Cybersecurity in the European Digital Single Market

Scientific Opinion - Main Issues

Meeting with stakeholders
13 Feb. 2017, Brussels

Prof. Pearl DYKSTRA
High Level Group (HLG)
Vision, Principles and Observations
• Cybersecurity for the growth of the European DSM

• Focus on issues of relevance to European policy in the next few years

• Cybersecurity relates to fundamental rights and principles

• Science has helped shed new light on future developments and technologies for which Europe needs to be ready, and on where European policies can play an important role in preparing the market and citizens.
PRINCIPLES

- Based on fundamental rights (EU Charter of Fundamental rights) and expressing European values

  Protection of personal data; right to private and family life; freedom of expression and information .. .

As well as

- Proposed by the HLG and underlying many of the findings/recommendations

  Duty of care towards customers; transparency by service providers, system developers
1. **State of art**: scientific study of cybersecurity in its infancy – limited rigorous evidence; multidisciplinary; multitude of publications, experts, surveys, anecdotes; nevertheless consensus on critical issues

2. **Tensions**, e.g. between:
   - Centralised and decentralised architectures and infrastructures
   - Open source and proprietary software/code
   - National security concerns and the need to share information and take collective action
   - Business interests to collect more data – citizens' rights to privacy
Key issues currently under consideration
High standards of cryptography needed to protect digital assets, transactions & communications – i.e. no backdoors (consensus among experts)

Europe should focus on reducing S/W vulnerabilities over the product life cycle, e.g. from design to testing and verification, including formal verification, long term maintenance and fast repair. In parallel, emphasis should be placed on timely fixing H/W vulnerabilities (testing and verification of H/W)

Incentivise disclosure of vulnerabilities
SYSTEMS APPROACH

Need to move away from a reliance on continuously patching of software
Encourage systems engineering approach to ICT development

CONTEXTUAL ID

Only the information needed for a digital transaction should be divulged as a default requirement – promote a more decentralized attribute-based digital ID management
CYBERSECURITY INDUSTRY

Encourage development of EU cybersecurity industry with products & practices that uphold EU principles and citizen/consumer rights
Incentivize "duty of care" & "open source" solutions by H/W & S/W system suppliers

EVIDENCE COLLECTION & SHARING

Support evidence collection methods and actual sharing of evidence and practices
An adequately resourced and empowered European body needed to set and monitor cybersecurity standards
TRAINING PROFESSIONALS

Engineers to be trained in factoring security principles into system design
Cybersecurity training to be increased in formal education and LLL (including by businesses) and made more attractive

ENGAGING CITIZENS

Increase citizen literacy and engagement in cybersecurity matters
Europe should be at the forefront of global cooperation to increase cybersecurity and in designing a worldwide coherent cybersecurity governance system which builds on a strong European framework.