raise awareness on global security and dependability challenges
  - more knowledge and technology
  - wider involvement of stake holders
  - more proactive attitude to secure our infrastructures

WEB sites

www.cordis.lu
www.cordis.lu/ist
www.cordis.lu/rtd2002

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

Instruments: http://www.cordis.lu/rtd2002/fp-activities/instruments.htm
EoI: http://www.cordis.lu/fp6/eoi-instruments/

IRG Workshop on T&S http://www.cordis.lu/ist/events/workshops.htm
ISTAG papers: ftp://ftp.cordis.lu/pub/ist/docs/istag_kk4402464encfull.pdf
Roadmap projects: http://www.cordis.lu/ist/ka2/rmapsecurity.html
T&S Workshops: http://www.cordis.lu/ist/ka2/rptspolicyconf.htm