Focus on Cyber Security

Fabio Martinelli
Co-Chair of EU NISP WG3

Istituto di Informatica e Telematica (IIT)
Consiglio Nazionale delle Ricerche (CNR)

Outline

- European Cyber Security Strategy
- Network and Information Security (NIS) Directive
- Network and Information Security (NIS) European Platform
  - NIS Working Group3 on Research and Innovation
  - NIS Cyber Security Strategic Research Agenda
- Concluding remarks and next steps

The EU Cybersecurity Strategy

EU Cybersecurity Strategy

Strategic priorities defined in 2013

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

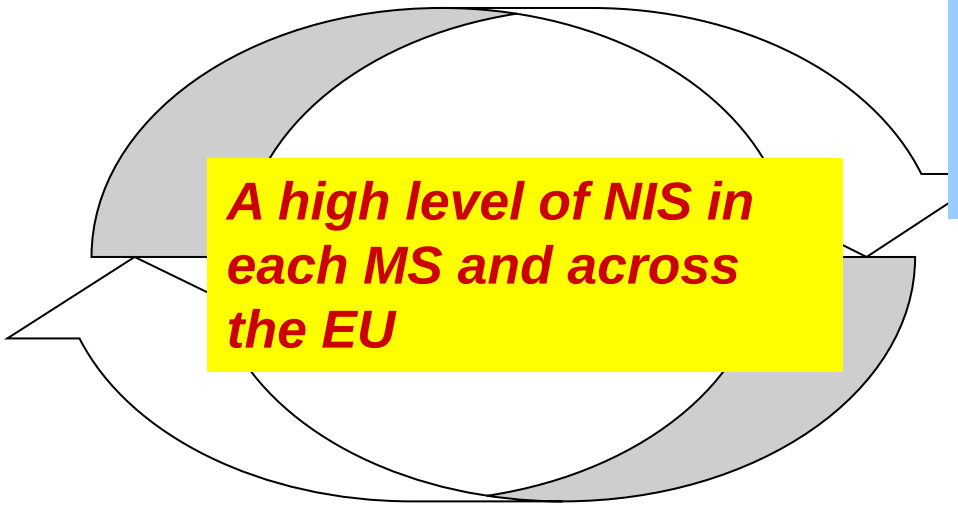
Network and Information Security Directive (NIS)

- An initiative launched by the Commission for member states and companies in order to support the adoption of the new Cyber Security Directive (launched on 2013 – politically agreed upon in December 2015)
- The aim of the proposed Directive is to ensure a high common level of network and information security (NIS).
  - This means improving the security of the Internet and the private networks and information systems underpinning the functioning of our societies and economies.
- The directive mainly addresses the necessity to increase the cyber security level of all the member states
  - In particular, consolidation and cooperation of national CERTs
    - able to share incidents information
  - creation of national preparedness plans for cyber security (including authorities etc)
    - including risk management plans
  - ...

Network and Information Security Directive (NIS) in a picture

PREPAREDNESS
National capabilities

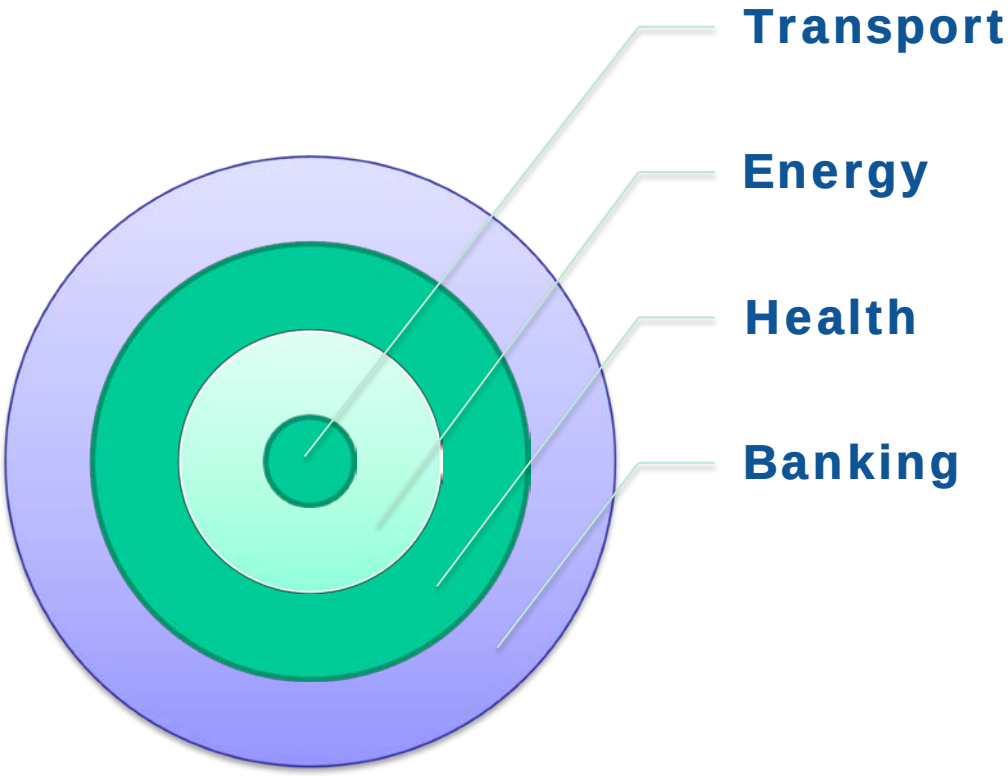
EU-LEVEL COOPERATION
Exchange of information and coordinated reaction



A CULTURE OF NIS ACROSS SECTORS

Main fields covered

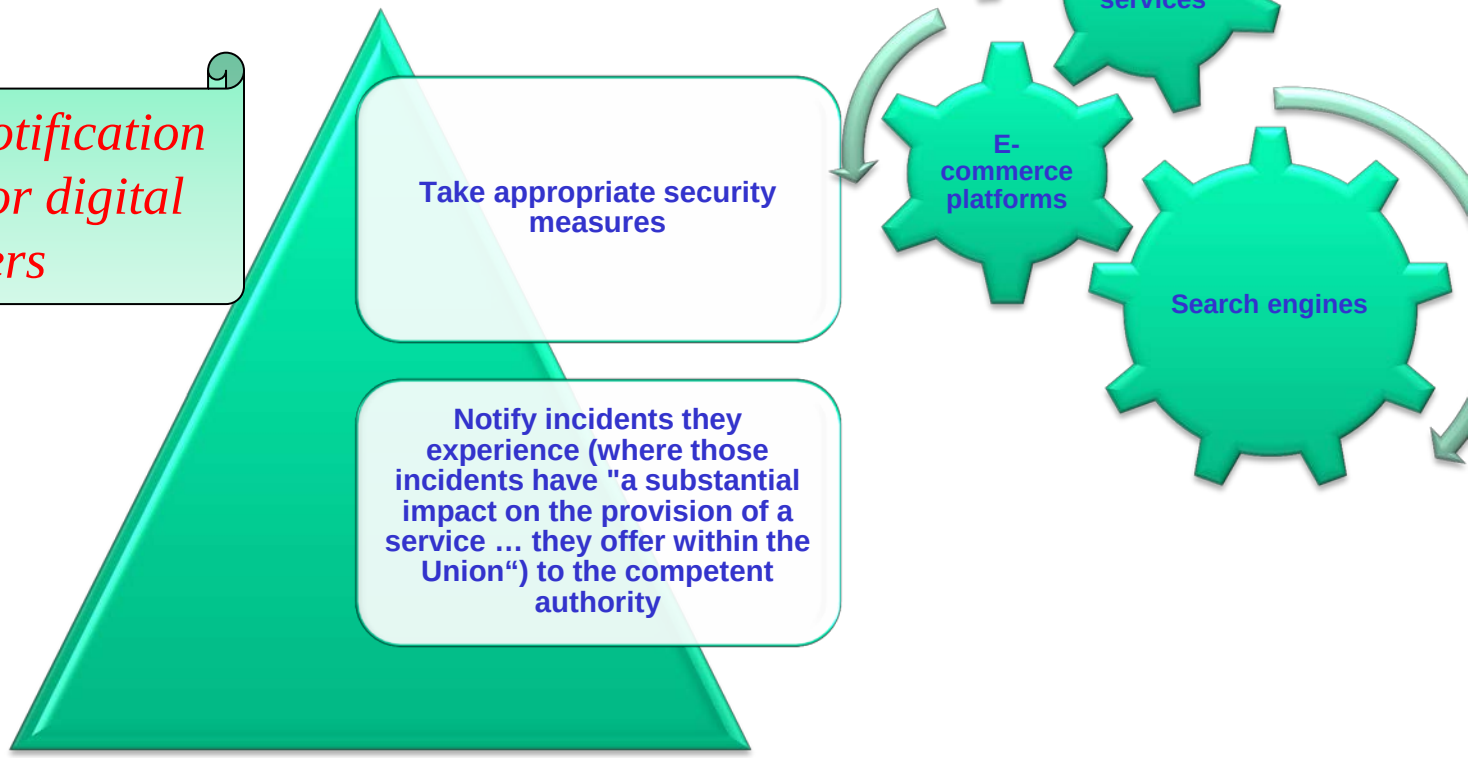
Obligations for companies doing business in critical infrastructures



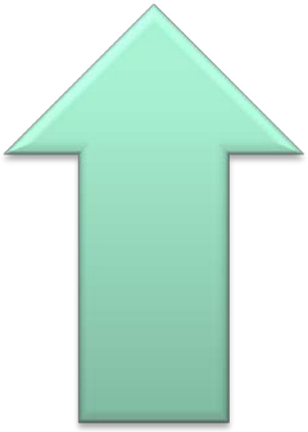
Companies will have to implement security measures and notify public authorities in cases of serious cyber incidents.

Digital service providers covered by the directive: duties

Security and notification requirements for digital service providers



Pros/Cons



Obligations are innovative since, currently, a large number of incidents do not reach the competent authorities, and go unnoticed.

Public authorities will be in a position to react, take the appropriate mitigating measures and set adequate strategic priorities

Strong reduction in terms of financial losses, estimated in a dozens of billion annually, related to the inadequacy in security of network and information systems which can compromise vital services

The NIS Directive contains some ambiguous provisions and equivocal definitions

At Italian Level

The Italian Government is particularly keen and proactive on Cyber Security

Already in Jan 2014 a national cyber security ***strategy*** and ***plan*** where depicted www.sicurezzanazionale.gov.it, with:

- Definition of cyber security authorities and responsibilities
- Creation of CERTs (including a national one), with information sharing capabilities among the main stakeholders
- Fostering of private/public/partnership

Recently, a national framework for cyber security has been recently by the CINI Cyber Security National Lab and undergone a public consultation

At EU level: The NIS platform

- To support the EU cyber security directive EU decided to create 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
- A platform for influencing future R&D in NIS issues

WGs structure of NIS

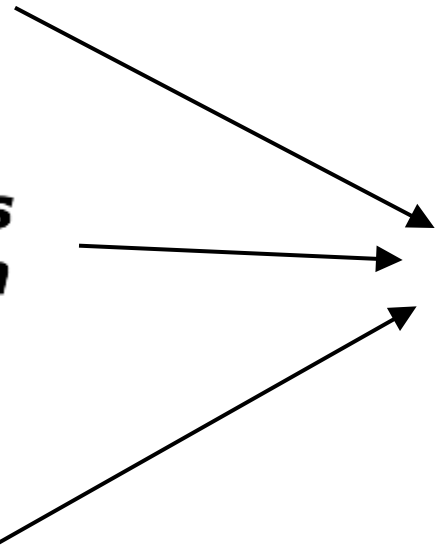
- Eventually 3 WGs have best established (two mainly operational and one mainly research&innovation oriented):
  - WG1 on Risk Management aims to identify best practice in cybersecurity risk management activities, provide guidance to enhance levels of information security and facilitate the voluntary 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.

About WG3

- **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
- **Constituency**
  - More than 200 members from industry, academia, member states, policy makers, etc.
  - All the main stakeholders at European level represented
- **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 deliverables produced!

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



- ***Strategic Research Agenda***

Driven by the vision states (areas of interest)

NIS WG3 SRA

CYBERSECURITY STRATEGIC RESEARCH AGENDA – SRA

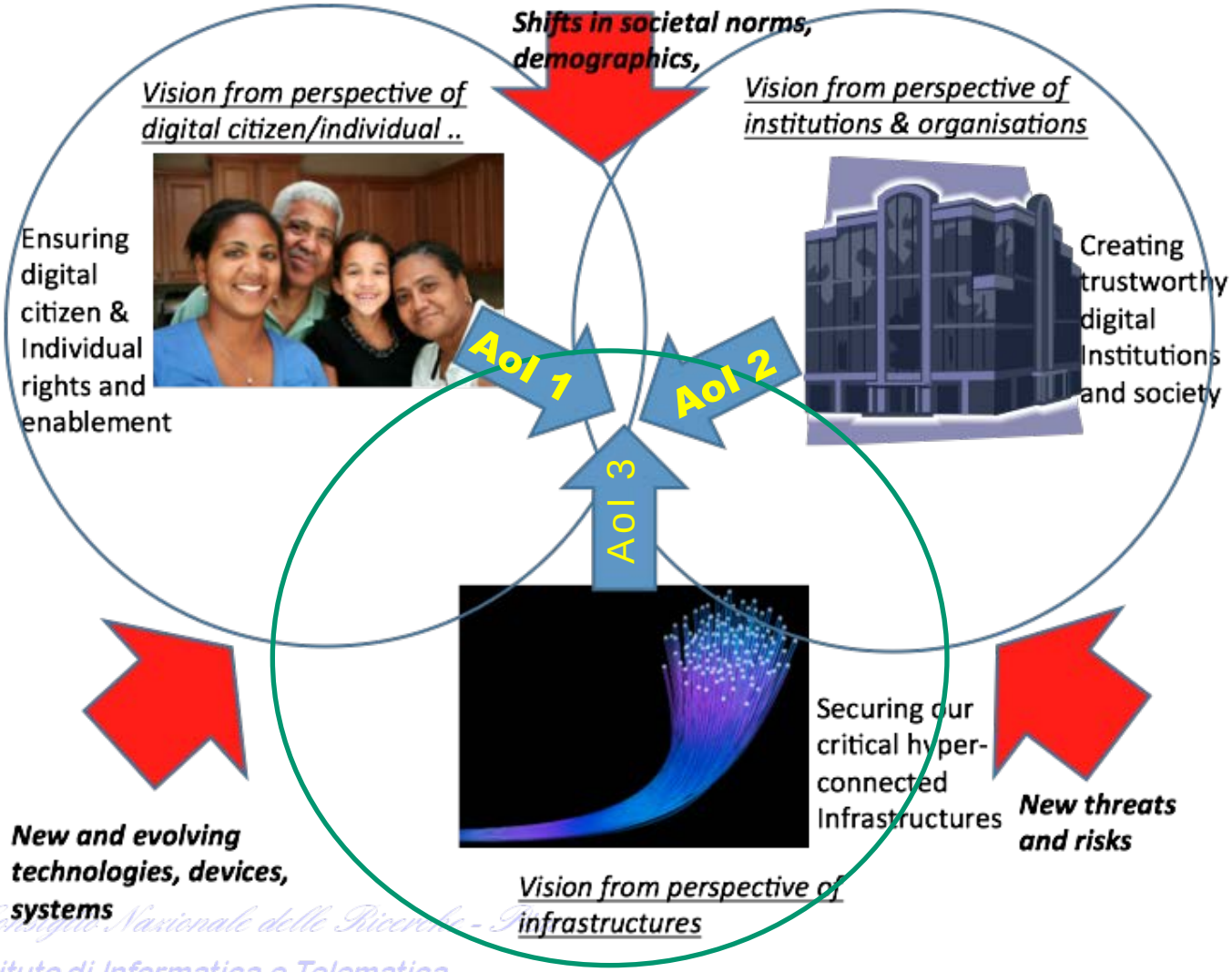
Produced by the
European Network and Information Security (NIS) Platform

Final version v0.96
Last modified: August 2015

Editors:

Pascal Bisson (Thales), Fabio Martinelli (CNR) and Raúl Riesco Granadino (INCIBE)

Three main areas of interest



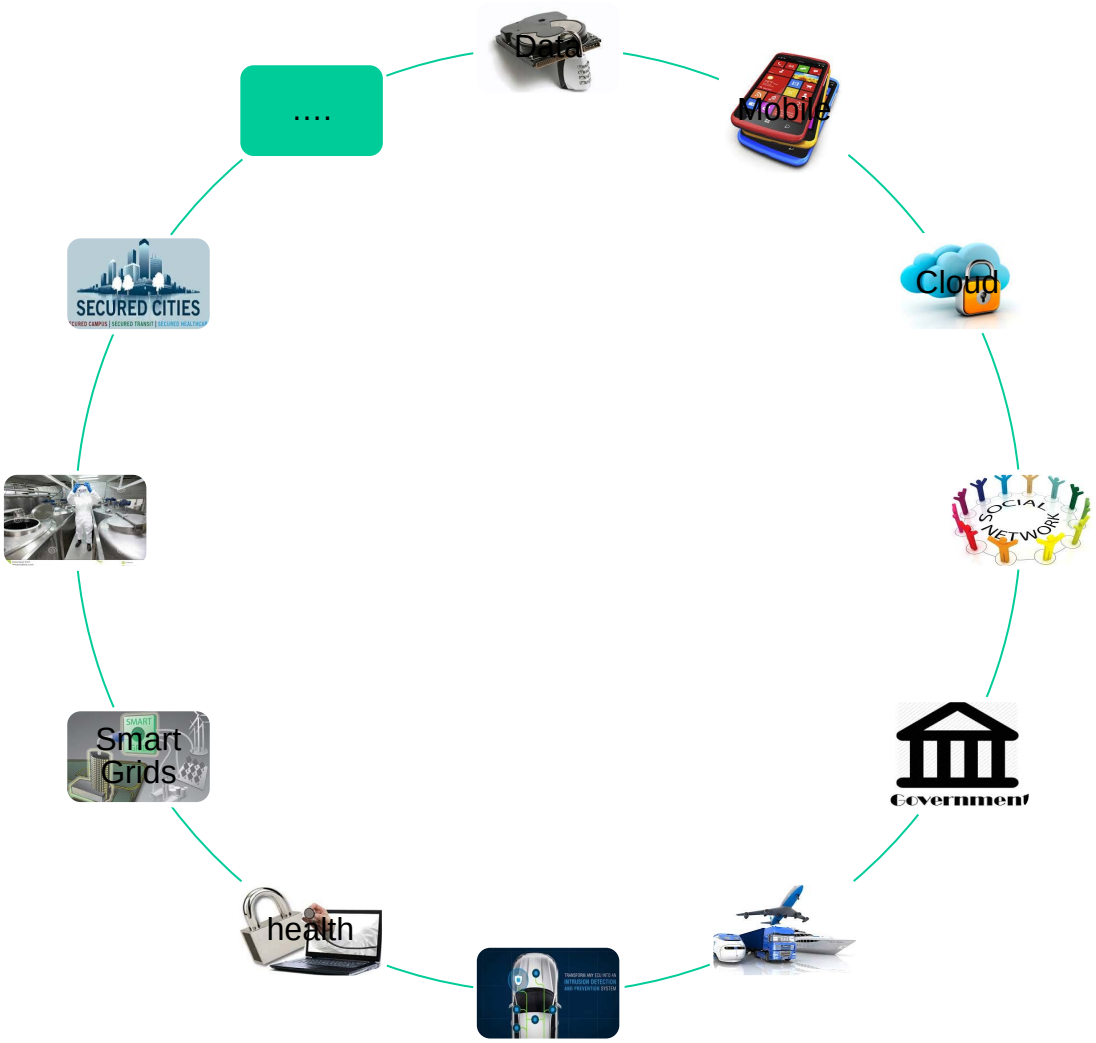
Process

Each area of interest was investigated separately for

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

A cross analysis was then performed in order to identify common emerging themes and possible divergences.

Cyber security application domains



Main topics identified

Fostering assurance

- Security Engineering
- Certification
- Cyber Insurance

Preserving privacy

- Privacy Enhancing Technologies
- Privacy-aware security mechanisms
- ID management

Focussing on data

- Data protection
- Data provenance
- Data-centric security policies
- Operations on encrypted data
- Economic value of personal data

Protecting ICT Infrastructure

- Networks
- Cloud
- Mobile
- IoT, others

Managing cyber risks

- Dynamic, composable risk assessment
- Integrated risk metrics and indicators
- Managing complexity and system evolution

Education and awareness

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

Standardization and Interoperability

- Crypto ("everywhere")
- Certification, assurance, risk, security metrics/indicators
- Information sharing

Enabling secure execution

- Secure platforms
- Intrusion Prevention/Detection
- Secure operating Systems

Increasing trust

- Dynamic trust assessment
- Computational Trust Models
- Trust and big data

Achieving user-centricity

- Focus on user centric design and engineering
- Usability of security mechanisms

General aspects

Several opportunities were identified:

- Fostering a contractual European cyber security and privacy cooperation and governance
- Balancing cyber security and privacy issues
- Mitigating European dependencies on external knowledge/technology

Supporting EU research projects

Contractual PPP

Mentioned in the Digital Single Market Strategy as opportunity for an European Cyber Security Industry consolidation

Consultation with the European Stakeholders (dec. 2015-june 2016)

https://ec.europa.eu/eusurvey/runner/CybersecurityContractualPPPandPossibleAccompanyingMeasuresConsultation

Great opportunity for the industrial community to integrate and cooperate at EU level (and national ones)

Links

- Cybersecurity Strategy of the European Union: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
- Commission proposal for a Directive on Network and Information Security: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666
- NIS Platform: https://resilience.enisa.europa.eu/nis-platform
- Towards a Europen cPPP on cyber security (consultation open)
  - https://ec.europa.eu/eusurvey/runner/CybersecurityContractualPPPandPossibleAccompanyingMeasuresConsultation