IT Security
in
the European Digital Agenda

DIGIT Direction-Générale de l'informatique

Marc FEIDT
Head of Unit
Directorate-General for Informatics
EUROPEAN COMMISSION

COMMISSION EUROPÉENNE

FIRST conference Vienna 16.6.2011

Cyber warfare ..... real or science fiction?

Agenda

1. **EU context**

2. **Trust & Security** in the Digital Agenda

3. **ENISA:** key EU trust & security partner

4. **CIIP** Critical Information Infrastructure Protection

5. **International Cooperation**

6. **Security@EC**

The EU is the result of a number of international Treaties since the ’50s (end of World War II) (⇨primary legislation)

A unique economic and political partnership between 27 democratic European countries aimed at:

- Creating an ever closer union among the peoples of Europe
- With decisions taken as closely as possible to the citizens
- Achieving peace, prosperity and freedom for the citizens in a fairer and safer world
- Through its competences in a large number of areas, exercised through **secondary legislation** (which prevails over national law)

To achieve these aims, the Treaties set up a number of EU Institutions, Agencies and Other Bodies (EUIs):

- A “core” of 7 Institutions (European Council,EC,EP,Council of the EU,CoJ,CoA, ECB, EEAS recently) based in Brussels / Luxembourg / Strasbourg / Frankfurt
- Various layers of other types of EUIs (40-80 depending on how they are counted !) scattered throughout the 27 Member States

The EC has a a mission

1. Be the engine behind the propoosal for EU legislation to be approved by the legislative branch: the Council, representing the EU Governments and the EP representing the Citizens
2. Be the guardian of the Treaties and take MS to court in case of proved infringement of EU legislation
3. Execute the EU budget to support the EU policies resulting from the EU legislation
4. In close cooperation with the newly created EEAS, represent EU on the international stage.

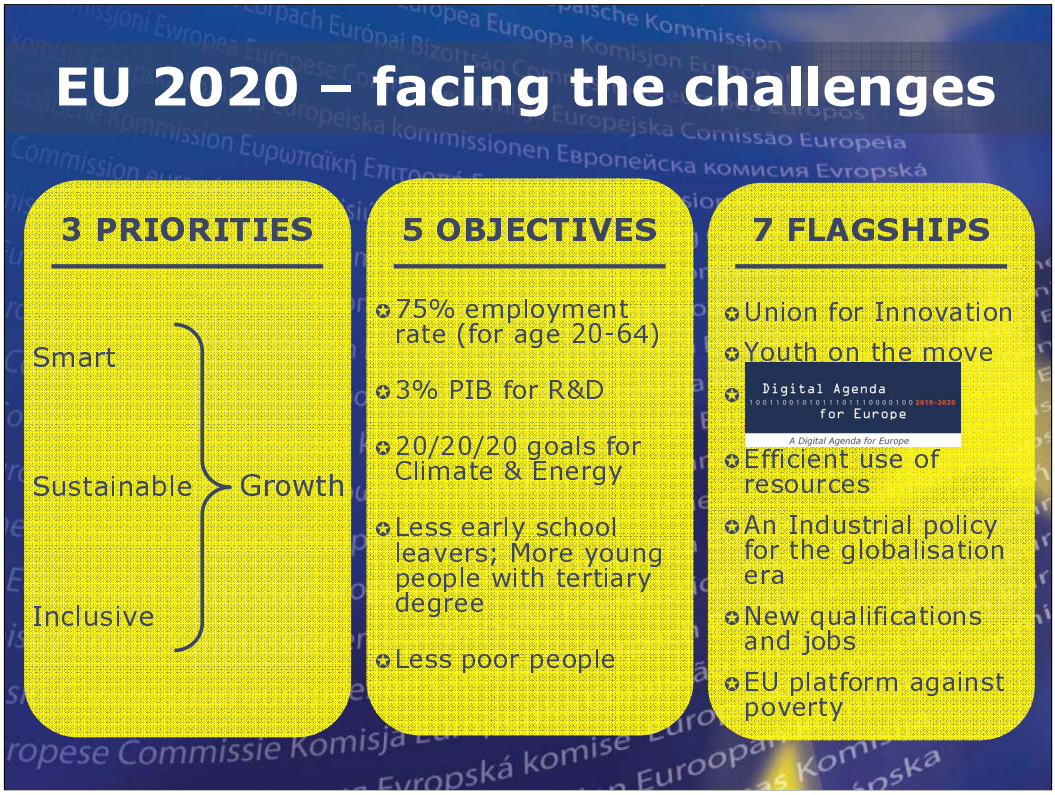
The EC is structured in DGs follwing the policies with the external services being transferred to the EEAS partially, internal services (one of which is DIGIT) and General Services. All in all around 30000 employees.

DIGIT reports to the Commissionner in charge of Inter-institutional affairs and Administration , Maros Sefcovic representative of Solovenia

Todays society has many challenges

Economy crisis, climate change, energy efficiency, ageing society, education, and security.

How are we tackling those challenges in the EU?



In March 2010, the Barroso II Commission issued the EU 2020 initiaitve, with three priorities around growth that should be smart, sustainable and inclusive. It defines 5 mutually reinforcing objectives and concentrates on 7 flagship initiatives, one of which is « The European Digital Agenda »

A Digital Agenda for Europe

Digital Agenda for Europe 2010-2020

"The aim is to deliver sustainable economic and social benefits from a Single Market based on fast and ultra fast internet and interoperable applications ."

COMMISSION EUROPÉENNE

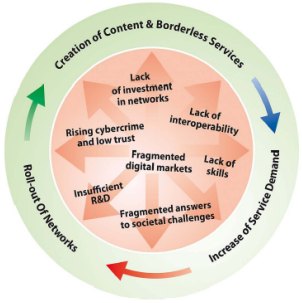
COM(2010) 2020

DIGIT Direction-Générale de l'informatique

8

The aim of the Digital Agenda turns around the use of ICT, Information and Communication technologies, to further develop the single market

The vision: « Every European Digital »



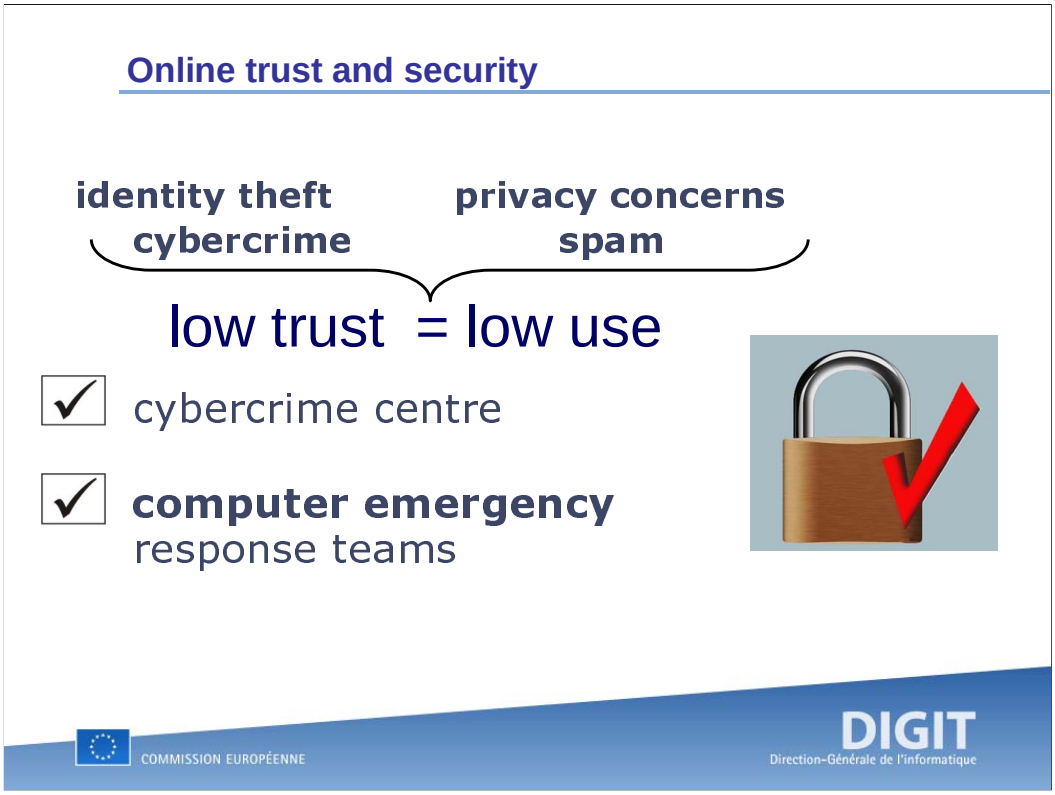
COMMISSION EUROPÉENNE

DIGIT
Direction-Générale de l'informatique

The motto is very simple, clear and direct: « Every European Digital »

Concretely this means that, at operational level, the EC should also act on ICT-enabled benefit for EU society.

2 Trust & Security in the Digital Agenda



80 to 98 % of all circulating e-mail traffic are spam

Cyber attacks increasing and often motivated by financial or even political purposes

Only 12% of European web users feel completely safe making online transactions. Threats such as malicious software and online fraud unsettle consumers and dog efforts to promote the online economy.

Europeans will not embrace technology they do not trust

The Digital Agenda proposes a number of practical solutions, including a coordinated European response to cyber-attacks and reinforced rules on personal data protection.

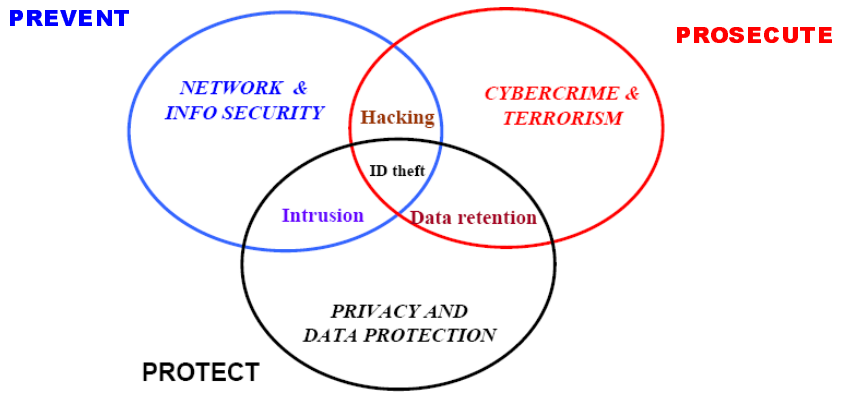
•Setting up a European rapid response system to cyber-attacks, including a network of Computer Emergency Response Teams (CERTs)

•Proposing in 2010 a reinforced role for the European Network and Information Security Agency (ENISA).

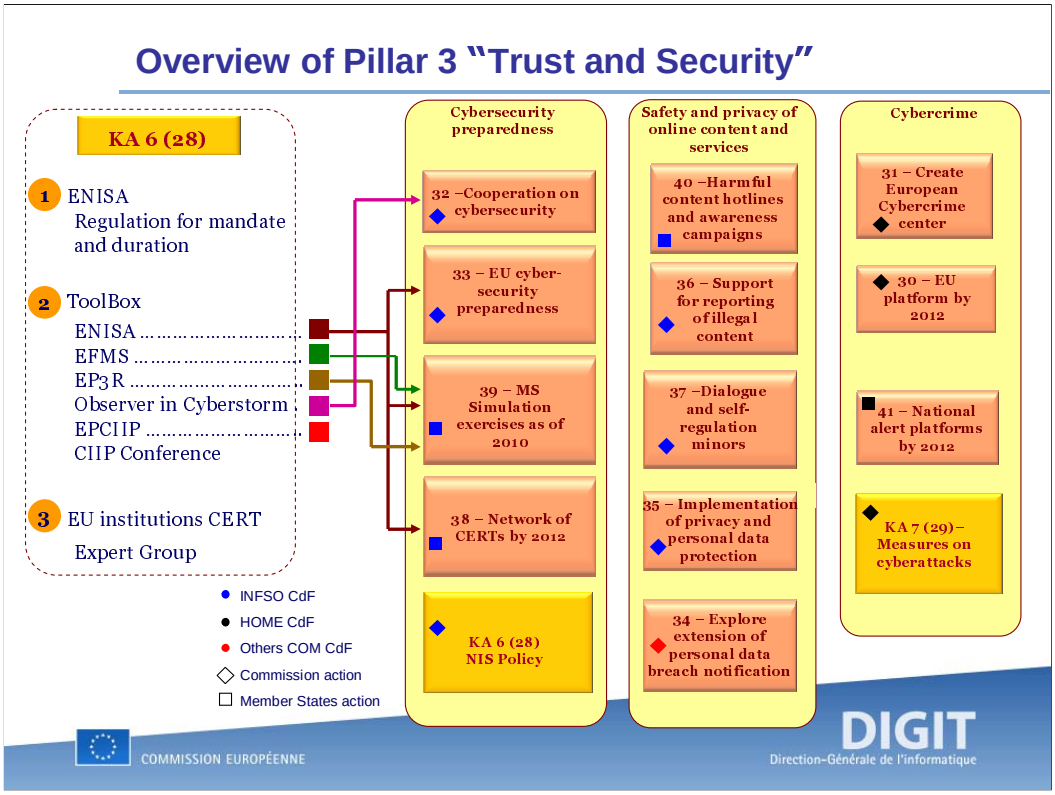
•Proposing tougher laws to combat cyber attacks against information systems in 2010 and by 2013 related rules on jurisdiction in cyberspace at European and international levels

Network and Information Security policy

Three angles



In terms of policy, we need to approach Network and Information Security from three angles: Prevent, Prosecute and Protect, knowing that sometimes there is tension among the three aproaches



This diagram sums up the actions that are taking place in the pillar 3 of the Digital Agenda. Three major threads of work: Cybersecurity Preparedness, Safety and privacy of content and services and fighting cybercrime. Pay attention to the color code and shape code of the symbols in every square. The color indicates which policy area is taking care: Information society, Home Affairs, other policy areas, etc), the shape, square or diamond whether it is a Commission action of a Member State action.

Action 28: Reinforced Network and Information Security Policy

The Commission will reinforce the Network and Information Security Policy and will modernise European Network and Information Security Agency (ENISA), and measures allowing faster reactions in the event of cyber attacks, including a CERT for the EU institutions

What is the problem? Networks are not secure

The internet has become a critical information infrastructure, encompassing IT systems and networks across the globe. It must be resilient and secure against all sorts of threats.

Why is EU action required? EU helps the states to cooperate

Strong cooperation between EU governments, public bodies and private companies is necessary to improve information exchange and to ensure that security problems are addressed quickly and effectively.

The European Network Information and Security Agency (ENISA) serves as a focal point for this exchange and cooperation. Enhanced ENISA is expected to have a significant positive economic impact, as the current costs associated with network and information security breaches are already considerable and are still growing.

To react to threats in real-time conditions, a well functioning and wider network of Computer Emergency Response Teams (CERTs) should also be established in Europe, including for European institutions (see Action 38 for more information on CERTs).

What will the Commission do?

The European Commission will:

In 2011

Publish a Communication containing the principles for internet resilience and stability at the European and global level.

Ensure that the heads of the respective institutions will sign the agreement to establish the CERT for the EU institutions. ----------→ done, iCERT being set up

In 2012

Ensure that the regulations on ENISA will be adopted at the EU level.

Make sure that CERT becomes operational.

Some examples of the actions that the Commission has planned since 2010 in close cooperation with Member States until 2013.

EU Institutions leading by example: iCERT@EU

iCERT@EU - Interinstitutional EU CERT Network

Key Action 6 of the Digital Agenda:

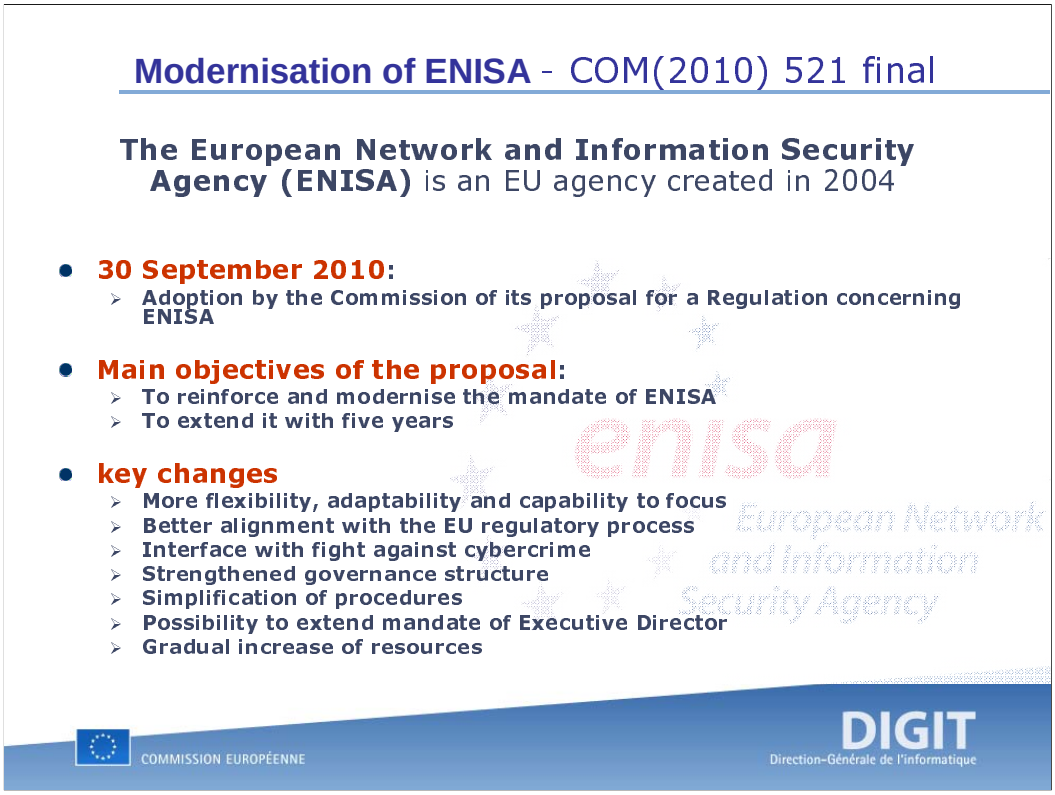
*"Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy, including … measures allowing faster reactions in the event of cyber-attacks, including a **CERT for the EU institutions**."*

- **2010 –**
  - August - Wisdom Council set up to advice on a CERT for the EU institutions
  - December – the "Rat der IT Weisen" report basis for the best conditions to establish iCERT@EU
- **June** – Preconfiguration team
  - EU Institutions and ENISA
- **2011 –** Assessment of the work (together with the network of national CERTs)
- **2012 –** Fully fledged iCERT@EU

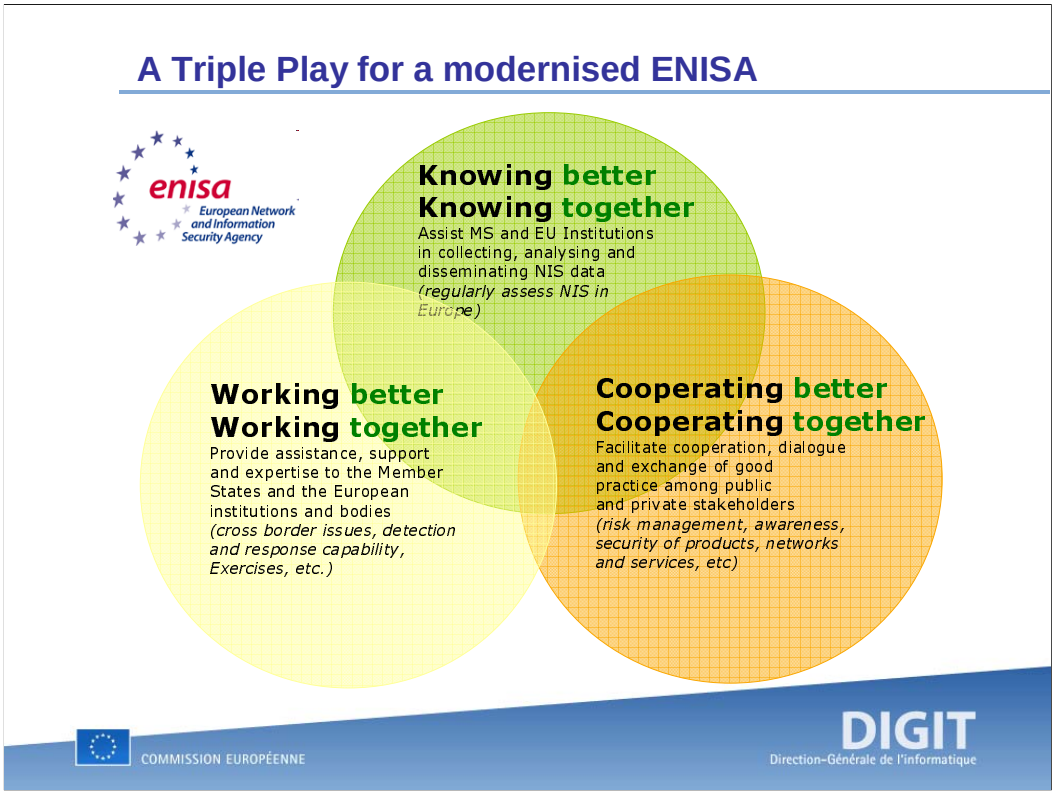
ENISA
key EU trust & security partner

COMMISSION EUROPÉENNE

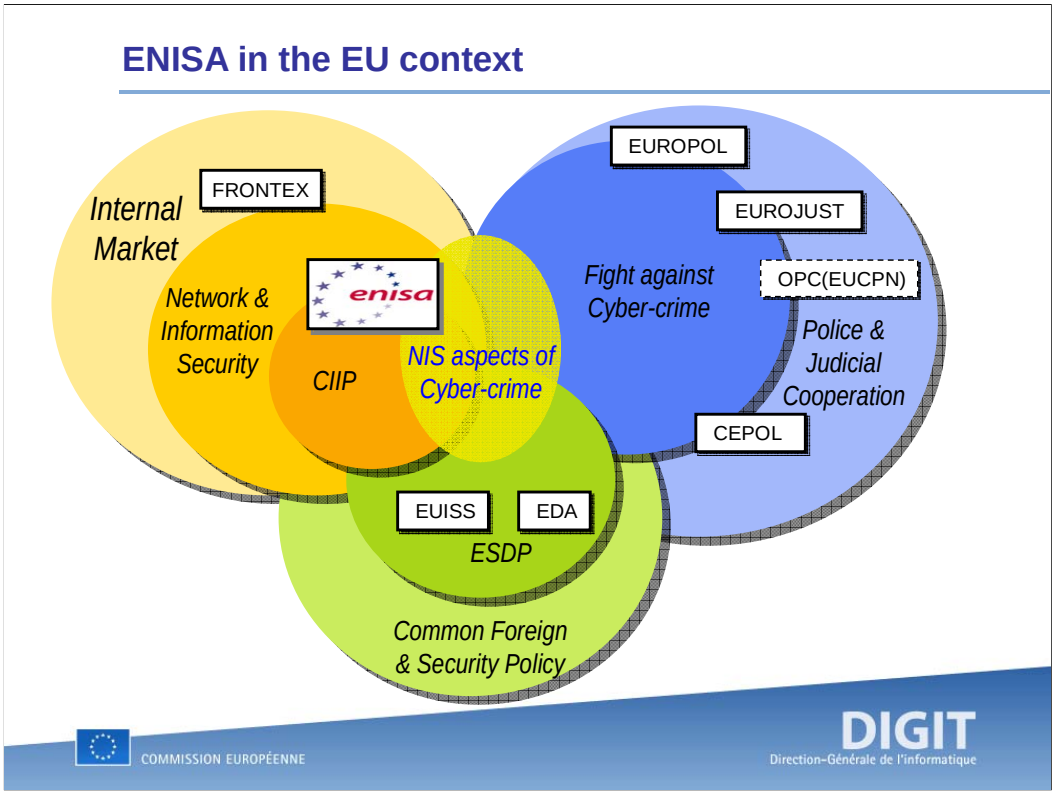
DIGIT
Direction-Générale de l'informatique



The legal base for the agency is in the process of being renewed. The current legal base will be valid until 2012 and we are currently going through the legislative process with the Parliament and the Council. ENISA is essential to cope with the NIS challenges in the EU. It has to be modernized and his mandate extended for 5 addtional years in order to allow it to complete its mission.



The three pillars on which the Agency will built its reputation will be Knowledge, Hard Work and Cooperation with high quality in close cooperation with member states, the industry, the consumers and the academia to deliver advice, organize cooperation, exchange of best practices and enhancing international cooperation.



ENISA legal base is based on the Internal Market and this diagramme presents its positioning with reference to other agencies and groups in the area of security, boundary protection and law enforcement as well as how it touches other policy areas.

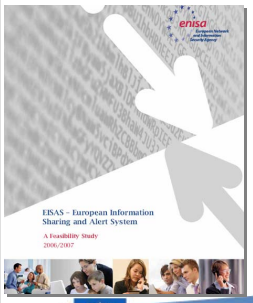
Critical Information Infrastructure Protection

CIIP Communication

Protecting Critical Information Infrastructures is high int the security agenda of the EU. To this end the Commission adopted a communication to the Council and the EP on CIIP. This comunication concentrates on preparedness and resilience.

It foresees 5 areas of action from preparedness and revention to international cooperation through to Detection, response, mitigation and recovery

1. Preparedness and prevention



2010:
- **ENISA's recommendations** on baseline capabilities for Nat/Gov CERTs**;** 20 MS with Nat/Gov CERTs in place;

2012:
- **ENISA to support** network of CERTs at national level**;**

2013:
- EISAS**, ENISA cooperating with Nat/Gov CERTs**

Continuous:
- EP3R **European Public-private Partnership for Resilience**
- EFMS **European Forum for Member States**

COMMISSION EUROPÉENNE

DIGIT
Direction-Générale de l'informatique

ON the first pillar of actions, the role of ENISA can be highlighted in setting up the EU Network of CERT and the Commission animating forums with member states to enhace preparedness

CIIP Actions 2 to 5

2. Detection and response
development and deployment of a **European Information Sharing and Alert System**, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems.

3. Mitigation and recovery
including the development by Member States of **national contingency plans** and the organization of regular exercises for large scale networks security incident response and disaster recovery; European **exercises on large-scale network security incidents**; reinforced **cooperation between** national/governmental **Computer Emergency Response Teams**.

4. Criteria for European Critical Infrastructures
criteria for the ICT sector including the development of ICT sector specific **criteria to identify European critical infrastructures in the ICT sector**.

5. International Cooperation → *Next section*

COMMISSION EUROPÉENNE

DIGIT
Direction-Générale de l'informatique

Those are the activities in the other actions mentioned before, starting with identification of what Critical Infrastructures, elaboration of contingency plans and the setting up of platforms for alarm, information exchange and crisis management

5 International Cooperation

COMMISSION EUROPÉENNE

DIGIT
Direction Générale de l'informatique

Finally, information security is more an more a global issue, international cooperation is therefore essential

A long-existing political aspiration

- Economies of scale, synergies, etc.

- We can not act alone anymore facing a global problem, we need to strengthen global risk management and coordinate our actions at global level to target computer-based crime and security attacks

- two recent exemples in international collaboration on Internet relsilience and preparedness exercises:

  - **European principles and guidelines for Internet resilience and stability** developed within EFMS

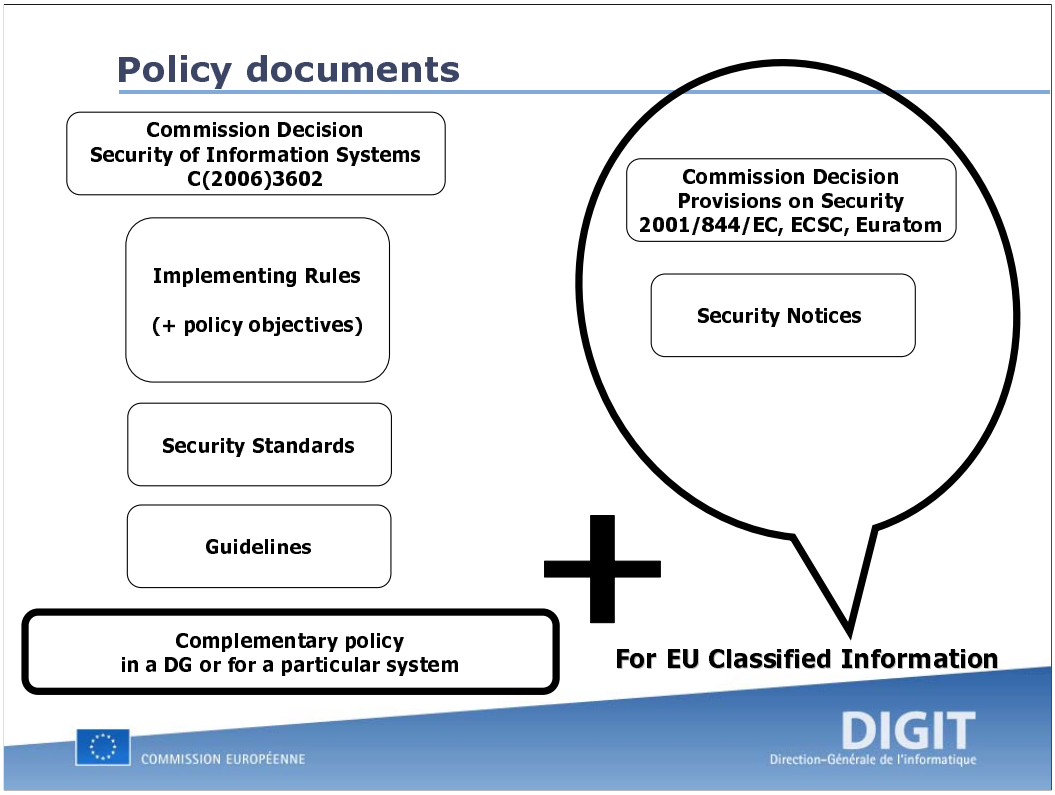
  - **7 EU MS** took part **in US exercise Cyber Storm III** (EC and ENISA observers)

Security @EC

COMMISSION EUROPÉENNE

DIGIT
Direction-Générale de l'informatique

Finally, information security applies to the EC as well.



Commission Decision Security of Information Systems C(2006)3602

General policy decision: definitions, overall objectives, scope, general principles, roles and responsibilities

further enhanced by implementing rules: detailed rules on implementation of the IS Security Policy systematic mgt and risk mgt process

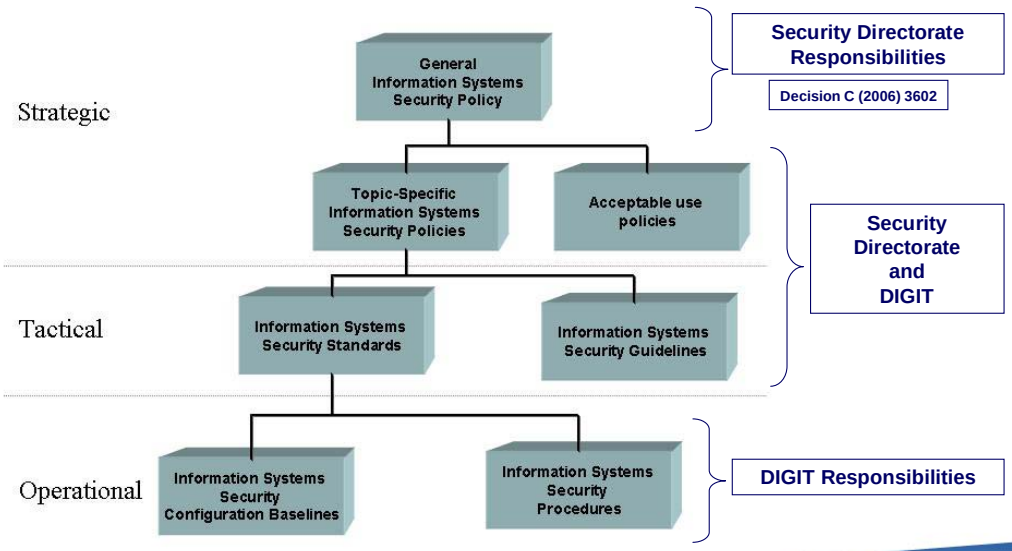
and security standards: how, who, when, where,….

In addition, **guidelines** in terms of best practices, recommendations in the various areas.

The decision applies to non classified information;

COM decision 2001 is applicable to EU classified.

DIGIT Information Systems Security Policy framework



II - Security measures

Overview of IT security measures in place

- physical
- technical
- procedural
- organisational

Security @ DIGIT... the organisation

- **An Information Security Steering Committee**
  - Defines the overall security strategy
  - Chaired by the Director General
- **A Local Information Security Officer**
  - Independent from operations
  - Advisor to the Information Security Steering Committe
  - Defines the local policies (in compliance with corporate rules) and provides assurance on its effective and efficient implementation
  - Leads DIGIT Security Operations Centre

Security in depth – Client layer

- **Hardened configurations (Desktop workstations, PDAs/Smart phones …)**
  - OS Layer with locked security settings
  - Internet Browser settings
  - Anti-malware (virus/spyware…)
  - Automatic asset inventory, patch management + internal security patch bulletin service …
  - End-of-life Disk Wiping
- **Strong Password, plus inactivity timeout**
- **Full encryption for Laptops**
- **Secure remote access (Token+VPN+Terminal Services)**
- **2-factor authentication**
- **PKI based secure e-mail**

Security in depth - Network layer

- High availability by design
- Hardened Firewalls, routers and switches configuration
- Several layers of firewalls (and more)
- Proxies and gateways

- 24x7 monitoring by a Network Operation Centre
- 24x7 monitoring by a (external) Security Operations Centre
- Peer-to-Peer moratorium
- WiFi (not connected to main network)
- Only Point-to-Point exceptions, after formal approval by DS

Security in depth - Hosting Services

- **Strong physical security (5 DC sites for corporate services and IS Hosting)**
- **Operations security (based on ITIL)**
  - Capacity planning
  - Change and version management
  - Back-up infrastructure (hot backups, tapes)
  - Media management (off-site storage)
- **Operational implementation of security policies**
- **Regular patching**
- **Business continuity and disaster recovery plans (regularly tested and improved)**

Security in depth - Information systems development

- Methodology based on RUP
- Solid Entreprise Architecture (CEAF)
- Application vulnerabilities will be reduced by integrating best practices such as OWASP (Open Web Application Security Project www.owasp.org) and adoption of Security Design Patterns (GOF applied to security)
- Service in place for evaluating vulnerabilities before production (part of stress testing)

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
  - Corporate anti-virus management
  - Centralized Patch management
  - Centralised vulnerability assessment


SECURITY IS YOUR RESPONSIBILITY
STOP AND THINK!


Thank You