Protecting Big Data and beyond:

The European Strategic Research Agenda

in Cybersecurity

Trust and Security Unit

DG CONNECT – Communications Networks, Content and Technology

Dr Afonso Ferreira
Policy Officer

Our Unit's Mission

- Develop policy, research and innovation solutions and carry out activities enhancing the security of Internet networks and services and the protection of citizens' on-line privacy and security.

The EU Cybersecurity Strategy

EU Cybersecurity Strategy – February 2013

Strategic priorities

- Achieve cyber resilience
- Drastically reduce cybercrime
- Develop cyber defence policy
- Develop industrial and technological resources
- Establish international cyberspace policy

EC Proposal for a Directive on Network and Information Security (NIS) – February 2013

- **Capabilities**: Common NIS requirements at national level
  - Strategy for NIS and cooperation plan
  - NIS competent authority
  - Computer Emergency Response Team (CERT)
- **Cooperation**: NIS competent authorities to cooperate at EU level
  - Early warnings and coordinated response
  - Capacity building
  - NIS exercises at EU level
  - ENISA to assist
- **Culture**: Risk management and incident reporting, mandatory in selected areas, eg:
  - Energy – electricity, gas and oil
  - Credit institutions and stock exchanges
  - Transport – air, maritime, rail
  - Healthcare
  - Others to be defined

The NIS Platform

The NIS Platform

- A key action of the EU Cybersecurity Strategy
  - Identify and develop incentives to adopt good cybersecurity practices
  - Promote the development and the adoption of secure ICT solutions

- A public-private platform
  - More than 200 participants
  - 18 MS + Norway: ministries, NIS agencies, NRAs, CERTs
  - Research & academia
  - Industry: ICT, finance, post, transport, healthcare, defence, energy, water sectors

- An open and inclusive multi-stakeholder Platform
  - Appropriate scientific, geographic, and sectorial coverage
  - Driven by the participants

Objectives & Output

- Prepare the ground for the implementation of the NIS Directive
  - Guidance on risk management (WG1) and information sharing (WG2) (Q2 2014)
  - Commission recommendations on cybersecurity (2015)
- Input to the secure ICT R&I agenda at EU, national and industry level
  - The Working Group 3 on secure ICT research and innovation
  - Produce view on secure ICT landscape and strategic research agenda in 2014/2015

The Working Group 3 on Secure ICT Research and Innovation

© Dreamstime

WG3 Scope and Objectives

- **Scope**
  - Address Cyber Security research and innovation in the context of the EU Cyber Security Strategy and the NIS Platform.
  - Identify key challenges and desired outcomes
  - Promote truly multidisciplinary research that foster collaboration among researchers, industry and policy makers
  - Examine ways to increase the impact and commercial uptake of research results in the area of secure ICT

- **Main objectives of WG3 within the NIS Platform**
  - Contribute to the coordination of the European activities in Research and Innovation in connection with the European Cyber Security strategy
  - Produce high quality deliverables (regularly updated) summarizing its main findings

WG3 Main deliverables

- **Secure ICT Research landscape**

https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents

- **Business cases and innovation paths**

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/business-cases-and-innovation-paths/business-cases-and-innovation-paths-interim-version/view

- **Snapshot of education & training**

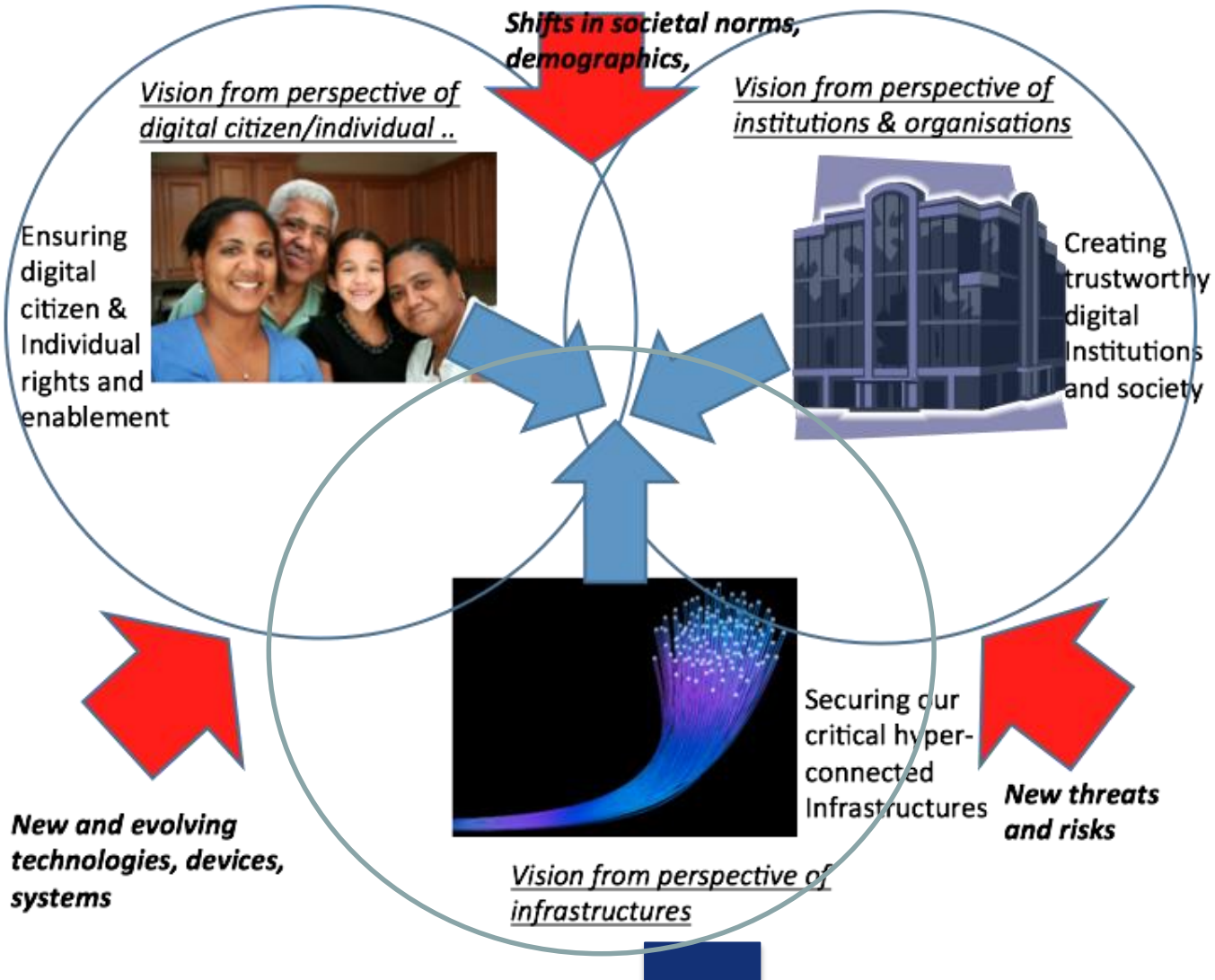
https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/snapshot-of-education-training-landscape-for-workforce-development/Education-Training.pdf/view

- **Strategic Research Agenda**

Driven by the vision states (areas of interest)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/the-strategic-research-agenda-sra/

Aols' View


Shifts in societal norms, demographics,
Vision from perspective of digital citizen/individual ..
Ensuring digital citizen & Individual rights and enablement
Vision from perspective of institutions & organisations
Creating trustworthy digital Institutions and society
Securing our critical hyper-connected Infrastructures
Vision from perspective of infrastructures
New and evolving technologies, devices, systems
New threats and risks

Common focus

- **User-centricity**
  - Focus on user centric technologies (individuals)
  - Usability

Education and awareness

- Multi-disciplinary focus
- Responsiveness to changes
- End-to-end skill development
- Continuous awareness

- **Privacy issues**
  - Privacy preserving technologies
  - Privacy aware security mechanisms
  - ID management

Focus on data

- Data protection
- Data processing for security

Managing risks

- Dynamic, composable risk assessment
- Managing complexity and system evolution

Increasing trust

- Dynamic trust assessment
- Trusted information management
- Economic models of trust

Standardization and Interoperability

- Crypto, Certification
- Assurance, risk, security metrics/indicators
- Information sharing

Secure execution environments

- Trusted IoT/Mobile/ Cloud Networks

Fostering assurance

- Security Engineering
- Certification
- Cyber Insurance

WG3 next steps

- Further detailing of the research topics and recommendations
- Finalizing public versions of the deliverables and the SRA (March 2015)
- Regular update process of the WG3 main findings/deliverables
- Continue to build consensus also outside WG3
- Reinforce the cooperation with all the main stakeholders, including SMEs
- Meeting in Brussels next Monday (March 2nd) on Research and Innovation

Participation

- More than 180 registered members
- Open to all who wish to contribute
- Want to join? Mailto:
  - CNECT-NIS@ec.europa.eu
- More information on:
  - https://resilience.enisa.europa.eu/nis-platform/shared-documents
  - http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

Concluding

Mission letter from President Juncker to Mr Oettinger, Commissioner for Digital Economy & Society

Develop and implement measures to make **Europe more trusted and secure online**, so that citizens and business can fully reap the benefits of the digital economy.

I would like you to work with the Vice-President for the Digital Single Market on a plan to make **the EU a leader in cyber security preparedness and trustworthy ICT**, and to increase the confidentiality of communications.

Thank you for your attention!