



Network and Information Security (NIS) Platform

WG3 Secure ICT Research & Innovation

Fabio Martinelli – CNR

Raul Riesco Granadino – INCIBE

(WG3 co-Chairs)



NIS Platform WG3 Secure ICT Research & Innovation



WG3 Scope and method of work

WG3 Main deliverables

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



- **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



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
- Sharing of work load/ownership

Methodology – members/communities/projects



- **Interactive sessions** within NIS WG3 + **cross-synchronization** with several EU initiatives (business, innovation, research, education...) (avg. >60 experts / session)

- **Virtual / online meetings:**
- **many subgroups**
(e.g. dedicated to **Business** deliverable)
- **x1 Steering Committee** (monthly) with all leaders

- **193 members (experts) inside NIS WG3** (coming from several EU initiatives already)

- **Many supporting EU projects**



Figure 11: A group of interactive discussions for the x-analysis phase

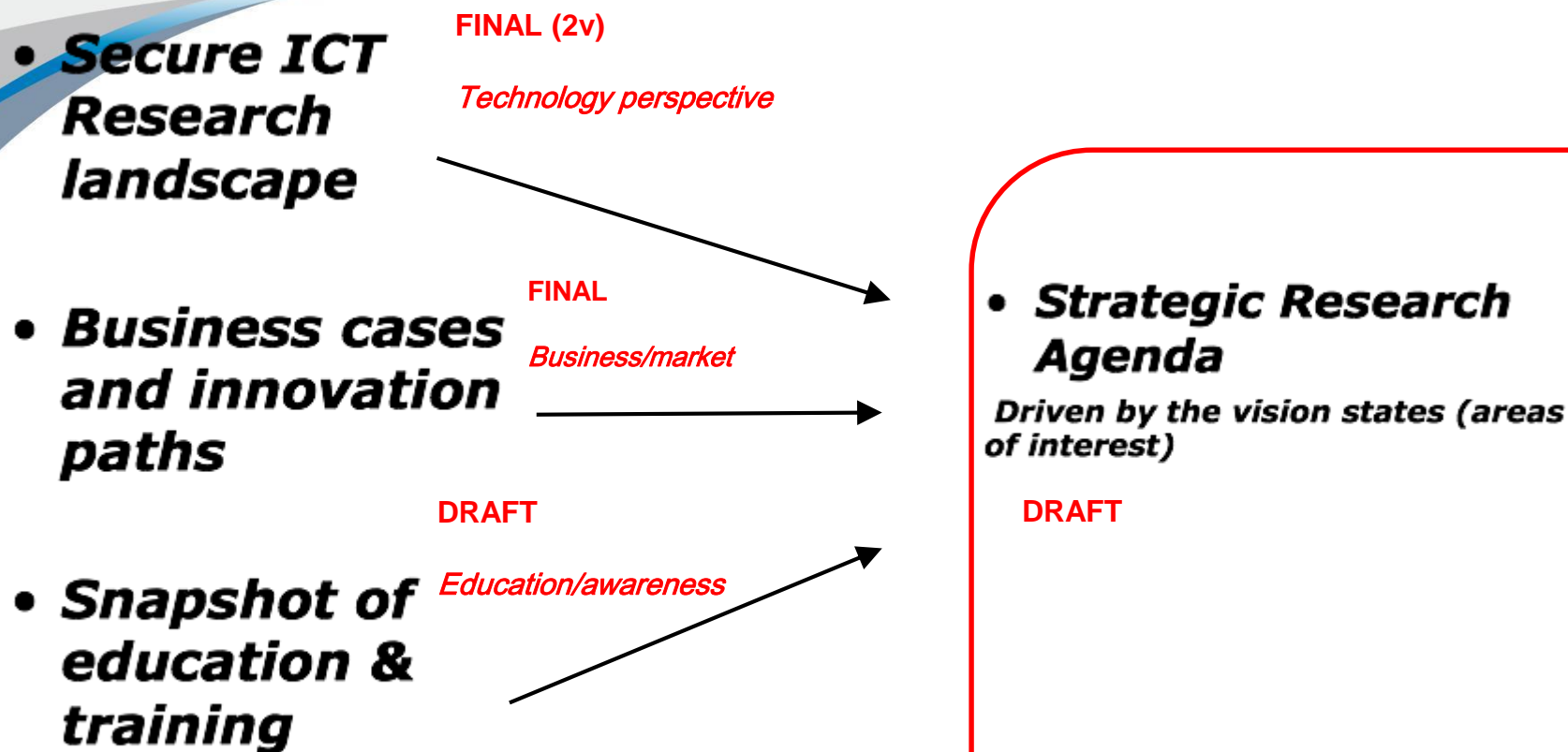
Each group appointed a leader and carried deep and meaningful conversations around its topic. At the end of the time allocated for such conversations each of the panel leaders gave a brief explanation of each of the panel discussions and agreements to all WG3.



Figure 12: Briefing of Panel 6 to all WG3

The answers are really helpful for X-analysis leaders to start their prioritization phase by providing some important clues as inputs.







Secure ICT Landscape (Editors):

Mari Kert, EOS
Javier Lopez, U. Malaga
Evangelos Markatos, FORTH
Bart Preneel, KU Leuven

Business cases (Editors):

Zeta Dooly, WIT
Paul Kearney, BT

Education and training (Editors):

Maritta Heisel, U. Duisburg Essen
Claire Vishik, 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

Aols Cross analysis leaders:

Herve' Debar, Telecom SuD Paris
Volkmar Lotz, SAP
Aljosa Pasic, ATOS
Neeraj Suri, TU Darmstadt



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, PET

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, Dual use technologies, 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. Economic benefits of NIS research and innovation
Growing the European NIS product and services sector
3. Market and Industry overview
Global technology vendors
European solutions for the cyber security market
4. An approach to prioritising research topics
Market demand and high impact use cases
5. Process Definition & Innovation Models
6. Summary of recommendations
7. Appendixes
Success stories in EU Innovation
High impact use cases
Example research topics and value statements



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. Objectives
3. Methodology for the study
4. Analysis
5. Achievements and gaps
6. Main findings and recommendations
7. Future work
8. Appendixes
 - Summary of key findings
 - List of institutions and courses
 - Secondary sources evaluated



The Strategic Research and Innovation Agenda (SRA)



NIS Platform WG3 Secure ICT Research & Innovation



- 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 2020
- Consider not just **technological**, but also **social**, **legal**, **business**, and **educational** aspects



- ***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)



Each area of interest has been investigated separately for

- Identifying challenges, enablers/inhibitors (technical, policy, organizational) and research gaps
- Those elements are useful to stakeholders mainly interested to one perspective

After a cross analysis has been performed in order identify common emerging themes and possible divergences.

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)
- ...

Purpose of cross-analysis activity



SRA Aols (and landscape document) look at research challenges from different angles

- State-of-the-art and challenges of current research streams
- Citizen-centric
- Institution-centric
- Infrastructure-centric

Analyse **consistency** and **complementarity** of the views

Identify **common challenges**

Check for potential **divergences** (gaps, contradictions, omissions)

Prioritise identified challenges based on scope, impact, urgency, timeline...

Common research and innovation priorities



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

ICT infrastructure protection

- Networks
- Devices
- IoT
- Others

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

- Operating System security
- Intrusion detection/prevention
- Security supporting services

Focus on data

- Data protection
- Data processing for security

Fostering assurance

- Security Engineering
- Certification
- Cyber Insurance



Example research priorities: Assurance

Security / Privacy by Design

- Security requirements engineering
- Secure engineering principles
- Secure (programming) languages and frameworks
- Secure computing

Security validation ->

Processes

- Metrics
- Quantification of security and privacy risks
- Cyber insurance
- Certification schemes

Interdisciplinary research

Topic / Timeframe	Short (1-3)	Medium (3-5)	Long (5-8)
...
Security validation	Static and dynamic analysis	Integrated analysis	Integrated analysis based on formal semantic models
Processes		Comprehensive set of security standards approved and established in practice	
Metrics	Security process KPIs	Security quality KPIs	
Quantification of risk	Risk metrics	Risk assessment frameworks based on publicly available data	
Cyber insurance			Operational insurance schemes
...

Some key observations and opportunities not to be missed



From the SRA and other WG3 deliverables, we derive the following considerations and opportunities to be addressed:

- **Fostering national and international** cyber security and privacy **cooperation** and **governance**, e.g. **considering contractual PPP**
- **Balancing** cyber **security** and **privacy** requirements
- Mitigating the **concentration** of **strategic** cyber security **resources** and **technologies outside Europe**
- **Focus on relevant application domains when cyber is increasingly relevant as critical infrastructures**
- **Providing facilities for NIS research experimentation**
- Further work to resolve **timescale mismatch** and use **agile / lean** R&I methodologies.
- **Comparing** innovation **theory with practice** in corporations vs. SMEs.
- Enhancing **Start-ups**, SMEs and other new entrants coming from **EU talent dedicated programmes**.
- Rapid **market driven education** (+ end to end skills development) and **awareness** changes.
- Alignment of curricula and training with demand for skills



- Further detailing of the research topics and recommendations, including related to markets
- Finalizing public versions of the deliverables and the SRA
- Regular update process of the WG3 main findings/deliverables, including on Skills (join specific panel today!)
- Continue to build consensus also outside WG3
- Reinforce the cooperation with all the main stakeholders, including SMEs



**Comments/suggestions are
very welcome!**



*NIS Platform
WG3 Secure ICT Research & Innovation*