European
Commission

The EU Cybersecurity Strategy

...and its implementation

Martin Mühleck
Trust and Security Unit
DG Communications Networks, Content and Technology

What is Cybersecurity?

Cybersecurity is the protection of networks and information systems against human mistakes, natural disasters, technical failures or malicious attacks

European
Commission

Cybersecurity Trends

- Cybersecurity a dynamic field and a moving target … and its more complex than we think

- Innovative Attackers - Defenders need to share and cooperate

⇒ Cyber security focus area for Horizon 2020

⇒ Cyber security will never be "solved" but will be "managed"

⇒ User centric perspective of cybersecurity

EU Cybersecurity Strategy
Protect open internet and online freedom

- ***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***

EU Cybersecurity Strategy

Principles for cybersecurity

- The same values apply on-line and off-line
- Security is a precondition for protecting fundamental rights
- Security as a shared responsibility

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

Our 3 key actions

1. Bringing cybersecurity capabilities and cooperation to maturity - Putting the NIS Directive to work (e.g. CEF)
2. Mainstreaming cybersecurity in EU policies
3. Making EU leader in cybersecurity (H2020)

1. Bringing Cybersecurity Capabilities and Cooperation to Maturity

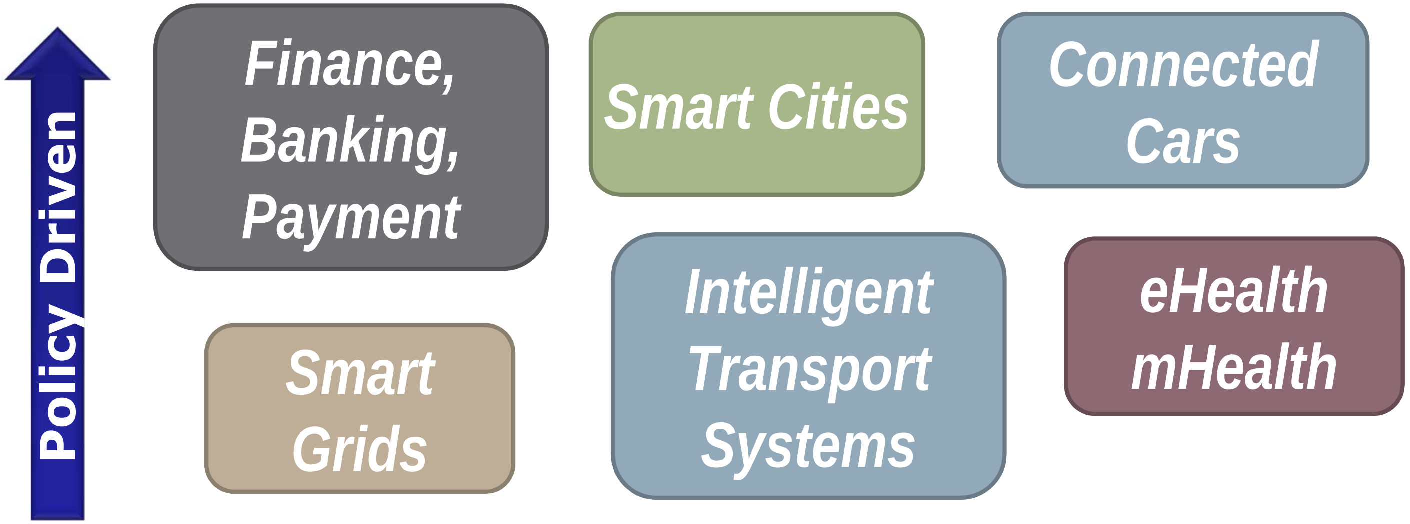
Instigate cooperation
(e.g. via ENISA)

Develop capabilities
(metrics, culture,
process, technology,
governance)

CEF initiative

Adoption of
cooperation
by all MS

NIS Cooperation
becomes mature



Policy Driven

Finance, Banking, Payment

Smart Cities

Connected Cars

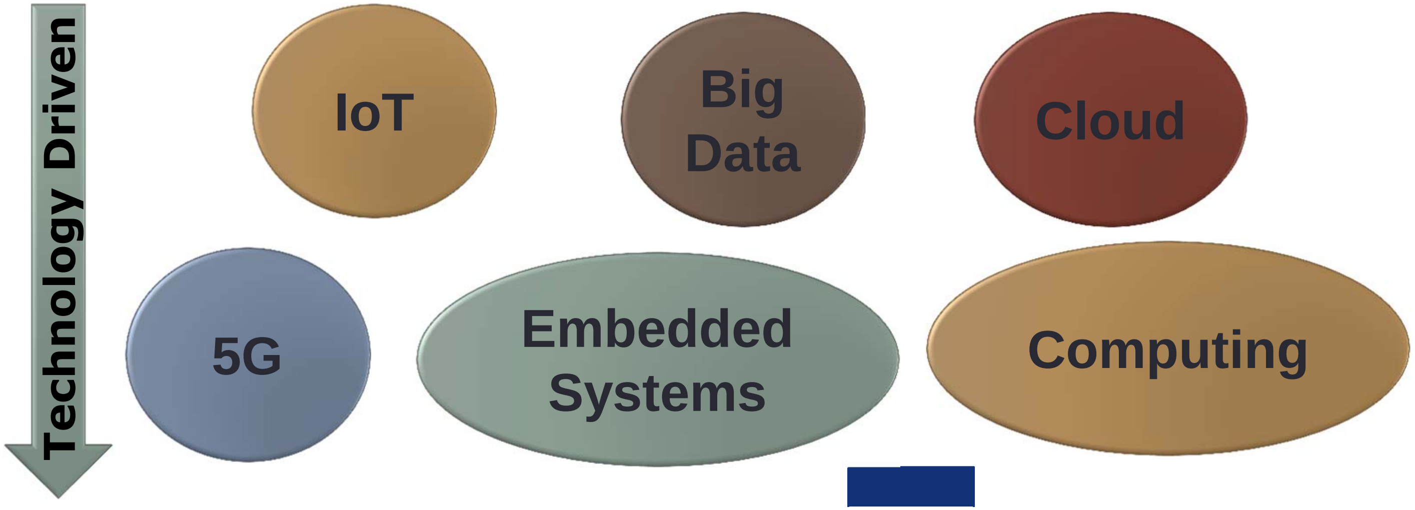
Smart Grids

Intelligent Transport Systems

eHealth mHealth

Securing Present & Future Critical Market Functions

2. Mainstreaming Cybersecurity



Technology Driven

IoT

Big Data

Cloud

5G

Embedded Systems

Computing

Securing Data Processing, Storage and Transmission

Delivering on policy objectives via H2020

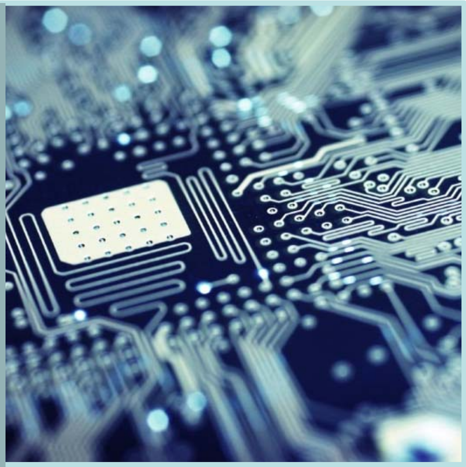
Towards a cPPP on Cybersecurity

- Foster innovative business cases for more security & privacy and European IT competitiveness
- Alignment of national and European Strategic Research Agendas (NIS-Platform)
- Leverage buy-in by industry and Member States
- Importance of governance

3. European leadership in cybersecurity (H2020)

Making the EU a leader in cybersecurity preparedness and trustworthy ICT

Maintain and develop a European industry and know-how in cyber, including through PPP



Identify and focus on a central technological areas

What should remain: innovation and competitiveness

Europe is not staying behind

European companies in position to meet current and emergent cybersecurity challenges

Privacy-by-design and security-by-design as competitive advantage

What remains to be done – challenges for H2020

From world-class research to market innovation

Europe competing globally

Industrial Policy

User trust in ICT

Linking the threads

So what are we doing in H2020?

- ***Dancing at two weddings: LEIT and Societal Challenges***
- ***Getting all others to take up Cybersecurity and Privacy***
- ***Going beyond the "usual stakeholder suspects"***
- ***Research, Innovation and Policy Feedback Loops***

Calls in 2014/15

LEIT (40 M€) Technology Building blocks in Security - 2014:

- Cryptography
- Security-by-Design

Societal Challenge 7: Digital Security (97M€):

2014:

- Privacy
- Access Control
- Risk management and assurance models

2015:

- The role of ICT in Critical Infrastructure Protection
- Information driven Cyber Security Management
- Trust eServices
- Value-sensitive technological innovation in Cybersecurity

And now…

Digital Focus Area in WP2016/17

Contractual Public-Private Partnership (launch in 2016, implemented in WP2018/19/20)

The new Work Programme for 2016/17

- Implementation of Digital Security Focus Area Call
- CNECT SME contribution has increased and spans over two years leading to changes in topics' budget
- SME instrument topic on cybersecurity

See draft programmes:

https://ec.europa.eu/programmes/horizon2020/en/draft-work-programmes-2016-17

Digital Security Focus Area Call 1/2

2016:

- *DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components **(LEIT-ICT)***
- *DS-02-2016: Cyber Security for SMEs, local public administration and Individuals*
- *DS-03-2016: Increasing digital security of health related data on a systemic level **(SC1)***
- *DS-04-2016: Economics of Cybersecurity*
- *DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation (now addressing security in SC7, LEIT-ICT and across H2020)*

Digital Security Focus Area Call 2/2

2017

- DS-06-2017 Cryptography **(LEIT-ICT)**
- DS-07-2017 Addressing Advanced Cyber Security Threats and Threat Actors
- DS-08-2017 Privacy, Data Protection, Digital Identities
- Cryptography Inducement Prize (**LEIT-ICT**)

Budget:

- SC7 - 65MEUR
- LEIT-ICT – 42MEUR (+1MEUR Crypto Inducement Prize in 2017)
- SC1 – 11MEUR

Total: 119MEUR (+20MEUR in CIP and 10,5MEUR for SME)

Our Challenges:

1. "EU to become a leader in cybersecurity preparedness and trustworthy ICT"
    - **Which is the right way?**
    - **How can we make "Trustworthy ICT" a EU label/trademark?**
2. Contractual Public Private Partnership (cPPP) on Cybersecurity.
    - **How can we identify the right priorities**
    - **Who needs to be involved?**

Thank you!

Martin.Muehleck@ec.europa.eu