IT Security @ EC

Challenges & Experiences

Francisco García Morán
Director General
DG Informatics
European Commission

Context

What we do

Policies

Experiences

Climate Action
Energy for a Changing World

1. Context

The 2020 Challenges

Climate change

Economical recovery

Jobs, ……

Energy consumption

Security

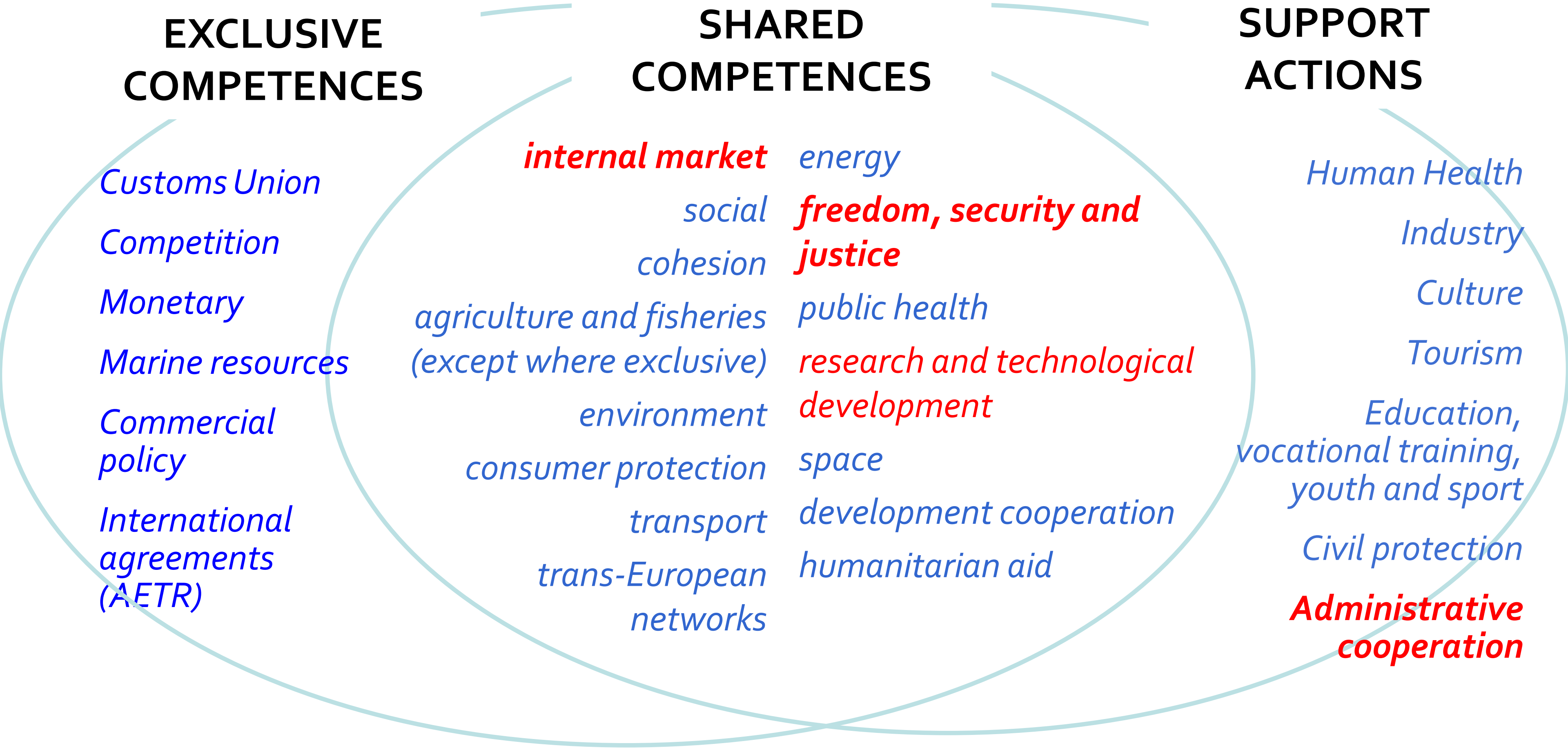
Ageing society

Transport efficiency

Empowering patients

Inclusion

EU Policies (Lisbon Treaty)



EXCLUSIVE COMPETENCES

- *Customs Union*
- *Competition*
- *Monetary*
- *Marine resources*
- *Commercial policy*
- *International agreements (AETR)*

SHARED COMPETENCES

- ***internal market***
- *social*
- *cohesion*
- *agriculture and fisheries (except where exclusive)*
- *environment*
- *consumer protection*
- *transport*
- *trans-European networks*
- *energy*
- ***freedom, security and justice***
- *public health*
- *research and technological development*
- *space*
- *development cooperation*
- *humanitarian aid*

SUPPORT ACTIONS

- *Human Health*
- *Industry*
- *Culture*
- *Tourism*
- *Education, vocational training, youth and sport*
- *Civil protection*
- ***Administrative cooperation***

Smart

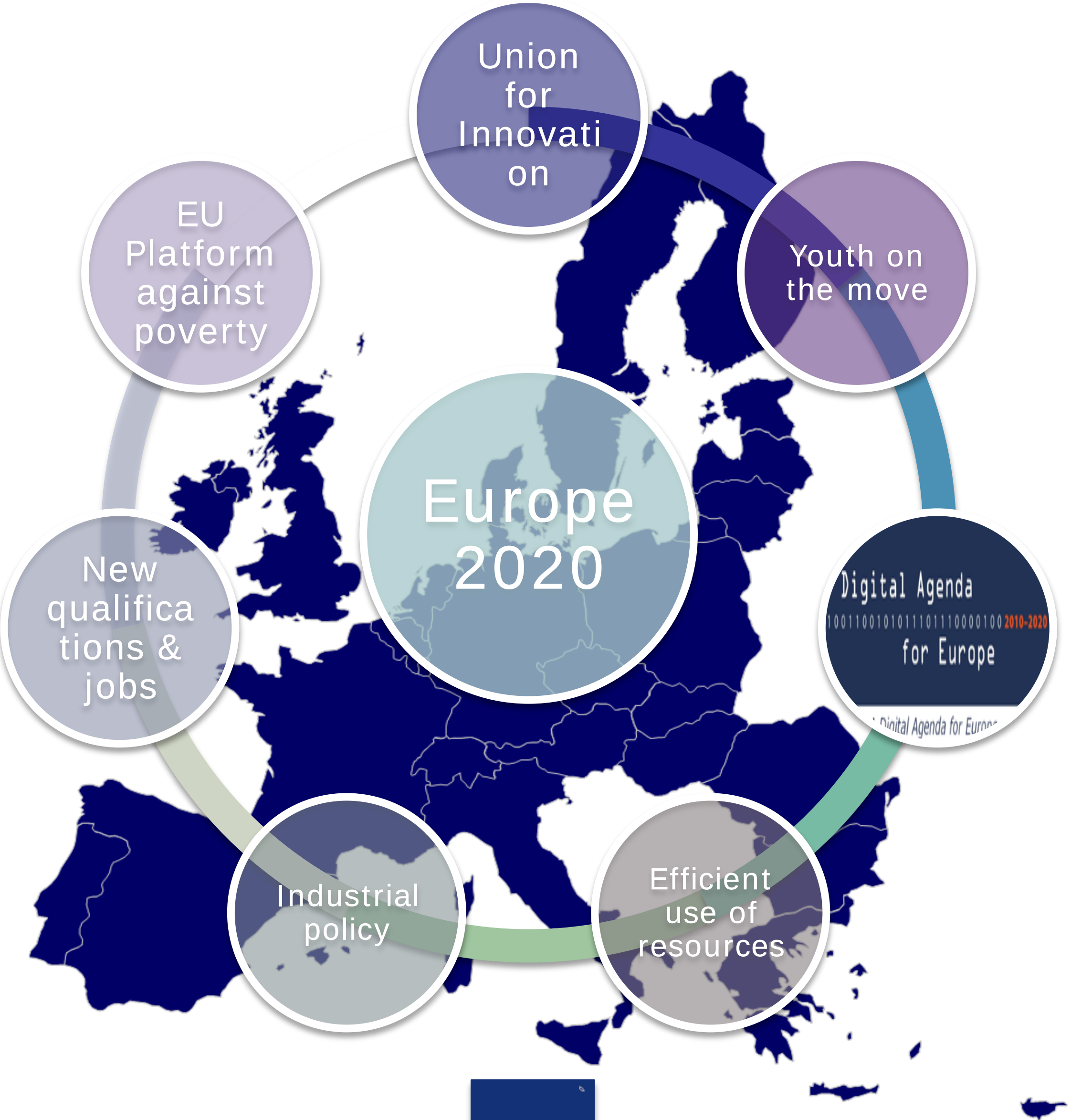
developing an economy based on knowledge and innovation

Sustainable

promoting a more efficient, greener and more competitive economy

Inclusive

fostering a high-employment economy delivering social and territorial cohesion



Europe 2020

Union for Innovation

Youth on the move

Digital Agenda for Europe

Efficient use of resources

Industrial policy

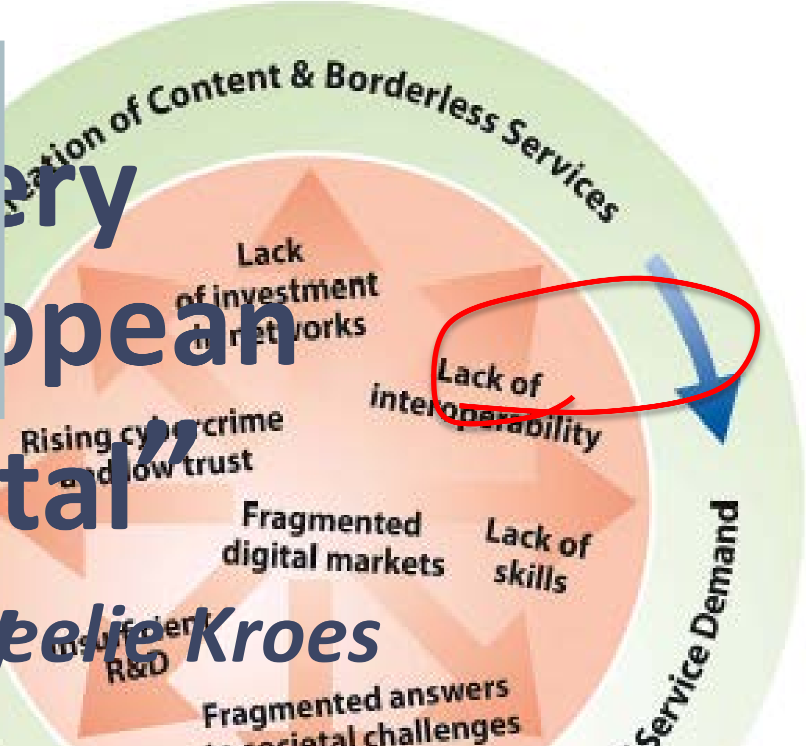
New qualifications & jobs

EU Platform against poverty

Trust & Security

ery
opean
Digital”

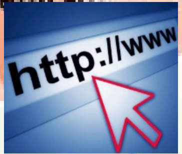
eelie Kroes


ation of Content & Borderless Services
Lack of investment in networks
Lack of interoperability
Rising cybercrime and low trust
Fragmented digital markets
Lack of skills
Insufficient R&D
Fragmented answers to societal challenges
Service Demand
Rollout Of Networks
Inc

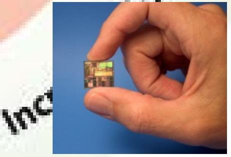
Digital Single Market

Interoperab. & standards

Trust & security



Very fast Internet


Research & Innovation

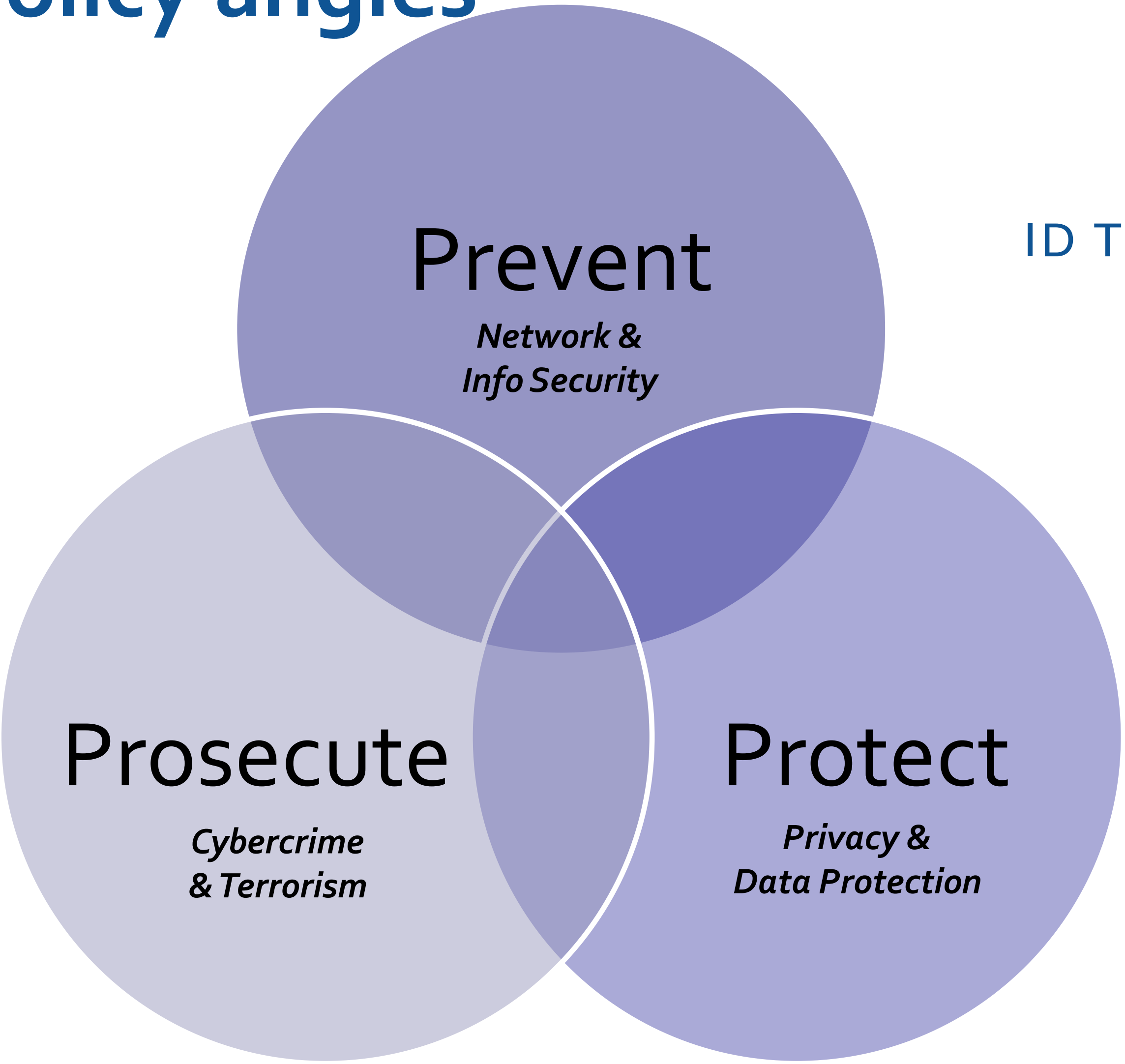
Enhancing e-skills

ICT for social challenges

2. What we do

Trust and Security Policies

The 3 policy angles



Hacking

ID Theft

Intrusion

Data retention

Internet security: the EU Policy

Focus on ***prevention, resilience and preparedness*** *(complementary to fighting* ***cyber crime****)*

Take into account the ***civilian*** *&* ***economic stakeholders****' role and capability (role of private sector & the* ***governance challenge****)*

Make ***security and resilience the frontline of defence***

Adopt an ***all-hazards approach***

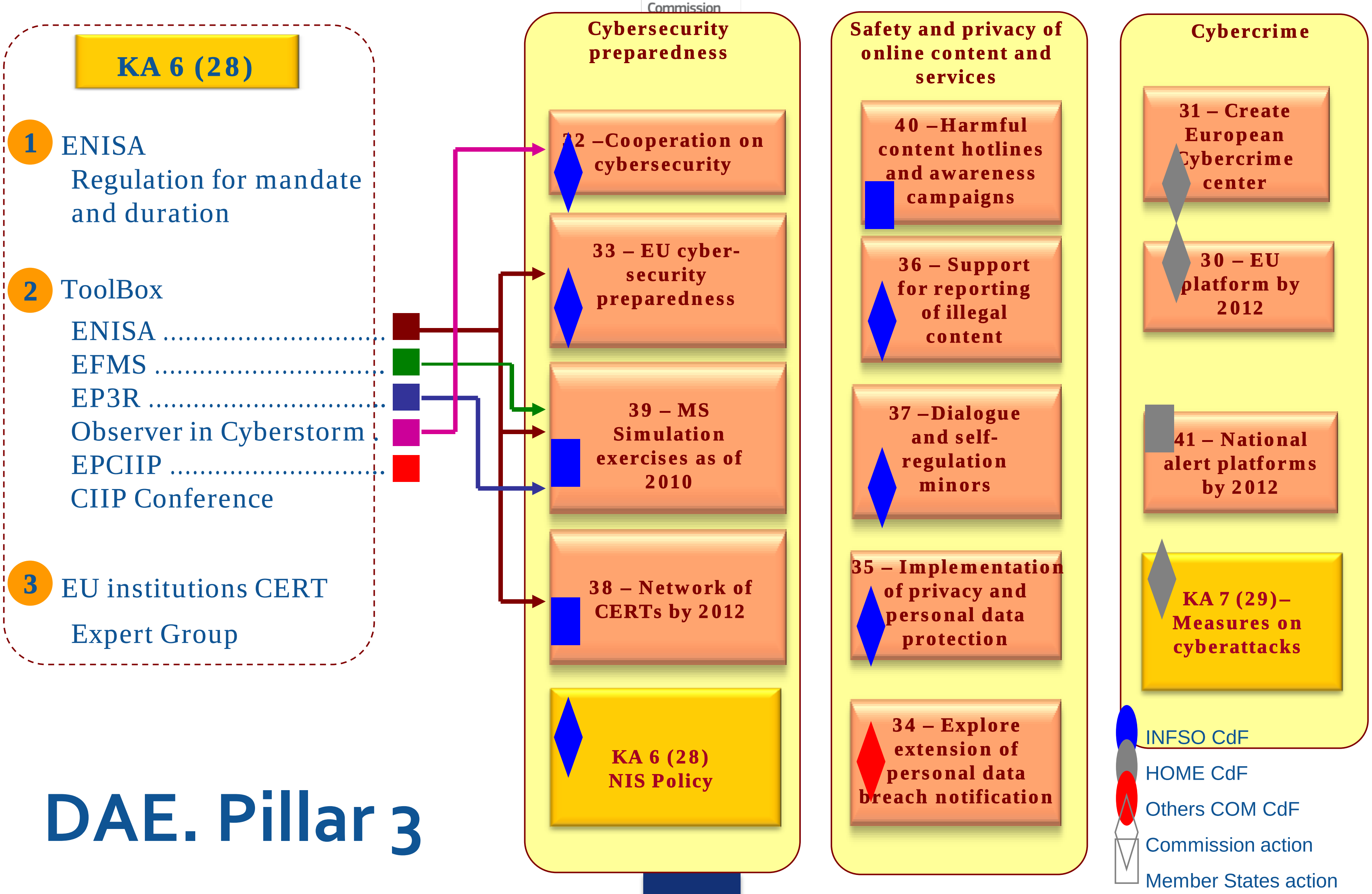
Develop a ***risk management*** *culture in the EU*

Focus on the role socio-economic ***incentives***

Promote ***openness, diversity, interoperability, usability, competition*** *as inherent security safeguards*

Boost a global ***collaborative policy*** *and* ***operational cooperation*** *across the EU, in particular on CIIP*

DAE. Pillar 3



KA 6 (28)

1 ENISA
Regulation for mandate and duration

2 ToolBox
ENISA ....
EFMS ....
EP3R ....
Observer in Cyberstorm .
EPCIIP ....
CIIP Conference

3 EU institutions CERT
Expert Group

Cybersecurity preparedness

- 32 –Cooperation on cybersecurity
- 33 – EU cyber-security preparedness
- 39 – MS Simulation exercises as of 2010
- 38 – Network of CERTs by 2012
- KA 6 (28) NIS Policy

Safety and privacy of online content and services

- 40 –Harmful content hotlines and awareness campaigns
- 36 – Support for reporting of illegal content
- 37 –Dialogue and self-regulation minors
- 35 – Implementation of privacy and personal data protection
- 34 – Explore extension of personal data breach notification

Cybercrime

- 31 – Create European Cybercrime center
- 30 – EU platform by 2012
- 41 – National alert platforms by 2012
- KA 7 (29)– Measures on cyberattacks

● INFSO CdF
● HOME CdF
● Others COM CdF
◇ Commission action
□ Member States action

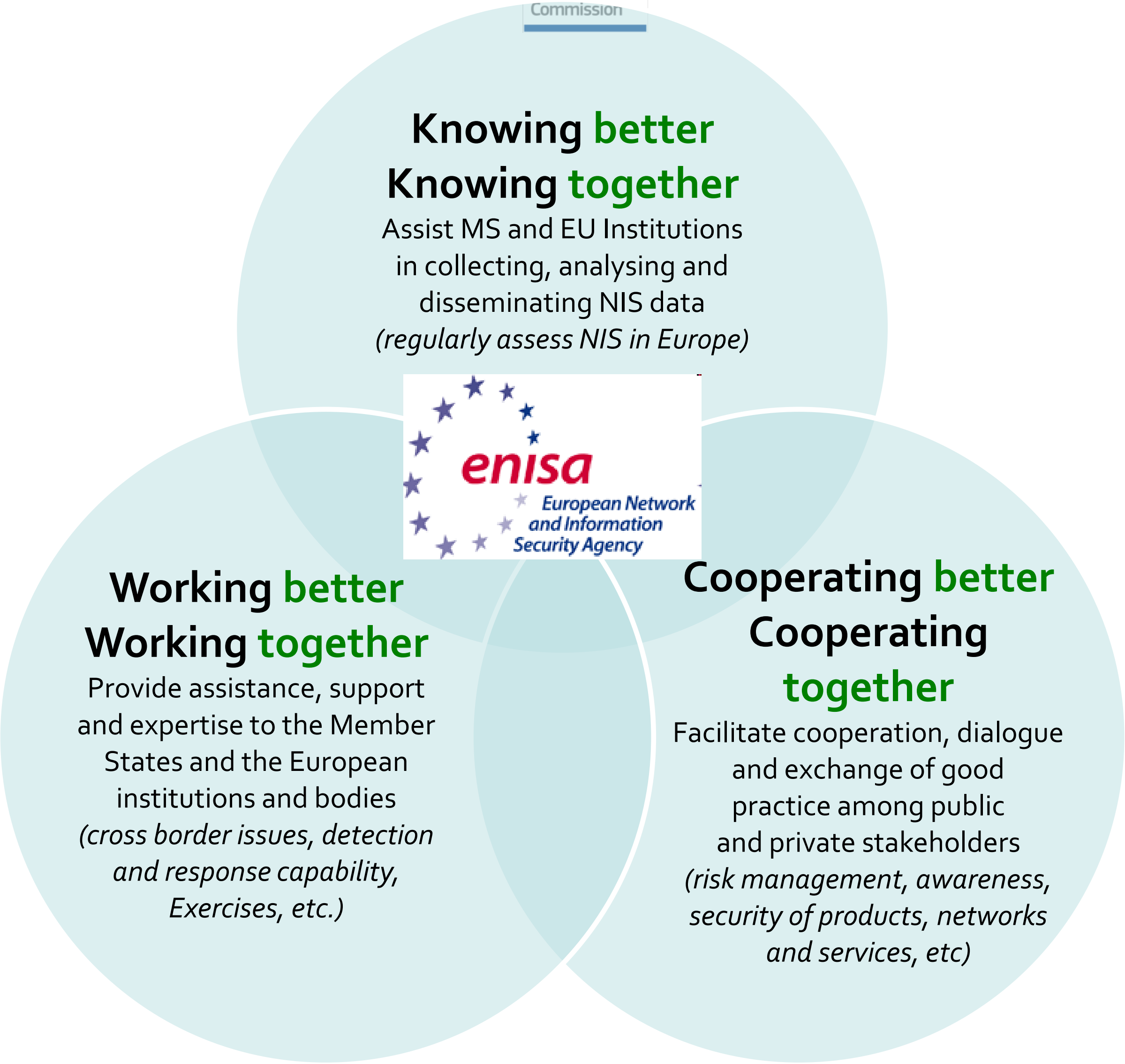
computer
emergency
response
team
CERT-EU
enisa
European Networ
and Information
Security Agen

- Critical Infrastructure Protection
- International Cooperation

computer emergency response team CERT-EU

Digital Agenda Key Action 6

*"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**."*



Knowing better
Knowing together

Assist MS and EU Institutions in collecting, analysing and disseminating NIS data *(regularly assess NIS in Europe)*

enisa
European Network and Information Security Agency

Working better
Working together

Provide assistance, support and expertise to the Member States and the European institutions and bodies *(cross border issues, detection and response capability, Exercises, etc.)*

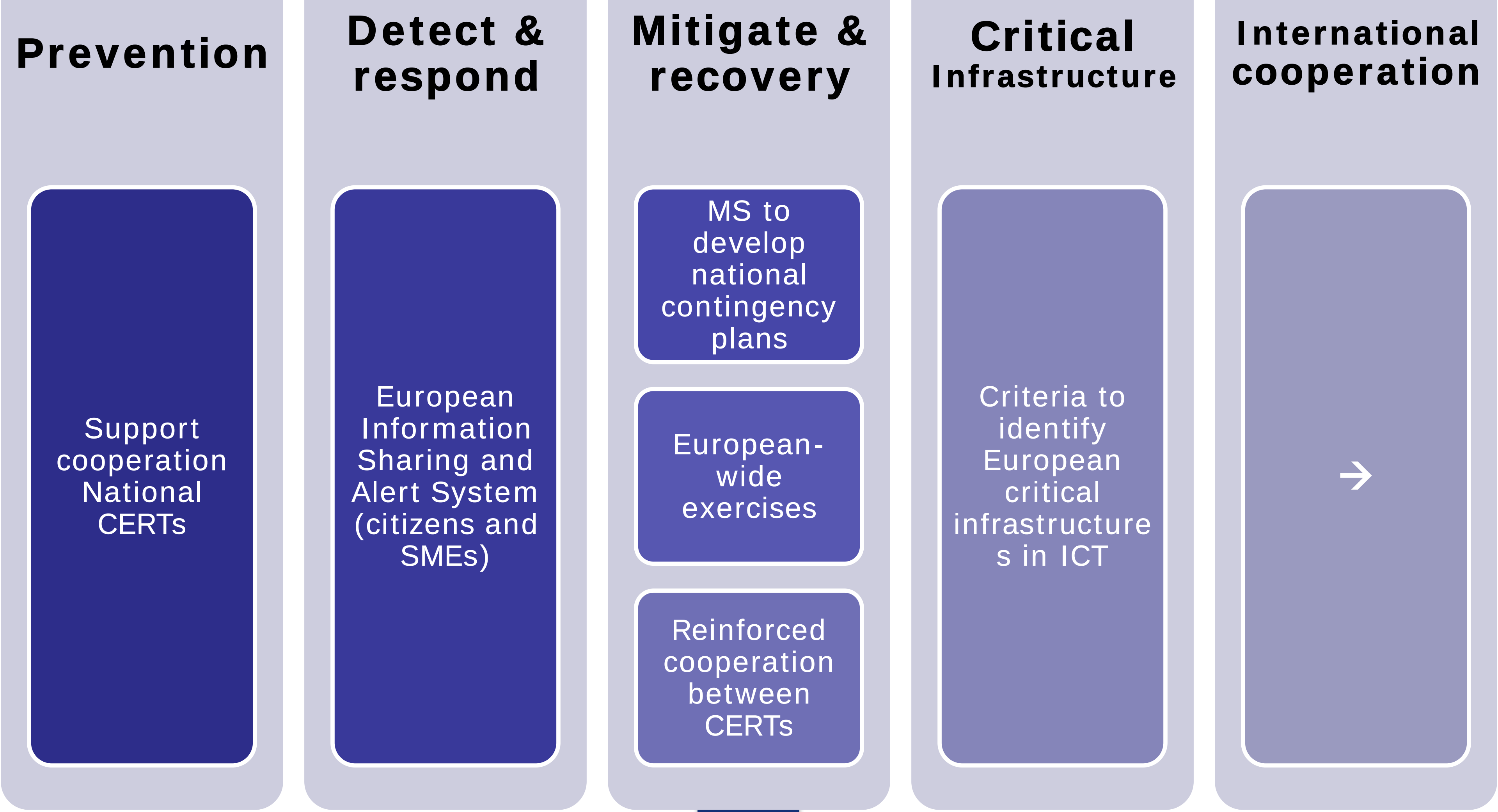
Cooperating better
Cooperating together

Facilitate cooperation, dialogue and exchange of good practice among public and private stakeholders *(risk management, awareness, security of products, networks and services, etc)*

European Commission

CIIP Communication. Actions

"Achievements and next steps: towards global cyber-security". COM(2011)163



Prevention

Support cooperation National CERTs

Detect & respond

European Information Sharing and Alert System (citizens and SMEs)

Mitigate & recovery

MS to develop national contingency plans

European-wide exercises

Reinforced cooperation between CERTs

Critical Infrastructure

Criteria to identify European critical infrastructures in ICT

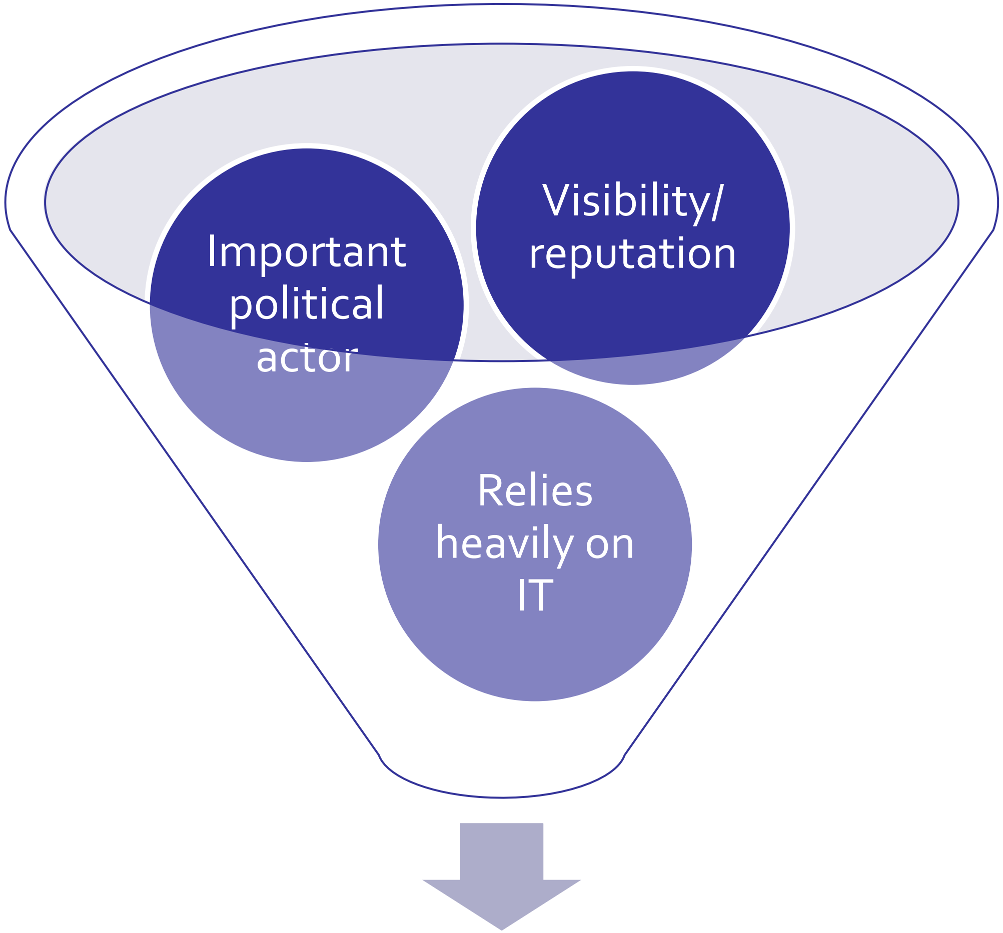
International cooperation

→

International Cooperation (IC)

Internet resilience and stability	•European principles and guidelines for Internet resilience and stability developed within EFMS
Global cyber-incident exercises	•7 EU MS took part in US exercise Cyber Storm III (EC and ENISA observers)
Internet resilience and stability	•Discuss and promote the principles at the international level – bilaterally and in multilateral fora (G8, OECD, NATO, OSCE, Meridian, ASEAN,...)
Global cyber-incident exercises	•EC and US are developing, under EU-US WG on Cyber-security and Cyber-crime, a common programme and roadmap towards joint/synchronised trans-continental cyber exercises in 2012/2013

Information security @ EC



Target for multiple threats

Policy framework

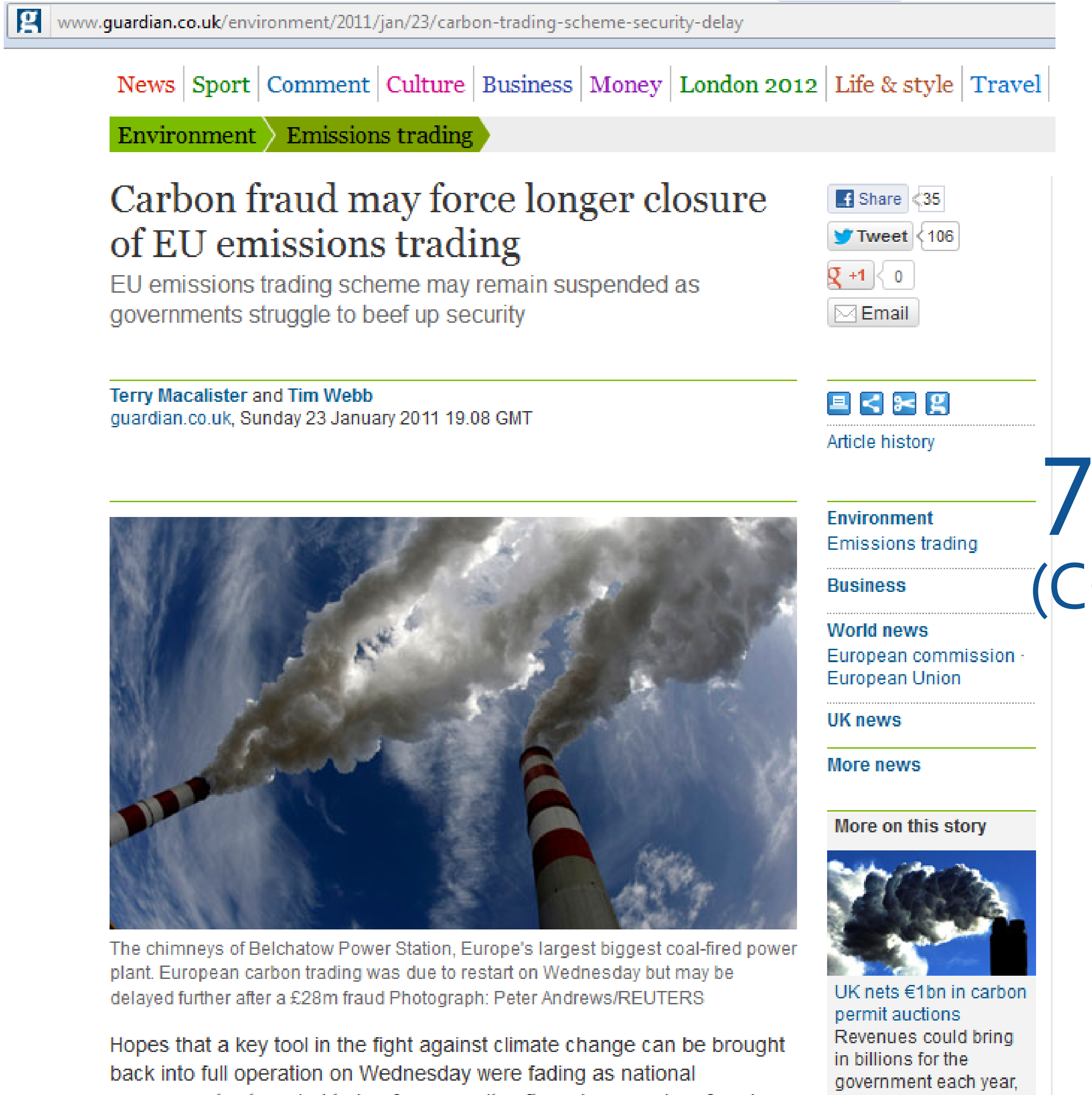
- *Regulation (EC)45/2001 on the protection of individuals with regard to the processing of personal data*
- *Commission provisions on security for classified information (2001/844/EC) to:*
  - **Define rules to follow (Legal requirements)**
  - **To exchange (classified) data between partners (Member states, Institutions, other governmental organizations), in confidence, since it is mandatory to share similar rules, mutually recognized**
- *Commission Decision C(2006)3602 concerning the security of information systems used by the European Commission*
- *EC internal security rules*
- *Similar regulation exists in the other institutions with equivalent principles (ex: Council Decision 5775/01)*

3. Experiences

European Commission

Climate Action
Energy for a Changing World

EU Emissions Trading Scheme



www.guardian.co.uk/environment/2011/jan/23/carbon-trading-scheme-security-delay

News | Sport | Comment | Culture | Business | Money | London 2012 | Life & style | Travel

Environment › Emissions trading

Carbon fraud may force longer closure of EU emissions trading

EU emissions trading scheme may remain suspended as governments struggle to beef up security

Share 35
Tweet 106
+1 0
Email

Terry Macalister and Tim Webb
guardian.co.uk, Sunday 23 January 2011 19.08 GMT

Environment
Emissions trading
Business
World news
European commission · European Union
UK news
More news

The chimneys of Belchatow Power Station, Europe's largest biggest coal-fired power plant. European carbon trading was due to restart on Wednesday but may be delayed further after a £28m fraud Photograph: Peter Andrews/REUTERS

Hopes that a key tool in the fight against climate change can be brought back into full operation on Wednesday were fading as national

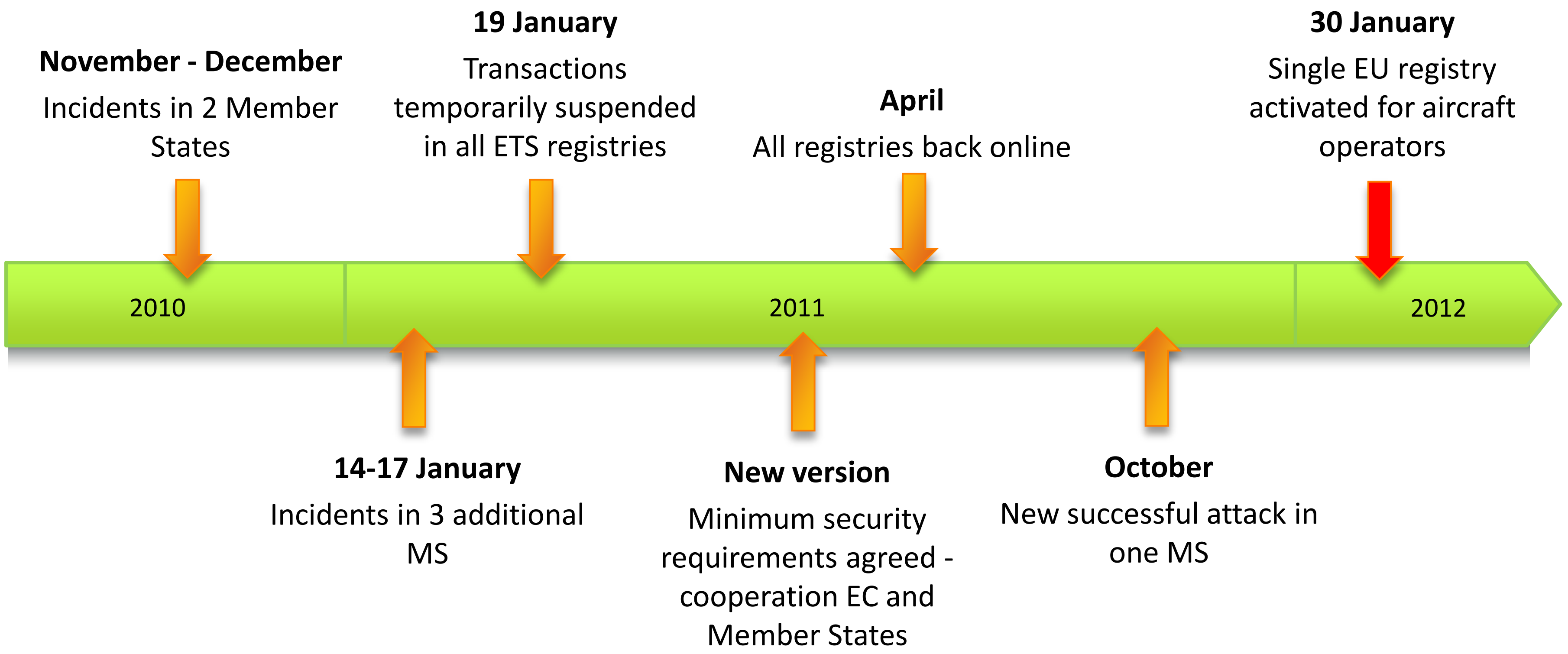
More on this story

UK nets €1bn in carbon permit auctions
Revenues could bring in billions for the government each year,

76,5 billion €

(CO_2 EU market value)

A rough ride?



November - December
Incidents in 2 Member States

14-17 January
Incidents in 3 additional MS

19 January
Transactions temporarily suspended in all ETS registries

New version
Minimum security requirements agreed - cooperation EC and Member States

April
All registries back online

October
New successful attack in one MS

30 January
Single EU registry activated for aircraft operators

ETS. Response

Two-factor authentication

"Out of band" confirmation of transactions

Introduction of a trusted account list

Obligatory 4-eyes principle

Transfers initiated only at some time periods

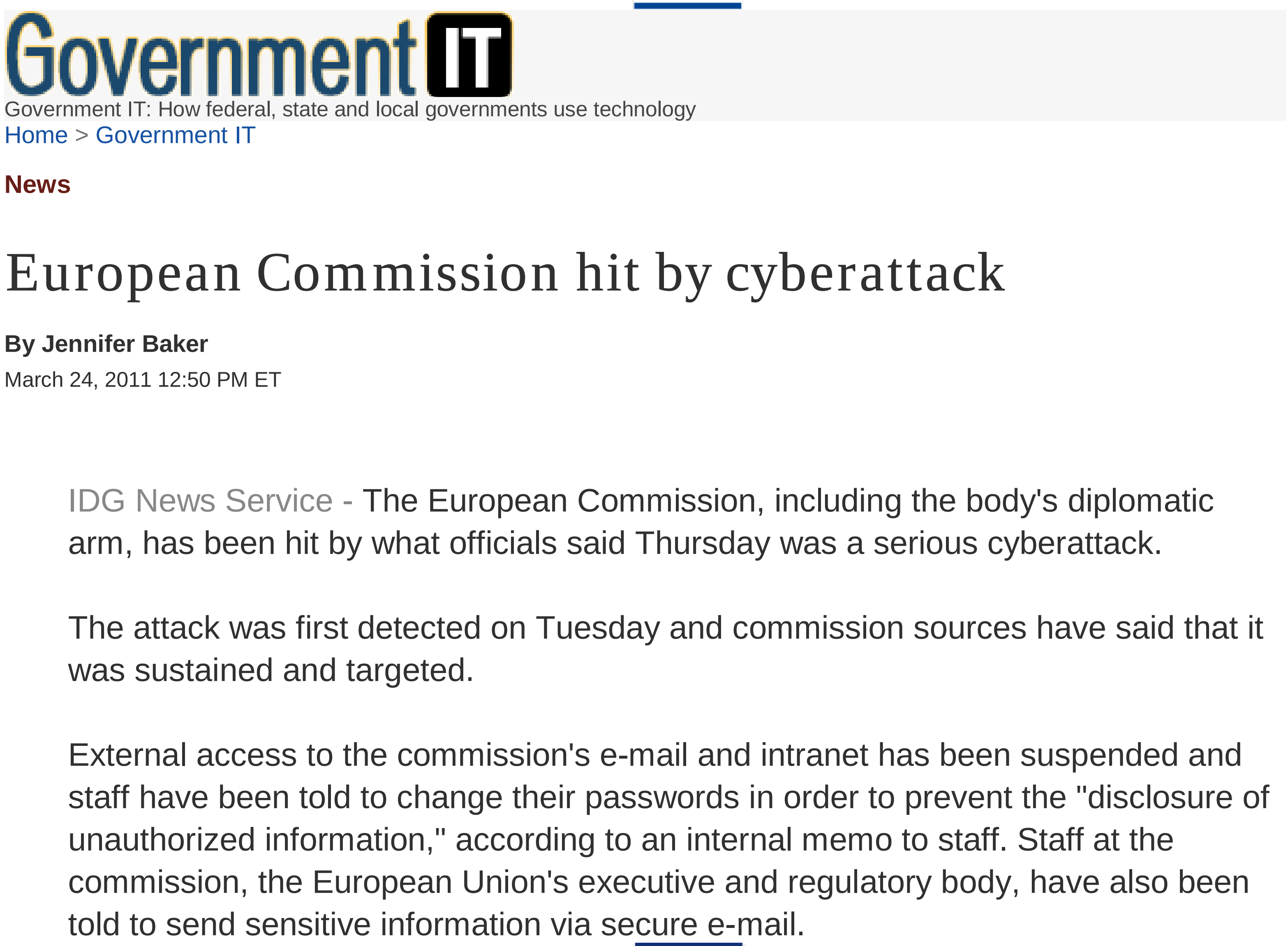
Strengthening of know your customer checks for account holders and their representatives

New account categories

New hosting infrastructure and services

- **Monitoring services**
- **Software security testing**
- **Security incident management procedure**

EC as a target
….. a real case



Government IT

Government IT: How federal, state and local governments use technology

Home > Government IT

News

European Commission hit by cyberattack

By Jennifer Baker

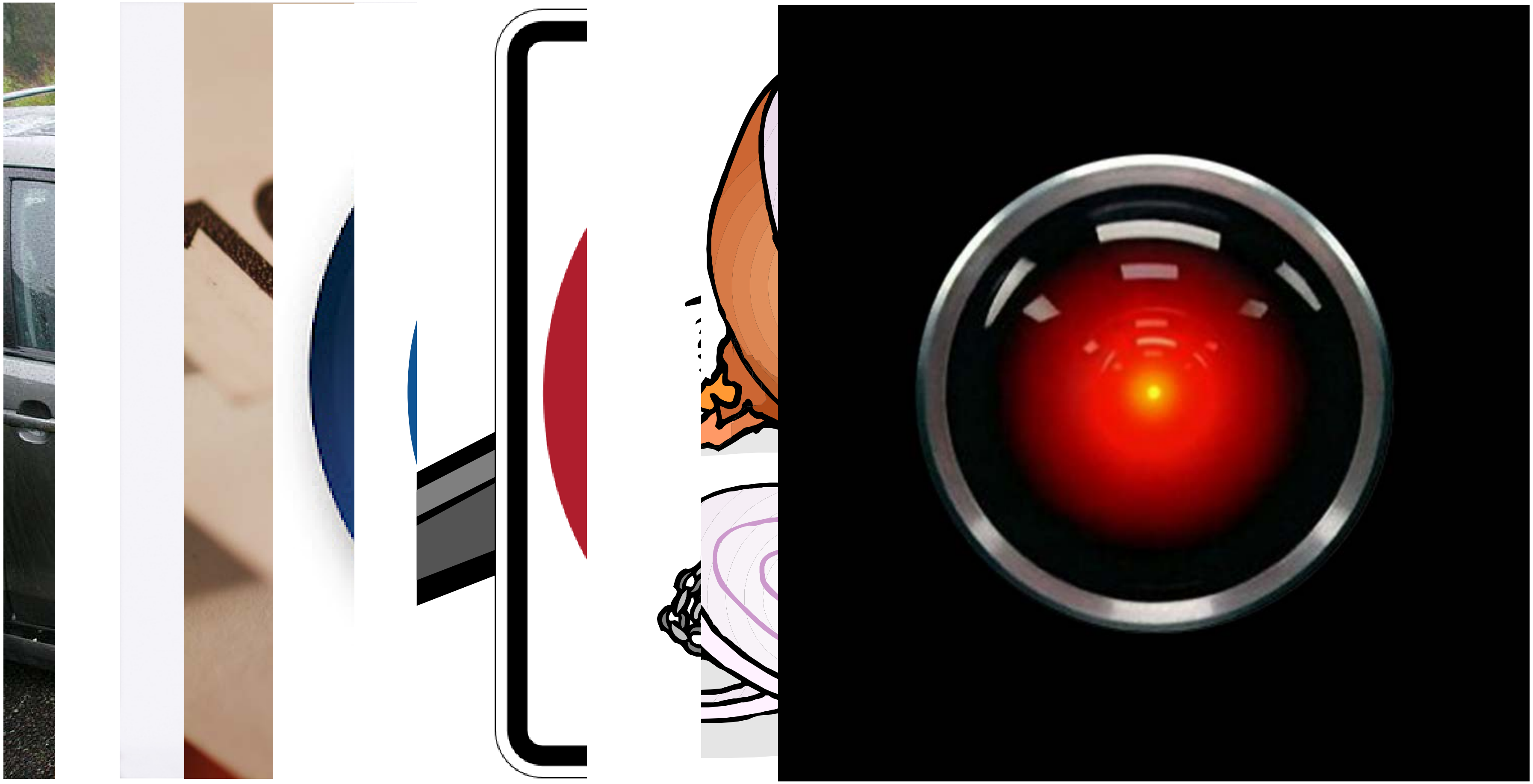
March 24, 2011 12:50 PM ET

IDG News Service - The European Commission, including the body's diplomatic arm, has been hit by what officials said Thursday was a serious cyberattack.

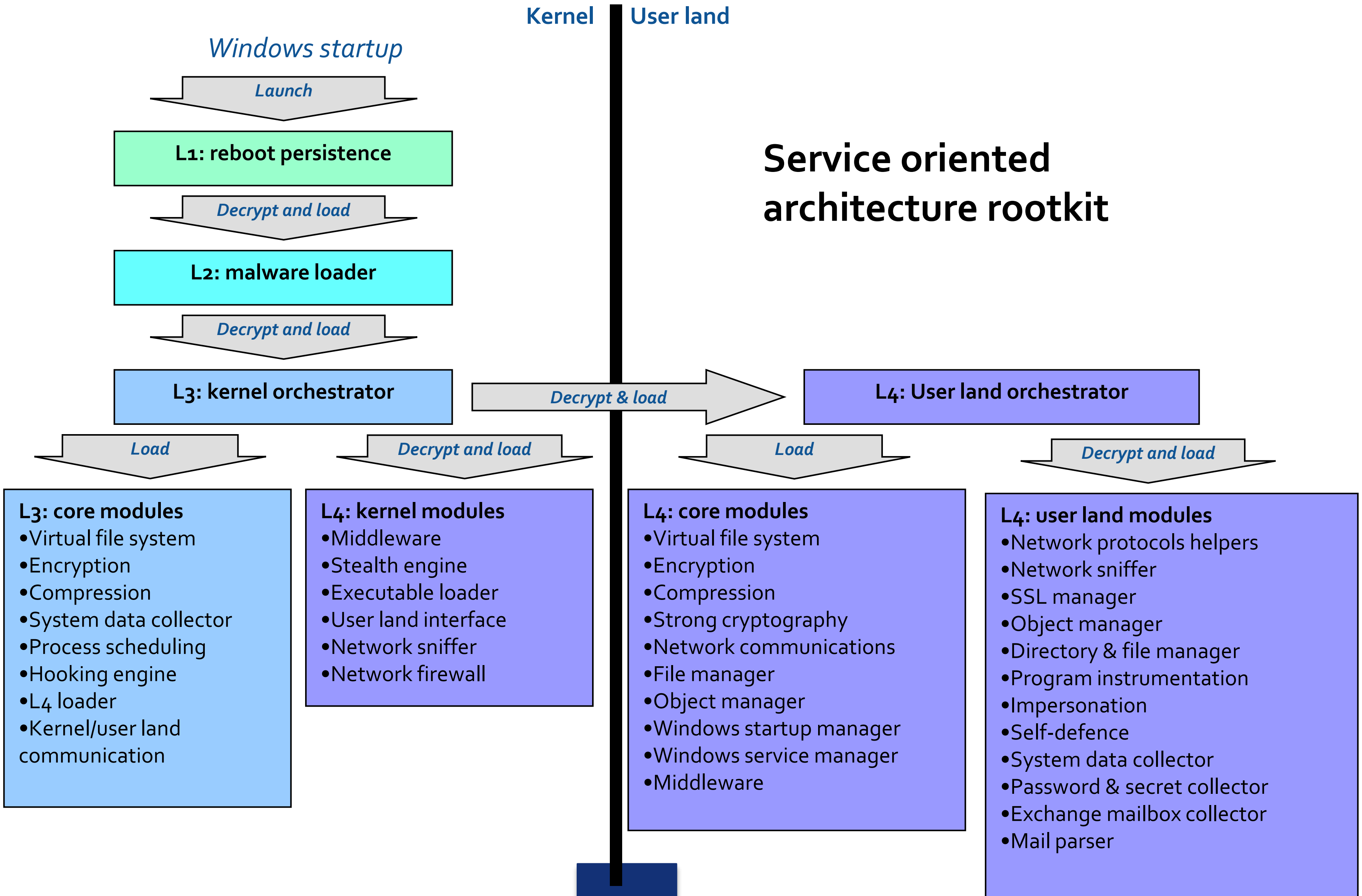
The attack was first detected on Tuesday and commission sources have said that it was sustained and targeted.

External access to the commission's e-mail and intranet has been suspended and staff have been told to change their passwords in order to prevent the "disclosure of unauthorized information," according to an internal memo to staff. Staff at the commission, the European Union's executive and regulatory body, have also been told to send sensitive information via secure e-mail.

A Real APT targeted at EC



Service oriented architecture rootkit



Kernel | User land

Windows startup

Launch

L1: reboot persistence

Decrypt and load

L2: malware loader

Decrypt and load

L3: kernel orchestrator

Decrypt & load

L4: User land orchestrator

Load

L3: core modules

- Virtual file system
- Encryption
- Compression
- System data collector
- Process scheduling
- Hooking engine
- L4 loader
- Kernel/user land communication

Decrypt and load

L4: kernel modules

- Middleware
- Stealth engine
- Executable loader
- User land interface
- Network sniffer
- Network firewall

Load

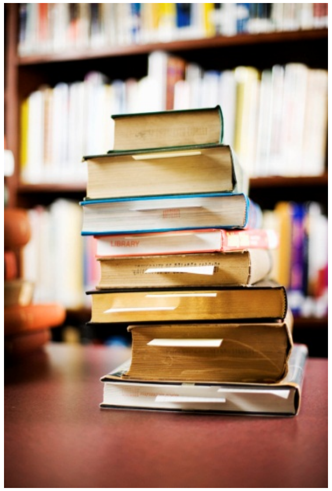
L4: core modules

- Virtual file system
- Encryption
- Compression
- Strong cryptography
- Network communications
- File manager
- Object manager
- Windows startup manager
- Windows service manager
- Middleware

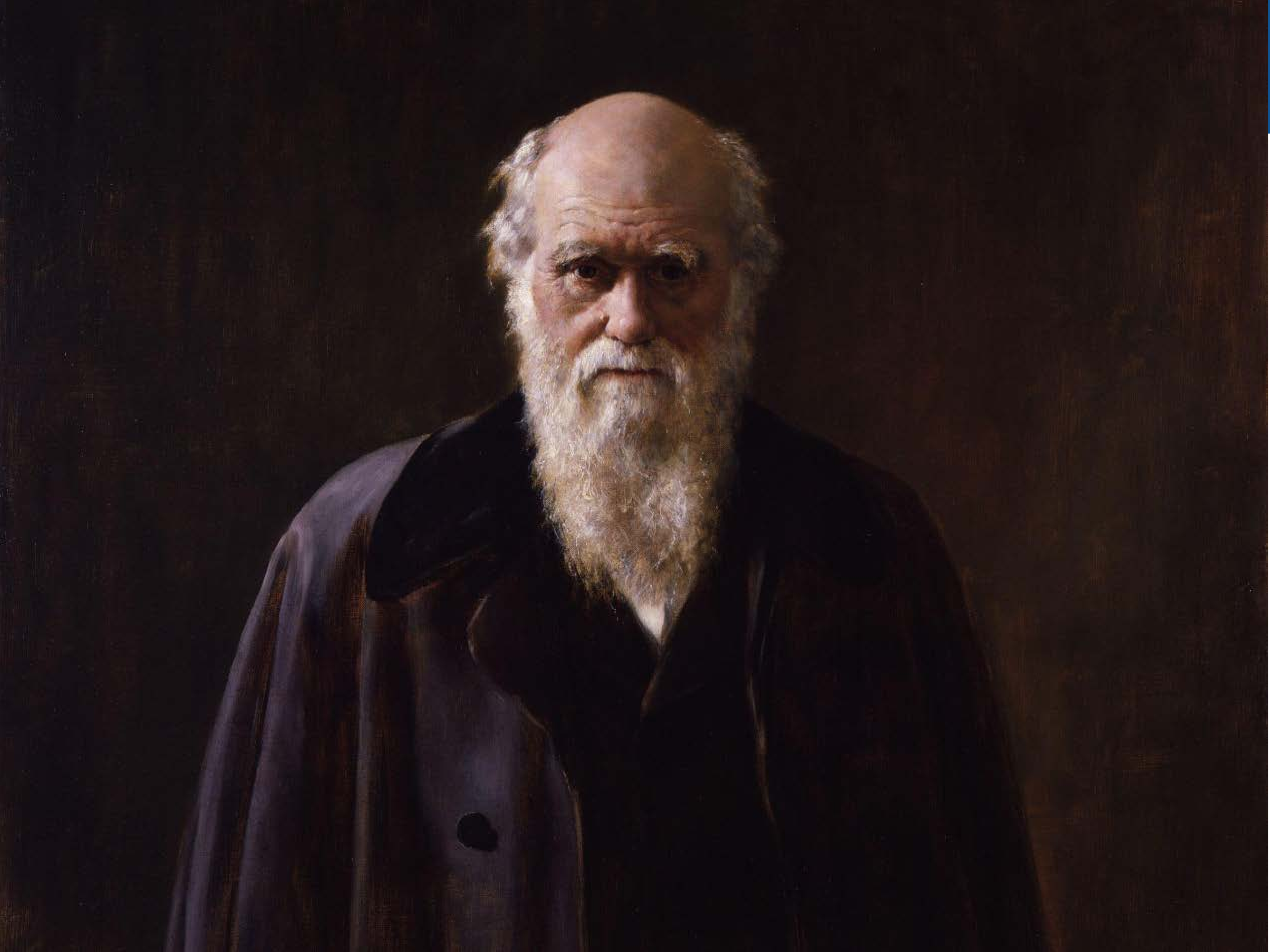
Decrypt and load

L4: user land modules

- Network protocols helpers
- Network sniffer
- SSL manager
- Object manager
- Directory & file manager
- Program instrumentation
- Impersonation
- Self-defence
- System data collector
- Password & secret collector
- Exchange mailbox collector
- Mail parser



What we have learnt
1. Strategy



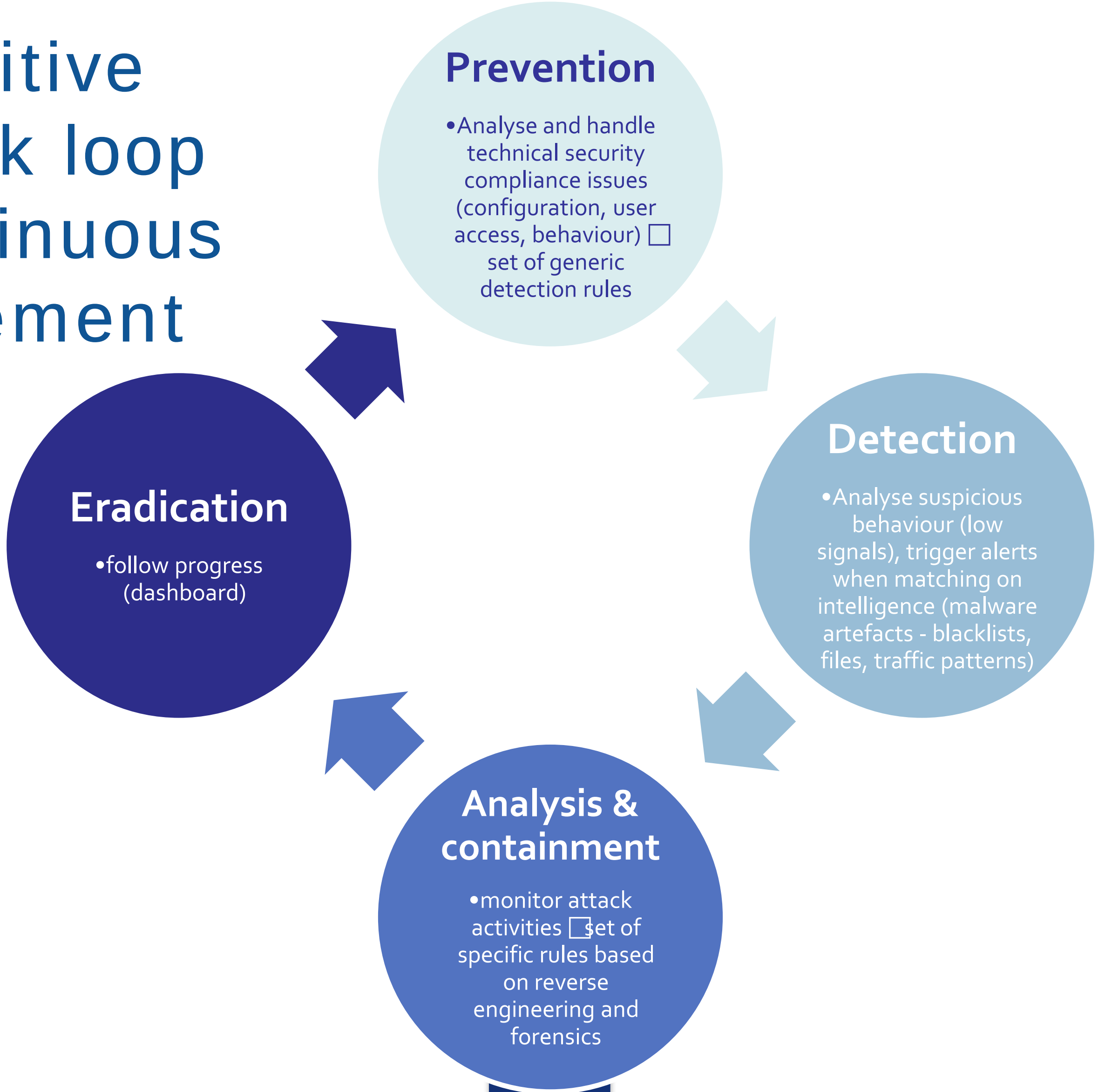
EC needs to constantly improve its security policy framework AND is implementing a cyber-defence program with several pillars:

- *Improve prevention measures dynamically based on lessons learnt from security incidents (post-mortem analysis is a key driver for security)*
- *Improve operational security capabilities*
  - **Vulnerability management program to proactively manage known vulnerabilities and weaknesses**
  - **Security monitoring → identify low signals of compromise**
  - **Incident response capabilities and cooperation (information exchange and assistance): live forensics, reverse engineering, networking**

And … get back to basics:

- *Review security posture (user rights, changes in configuration, deviations from baselines)*
- *Harden, harden, harden*
- *Improve privileged users practices*
  - **Use administration networks and hardened workstations for systems management**
  - **Use strong authentication for any privileged users activities**
- *Segregate critical infrastructre assets and monitor network and system behavior*
- *Use Secure coding practices (OWASP top 10 …)*

The positive feedback loop for continuous improvement



Prevention

- Analyse and handle technical security compliance issues (configuration, user access, behaviour) □ set of generic detection rules

Detection

- Analyse suspicious behaviour (low signals), trigger alerts when matching on intelligence (malware artefacts - blacklists, files, traffic patterns)

Analysis & containment

- monitor attack activities □set of specific rules based on reverse engineering and forensics

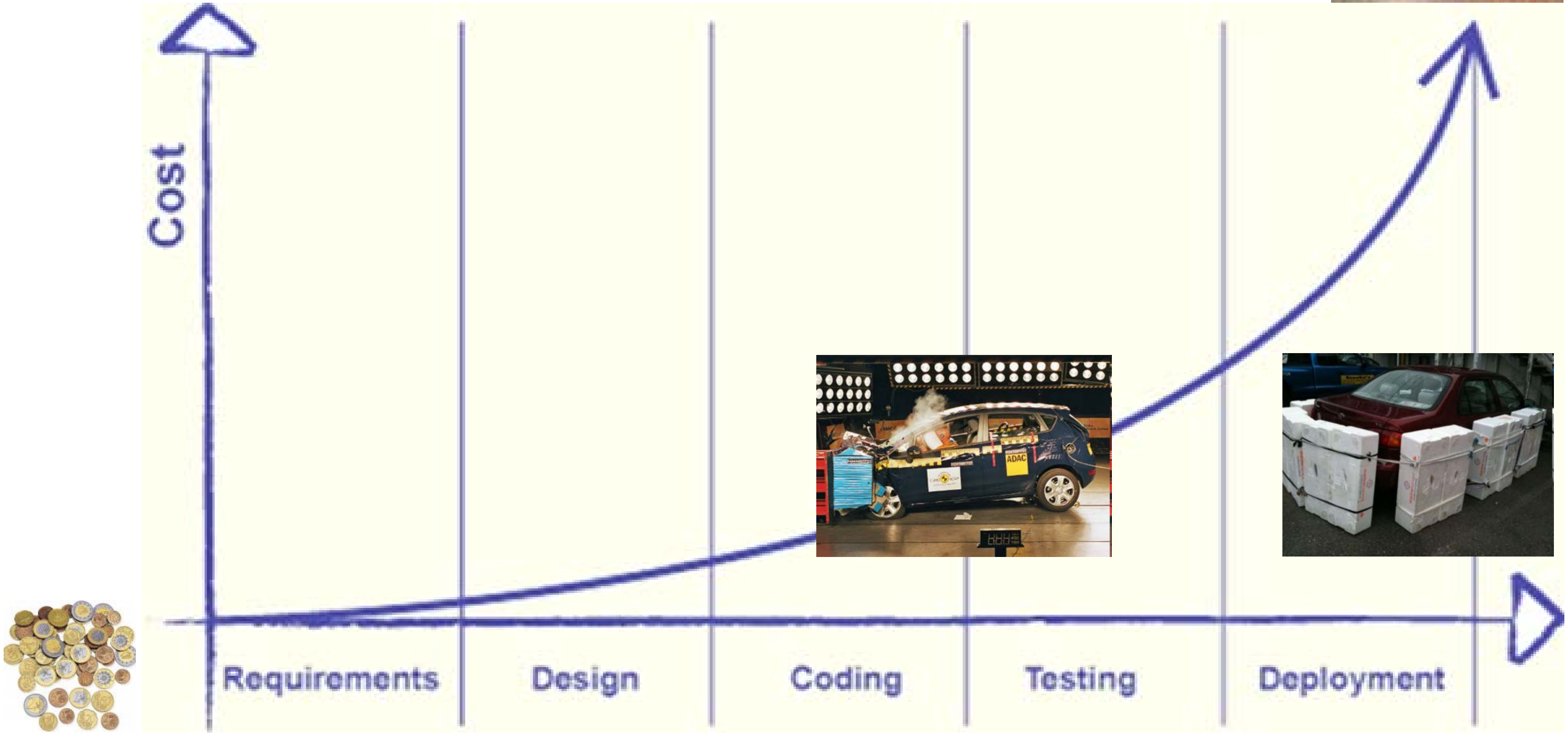
Eradication

- follow progress (dashboard)

Vulnerability management:

- *Vulnerability watch: Alerts and warnings + advisories performed by CERT-EU for most common technologies, completed internally*
- *Mandatory Vulnerability assessment activities before going in production (proportional to system criticality*
    1) White-box testing
    2) White-box + Black box testing
    3) White-box + Black-box + penetration testing
- *Regular testing of infrastructure components (vulnerability assessment + technical compliance)*

The sooner the better !



Peripheral security insufficient … Test Test Test … !

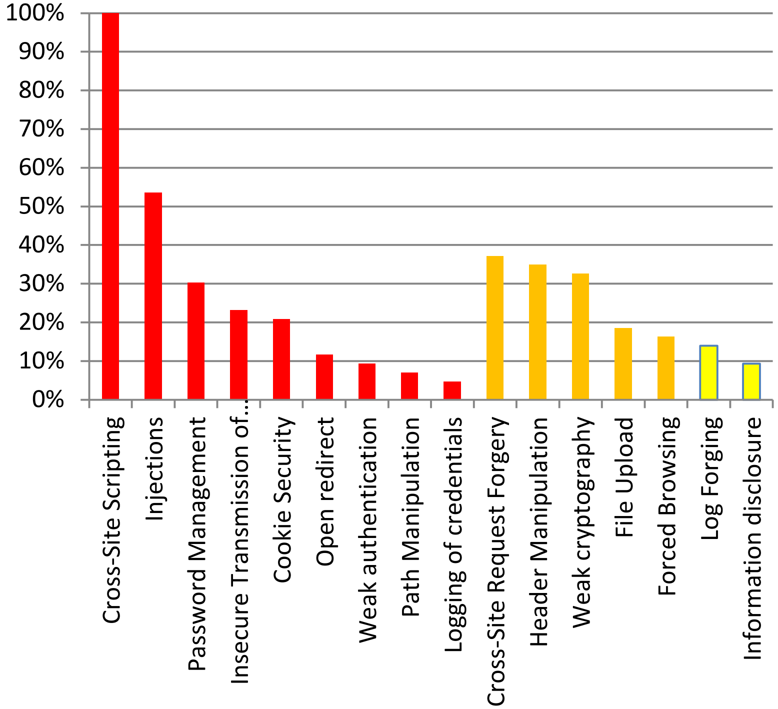
White Box tests (Static)

- Automatic source code scanning
- Manual revision to avoid false positives
- Support for all recommended languages (ex: Java, CF…)
- More vulnerabilities detected

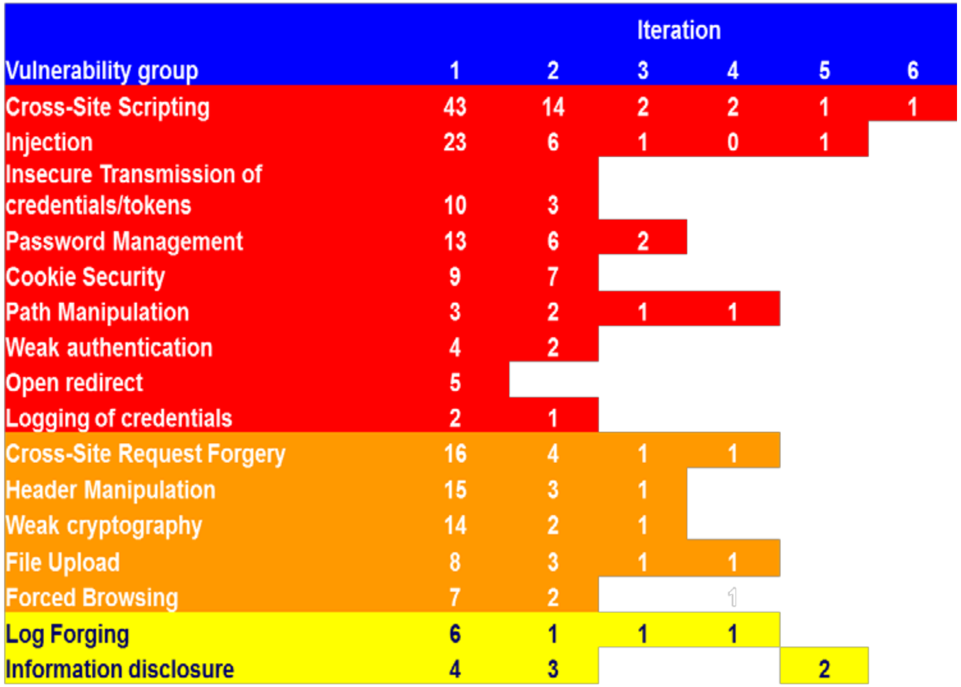
Black Box tests (Dynamic)

- No source code required, no specific language
- Requires working application target (closest to PROD)
- Automatic + manual testing
- Complement to White Box testing and Penetration tests

Feedback from the front…

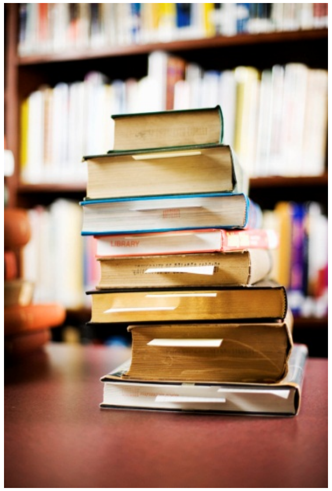


Findings on 1st ITERATION



	Iteration					
Vulnerability group	1	2	3	4	5	6
Cross-Site Scripting	43	14	2	2	1	1
Injection	23	6	1	0	1	
Insecure Transmission of credentials/tokens	10	3				
Password Management	13	6	2			
Cookie Security	9	7				
Path Manipulation	3	2	1	1		
Weak authentication	4	2				
Open redirect	5					
Logging of credentials	2	1				
Cross-Site Request Forgery	16	4	1	1		
Header Manipulation	15	3	1			
Weak cryptography	14	2	1			
File Upload	8	3	1	1		
Forced Browsing	7	2		1		
Log Forging	6	1	1	1		
Information disclosure	4	3			2	

Improvements over iterations



What we have learnt

2. React early

Security monitoring:

- *Focus on critical (infrastructure) assets*
- *Monitor security components at all levels (network layer, system and end-point protection, AV…)*
- *Focus on identifying low signals: changes in behaviour (network and system level)*
- *Use existing technologies (Proxies, IDS, NBA …) for cyber defence purpose (specific signatures/patterns)*
- *Establish strong synergies between Security Operations Centre and Incident Response Capability/Team*

Security Operations Centre

Technical

- **SIEM**
  - real-time analysis (filtering, correlation, analysis, reporting/dashboards)
  - Log preservation (forensics investigation)
- **Security solutions**
  - IDS, Network Behaviour Analysis, Vulnerability management, e-discovery, compliance …
- **Data feeds**
  - Critical assets (network, operating systems, Databases, middleware, applications, user identities)

Human

- Exchange of intelligence information with cyber-defence partners
- Information gathered during attacks, analysis (system and network forensics, reverse engineering, signatures)
- Content engineering skills (defining efficient detection scenarios)
- Technical and analytical skills

Security Incident Management:

- *Technical skills and toolkits (live-forensics, reverse engineering, and lot more)*
- *Personal skills (manage complex issues, many parallel activities, see the big picture, manage relations …over long periods …)*
- *Processes and procedures*
- *Cooperation and Networking with community (Trust, exchange of practices and information, assistance)*

The real challenges

- *Resources !!! Funding, increase it on demand …*
- *Scarcity of skilled resources*
- *Increasing complexity of (some) attacks*
- *Security IT landscape: cloud/virtualisation, mobility/BYOD*

Security is about risk management :
the challenge is to find the right balance