Security Policy & implementation:
The European Commission Perspective

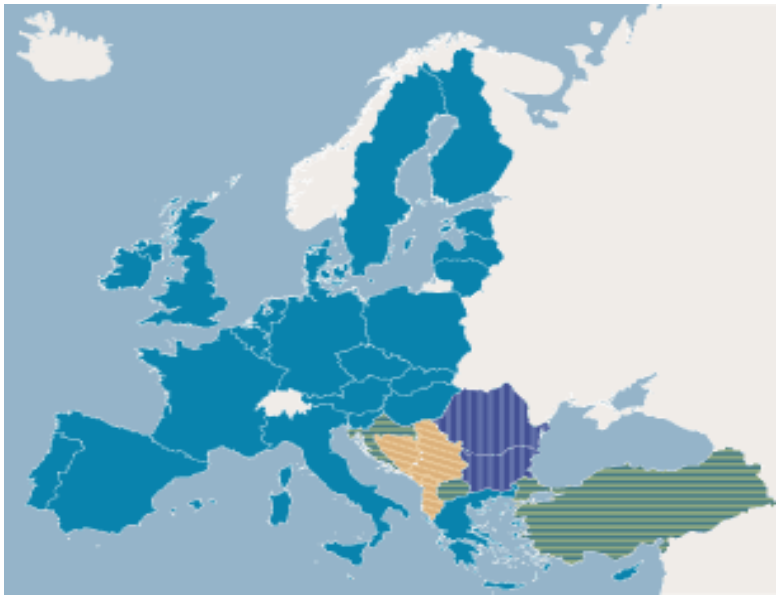
Francisco García Morán
Director General
Directorate General for Informatics
European Commission

Agenda

- Who we are and what we do…..
- Security in the EU
- ITC Security policy initiatives @ EC
- Internal security policies @ EC
- IT security implementation @ EC
- Some acronyms…
  - EC: European Commission; EU: European Union; DG: Directorate General; DIGIT: Directorate General for Informatics
  - IT: Information technologies; ITC: Information and TeleComunication technologies; NIS: Network and Information Security

EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

DIGIT



The European Commission

- The EC is politically independent and ***represents and upholds the interests of the EU as a whole***. It is the driving force within the EU institutional system.
- Roles
  - To ***propose*** legislation, policies and programmes to the European Parliament (EP) and the Council
  - To ***implement*** EU ***policies*** approved by the EP and the Council and to ***manage*** the EU ***budget*** necessary to implement them
  - To ***enforce*** EU law (together with Court of Justice)
  - To ***represent*** the EU on the international stage (ex: WTO neg.)

The EC works with other institutions and bodies

- Other EU Institutions: Council, European Parliament (EP) ,Court of Justice (CoJ), Court of Auditors (CoA), Ombudsman, European Data Protection Supervisor (EDPS)
- EU advisory bodies: European Social Committee, European Regions Committee (CES/CDR)
- EU financial bodies: European Central Bank (ECB), European Investment Bank (EIB)
- Interinstitutional bodies: Office for Official Publications (OPOCE), European Personal Selection Office (EPSO)
- Other EU bodies: Regulatory, non-regulatory, executive agencies, Common Foreign and Security Policy, Police and Judicial Cooperation in criminal matters
- More info: ***http://europa.eu***

The European Commission

- Organisation
  - Two main places of work (***Brussels and Luxembourg***), several research centres around the EU, ***representations in every Member State*** and more than 100 ***delegations around the world***
  - 40 organisational entities
  - Directorate General, Offices and other inter-institutional services (OLAF, SCIC, OPOCE, EPSO, etc)
  - More than ***35000 IT users***

POLICIES

- Agriculture and Rural Development
- Competition
- Economic and Financial Affairs
- Education and Culture
- Employment, Social Affairs and Equal Opportunities
- Enterprise and Industry
- Environment
- Fisheries and Maritime Affairs
- Health and Consumer Protection
- Information Society and Media
- Internal Market and Services
- Joint Research Centre
- Justice, Freedom and Security
- Regional Policy
- Research
- Taxation and Customs Union
- Transport and Energy

EXTERNAL RELATIONS

- Development
- Enlargement
- EuropeAid - Co-operation Office
- External Relations
- Humanitarian Aid Office - ECHO
- Trade

GENERAL SERVICES

- European Anti-Fraud Office
- Eurostat
- Press and Communication
- Publications Office
- Secretariat General

INTERNAL SERVICES

- Budget
- Group of Policy Advisers
- Informatics
- Infrastructures and Logistics
- Internal Audit Service
- Interpretation
- Legal Service
- Personnel and Administration
- Translation

Organisation of I.T. in the European Union

- Based on a decentralised approach but where appropriate **sharing of services**
- Each Institution has its **own IT team**
  - Responsible for the delivery of the IT services locally and the development of information systems needed
  - Varying degrees of IT maturity and of professional practices
- Some global coordination and federation by the **Comité Informatique Interinstitutionnel (CII) – « rolling presidency »**
  - **The Commission cooperates and coordinates in IT matters with the IT services of the other EU Institutions and Bodies through the work of the CII mainly on:**
    - IT infrastructure
    - Common IT services (e.g. product management, IT architecture, CfTs & Contracts)
    - Information Systems Hosting

Organisation of I.T. in the Commission

- **Hybrid model**: Central and Local organisations
  - Directorate-General for Informatics - **DIGIT** (approximately 420 officials and 450 external staff)
    - Corporate IT services
    - IT Strategy and Coherence
    - Development of Corporate Information Systems
    - IT Support (2nd level), Corporate Logistic Services, Corporate Contracts and Budget Management
  - Local Organisations (approximately 650 staff)
    - Management of local IT infrastructure
    - IT User Support (1st level)
    - Development of Information Systems in support of EU operational policies
  - Budget
    - ~ 125 M€/year for Corporate IT Infrastructure and Services
    - Information Systems (administrative ~ 20 M€, in support of EU policies (~180 M€)

DIGIT's Mission Statement

"Providing the European Commission with high quality information technology and telecommunications services and contributing to the development of Pan-european eGovernment Services"

The mission of the Directorate-General is to define the IT strategy of the Commission and to provide a modern and high-performance information technology and telecommunications infrastructure.
In this context, the Directorate-General for Informatics is responsible for the management and co-ordination of information and telecommunications technology for the Commission's services and in particular, for identifying, articulating and implementing a modern and dynamic corporate Information Technology vision and strategy which are fully aligned with the Commission's overall priorities. By means of the IDAbc programme we contribute to the development of pan european eGoverment Services"

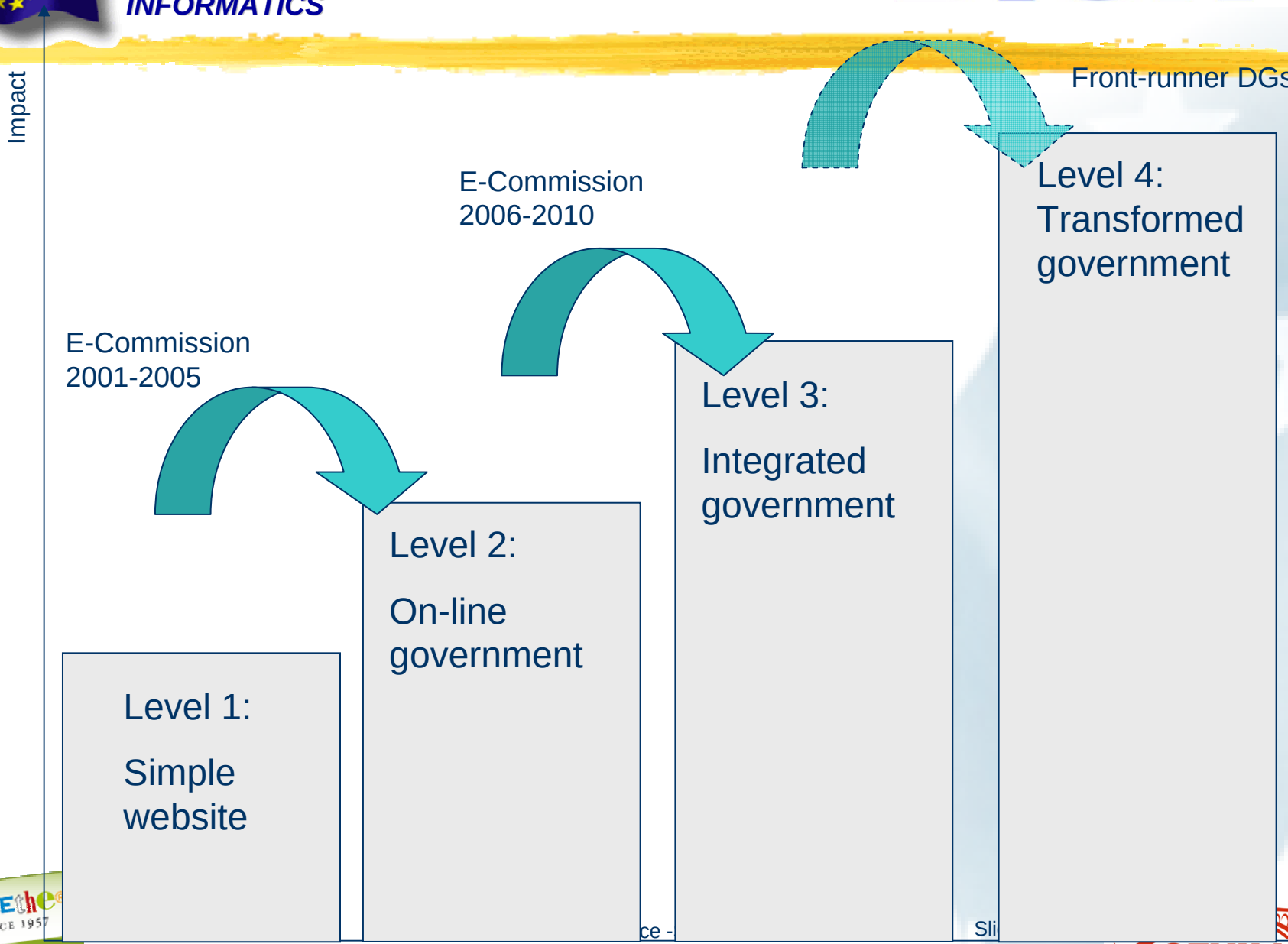
DG DIGIT Organisation

4 x DIRECTORATES (in Luxembourg & Brussels)

- Corporate I.T. Solutions and Services
- Information Systems
- Infrastructure Services Provision
- Resources and Logistics

1 x Specific UNIT

- Pan-European e-Government Services (IDABC)


Impact
Front-runner DGs
E-Commission
2006-2010
E-Commission
2001-2005
Level 4:
Transformed
government
Level 3:
Integrated
government
Level 2:
On-line
government
Level 1:
Simple
website

External Dimension

Support to Specific Policies

- Move towards a paperless environment for customs and trade
- Large scale ICT projects in the JLS area
- Support to trade policy
- Support to competition policy
- Support to rural development policy
- Support to exchange of transport related data
- Trace
- Observation of volatile energy markets
- CITL
- CECIS
- SFC 2007
- Support to FP6 & FP7
- IMI

Horizontal Actions

- Transparency Portal
- ESTAT Portal
- Support to the Commission's communication strategy
- IDABC projects

Internal Dimension

Support to Specific Domains

- Decision-making Portal
- E-College
- ARGUS
- Developing & deploying e-learning capacities
- Defining & implementing the strategy to deploy e-procurement facilities
- Studying impact on infrastructure & IS of proper management of EU classified information
- Deployment of electronic identity management

Corporate Systems

- Corporate Portal
- Corporate Data warehouse
- Corporate Planning & Reporting Tool
- eHR service provision
- Functional evolution of Sysper2
- Functional evolution of ABAC
- E-Domec Projects

Organisational Enablers

IT Governance

- Applying ICS consistently
- Assessing sustainability of IS developed under various programmes
- Creating ad-hoc MAP groups to reduce duplication in targeted domains
- Defining ICT development strategies by domain
- Common approach to ICT risk management
- Revising security requirements for IS

Foundations for Operational Excellence

- Defining & implementing a teleworking deployment strategy
- Study of potential consolidation of infrastructure
- Introduction of technical innovations
- Allocating resources & adapting ICT support
- ID all COM mission critical systems & set-up business continuity measures
- Building on ITIL to give focus on ICT operational activities
- Defining business continuity & disaster recovery plan guidelines

Methodologies

- Defining an information management strategy
- Embedding data protection and security requirements in RUP & CEAF
- Deploying RUP & CEAF

Training & Awareness Raising

- Further deploy ECDL certifications
- Training of all new IT recruits
- Training courses on IT Governance & CEAF
- Developing a culture of continuous improvement

Technical Enablers

Information Systems

- Deploying electronic workflows
- Multilingualism
- Development & deployment of e-Domec infrastructure
- Unique IS to manage user profiles, access rights, delegations
- Defining, adopting & applying common ergonomics standards
- *Global ID and access management strategy*
- ***E-Signatures***
- Establish a Commission SOA of IS
- Optimising data flows to ensure single storage & multiple use
- Definition of a Commission wide integration architecture

Infrastructure

- Next Generation Telephony Services
- *Tracking of security requirements within development environment*
- Defining a strategy to reinforce security & to enrich end-user functionality
- Guaranteeing infrastructure availability & quality of service to Commission's delegations
- Engineering & testing future IT reference solutions on all kinds of devices
- ***Defining and implementing Commission standards for (well tested) high-availability IS***
- Upgrading storage capacity

Roadmap Management Activities

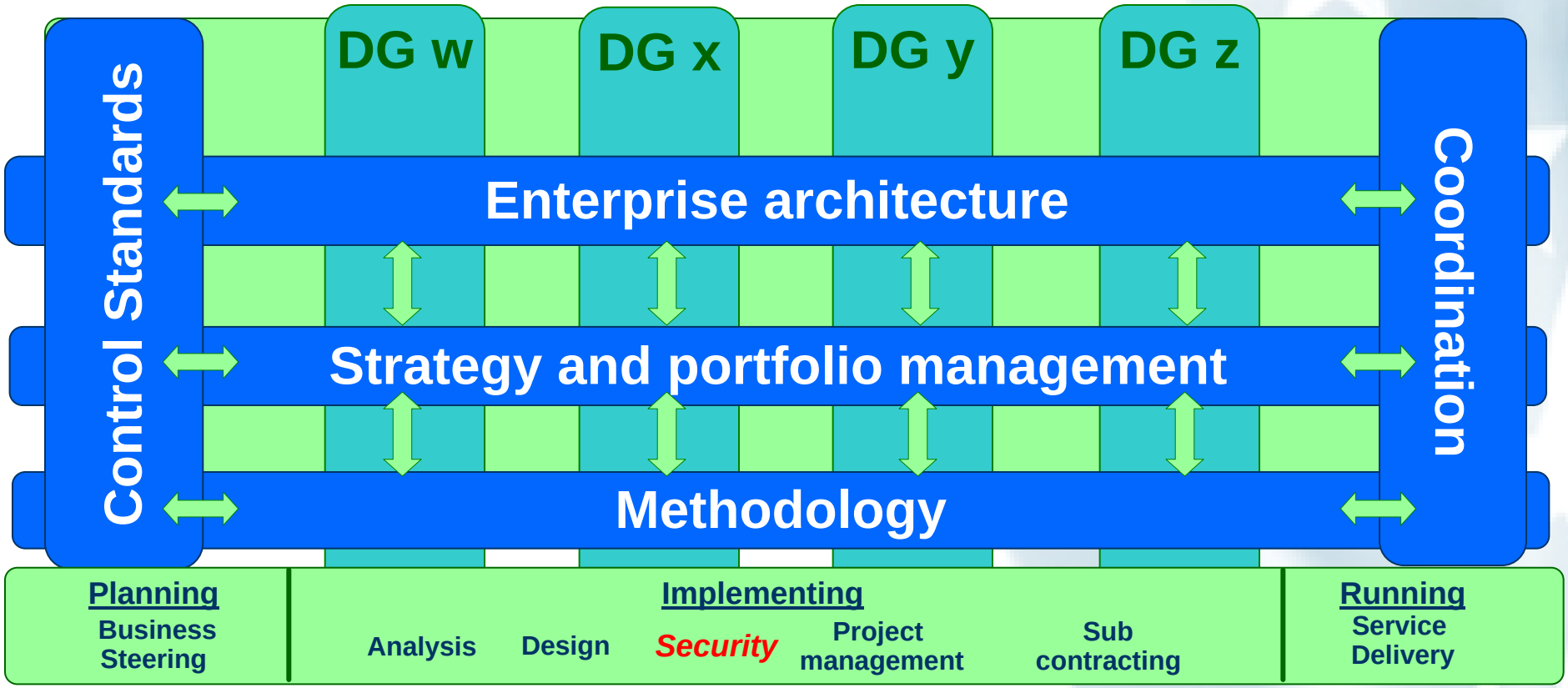
Coordination

- e-Government maturity survey
- Mid-term review
- Writing & presenting annual e-Commission progress reports
- Defining an e-Commission communication strategy
- Managing coordination structure

Follow-up of Related Policies

- Establishing a partnership with ICT research activities
- Follow-up & participation in i2010 & e-Government action plan committees
- Follow-up of EPAN activities
- Follow-up & integration of IDABC results/projects

I.T. Governance model in the Commission



EU vision on security

"Security is one particular **global challenge** that has relatively recently come to the fore due to world events and societal changes. Europe needs to invest in a **security culture** that harnesses the combined and relatively untapped strengths of the **security industry and the research community** in order to effectively and innovatively **address** existing and future **security challenges**."

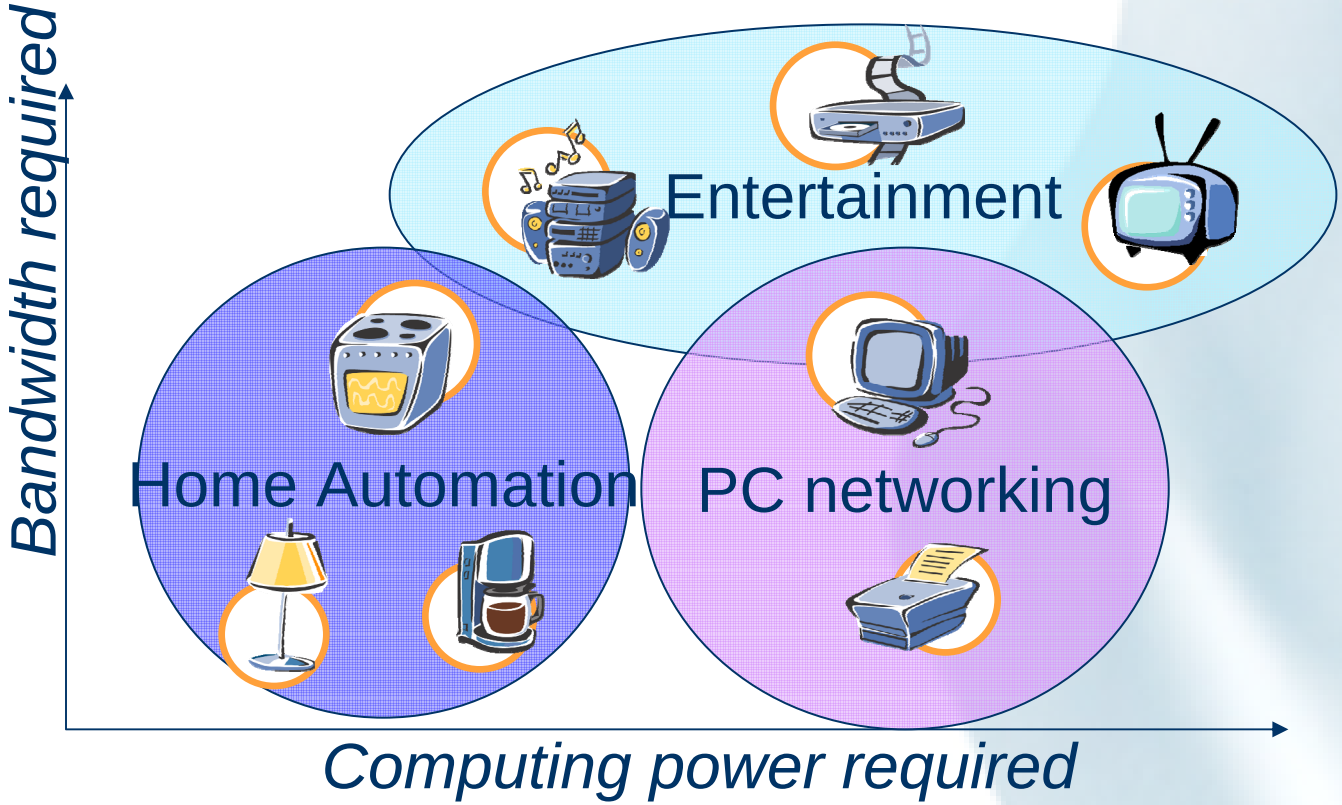
A Secure Europe in a Better World

- EU Council 12-13/12/2003 approved the «EU Security Strategy » proposed by the Secretary General/High representative (Mr. J. Solana)
- Strategic objectives
  - Addressing Threats (terrorism, regional conflicts, organised crime)
  - Building security in our neighbourhood (consistent high level of security established across its enlarged and more diverse territory)
  - An international order based on effective multilateralism (no single European country will be able to tackle present or future security problems on its own)
- Meeting these ambitions requires advanced security technology and instruments for anticipating new security threats

Security @ EC

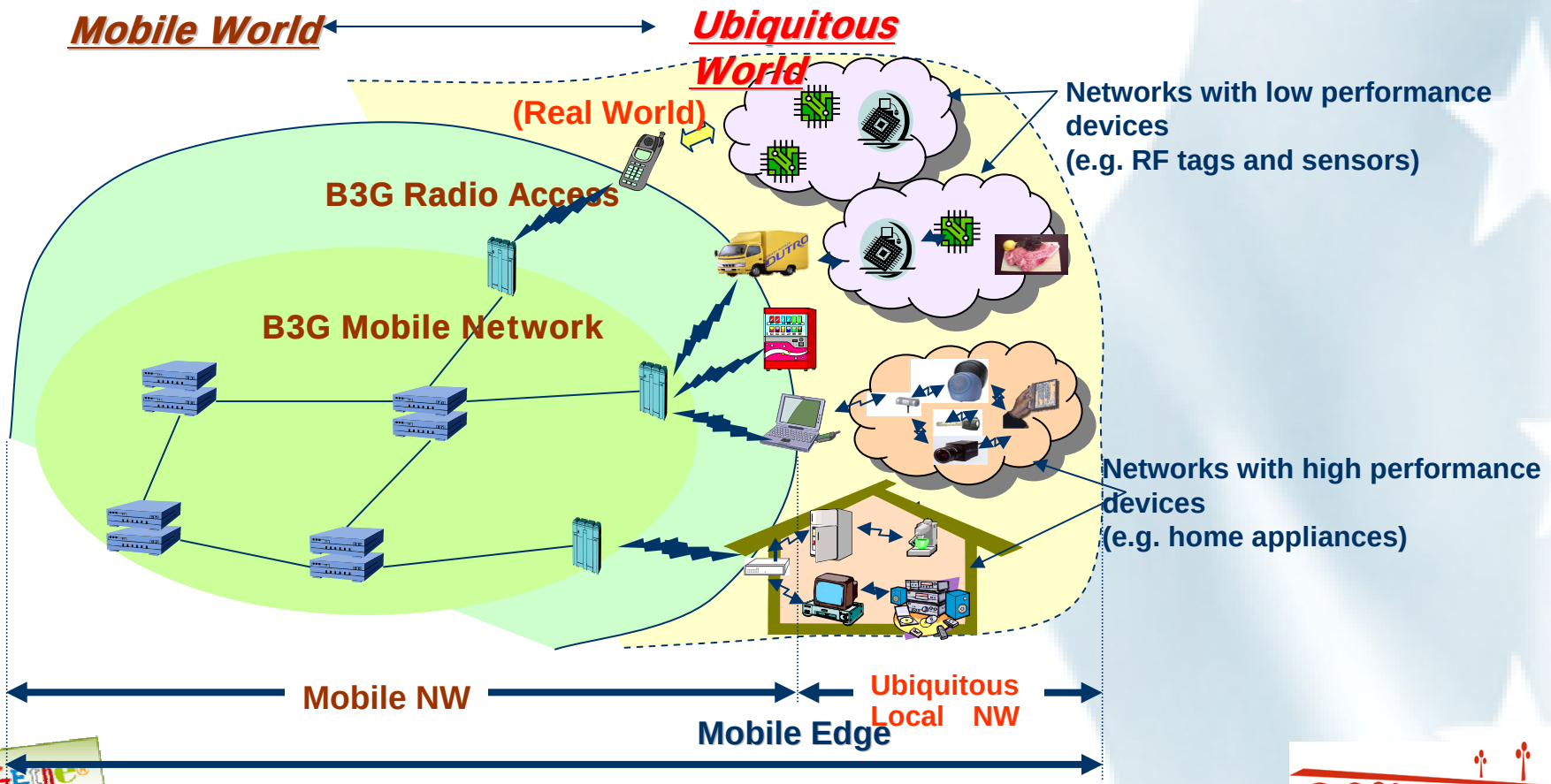
- Several DGs deal with definition and/or implementation of security policies
  - Information Society, Research, Enterprise & Industry, Joint Research Center (Institute for the Protection and the Security of the Citizens), Justice and Home Affairs, Internal Market, DIGIT (IDAbc)
- Others are involved in internal security
  - Secrétariat Général, DG Personnel & Administration (Security Directorate), DG External Relations (communications with EC delegations); DIGIT (implementation on the corporate infrastructure)
- Nearly every DG needs security for the exchange of information internally, with other EU institutions or with Member States
- Internal use of EU classified information is defined in the « EC security regulation » (2001/844/EC (3031)) (come back later)

Heterogeneous Networks and platforms



Mobile ubiquitous environments

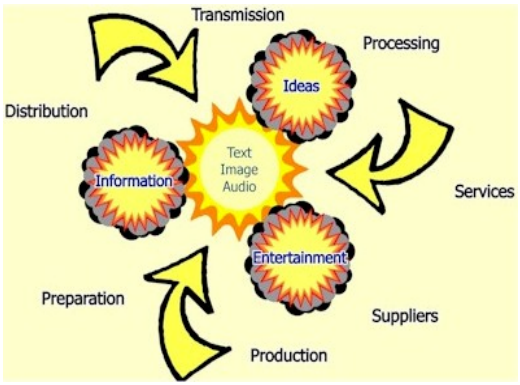
Broaden communication parties, networking, and business opportunities



What's driving the future?

CONVERGENCE OF:

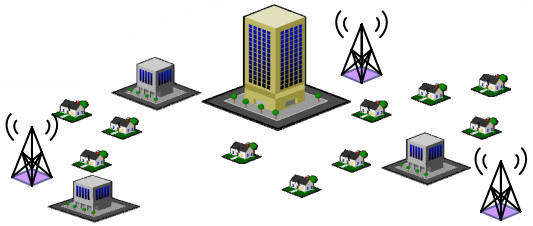
MEDIA



PROCESSES

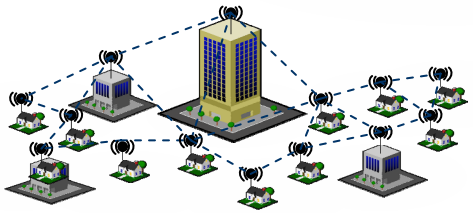
IP & NETWORKS

A magnifying factor: the scale of networking



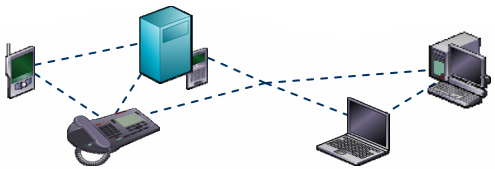
The wide area networks of yesterday (e.g. GSM)

> A Million nodes @ €50k



The Nomadic local area networks of today (e.g. WiFi)

> Millions of Nodes @ €100



The Sensor and Personal area network of tomorrow

> Billions of Nodes @ €1

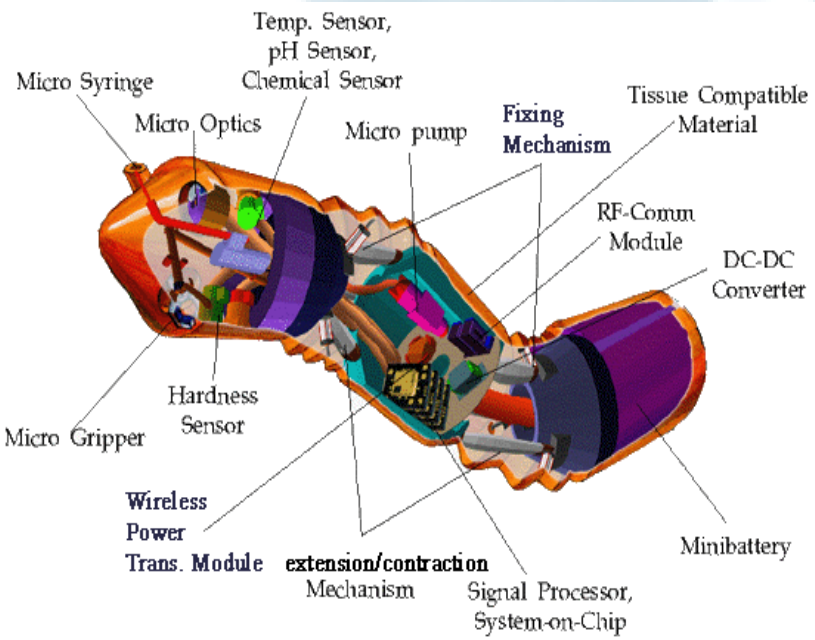
Challenges:

Removing social, geographical, economic and capacity impediments through the provision of cost effective infrastructures, allowing an “Always on” network existence.

The future: *Ambient intelligence*

Around us ...

Micro-capsule



Products and equipment at the service of individuals

... inside us ?

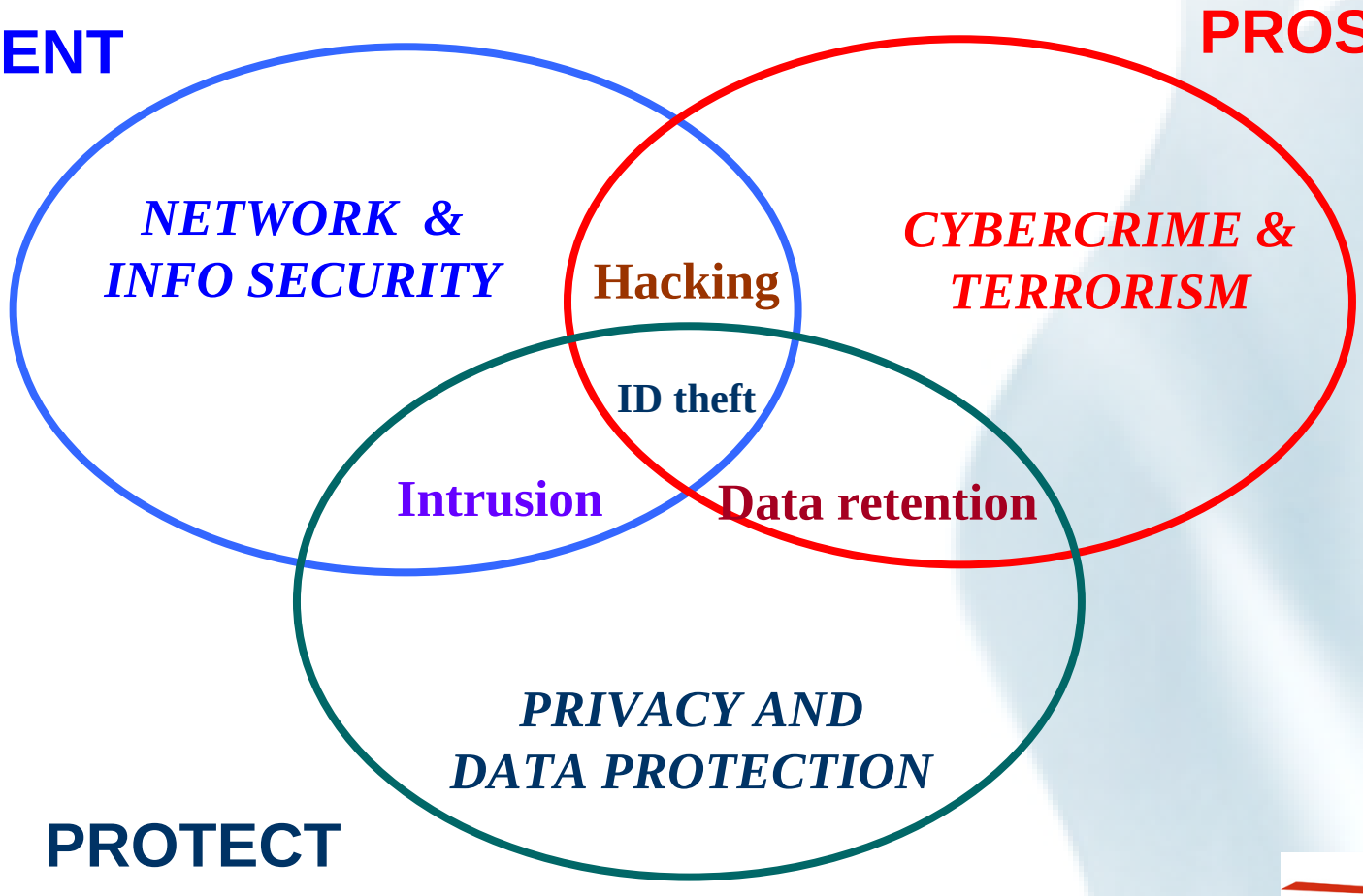
Towards a culture of security

- Effective security policies should be based on well developed risk assessment methods in both public and private sectors, but presently there is no common practice for their efficient application;
- If requirements for the security guarantee to be built into goods and services were to differ substantially from one Member State to another, they could ultimately lead to obstacles to free trade across the EU.
- The need to get the solutions right justifies the joint decision by the European Parliament and the Council to create an agency (ENISA - European Network and Information Security Agency) which, at European level, will provide guidance, advice and, when called upon, assistance to the European Parliament, Commission and any competent body appointed by Member States.

Enisa's Objectives

- Building on national and Community efforts, the Agency shall provide a high level of expertise in the field and stimulate broad co-operation between the public and private sectors.
- Help MS and Community to reach high level of network and information security;
- Develop mechanisms designed to support effective responses to trans-national and global security threats and in so doing reduce the potential for terrorist and cyber attacks;
- Contribute to the harmonise application of security technical options and organisational arrangements which would lead to improvements in the functioning of the Internal Market
- More about ENISA tomorrow 22/06/07 (Keynote speech by Enisa's ED A. Pirotti)

Three angles for actions on security Policy



EU Activities on Information and Network Security

Regulatory Framework

- Electronic Signature Directive
- Data protection in electronic communications
- Council Resolution on Information & network security
- Council Resolution on EU approach to a culture of security
- Regulation of EP and Council establishing ENISA
- Framework Decision on attacks against information systems
- Framework Decision on combating terrorism
- Council Resolution on a strategy for a secure Information Society of 2007

R&D Activities

- Trust & Security
- Dependability
- R&D in information security key in FP6/FP7
  - More than 150 M€

Policy

- i2010
  - Safer Internet
  - 'Culture of security'
- IDAbc
  - Architecture Guidelines
  - TESTA/S-Testa certification
  - PKI
  - Advice to sectoral networks
- JLS initiative on secure VISA/SIS
  - use of biometrics
  - smart travel documents
  - secure data exchange
  - AEGIS
- International Fora
  - OECD
  - GBDe,
  - CoE,
  - G8
  - …

Security and resilience in Information Society
The EC Strategy

EU NIS Policy – the history

- **1997**: COM(97) 503 on ensuring security & trust in electronic communications
- **1999**: Electronic Signature Directive (1999/93/EC)
- **1999**: eEurope 2002 Action Plan – *smart card & secure access*
- **2001**: COM(2001) 298 a EU policy on NIS
- **2002 & 2003**: Council Resolutions
- **2002**: eEurope 2005 Action Plan – *a task force proposed*
- **2004**: ENISA is established
- **2005**: the i2010 initiative – a *security strategy is announced*
- **31 May 2006: COM(2006) 251 is adopted**

The key objectives of the strategy

… to revitalise the EC strategy set out in 2001

- By reviewing the NIS situation and challenges posed by convergence of technologies, media and markets
- By building better coordination between the various EC policy initiatives (e.g. spam, 2006 Review, CIIP, cyber crime, RFID, etc)
- By mobilising all stakeholders to strengthen the cooperation in the EU

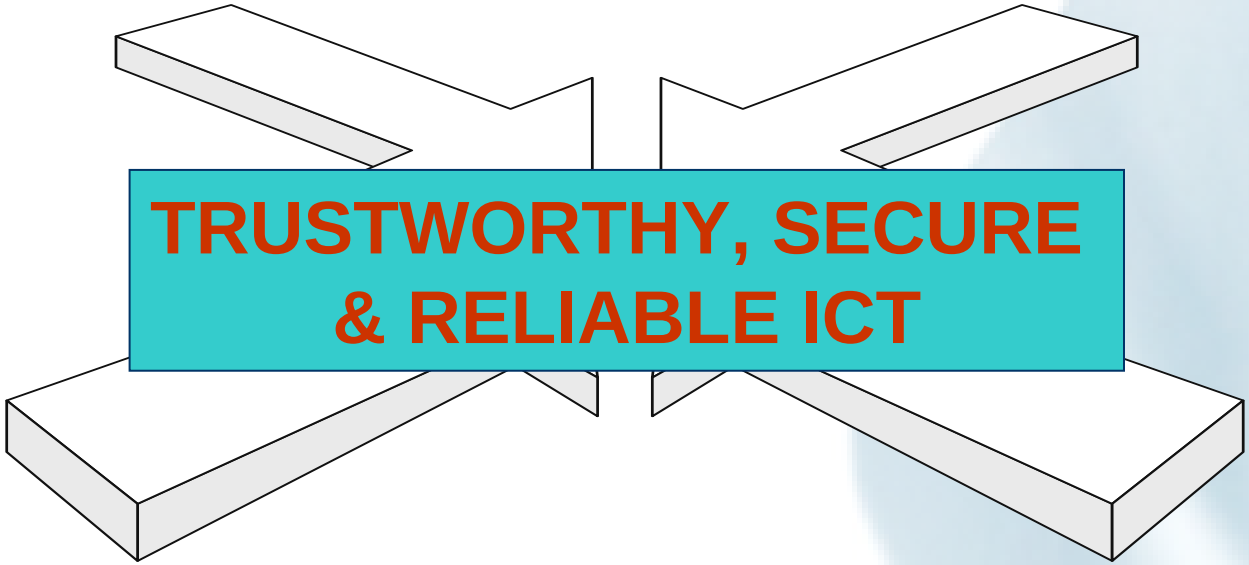
… to adapt the EU approach to future challenges

- By strengthening the role of ENISA
- By emphasising the value and benefits of measuring and learning
- By launching few actions to stimulate the exchange of good policy practice across the EU

NIS in the Information Society

TECHNICAL dimension

SOCIAL dimension



ECONOMIC dimension

LEGAL dimension

Depending on ICT

Today issues

Pervasiveness, interdependencies and intrusiveness

Influencing factors

- **incompatibility** between technology and human systems
- **technology-push** with no thinking in terms of **societal impact** (DRM, TC, biometrics, IPv6, etc.)
- emergence of new **social and governance** models
- little understanding of **human factor**
- excessive technical control **may put at risk "rights"** (DRM, biometrics, TC, etc.)
- there are **no safeguards** for users
- no attention to **economic and societal costs** of faulty software

Future objective

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

How to go about it

- develop a new **ethics of digital behaviour and commercial conduct**
- **enforce everywhere the principle of user's choice**
- promote **the respect of the personal sphere** also by ensuring **resiliency and accountability of systems**
- investigate **interdependencies** between **technology & societal systems**
- develop **a vision on how to depend on technology** (including international governance) in societal systems
- **education** and awareness

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 …

… to take responsibility for their respective roles

- **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”

Conclusions

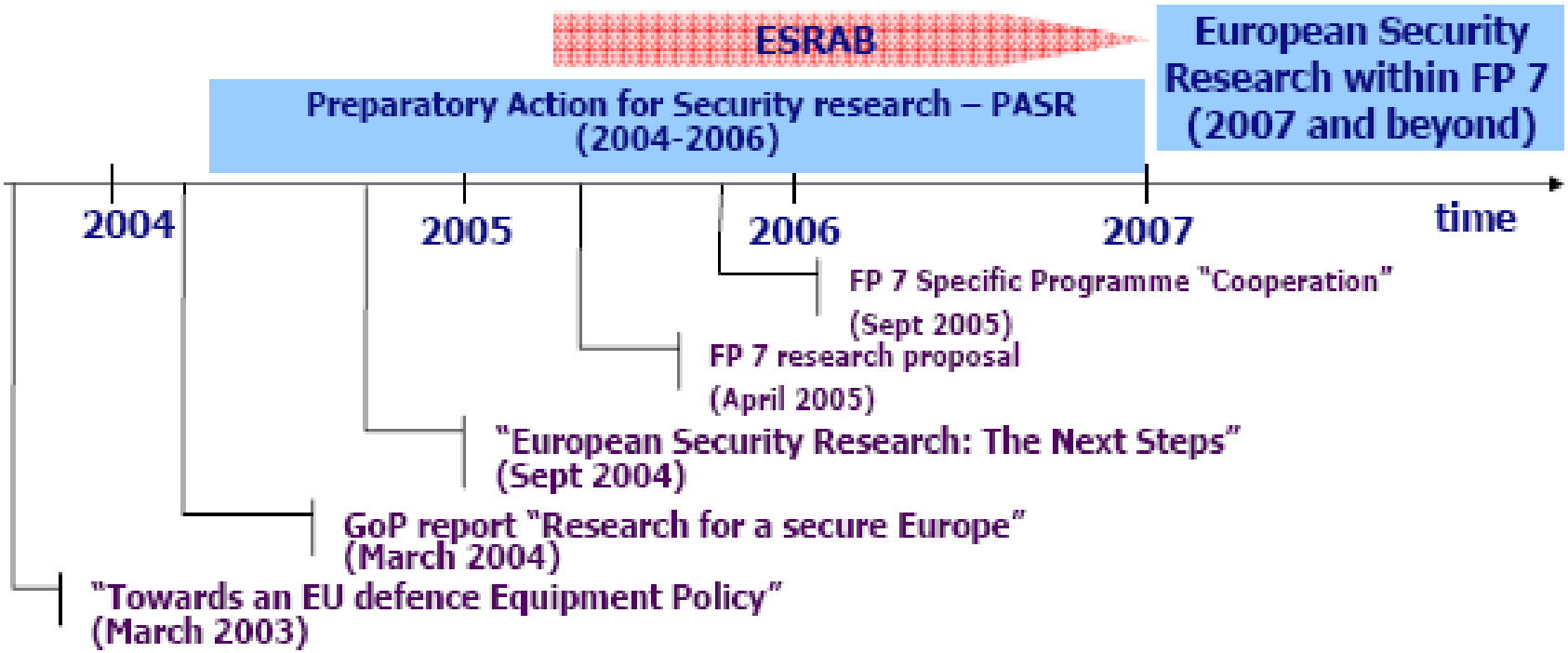
- Meeting **future NIS** challenges requires **the full commitment and contribution** of all stakeholders.
- The proposed policy strategy seeks to achieve this by **reinforcing the multi-stakeholders approach.**
- This will build on mutual interests, identify respective roles and **develop a dynamic framework for public-policy making and private sector initiatives.**
- The strategy is not in the vacuum as it sets **the framework for future** European initiatives on NIS.
- The Commission will report to Council and Parliament at the beginning of 2008.

EC approach to RESEARCH on SECURITY

Need for better EU-wide RTD security approach

- Avoiding duplication and fragmentation of structures and programs
- Increasing interoperability and cost efficiency of security systems and infrastructures
- Utilising the potential for cross-fertilization of ideas and results between the civil and non-civil security-related research fields
- Increasing investment in Research and Technology Development is this area where the EU lags in comparison to other regions in the world.

PASR - ESRAB – ESRP relation



Security Research in FP7 (2007-2013) :

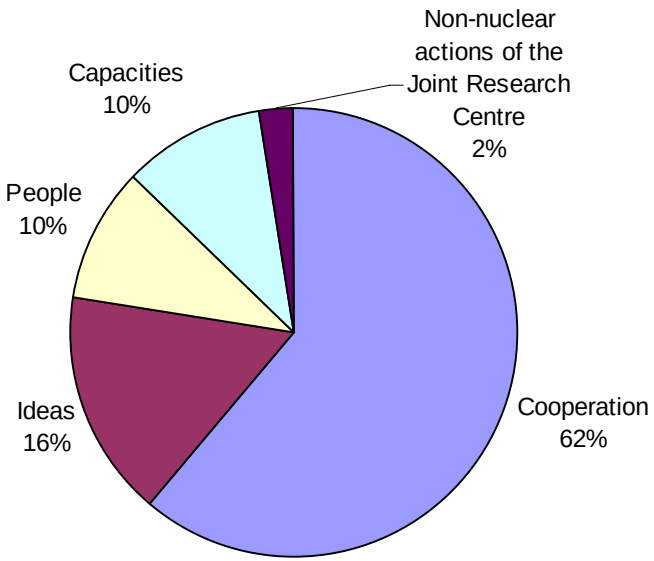
COOPERATION:

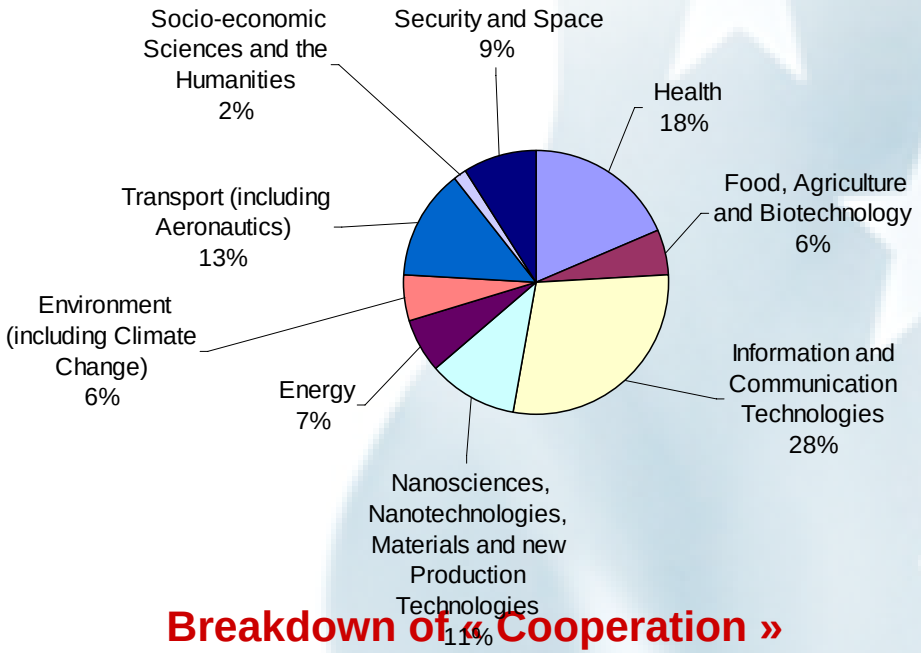
- 1. Health
- 2. Food, Agriculture &Biotechnology
- 3. Information & Communication Technologies
- 4. Nanosciences, Nanotechnologies,
- Materials & new Production Technologies
- 5. Energy
- 6. Environment (including Climate Change)
- 7. Transport (including Aeronautics)
- 8. Socio-economic Sciences & Humanities
- 9. Space
- **10. Security => 1,400 M€**

FP7 Budget Breakdown

Total FP7 budget

M€ 73 215





Breakdown of « Cooperation »

(M€ 44 735)

Security FP7 Activities (Mission Areas)

4 mission areas:

1. Security of citizens
2. Security of infrastructure and utilities
3. Intelligent surveillance and border security
4. Restoring security and safety in case of crisis

3 Cross cutting activities:

5. Security systems integration, interconnectivity and interoperability
6. Security and Society
7. Security Research coordination and structuring

FP7 security theme funding schemes

Collaborative projects

- very large → Demonstration projects (30-40 Meuros)
- large → Integration projects (10-25 Meuros)
- small to medium → Capability projects (2-5 Meuros)

Demonstration projects, Integration projects → In the missions (#1 to 4)

Capability projects → for Security and society (#6)

Coordination and support actions → Studies, networks, supporting actions → for Security research coordination and structuring (#7)

EU: An area of Freedom, Security and Justice

- The Treaty of Amsterdam on the European Union (EU) which came into force on 1 May 1999 states that the EU:
  - must be maintained and developed as an area of freedom, security and justice;
  - (an area) in which the free movement of persons is assured;
  - in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime.

Security in the area of Justice Freedom and Security

- Framework decision on attacks against information systems (April 2002)
  - Politically agreed text aiming at
    - Common level of approximation of criminal law
    - Prosecuting significant forms of illegal access, illegal systems and data interference (DoS, Web-sites defacement, virus attacks, etc)
    - Facilitate response of law enforcement and judicial authorities (avoiding crime heavens)
    - Improve international cooperation (all MS will have appropriate jurisdictional powers)

Security in the area of Justice Freedom and Security

- Enhancing access to information by law enforcement agencies to fight terrorism and organised crime (Communication from the EC to EP and Council 16/06/2004)
  - compatible information systems protected against unlawful access with appropriate data protection
  - common standards for information collection, storage, analysis and exchange including data protection and data security
  - promote research on secure and confidential communication channels through the AGIS programme
  - provide additional support through research activities (e.g. CTOSE)
  - develop an EU Cyber-crime-reporting manual

Towards a general policy on the fight against cyber crime

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE

May 2007

« Cybercrime »

- Understood as “criminal acts committed using electronic communications networks and information systems or against such networks and systems”
- Applies to three categories of criminal activities
  - **traditional forms of crime** such as fraud or forgery over electronic communication networks and information systems (electronic networks).
  - publication of **illegal content** over electronic media (i.a. child sexual abuse material or incitement to racial hatred).
  - **crimes unique to electronic networks**, i.e. attacks against information systems, denial of service and hacking. Attacks directed against the crucial critical infrastructures in Europe possibly affecting existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society

Current Situation

- The combination of constantly evolving criminal activities and a lack of reliable information makes it difficult to obtain an exact picture of the current situation
- Some general trends can be discerned
  - number of cyber crimes is growing and criminal activities becoming increasingly sophisticated and internationalised
  - Clear indications point to a growing involvement of organised crime groups in cyber crime
  - However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase
  - Instruments such as identity theft, phishing, spams and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms
  - A growing number of illegal content sites are accessible in Europe, covering child sexual abuse material, incitement to terrorist acts, illegal glorification of violence, terrorism, racism and xenophobia

Objective & focus of the initiative

- Targeting the strengthening of fight against cyber crime at national, European and international level therefore meeting the priority identified by Member States and the Commission
- Focus on the law enforcement and criminal law dimensions in complement to other EU actions to improve security in cyber space in general
- will eventually include: improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; reinforced dialogue with industry and possible legislative action
- defined and implemented in fully respecting fundamental rights, in particular freedom of expression, respect for private and family life and protection of personal data. Any legislative action taken in the context of this policy will be first scrutinised for compatibility with such rights, in particular the EU Charter of Fundamental Rights

Objectives of the Communication

- **Three main operational strands**:
  - To improve and facilitate coordination and cooperation between cyber crime units, other relevant authorities and other experts in the European Union building on already existing EU and international legal instruments
  - To develop, in coordination with Member States, relevant EU and international organisations and other stakeholders, a coherent EU Policy framework on the fight against cyber crime
  - To raise awareness of costs and dangers posed by cyber crime
- **Further development of specific instruments in the fight against cyber crime**
  - Strengthening operational law enforcement cooperation and EU-level training efforts
  - Strengthen the dialogue with industry
  - Legislation (**harmonised definitions and legislation**, **protection of children** , , **identity theft…..)**
  - Development of statistical data

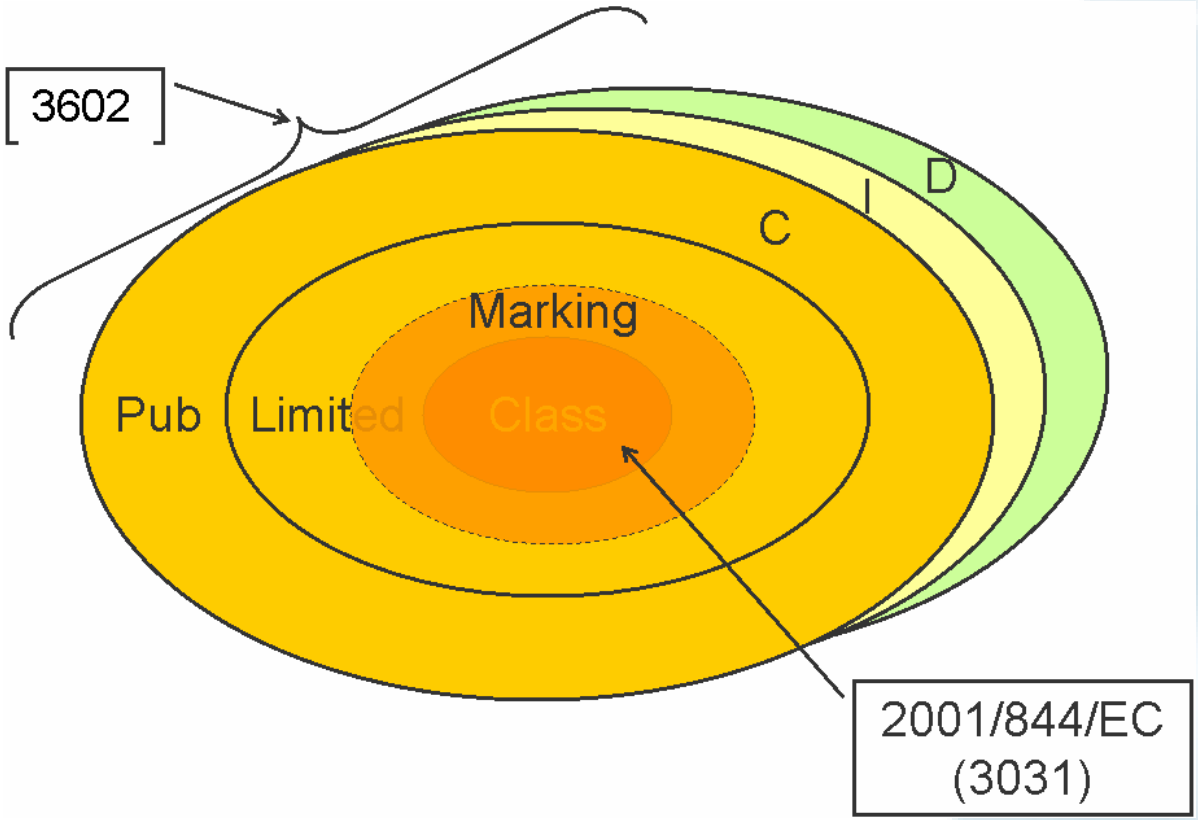
EC internal security rules

- "Doing what we preach" or "Eating our own dog food"
- Commission provisions on security for classified information (2001/844/EC (3031))
  - Objective :
    - Define rules to follow (Legal requirements)
    - To exchange (classified) data between partners (Member states, Institutions, other governmental organizations), **in confidence**, since it is mandatory to share similar rules, mutually recognized
  - Similar regulation exists in the other institutions with equivalent principles (ex: Council Decision 5775/01)

EC internal Security Regulations

- **Regulation (EC) No 45/2001** on the protection of individuals with regard to the processing of personal data
- **Commission Decision C (2006) 3602** concerning the security of information systems used by the European Commission
- **Commission Decision C (2001) 844** Provisions on security for the processing of EU Classified Information

EC internal information classification



In practice, only a very small subset comparing to the amount of data handled

EC's IT Security Architectural Approach

C \ IT	N S	Sens	Crit	Strat
NS	Public	Standard Architecture		
Se	Limited (Marked)			
Cr	EU Restricted	Reinforced Architecture		
St	EU Confid EU Secret EU T Sec	Exceptional Architecture		

Security in DIGIT… towards a business driven approach

- DIGIT customers (DGs, institutions, … and now national governments and administrations cf. Testa/sTESTA) are now increasingly demanding in security issues and request from us to demonstrate that we do it right !
- Security is a now a business need
- Information security it is not anymore an issue « nice to have » but a crucial requirement and therefore it has to be approached professionally
- Doing it right, will allow us to be seen as a strong value adding partner both internally (ex. internal infrastructure consolidation) and externally (managing infrastructure for trans-European networks)

Security in DIGIT .....towards a business driven approach

- Building security from inception in every service ce we deliver in order to
  - Reduce cost of failures, attacks
  - Provide response to continuity
  - Give assurance in term of CIA to our customers
  - Maintain and increase the robustness and resiliency of critical infrastructures

- Our “custumer’s” trust and confidence is crucial

Security organisation within the EC

Security Directorate

The equivalent to government NSA in Member States
EC INFOSEC authority

Defines and control application of corporate policies and standards

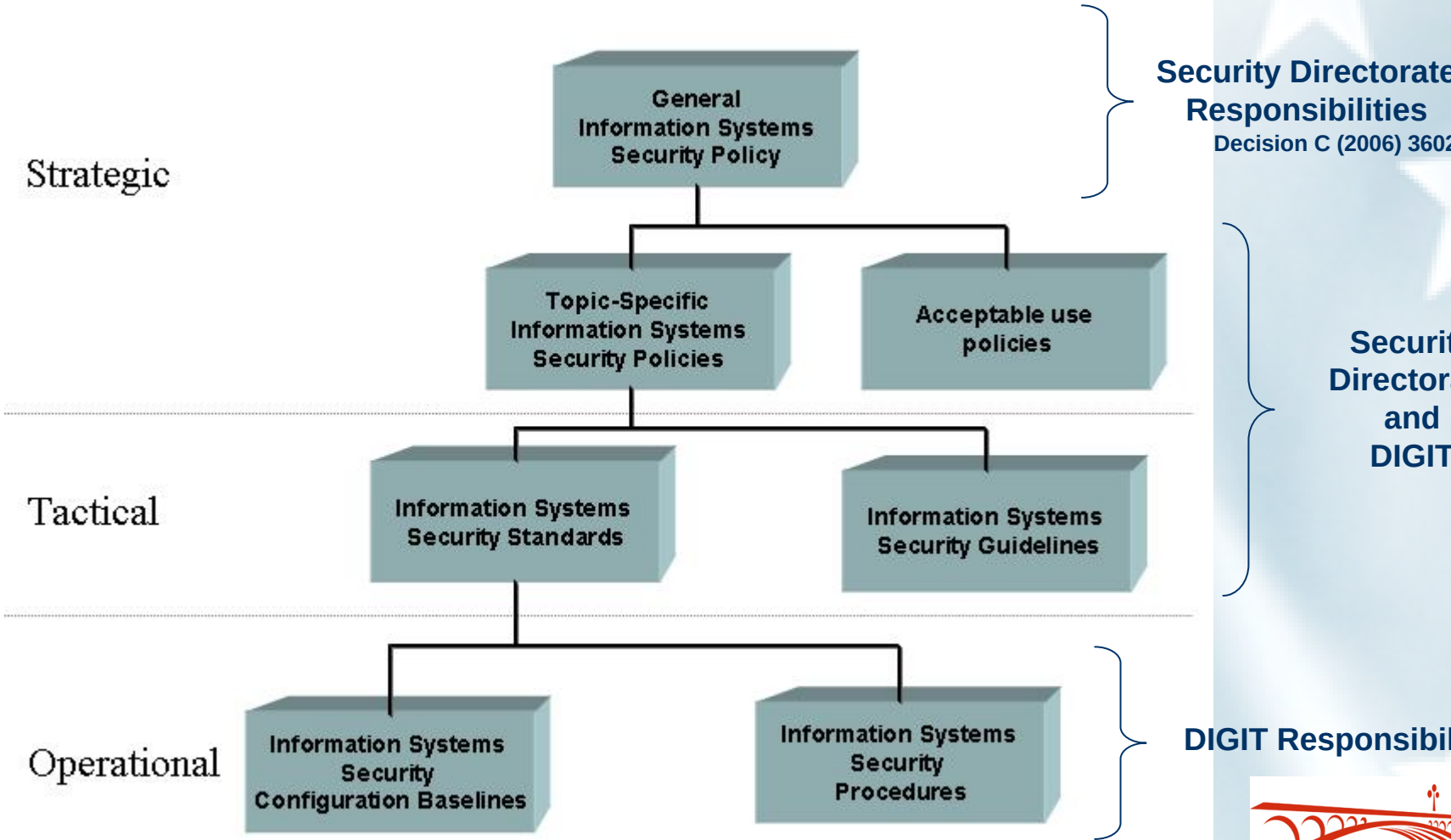
Similar to ministries in member states

Define local policies, standards and procedures

Directorate General X | **Directorate General W** | **Directorate General Z**

Director General	Informatics Security Officer	Information Owners	System Owners	Project Managers	System Suppliers
Has the ultimate responsibility for security within its DG	**Defines local policies and security plans, audit application …**	Defines the security needs of the information (CIA)	Bear responsibility for the security of their IS Approve the security requirements and security measures	Specify the security requirements on the basis of the security needs defined Define and implement specific security measures	Construct the information system in accordance with the security requirements drawn up by the project leader

Internal Information Security Policies



Security governance

- Adopt best practices in term of security management system (ISO 27001, NIST 800 series) to develop, sustain and improve security processes
- Risk analysis and management using an home-made methodology using best of breed (EBIOS, ISO 13335, BS 7799-3, CRAMM, MEHARI)
- Security Controls from best standards (ISO 17799:2000, NIST 800-53, IT BPM (German BSI, COBIT, ISF …)
- Alignment of business risks (identified through BIA) and controls by developing security baselines based on information systems classification (C,I,A)

Client layer

- Hardened configurations (Desktop workstations, PDAs/Smart phones …)
  - OS Layer
  - Internet Browser settings
  - Anti-malware (virus/spyware…)
  - Automatic asset inventory, patch management …
- Full encryption for Laptops on request
- Secure remote access (Token+VPN+Terminal Services) for roaminf users, day extenders and teleworkers
- PKI based secure e-mail

Network layer

- Hardened Firewalls, routers and switches configuration
- High availability by design
- 3 layers of firewalls
- IDS/IPS
- Proxies and gateways
- 24h/24 monitoring by a Network Operation Centre

- In the future ?
  - Network access control
  - Strong network segregation (MPLS)

Security in Hosting Services

- Strong physical security (4 sites)
- Operations security (ITIL)
  - Capacity planning
  - Change management
  - Back-up infrastructure (disk based Virtual libraries, High quality Backup robot)
  - Media management (off-site storage) on going
- Infrastructure built for fall-back and disaster recovery. Business continuity plans fully documented for mission critical systems progressing. Some “live rehersal”….

Information systems developement

- Methodology based on RUP (RUP@EC)
- Solid Entreprise Architecture Framework (CEAF)
- In the near future
  - Application vulnerabilities to be reduced by integrating best practices such as OWASP (Open Web Application Security Project www.owasp.org)
  - Adoption of Security Design Patterns (Group of Four at the origin of RUP) applied to security

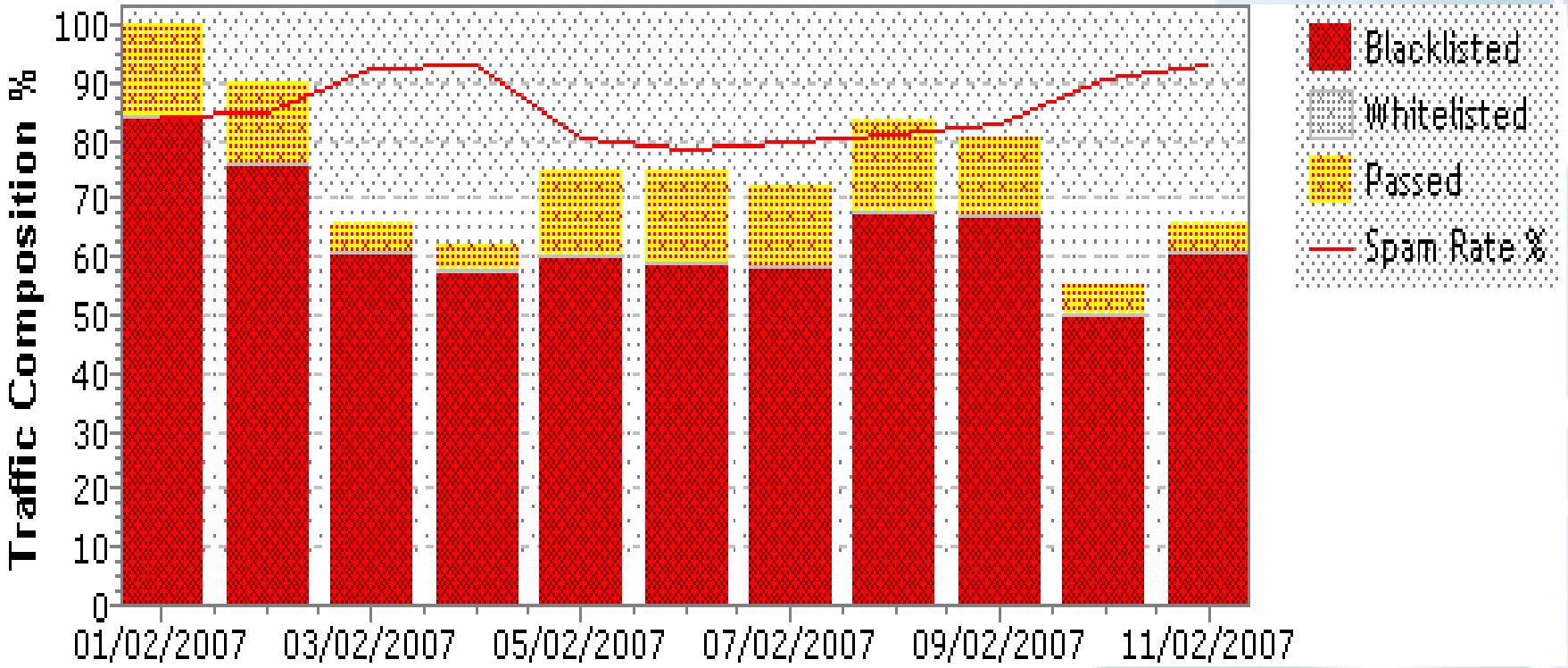
Horizontal services

- Training and awareness
  - Specialised training in security (Security managment, Risk assessment, ethical hacking …)
  - Specific Awareness courses targeted to audiance
- Vulnerability Management
  - Vulnerability watch
  - Centralized Patch management
  - In the near future: Centralised vulnerability assessment

Horizontal Services

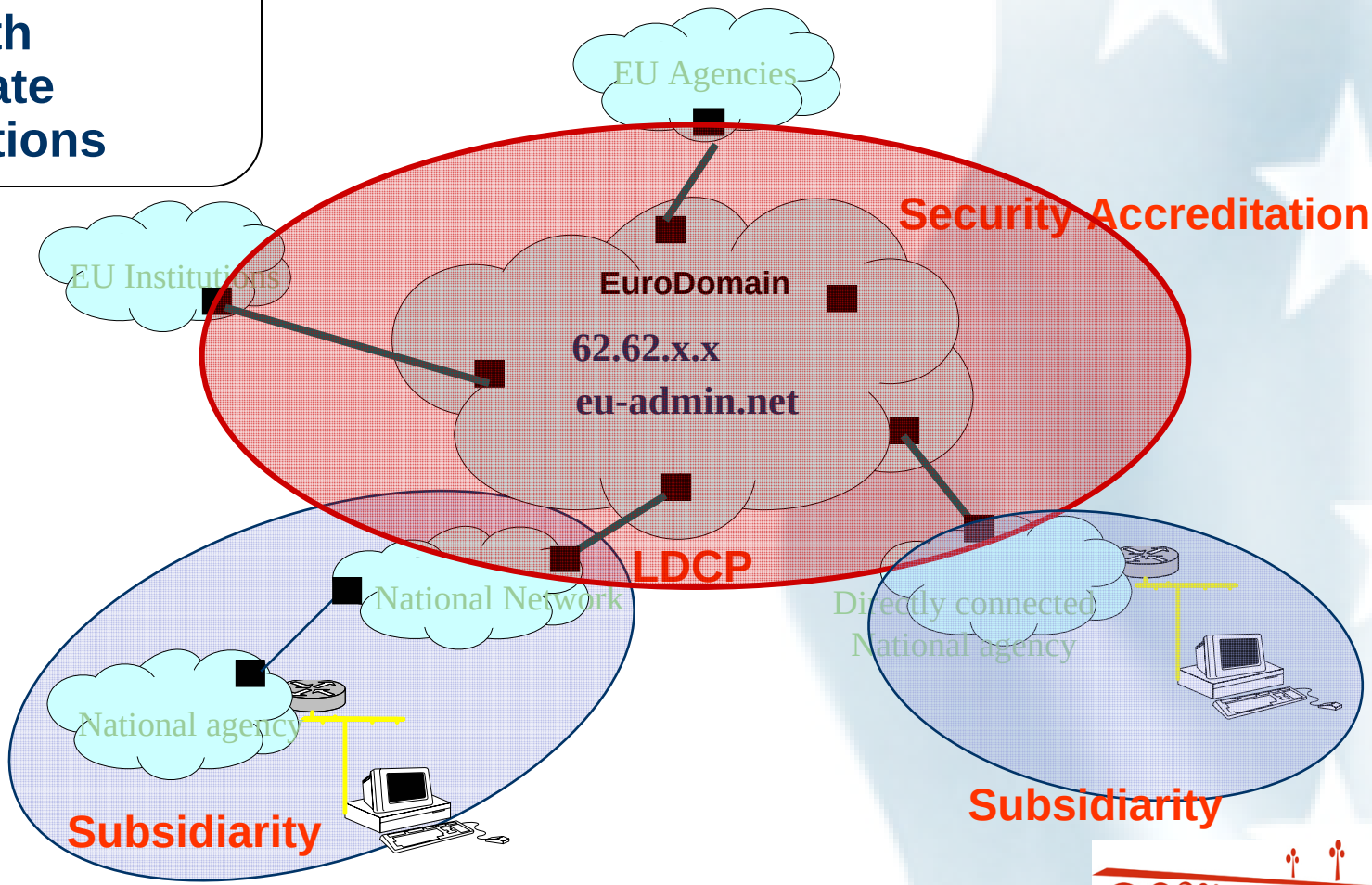
- Strong authentication services (SSO)
  - ECAS
  - PKI (secure e-mail …). Certificates issued by internal RA
- Anti-Virus (centralised AV signatures and management of updates)

Fight against SPAM - Statistics (2)



(TESTA/S-Testa) accredited close network with Member State Administrations

MPLS-based network - Dedicated IP addressing plan, not connected to the internet



Security is like contraception...

- Will never be 100% effective.
- Does not contribute to performance.
- Never sure you actually need it all the time.
- Don't know whether it has worked until after (even long after..) the event
- The measure of effectiveness is in terms of failures.
- A combination of methods gives the greatest reduction in risk.
- Should never rely on someone else's precautions - *take care yourself*.

Everybody's responsibility

Security policy & implementation:
The European Commission Perspective

Thank you very much for your attention

Francisco.garcia-moran@ec.europa.eu
http://europa.eu