Cybersecurity in the EU and at Huawei

Nigel Jefferies
Industry & Standards
Huawei Technologies

The EU cyber security landscape

- European Parliament
- European Commission
- ENISA
- European governments
- Standardisation & certification bodies
- Academia & Think tanks
- Industry
- Non-European governments
- International institutions

EU Cyber Security

- Cloud computing
- R&D
- Consumer protection
- National security
- Standards
- Trade
- International relations
- Critical (Information) Infrastructure Protection
- Industrial policy

Relevant industry associations / groupings

Association	Membership	Focus	Shape
DigitalEurope	ICT industry	Security & DP	Working group, meeting monthly
ECTA	Telecoms operators	DP	Adhoc working group
ETNO	Telecoms operators	Security & DP	Working group, meeting monthly
GSMA	Telecoms operators	Security & DP	Adhoc working group
eSRT	Critical infrastructures	Security	9 roundtables throughout the year
SDA cyber initiative	Security industry	Security	9 roundtables throughout the year
DEF	ICT industry / academia	DP	1 Conference per year - informal contacts with high-level experts for intelligence
LSEC	ICT industry / security industry	Security	Workshops, knowledge sharing, white papers
TechAmerica	US ICT industry	Security & DP	Working group, meeting monthly
EOS	Security industry	Security	Working group, meeting monthly
European Privacy Association	ICT industry	Privacy	Regular events & white papers

The EU Cyber Security Strategy

■Commissioner Cecilia Malmström (Sweden)
■DG Home Affairs

■Vice President Neelie Kroes (NL)
■DG Communications Networks, Content & Technology

■High Rep. for Foreign Affairs and Security Policy
■Catherine Ashton (UK)
■European External Action Service

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, XXX
[...](2012) XXX draft

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

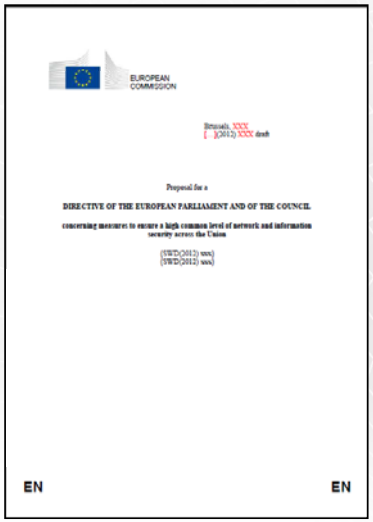
CyberSecurity Strategy of the European Union

An Open, Safe and Secure Cyberspace

EN EN

■5 Strategic priorities in the EU Cyber Security Strategy…

- Becoming cyber resilient
- Reducing cyber crime
- Developing cyber defence policy and capabilities
- Developing industrial and technological resources for cyber security
- Establish a coherent international cyber space policy for the European Union and promote core EU values



EUROPEAN COMMISSION

Brussels, XXX
[...](2012) XXX draft

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures to ensure a high common level of network and information security across the Union

{SWD(2012) xxx}
{SWD(2012) xxx}

EN EN

■…supported by a Directive on Network and Information Security:

- National frameworks on network and information security
- Cooperation between competent authorities
- Security of the networks and information systems of public administrations and market operators

Establishment of the NIS platform

- **NIS Platform is complementing and underpinning the NIS Directive.**
- **It will help implement the measures set out in the Directive, e.g. by simplifying incident reporting, and ensure its convergent and harmonised application across the EU.**
- **On top of that, the NIS platform is expected to provide input to the secure ICT R&I agenda.**
- **Three working groups:**
  - WG1 on risk management, including information assurance, risks metrics and awareness raising
  - WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange
  - **WG3 on secure ICT research and innovation**

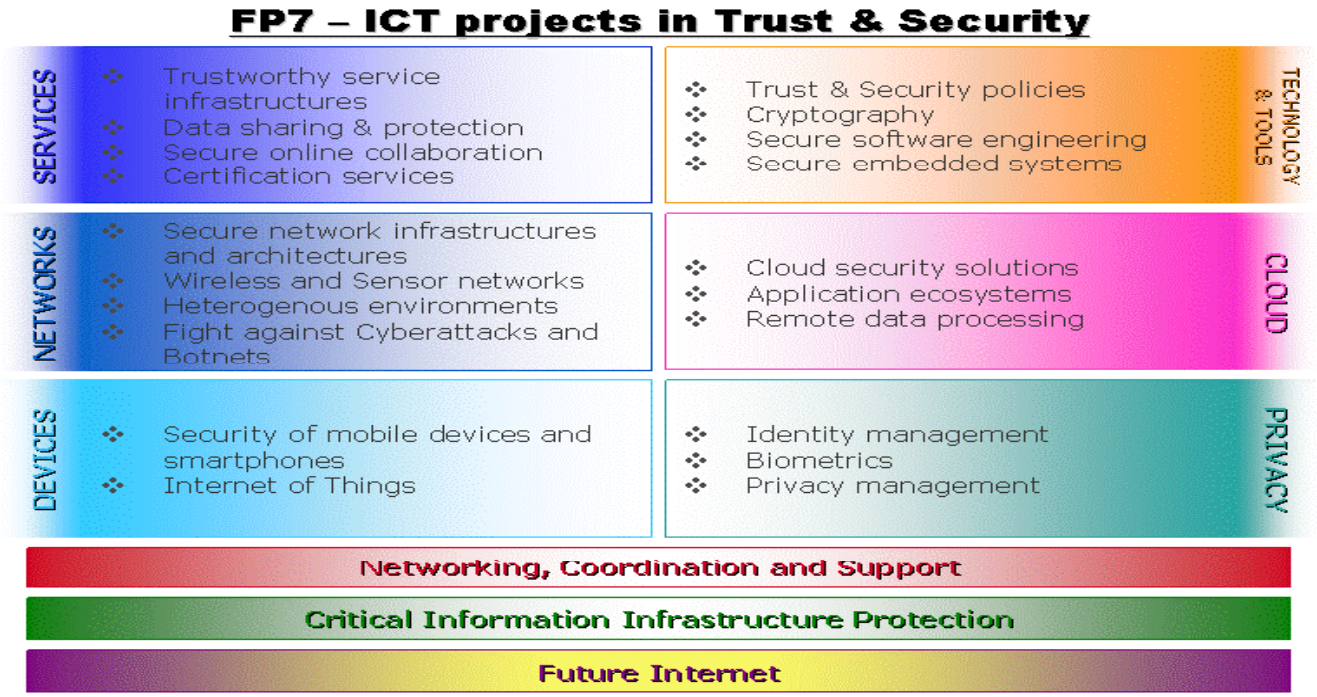
Renewal of mandate for ENISA till 2020

- The European Network & Information Security Agency (ENISA) was formed in 2004.
- The Agency is a *Centre of Expertise that supports the Commission and the EU Member States in the area of information security.*
- It facilitates the exchange of information between EU institutions, the public sector and the private sector.

EU Cyber Crime Centre

- **The centre would be part of Europol and located within its existing structures**
- **The centre would focus on:**
  - Cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud
  - Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation; and
  - Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union
- **And would have four core functions:**
  - Serve as the European cybercrime information focal point
  - Pool European cybercrime expertise to support Members States in capacity building
  - Become the collective voice of European cybercrime investigators across law
  - Enforcement and the judiciary

R&D (FP7 / Horizon2020)



- FP7: 2007-2013: ca. €300mln in funding
- H2020: 2014-2020, funding: ???
- http://cordis.europa.eu/fp7/ict/security/projects_en.html

Huawei Cybersecurity White Paper Perspectives: Making cyber security a part of a company's DNA

- **Published in October 2013**
- **Launched by John Suffolk, Global Cyber Security Officer**
- **Available at**
  - http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-310548.htm
- **Aims**
  - contribute to discussion around the policies, procedures, norms and challenges of cyber security
  - call for a common international cyber security standard to be agreed and implemented globally
  - discuss transformations that vendors, such as Huawei, are considering in relation to cyber security

Strategy, plans, governance, processes, accountability and supporting technology must be integrated, seamless, repeatable and auditable. They must dynamically change to new challenges and new requirements