Network and Information Security (NIS) Platform

WG3 Secure ICT Research & Innovation

Fabio Martinelli – CNR

Raul Riesco Granadino – INCIBE

(Chairs)

Outline

WG3 Objectives and scope

WG3 Main deliverables

- **Secure ICT landscape**
- **Business cases and innovation paths**
- **Education and training**
- **Strategic research agenda (SRA)**

WG3 next steps

WG3 Objectives and scope

- **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
- **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

WG3 Main deliverables

- **Secure ICT Research landscape**

(**First public version available**)

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

- **Business cases and innovation paths**

(draft version Sept., first public release Dec. 2014)

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**

(draft version Sept., first public release Dec. 2014)

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)

(draft version Sept., first public release Dec. 2014)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/the-strategic-research-agenda-sra/SRA-draft-2.05.pdf/view

WG3 Steering Committee

Secure ICT Landscape (Editors):
Mari Kert, EOS
Javier Lopez, U. Malaga
Evangelos Markatos, FORTH
Bart Preneel, KI Leuven

Business cases (Editors):
Zeta Dooly, WIT
Paul Kearney, BT

Education and training (Editors):
Maritta Heisel, U. Duisburg Essen
Claire Vishek, INTEL

Strategic Research Agenda (Editors):
Pascal Bisson, Thales
Fabio Martinelli, CNR,
Raúl Riesco Granadino, INCIBE

Area of Interest (AoI) - Leaders:
AoI#1: Citizen Digital Rights and Capabilities (individual layer)
Kai Rannenberg, Goethe University
Gisela Meister, GI-DE

AoI#2: Resilient Digital Civilisation (I) (collective layer)
Nick Wainwright, HP
Jim Clarke, TSSG

AoI#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)
Steffen Wendzel, U. Bonn
Piero Corte, Engineering

AoIs Cross analysis leaders:
Volkmar Lotz, SAP
Neeraj Suri, TU Dortmund

Deliverable: Secure ICT Landscape

Goal:

- Describe Current State of the Art in Cyber Security Technologies and application domains
- Identify the current treats and corresponding short term Research Challenges

Structure:

Basic technologies

Metrics in cybersecurity, Authentication, Authorization and Access Control, System integrity - Antivirus – Antispyware, Cryptology, Audit and monitoring, Configuration Management and Assurance, Software security and secure software development, Hardware and platform security, Network and mobile security, Cybersecurity threat technologies/ Offensive technologies, Information Sharing technologies, Big data, Data Protection

Focus on Cloud/Internet of Things (IoT):

Models, current approaches and projects, open challenges

Application Domains:

e-Government, Energy-GRIDS, Smart transport/Automotive, Banking and finance, Smart cities, Telecommunications/ICT services, Military and defense, Food, Drinking water and water treatment systems, Agriculture, Cyber security awareness and training

Deliverable: Business cases and innovation paths

Goal:

To ensure that cybersecurity research is exploited rapidly and effectively to benefit European business and society by:

- Identifying those challenges whose resolution will result in greatest impact.
- Proposing processes that will ensure that research remains focused on priority areas, and that results are translated efficiently into products and active use.

Structure:

1. Introduction and problem definition
2. Methodology for the study
3. Business cases
   - Initial sample market and industry analysis
   - Identification of stakeholder requirements
   - Selection and analysis of high impact use cases
   - Cost-benefit analysis of research topics in relation to use cases
   - Initial economic incentive analysis
4. Process Definition & Innovation Models
   - Survey of best practices in innovation (SOTA)
   - Technology and research analysis link with 'Secure ICT landscape' deliverable
   - Recommendations to H2020 on innovation processes
5. Summary of recommendations

Deliverable: Education & Training

Goal:

Collect information on cybersecurity higher education curriculum in member states of EU

Collect sample information about training available in cybersecurity in EU

Formulate recommendations for development based on findings.

Structure:

1. Introduction and background
2. Methodology for the study
3. Data collection from primary and secondary sources
4. Including automated DB production (available on ENISA platform)
5. Data and Gap Analysis
6. Main findings and recommendations
7. Appendix

The Strategic Research and Innovation Agenda (SRA)

NIS Platform WG3 Secure ICT Research & Innovation

Goal

- Define a strategic research and innovation agenda on cyber security
- Start from the desired vision states (or Areas of Interest) we wish to achieve in 2025
- Consider not just technological, but also social, legal, business, and educational aspects

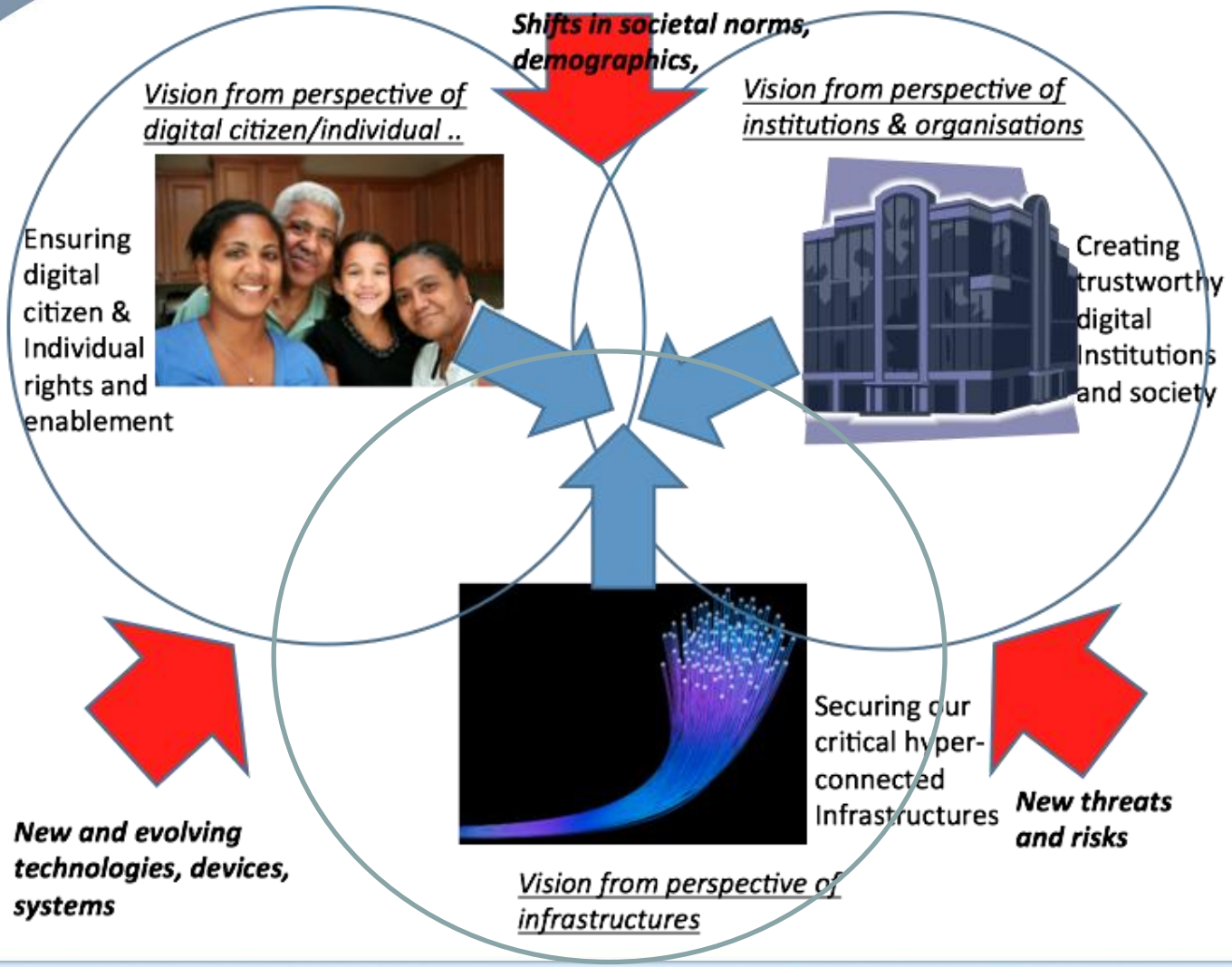
SRA's Areas of Interests (AoIs)

- ***Several concepts emerged during the meetings:***
  - Citizen and people centric computing
  - Interconnected and vulnerable society
  - Privacy, security and civilization
  - Resilient infrastructure and services heavily depending on ICT
  - Multi-disciplinary skills, knowledge and awareness

- ***Eventually summarized in 3 main areas of interest:***
  - Individuals' Digital Rights and Capabilities (**Individual** layer)
  - Resilient Digital Civilisation (**Collective** layer)
  - Trustworthy (Hyperconnected) Infrastructures (**Infrastructure** layer)

Investigate relationships among Areas of Interest

Aol's View



AoI#1 Individuals' Digital Rights and Capabilities (Individual layer)

Scope:

"Citizen centric view " incorporating

- how to design, manage, and control network and information and communications technologies
- respecting privacy, freedom of expression, safety
- enhancing technical aspects by social, legal and regulatory aspects of security and privacy

Individuality includes

- respect for citizens and consumers
- and transparency (without intrusiveness) to be provided at all times

Focus on:

Technology:

- **Secure computing** in untrusted platforms
- Provision of a **secure personal device** based on a secure core
- **Personal Identity Management**
- Sufficiently advanced **security and privacy** enablers together with **user friendliness**
- Technologies, that reduce the chances and the impact of **users giving up their privacy**
- **Policy-based** technologies for improving **compliance**
- Easing engineering of complex systems

From a social, policy, regulatory point of view

- Demand and support **user friendliness** of technical and IT security interfaces
- Provide **Privacy** in a heavily **controlled** world
- **Control of surveillance**
- **Assurance** in the digital world
- Support for open source technology production and evaluation tools
- Research on "trustworthiness/trust"

AoI#2 – Resilient Digital Civilisation (collective layer)

Scope:

Ensure trust in the digital form of (social) institutions/organizations.

- Organizations operate under a whole series of obligations that include:

➢ regulation, contracts, societal norms, risk management, security, secure handling of information and respect of fundamental rights of the customers/citizens.

Focus on:

Technology

•**Cryptography** with high strength
•**Privacy protecting**, yet **trustworthy identification technologies**
•**Transparency** about who has data at all times and knowledge of what it is being used for;
•New forms of **fraud protection** for digital currency;
•**Cyber forensics** that will provide the user with strong security
•**Secure data channels**
•**Secure shared computation environments**
•**Security and dependability** of Critical Information Infrastructure protection **(CIIP)**

From a social, policy, regulatory point of view

•**Balancing the societal needs**
•Stronger **coordination and cohesion** of the stakeholders groups:
•**R&I undertakings and results catch up with the faster requirements** of the **industry**
•**Standardization**

AoI#3 Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer)

Scope:

- ICT as pervasive enabler in a world that is more and more highly interconnected
- Provision of cyber security in order to avoid ICT as weaker point in the security chain
- Study of the overall relationships among infrastructures

Focus on:

Global Hyperconnected vision, with main focus on:

- ICT
- Energy/Smart Grids
- Transportation
- Civil administration
- Smart Cities
- Automotive
- Control systems for water, food
- Healthcare
- Finance (Cyber Insurance)
- …

Cross analysis for commonalities / differences

After performing a cross-analysis the following common topics emerged:

- Assurance / Insurance
- Integration of data / system view
- Secure execution environments/secure devices for everybody
- Establish privacy enhancing technologies and digital identities
- Trust management
- Standardization and interoperability
- Managing complexity of systems; risk assessment and management
- Usability and user centricity
- Education and awareness

WG3 next steps

- Finalizing public versions of the deliverables and the SRA (Dec. / Jan.)
- 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

Thank you.

NIS Platform
WG3 Secure ICT Research & Innovation