National Research Council of Italy

Research and Innovation for Cyber Security in Europe: NIS platform and the cPPP ECS

Fabio Martinelli

Institute of Informatics and Telematics (IIT)

National Research Council of Italy (CNR)

National Research Council of Italy

Outline

- The relevance of Cyber
- NIS platform
- The European Cyber Security Organization (ECSO) and the ECS cPPP

In the news

- When I need to make a presentation on cybersecurity for awareness … I just go in the web and get the latest news

EDIZIONI LOCALI | CORRIERE TV | ARCHIVIO | TROVOCASA | TROVOLAVORO | SERVIZI

DDOS

Il cyber attacco contro Internet negli Usa partito dalle case «intelligenti»

L'attacco è arrivato da oggetti «smart»: videoregistratori, frigoriferi, telecamere di sicurezza, router e sistemi per il controllo dei neonati. Wikileaks rivendica

di FEDERICO CELLA ★ 32

Scientific and Technological Relevance

- The Scientific Advise Mechanism (SAM) of the EC and its high level expert group selected cyber security as one of the two first topics for action

National Research Council of Italy

Europe is acting

- The European Commission
  - Set up a directive on Network and Information Security (NIS)
  - Set up a contractual Public Private Partnership (cPPP) for boosting research and innovation in the area
    - cPPP on cyber security (ECS)

The Network and Information Security Directive and Platform

The Network and Information Security (NIS) directive was lunched by the Commission for member states and companies in order to support **to increase the cyber security level of all the member states** (launched on 2013; politically agreed upon in December 2015)

- To support the EU cyber security NIS directive EU created the **NIS platform**
  - To better understand NIS Challenges, Threats and Risks
  - To bring together policy and technical experts to debate about the current and future challenges
  - To influence future R&D in NIS issues

- Three WGs have best established (two mainly operational and one mainly research & innovation oriented):
  - **WG1 on Risk Management including information assurance, risks metrics and awareness raising;** it aims to identify best practices in cyber-security risk management activities, provide guidance to enhance levels of information security and facilitate the voluntary take-up of the practices;
  - **WG2 on Information exchange, including incident reporting and risks metrics for the purpose of information exchange; it** aims to promote the sharing of cyber-threat information and allowing coordination in both the public and private segments of the EU;

NIS WG3 and the SRIA

National Research Council of Italy

WG3 on Secure ICT Research and Innovation (co-chaired by CNR):

Identify key challenges

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

ABOUT THE CYBERSECURITY cPPP

National Research Council of Italy

AIM

1. Foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right for privacy.

2. Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).

3. Coordinate digital security industrial resources in Europe.

BUDGET

The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4 years). Cybersecurity market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) for a total of €1800 mln.

The European Cyber Security Organization (ECSO)

National Research Council of Italy

The private components of the cPPP: The European Cyber Security Organization.

The creation process started on Jan 20th in Brussels with a meeting of near 50 organizations + experts invited by the commission

5 facilitators among the experts present were selected for coordinating the effort of setting up the cPPP. CNR was among the 5 (managing the SRIA WG).

Eventually the ECSO was created and the following documents produced and approved by the EC.

REFERENCE DOCUMENTS

1. Industry proposal
2. Strategic Research and Innovation Agenda (SRIA) proposal

ECSO MEMBERS

National Research Council of Italy

ECSO has been established during June 2016 and on July 5th the ECS-cPPP has been approved by the European Parliament.

218 organisations having formally requested membership … from 27 countries and counting… divided in categories (each represented at the Board of Directors).

- Associations : 18
- Large companies: 55
- Public Administrations: 14 (UK, ES, IT, FR, DE, SK, EE, FI, NO, CY, PL, NL, CZ, AT)
- Regional clusters; 2
- RTO/Universities: 51
- SMEs: 40
- Users/Operators (users are also in large supplier companies): 8

AUSTRIA	6	ITALY	30
BELGIUM	4	LATVIA	1
BE - EU ASS	8	LUXEMBOURG	3
CYPRUS	4	NORWAY	4
CZECH REP.	1	POLAND	6
DENMARK	2	PORTUGAL	5
ESTONIA	4	ROMANIA	2
FINLAND	7	SLOVAKIA	2
FRANCE	21	SPAIN	29
GERMANY	16	SWEDEN	1
GREECE	2	SWITZERLAND	3
HUNGARY	1	THE NETHERLANDS	10
IRELAND	1	TURKEY	2
ISRAEL	2	UNITED KINGDOM	10

European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, …)

ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN COMMISSION

Governance

ECSO - Board of Directors
(management of the ECSO Association: policy / market actions)

INDUSTRIAL POLICY

Coordination / Strategy Committee

R&I

Scientific & Technology Committee

WG 1	WG 2	WG 3	WG 4	WG 5	WG 6
Standardisation Certification / Labelling / Supply Chain Management	Market development / Investments	Sectoral demand (vertical market applications)	Support SME, East EU, Regions …	Education, training, awareness, exercises	SRIA Technical areas Products Services areas

- SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators
- Others (financing bodies, insurance, etc.)
- Large companies Solutions / Services Providers; National or European Organisation / Associations
- Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users
- Public or private users / operators: large companies and SMEs
- NATIONAL PUBLIC AUTHORITY REPRESENTATIVES COMMITTEE: R&I Group Policy Group
- Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO
General Assembly

WG6 SRIA:
Technical areas, Products, Services areas

National Research Council of Italy

Link to KPI (consistent with SRIA and Industry Proposal)

KPI 8 - PRIVACY & SECURITY BY DESIGN: Development and implementation of European approaches for cybersecurity, trust and privacy by design.

KPI 12 - cPPP IMPLEMENTATION MONITORING: Efficiency, openness and transparency of the cybersecurity cPPP implementation process.

Link to EU policies

Activities should be coordinated with the future activities envisaged by the E. Commission as announced in its Communication “Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry”

Objectives

O6.1: Coordination of results and expectations from EC R&I projects

O6.2: Coordination of cybersecurity activities across cPPPs and EIT

O6.3: Support cPPP implementation and H2020 cybersecurity projects

O6.4: Detailed suggestions for the WorkProgramme 2018 - 2020 using an updated and focussed SRIA

WG6 SRIA: Segmentation

National Research Council of Italy

WG 6.1: Coordination and support activities at several levels

- **6.1.1** Link across R&I projects
- **6.1.2** Link with other cPPP / EC initiatives (5G, Cloud, IoT, Big Data, EIT etc.)

WG 6.2: Technical priority areas

- **6.2.1** Assurance / risk management and security / privacy by design
- **6.2.2** Identity, access and trust management (including Identity and Access Management, Trust Management)
- **6.2.3** Data security
- **6.2.4** Protecting the ICT Infrastructure (including Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
- **6.2.5** Security services

WG 6.3: Trustworthy infrastructures

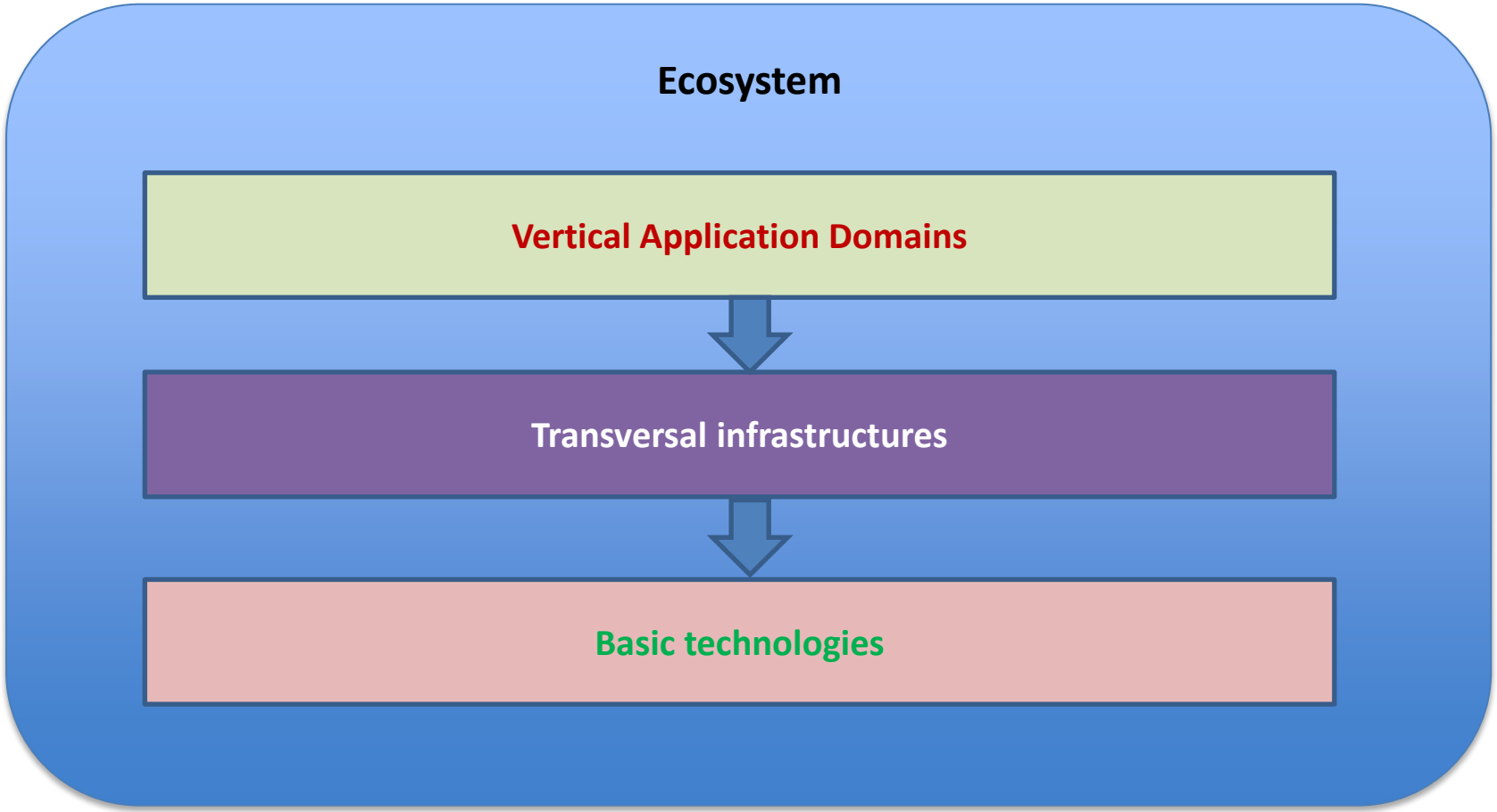
- **6.3.1** Digital citizenships (including identity management)
- **6.3.2** Risk management for managing SOC, increasing cyber risk preparedness plans for NIS etc.
- **6.3.3** Information sharing and analytics for CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)
- **6.3.4** Secure Networks and ICT (Secure and trusted Routers, Secure and Trusted Network IDS, Secure Integration, Open source OS).

WG 6.4: R&I Demonstration / Pilot projects (solutions in different applications); close link with WG3 (verticals) for policy issues

- **6.4.1** Energy, including smart grids
- **6.4.2** Transport
- **6.4.3** Finance
- **6.4.4** Healthcare
- **6.4.5** Smart & Secure Cities
- **6.4.6** Public Services / eGovernment
- **6.4.7** Industrial Critical Systems / Industry 4.0

Linking demand and supply

National Research Council of Italy



Clustering priorities

National Research Council of Italy

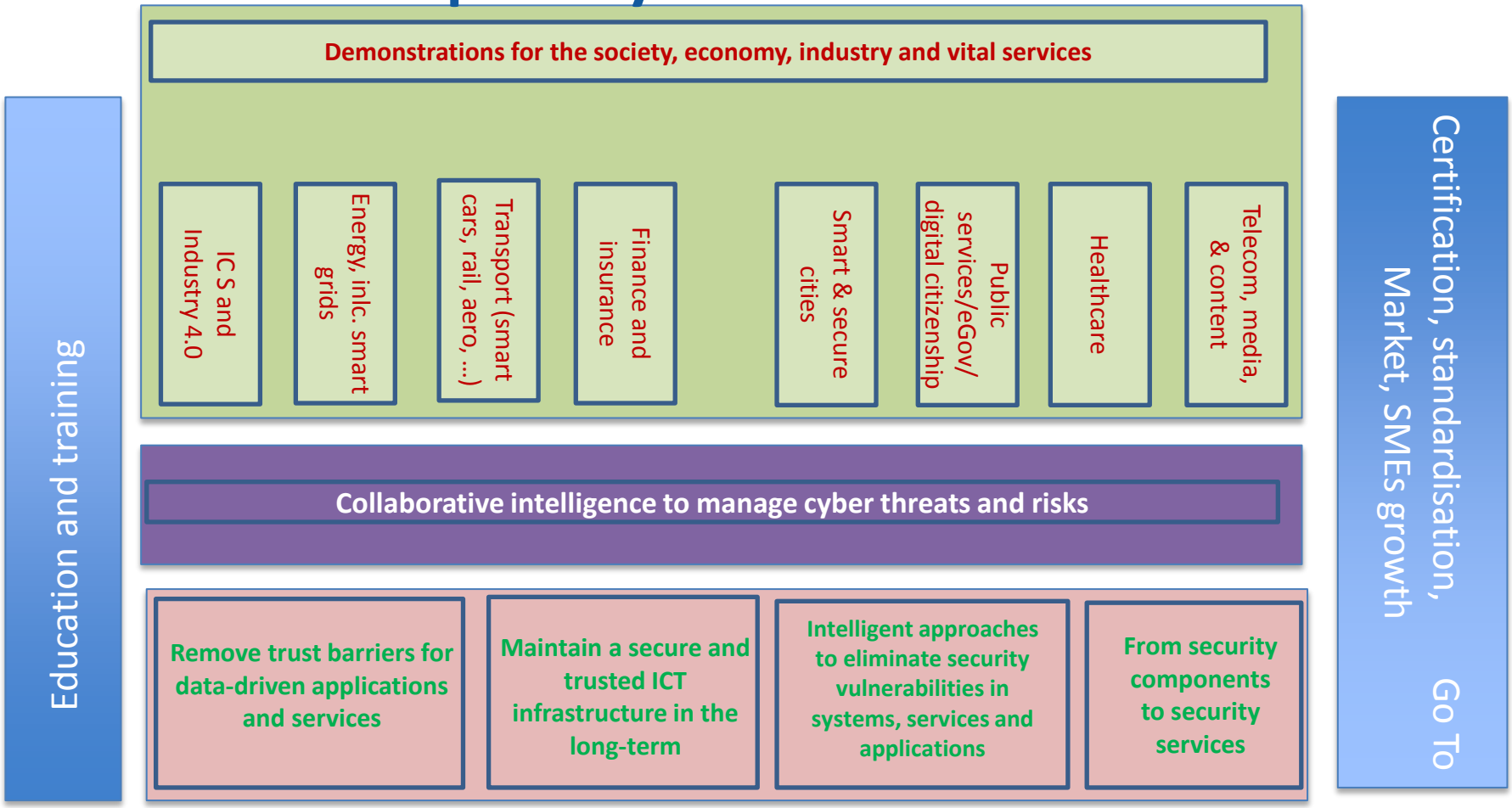
- **4 main thrusts:**
  1. Developing a **European Ecosystem** for the Cybersecurity Market and Digital Society
  2. Applying cybersecurity **technologies and infrastructures** for **protecting vital societal services and the economy**
  3. Developing European **trustworthy cyber solutions for supporting the European cybersecurity strategies** (and policies)
  4. Increase **European excellence and competitiveness** on cybersecurity
- **8 main thematic priority areas (practically the full spectrum of needs, clustered in main areas):**
  - Education and training
  - Certification, standardisation, Go To Market, SMEs growth
  - Demonstrations for the society, economy, industry and vital services
  - Collaborative intelligence to manage cyber threats and risks
  - Remove trust barriers for data-driven applications and services
  - Maintain a secure and trusted ICT infrastructure in the long-term
  - Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
  - From security components to security services

Detailed structure: 8 main thematic priority areas

National Research Council of Italy

- **Education and training**
  - Education, awareness and skills development
  - Simulation and Cyber range facilities
- **Certification, Standardisation, Go To Market, SMEs growth**
  - Certification
  - Goto- market
  - Digital instruments for SMEs
- **Demonstrations for the society, economy, industry and vital services**
  - Industry 4.0, Energy, Smart Cities, Transportation, Public sector/E-government, Healthcare, Finance and Insurance, Telecom, media, and content
- **Collaborative intelligence to manage cyber threats and risks**
  - Situation Awareness and risk assessment
  - High-assurance prevention and protection
  - Information sharing and security analytics
  - Cyber threat management: response and recovery
- **Remove trust barriers for data-driven applications and services**
  - Data security and privacy
  - ID and Distributed trust management (including DLT)
  - User centric security and privacy
- **Maintain a secure and trusted infrastructure in the long-term**
  - Network and system security, migration strategies
  - Trusted execution in a virtualised environment
  - Quantum resistant crypto
- **Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain
  - Security-by-design
- **From security components to security services**

Main thematic priority areas



Conclusion

- Cybersecurity is very relevant
- Europe is acting
- CNR had a facilitator role for NIS platform and cPPP
- ECSO started very well
- The field is still growing in the cyber crime and defence part
  - New preparatory action in defence research (EDA)
- The next step for FP9 (2021+)
  - Consider a Joint Undertaking (see the recent strategy)