Towards a European strategy for cyberspace

Paul Timmers
European Commission
DG Communications Networks, Content and Technology

Agenda

1. The need for further EU action
2. Policies
3. Legislation
4. Networks and Organisations
5. EU-funded Research and Innovation
6. Some sectorial approaches
7. Overview on international activities
8. Overview on Privacy

Cybersecurity
The need for further EU action

- Economic and social benefits of the digital world and open Internet
- Risks, incidents and cybercrime on the rise
- Cross-border/global issue
- Need for a comprehensive EU vision

Cyber Attacks - recent examples

Bundestag: servers infected with malware

-> rebuilding of nearly all IT systems

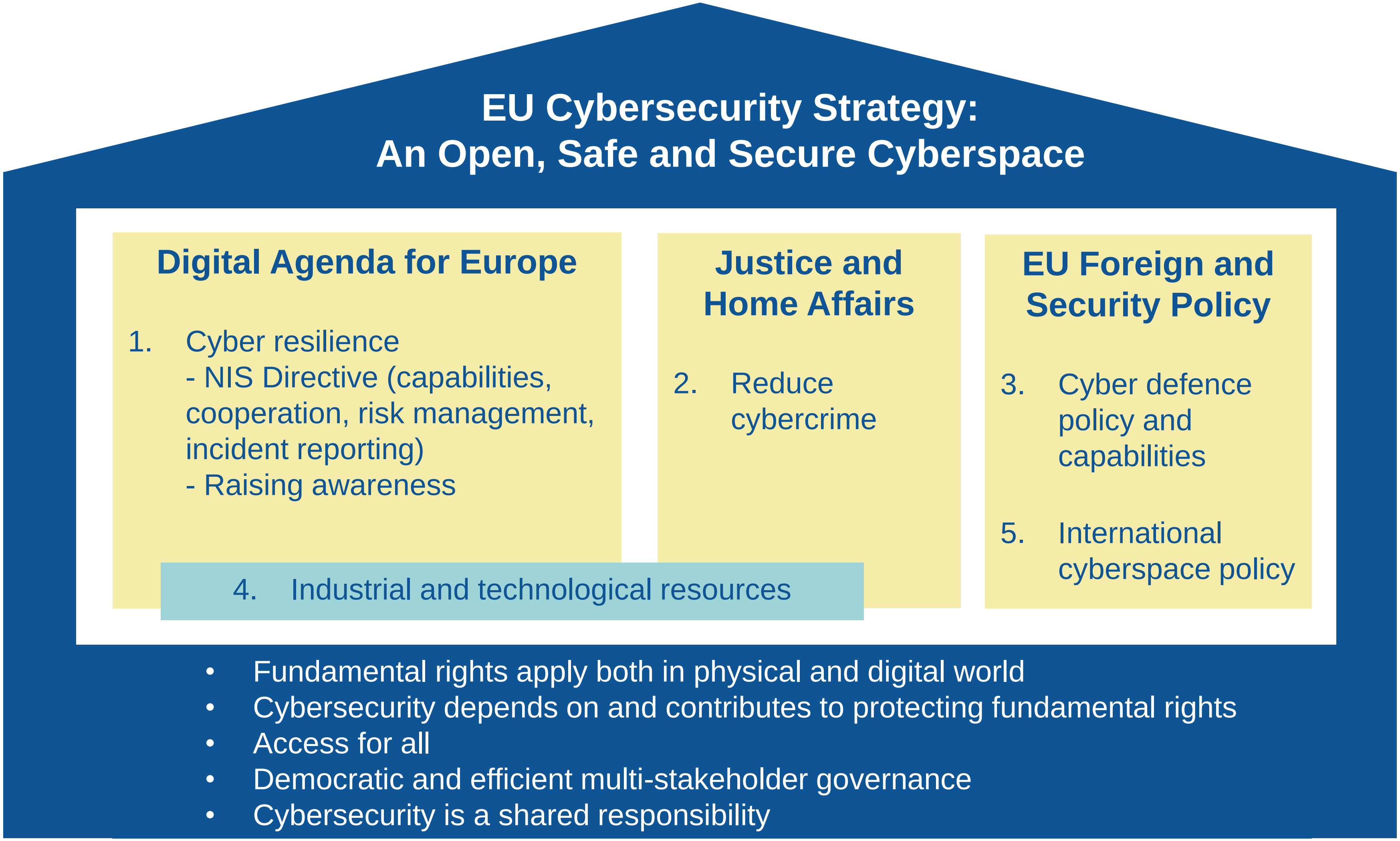
TALKTALK: "significant cyber-attack" -> 4+ million customers' data potentially accessed

TalkTalk

Key EU Objectives and Actions

Increase capabilities & cooperation	NIS Directive - NIS platform – ENISA - CEF
Strengthen EU Cybersecurity industry	Strengthening industrial capabilities– cPPP - ≈500M in H2020
Mainstream cybersecurity in EU policy	Cooperation on new policy initiatives – Sectorial cybersecurity strategies

Policies



EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace

Digital Agenda for Europe

1. Cyber resilience
   - NIS Directive (capabilities, cooperation, risk management, incident reporting)
   - Raising awareness

Justice and Home Affairs

2. Reduce cybercrime

EU Foreign and Security Policy

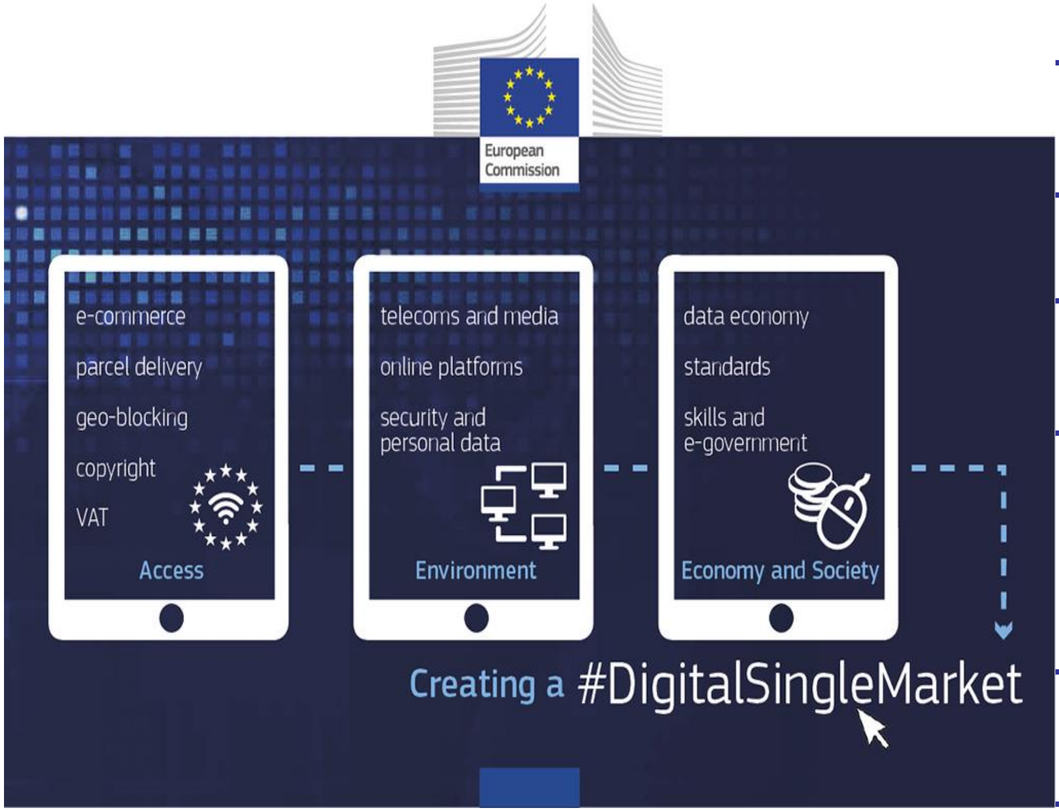
3. Cyber defence policy and capabilities

5. International cyberspace policy

4. Industrial and technological resources

- Fundamental rights apply both in physical and digital world
- Cybersecurity depends on and contributes to protecting fundamental rights
- Access for all
- Democratic and efficient multi-stakeholder governance
- Cybersecurity is a shared responsibility

The Digital Single Market Strategy

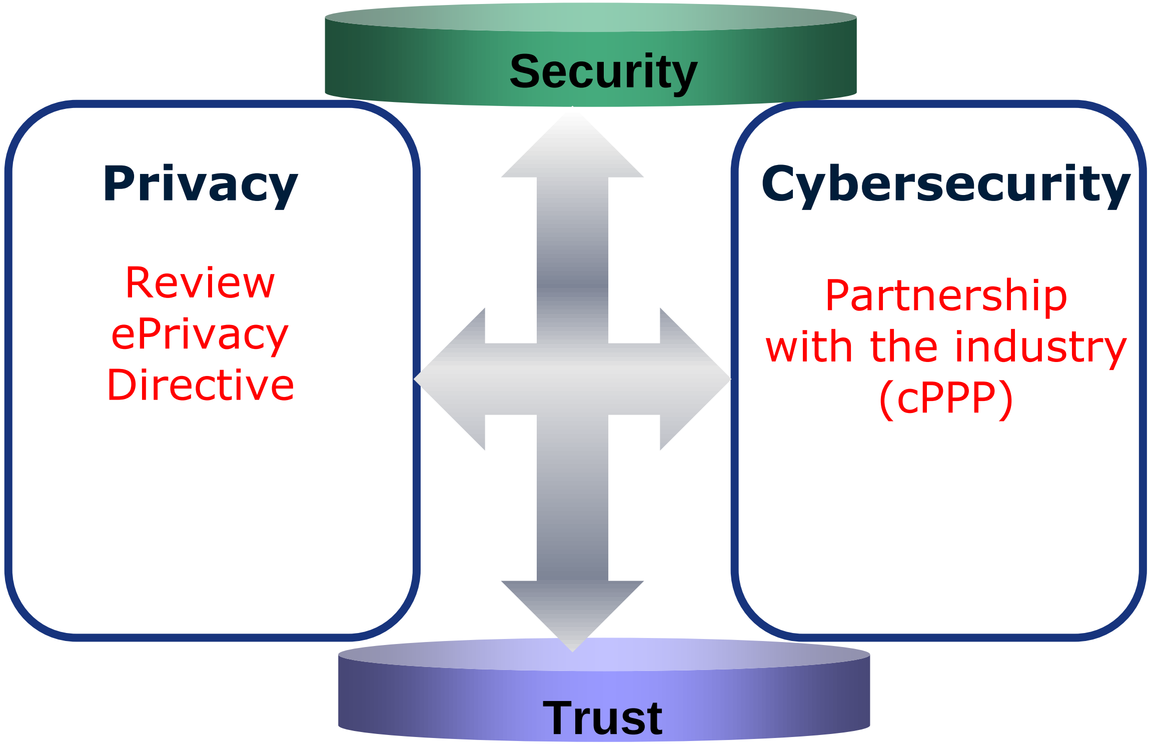


Adopted on 6th May 2015

16 initiatives to be delivered by 2016

Completing DSM could contribute € 415 billion per year to Europe's economy.

Trust and Security in the DSM



Security

Privacy

Review ePrivacy Directive

Cybersecurity

Partnership with the industry (cPPP)

Trust

The contractual Public Private Partnership on Cybersecurity

The context

A global opportunity

The global CS market is growing very fast

- In 2013 the global cybersecurity market was worth $65.9 billion

- It is expected to grow to $80-120 billion by 2018.

The EU context

The EU CS market is highly fragmented

- Historical dependence of EU companies on national public procurement
- Existence of different NIS policies across Member States
- Lack of standards and sound mechanisms of certification
- Lack of trust for cross-border purchase

European Commission

The contractual Public Private Partnership on Cybersecurity

Overall Aim

- ❖ Overcome fragmentation of R&D funding
- ❖ Encourage supply of more secure solutions and stimulate their take-up

Actors

Cybersecurity industry in Europe, producers of components and equipment, operators of critical infrastructures and users.

Resources

EU (including R&D – H2020), national, regional and private efforts and resources.

The contractual Public Private Partnership on Cybersecurity

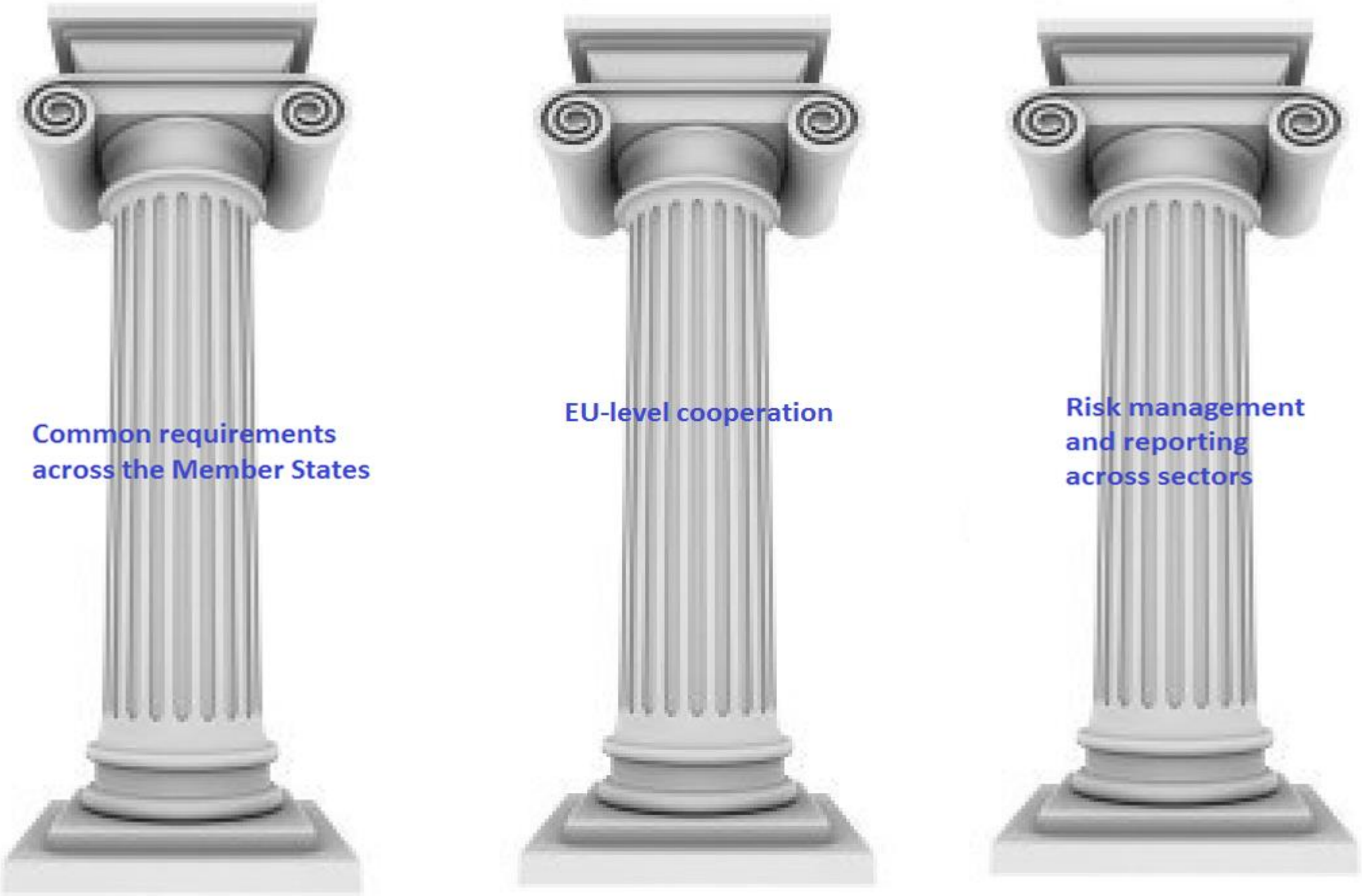
The cPPP will help:

- leverage innovation to stimulate competitiveness
- move from world-class research to market-driven innovation
- mobilize public and private resources against a joint strategic agenda
- ensure a sustained supply of innovative cybersecurity products and services

Launch of public consultation – December 2015
Launch of cPPP – mid 2016

Legislation

Proposal for a directive on Network and Information Security (NIS)



Common requirements across the Member States

EU-level cooperation

Risk management and reporting across sectors

Proposal for a Directive on NIS Key elements (1/3)

1) Capabilities: Common NIS requirements at national level

- NIS strategy and cooperation plan
- NIS competent authority
- Computer Emergency Response Team (CERT)

Proposal for a Directive on NIS
Key elements (2/3)

2) Cooperation: NIS competent authorities to cooperate within a network at EU level

- Early warnings and coordinated response
- Capacity building
- NIS exercises at EU level
- ENISA to assist

Proposal for a Directive on NIS
Key elements (3/3)

3) **Risk management** and **incident reporting** for:

- Energy – electricity, gas and oil
- Credit institutions and stock exchanges
- Transport – air, maritime, rail
- Healthcare
- Internet enablers

Proposal for a Directive on NIS Next Steps

- Political agreement by the end of 2015
- Adoption in early 2016
- Transposition into national laws *asap*

European Commission

Networks and Organisations

The NIS Platform

- A key action of the EU Cybersecurity Strategy
- Identify - develop incentives to adopt good practices
- Draw from working practices, incl. relevant standards
- Process-related and technology-neutral
- Incentives for voluntary adoption
- Cross-cutting / horizontal approach
- Focus on SMEs

The NIS Platform – Working Groups

- **WG1: Risk management**
- **WG2: Information sharing and incident notification**
- **WG3: Secure ICT Research and Innovation**

The NIS Platform – State of play

- The platform finalised a first set of guidelines that will help all kinds of organisations to address risk management and information sharing.

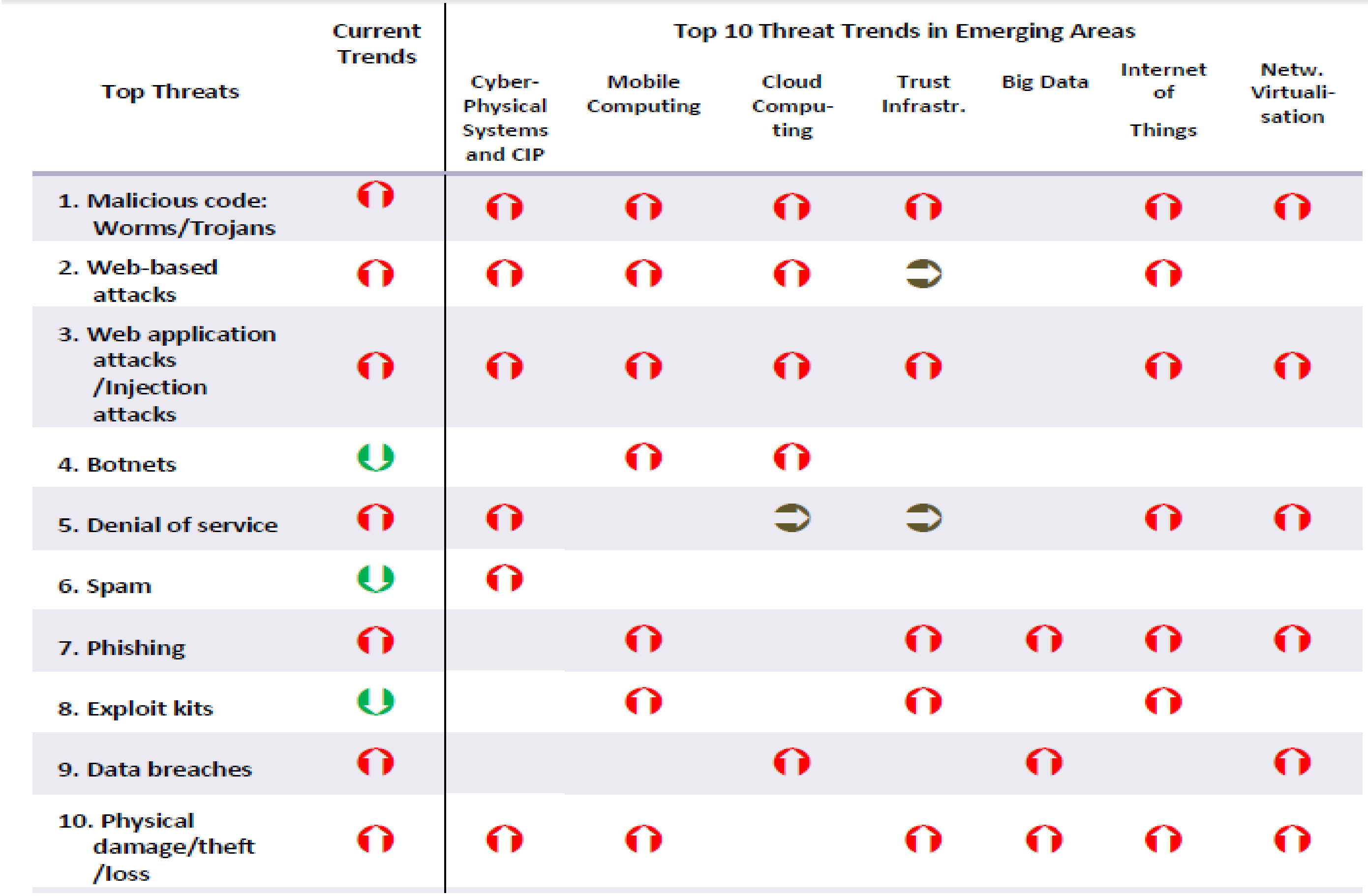
- The platform delivered the Strategic Research Agenda, based on the state of the art of secure ICT and NIS innovation and businesses cases.

- The Strategic Research Agenda provides input to the secure ICT R&I agenda at national and EU level, including H2020

ENISA

- Set up in 2004 to contribute to ensuring a high level of network and information security within the EU.
- It helps the EC, the Member States and the business community to address, respond and especially to prevent NIS problems.
- Some key deliverables: training to support MS capabilities; yearly threat landscape report; pan-European cyber exercises; Cybersecurity Month awareness campaign
- According to NIS Directive, ENISA will gain new responsibilities (e.g. provide the secretariat to the CSIRTs network)

ENISA's Threat Landscape Report 2014



Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑

CERT-EU

- **CERTs responds to cyber incidents but also provide a wealth of services (technical support; information sharing) to their constituencies.**

- **The EU institutions, agencies and bodies have their own CERT since 2012 to provide effective and efficient response to information security incidents and cyber threats.**

- **CERT EU cooperates with other CERTs in the Member States and beyond as well as with specialised IT security companies.**

EU-funded Research and Innovation

7th Framework Programme
Competitiveness and Innovation Programme

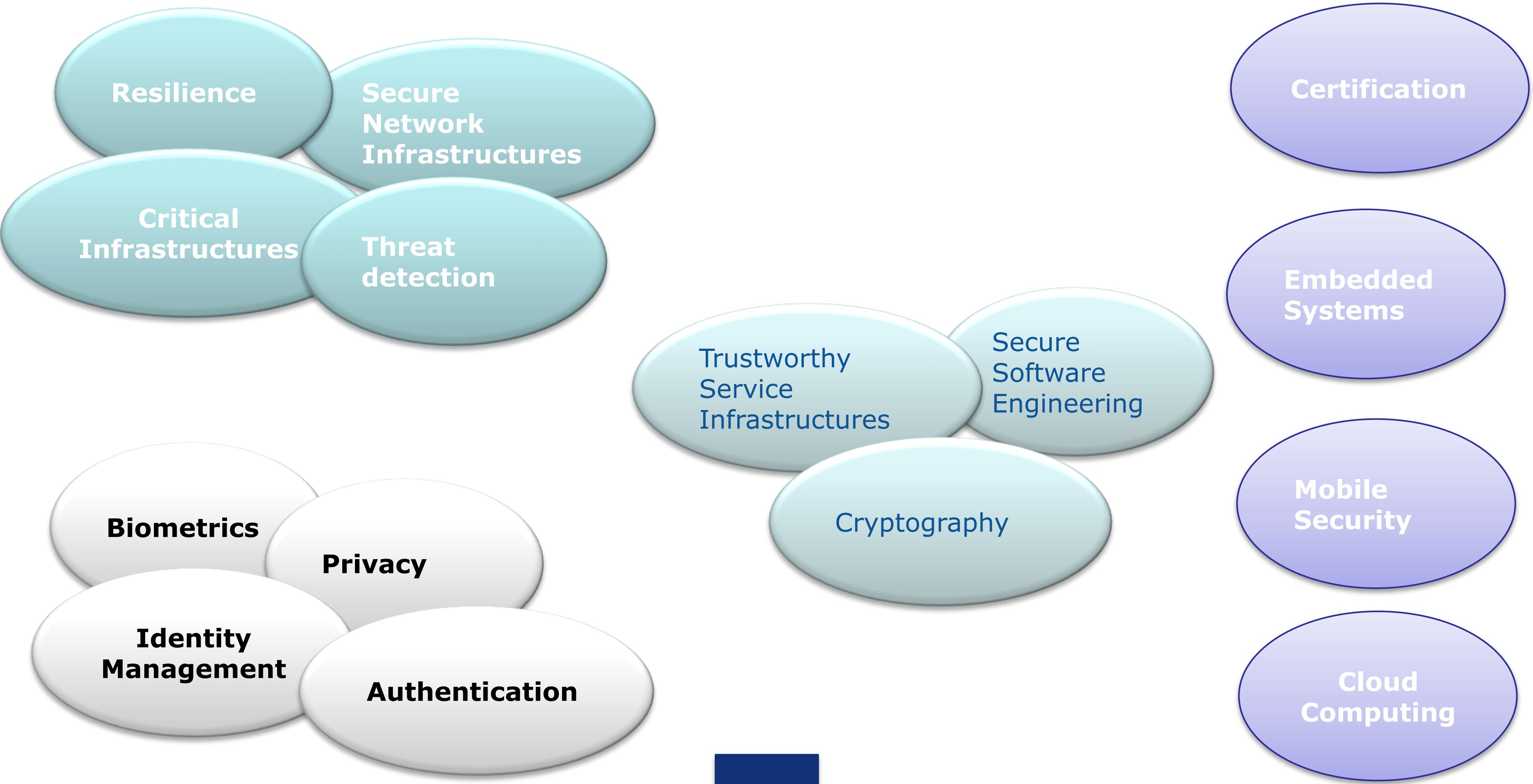
In the 2007-2013 financial period 9 calls in total

101 Projects for 334 M€ EU funding

SEVENTH FRAMEWORK
PROGRAMME

cip competitiveness and innovation
framework programme
2007–2013

FP7 and CIP- Topics



Resilience

Secure Network Infrastructures

Critical Infrastructures

Threat detection

Trustworthy Service Infrastructures

Secure Software Engineering

Cryptography

Biometrics

Privacy

Identity Management

Authentication

Certification

Embedded Systems

Mobile Security

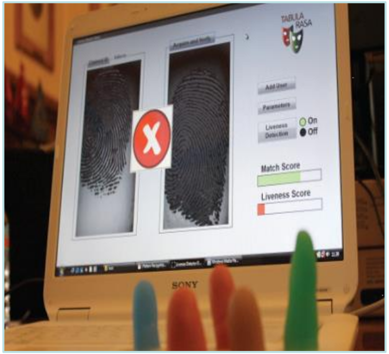
Cloud Computing

What stays: success stories

European support to:

- **Spin-offs and Start ups**
- **Academic Research**
- **Support European Champions to test new waters**
- **Better protection of users**

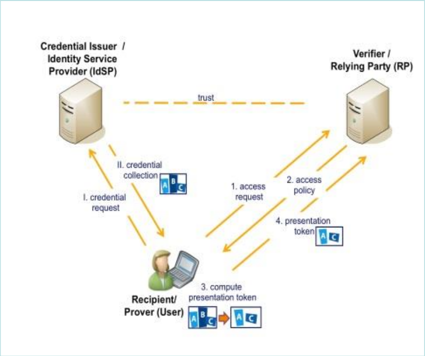
Project with market results



TABULA RASA developed countermeasures to improve security of biometric systems

CACE delivered a toolbox for cryptography software development

SPaCIoS delivered a tool for Internet services security certification, verification and testing.



ABC4Trust: developed a system that puts users' electronic identities in their hands.

Full stories: http://bit.ly/fromLab2Market

Challenges for H2020

- **Deployment – moving from world-class research to innovation on the markets**
- **Bring European products and services on a global market**
- **strengthen our cybersecurity industry**
- **Providing support for users and build stronger trust in ICT**
- **Address cybersecurity issues in application fields (e.g. mhealth)**

H2020

- About 500M€ for cybersecurity& privacy in Societal Challenges (SC) and Leadership in enabling and industrial technologies (LEIT)

- SC7 ("Secure societies") + "digital focus area" in SC1 (ehealth), SC3 (energy), SC4 (transport), and SC6 (public administration).

- LEIT: projects on dedicated technology-driven digital security building blocks +security integrated as a functional requirement in IoT, 5G, Cloud.

Some sectorial approaches

Automotive

- Reference for connected and (future) driverless cars: Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems
- Europe also supports the Cooperative Intelligent Transport system (C-ITS) initiative through the Connected Europe Facility Regulation (CEF) to boost network connectivity.
- The C-ITS expert group on cybersecurity will develop voluntary certification and audit schemes to ensure that new cars have built in state of the art cybersecurity solutions.

Aviation

- The Aviation Safety regulation EU 300/2008 is under revision to include cybersecurity as an essential element.
- The new regulation will include provisions for cyber threat information sharing. The existing Safety Information Bulletin (SIB) will in the future also be used to disseminate critical cybersecurity threat information.
- The European Aviation safety Agency considers the certification for cybersecurity for new equipment on board of aircrafts.

Energy (1/2)

- **Ensuring resilience of the energy supply system against cyber-threats is crucial as wide-spread use of IT and data traffic becomes the foundation for the functioning of infrastructures underlying the energy system.**

- **Increased efficiency in supply services comes with increased exposure to cyber-attacks with the potential to impair confidentiality, integrity, availability of the system.**

Energy (2/2)

- **Legislation: Directive 2009/72/EC covers the rules for the internal energy market.**

- **The Commission Recommendation 2012/14/EU on the preparations of for the roll-out of smart metering systems address data protection and security.**

- **Policy: the European Commission as created an Energy Expert Cybersecurity Platform to cover all cyber threats impacting the energy sector.**

Overview on international activities

What we aim for

- **A country and interlocutor-tailored DSM outreach programme**
- **Regulatory adoption or approximation of the EU acquis and mutual recognition agreements**
- **Market access to safeguard and promote EU investments and a global level playing field**
- **Promotion of research cooperation and reciprocity of access to research programmes**
- **The creation of exchange networks & coalitions to share and gain knowledge, shape global policies.**

Bilateral and multilateral cooperation

- **Bilateral dialogues (together with EEAS) with many countries, in particular with US, Brazil, South Korea, China and India.**

- **Multilateral organisations: ITU (spectrum, telecommunications regulations, standards, and development), OECD (digital economy), ICANN (Internet governance), Council of Europe (Media and Internet governance), WTO/WIPO (trade, copyright) and various others.**

European Commission

Overview on Privacy

ePrivacy Directive

- A framework governing the protection of privacy and personal data in the electronic communications sector.

- It specifies and complements the EU Data Protection Directive (currently under review) to address the specificities of this sector.

- Main provisions: the principle of confidentiality of communications; rules to limit the use of traffic and location data for purposes unrelated to the provision of the service.

- It will be reviewed once the reform of the EU Data Protection Directive is completed (2016).

Privacy and ICT policies

- **The EU Data Protection Directive sets forth horizontal rules, but often ICT policies require complementary actions addressing targeted privacy aspects (e.g. ongoing work on cloud computing and eHealth codes of conduct).**

- **International issues such as the recent developments on the EU-US Safe harbour agreement are also relevant in an increasingly global data economy.**

Thank you for your attention!

paul.timmers@ec.europa.eu