Network and Information Security (NIS) Platform

Fabio Martinelli
National Research Council of Italy
Chair of WG3 of the NISP

(Fabio.Martinelli@iit.cnr.it)

The NIS platform

- To support the EU cyber security directive EU decided to create a public/private/cooperation in the form of a EU platform on Network and Information Security (NIS)
- Unique opportunity to better understand NIS Challenges, Threats and Risks
- A platform for bringing together policy and technical experts to debate about the current and future challenges
  - Identify and develop incentives to adopt good cybersecurity practices
  - Promote the development and the adoption of secure ICT solutions
- A platform for influencing future R&D in NIS issues

Constituency based on Public/Private

- Multi-stakeholder Platform with strong emphasis on public/private cooperation
  - Crucial due to the pervasive nature of the cyber space!
- Appropriate stakeholders coverage, including scientific, geographic, and sectorial aspects
  - MS: ministries, NIS agencies, NRAs, CERTs
  - Research & academia
  - Industry: ICT, finance, transport, healthcare, defence, energy, water sectors, …
- Driven by the participants (on a volunteer basis)
- Commission and ENISA to provide operational support to the chairs/members

Topics of the NIS platform

1. Organisational measures: practices to define, guide or evaluate an organisation's cybersecurity, specifically its capability to identify, assess and mitigate cybersecurity risks, and to deter and handle incidents; **(Risk management for cyber security**)
2. Secure products and services: practices to demonstrate the ability of products or services to provide a "good" level of cybersecurity performance as part of the ICT value chain; **(Assurance)**
3. Metrics, measurement and language / taxonomy for cyber risk: practices for measuring, describing and evaluating cyber risks, impacts, threats, controls, etc. **(Metrics and measurements for cybersecurity)**
4. **Information exchange**: practices for the exchange of cyber incident information, to allow cyber incident reports to be understood and acted upon in the framework of complex cooperation schemes; to facilitate a high level view of all cyber incidents which facilitates spotting trends and directing resources; (**Information sharing)**
5. Cybersecurity resources: practices to manage and develop cybersecurity knowledge, skills and resources within an organisation or a sector. (**Cybersecurity best practices**)

WGs structure

- Eventually 3 WGs have been established (two mainly operational and one mainly research&innovation oriented):

  - WG1 on Risk Management aims to identify best practice in cybersecurity risk management activities, provide guidance to enhance levels of information security and facilitate the voluntary take-up of the practices;
  - WG2 on Information Sharing aims to promote the sharing of cyber threat information and incidents and allowing coordination in both the public and private segments of the EU;
  - WG3 on Secure ICT R&I WG3 will address issues related to Cyber Security research and innovation in the context of the EU Strategy for Cyber Security.

Work methodology

- Work in the Platform is carried out with the following principles in mind:
  - Be results-oriented and focused on impact
  - Be of value to the stakeholders
  - Follow a bottom-up and consensus building approach
  - Adopt a deadline-driven approach
  - Ensure active participation and continuity in the participation
  - Confidentiality rules and supporting tools

Meetings

- Two plenary meetings (June/Dec 2013)
- WG kick-off meetings in September 2013
- Third plenary meeting foreseen in April 2014
  - Consolidation of the first outputs

WG1 Risk Management

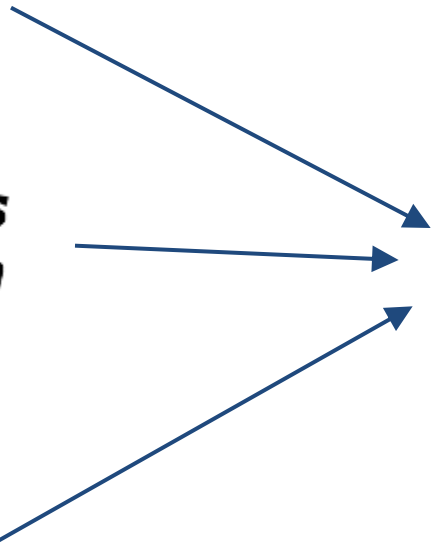
- WG1 – Risk Management
  - Cybersecurity Risk Management Methods and Standards
  - Cybersecurity Risk Management Metrics
  - Cybersecurity Risk Management Frameworks and Maturity Models
  - Cybersecurity Risk Management Awareness and Education

WG2 Information Sharing

- WG2 – Information sharing
  - Frameworks and standards for information sharing
  - Addressing barriers to information sharing, incl. privacy and trust
  - Protocols

WG3 Secure ICT Research & Innovation

- ***Secure ICT Research landscape***
- ***Business cases and innovation paths***
- ***Snapshot of education & training***



- ***Strategic Research Agenda***

Driven by the vision states (areas of interest)

WG3 Steps achieved: Secure ICT landscape group

ToC (draft):

1. **Basic technologies: typology of technologies**

es, access control, system integrity, cryptology, audit and monitoring, configuration management and assurance, privacy related technologies, hardware and platform security, software security and secure software development, network and mobile security, cybersecurity threat technologies, information sharing technologies

2. **Cloud/IoT:**

Models, current approaches and projects, open challenges

WG3 Steps achieved: Secure ICT landscape group (cont.)

<u>ToC (draft)</u>: (cont.)

3. **Applications:**

e-Government; Energy/smart grids/industrial control systems; Smart transport; Banking and finance; eHealth; Smart cities; Telecommunications/ICT services; Military and defence; Food; Agriculture; Media; Air traffic management; Space systems.

4. **Comparison of cybersecurity technologies in application domains**

WG3 Steps achieved: Business deliverable group

ToC (draft):

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

WG3 Steps achieved Education & training group

ToC (draft):

1. Introduction
2. Concepts and definitions Methodology
3. Curricular and courses
4. Training
5. Summary of the results
6. Recommendations

WG3 Strategic Research Agenda

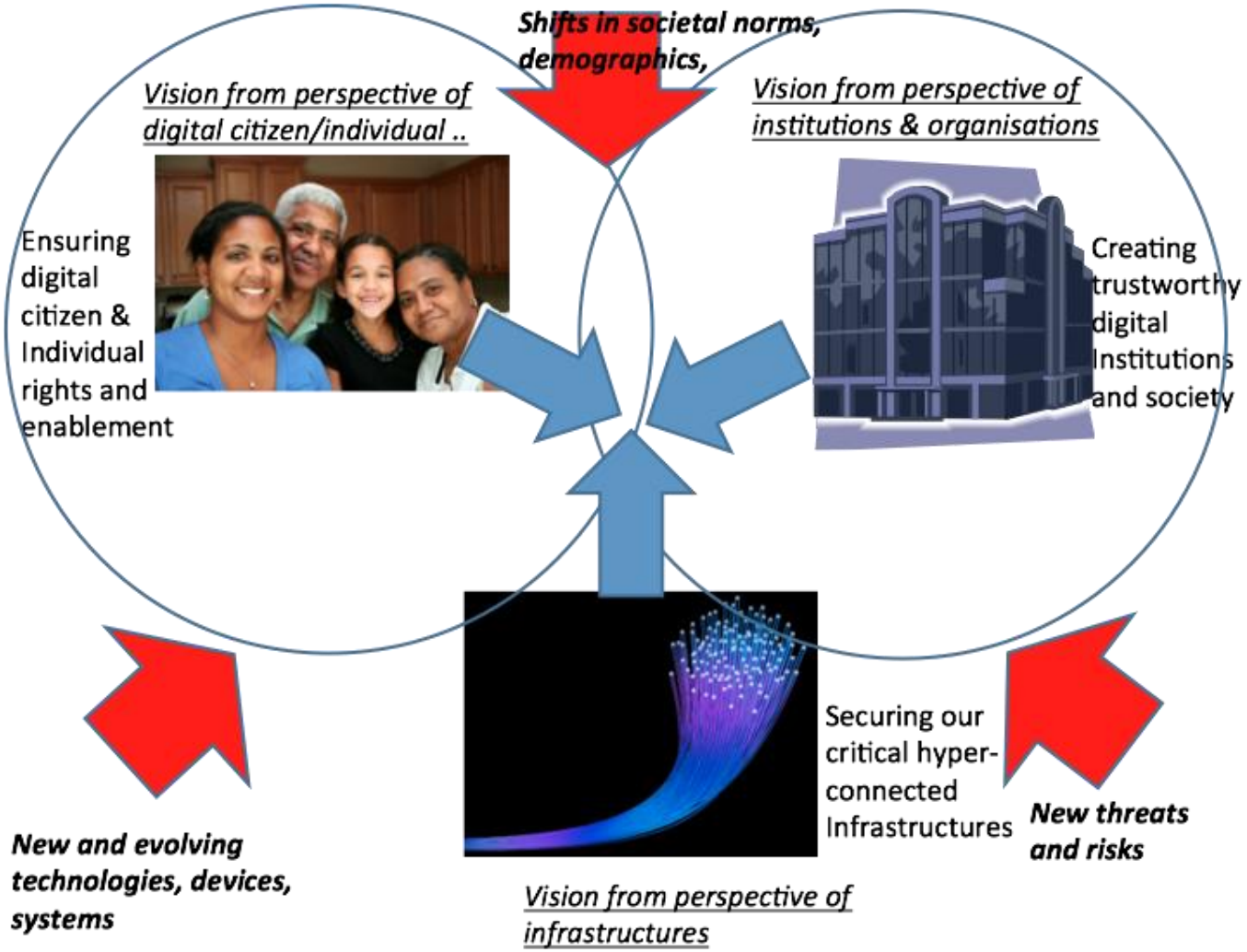
- The Strategic Research Agenda (SRA) of the NIS Platform, which is a living document stemming from WG3 and uses the other deliverables as input. The SRA will include the following:

- Identification of the desired states (Areas of Interest - AoI) for European Research and Innovation

- Challenges for achieving those states

- Enablers and inhibitors (from several perspectives)
  - Gap and cross analysis;
  - Identification of R&D instruments;
  - Priorities & timeline;
  - Roadmap;
  - Key performance indicators

Areas of Interest



Contacts

- 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

- CNECT-NIS@ec.europa.eu