ECSO WG6
Strategic Research and Innovation Agenda

Hervé Debar

Télécom SudParis

EUNITY Coordinator

What is EUNITY

- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan
- Our goals:
  - Raise awareness of European views and activities on cybersecurity in Japan
  - Understand similar activities in Japan to complete European research roadmaps, e.g. with joint activities

What is ECSO

- Association established in Brussels
  - “Industry Proposal”
- Contractual Public-Private Partnership (cPPP)
  - Joint effort between the European Commission and the private sector
  - Leverage public research funding to develop business activity.
- Signed July 2016
  - Other cPPPs exist: DVA (big data); 5G (mobile 5G); EFFRA (smart industry), …
  - cPPP could evolve into a more ambitious structure (Joint Undertaking- like) following the recent EU cybersecurity strategy (Sept 2017)

ECSO Intro/L.Rebuffi

6 working groups

- WG1 (standards / certification / label / trusted supply chain)
- WG2 (market / funds / international cooperation / cPPP monitoring)
- WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities)
- WG4 (SMEs, Regions, East EU)
- WG5 (education, training, awareness, cyber ranges…)
- *WG6 (SRIA)*

WG6 Subgroups

- SWG 6.1: Ecosystem
  - 6.1.1 Link across R&I projects
  - 6.1.2 Link with other cPPP / EC initiatives (5G, Cloud, IoT, Big Data, EIT etc.)
- SWG 6.2: Vertical application domains
  - 6.2.1 Energy, including smart grids
  - 6.2.2 Transport
  - 6.2.3 Finance
  - 6.2.4 Healthcare
  - 6.2.5 Smart & Secure Cities
  - 6.2.6 Public Services / eGovernment
  - 6.2.7 Industrial Critical Systems / Industry 4.0
- SWG 6.3: Trustworthy transversal 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).
- SWG 6.4: Technical priority areas
  - 6.4.1 Assurance / risk management and security / privacy by design
  - 6.4.2 Identity, access and trust management (including Identity and Access Management, Trust Management)
  - 6.4.3 Data security
  - 6.4.4 Protecting the ICT Infrastructure (including Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
  - 6.4.5 Security services

Detailed structure: 7 main thematic priority areas

6.1

- 1 European Ecosystem for the Cybersecurity
  - Cyber Range and simulation
  - Education and training
  - Certification and standardisation
  - Dedicated support to SMEs

6.2

- **2 Demonstrations for the society, economy, industry and vital services**
  - Industry 4.0
  - Energy
  - Smart Buildings & Smart Cities
  - Transportation
  - Healthcare
  - E-services for public sector, finance, and telco

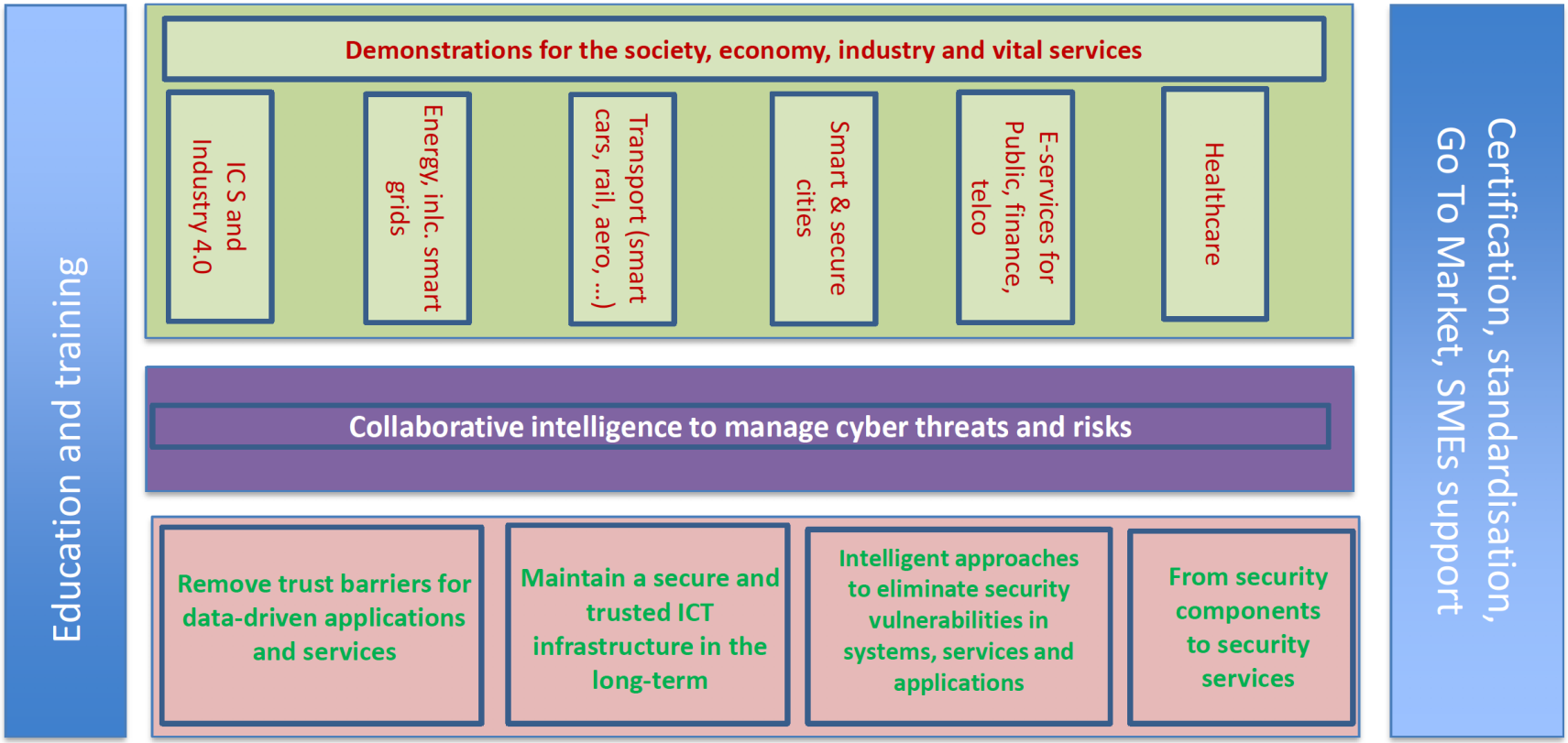
6.3

- **3 Collaborative intelligence to manage cyber threats and risks**
  - GRC: Security Assessment and Risk Management
  - PROTECT: High-assurance prevention and protection
  - DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection
  - RESPONSE and RECOVERY: Cyber threat management: response and recovery

6.4

- **4 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
- **5 Maintain a secure and trusted infrastructure in the long-term**
  - ICT protection
  - Quantum resistant crypto
- **6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain for resilient systems
  - Security and privacy by-design
- **7 From security components to security services**

From basic R&I building blocks to products



WG6 Initial Activities

- Informal suggestions delivered to the European Commission for the 2018 – 2020 H2020 Work Programme:
  - organisation of the priority topics identified by ECSO in the SRIA (good acceptance of suggested priorities).
- Contacts with other PPPs and similar EU activities to coordinate objectives.

ICT WP2018-2020

Indirect contribution to cyber-security

- ICT-08-2019: Security and resilience for collaborative manufacturing environments (Joint with FoF)
  - Practical solutions for securing digital collaboration between manufacturing environments
- ICT-10-2019-2020: Robotics Core Technology
  - Security by design for standardized robotics environments.
- ICT-11-2018-2019: HPC and Big Data enabled Large-scale Test-beds and Applications
  - Secure access and provisionning
- ICT-15-2019-2020: Cloud Computing
  - Address stringent security and data protection requirements
- ICT-27-2018-2020: Internet of Things
  - End-user trust in security and privacy of the IoT
- ICT-28-2018: Future Hyper-connected Sociality
  - Trustful and Secure Data Ecosystem for Social Media and Media
    - Content verification
- Calls schedule january 2018, april 2018, november 2018, january 2019, march 2019

Digital Europe 2018-2020

Indirect contribution to cyber-security

- DT-ICT-01-2019: Smart Anything Everywhere
  - Man-machine collaboration
  - Security and privacy
- DT-ICT-02-2018: Robotics - Digital Innovation Hubs (DIH)
  - DIHs should address ethical, data privacy and protection issues, and consider cyber-security issues (including security by design).
- DT-ICT-06-2018: Coordination and Support Activities for Digital Innovation Hub network
  - Secure and safe implementation of pilots
- DT-ICT-08-2019: Agricultural digital integration platforms
- Calls opening end of October, deadline April 2018

Cybersecurity (*H2020-SU-ICT-2018-2020*)

Directly contributing to cybersecurity cPPP

- SU-ICT-01-2018: Dynamic countering of cyber-attacks
  - Cyber-attacks management - advanced assurance and protection
    - Recognition of malicious blocks
    - Secure execution environments
    - Feedback to users
  - Cyber-attacks management – advanced response and recovery
    - Support human operators
    - Include theat intelligence and information sharing
    - Explore forensics, penetration testing, investigation and attack attribution services
    - Handling of encrypted network traffic
- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems
  - Cybersecurity/privacy audit, certification and standardisation
  - Trusted supply chains of ICT systems
  - Designing and developing privacy-friendly and secure software and hardware
- SU-ICT-04-2019: Quantum Key Distribution testbed

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (1)

- Cybersecurity/privacy audit, certification and standardisation
  - (i) design and develop automated security validation and testing, exploiting the knowledge of architecture, code, and development environments (e.g. white box)
  - (ii) design and develop automated security verification at code level, focusing on scalable taint analysis, information-flow analysis, control-flow integrity, security policy, and considering the relation to secure development lifecycles,
  - (iii) develop mechanisms, key performance indicators and measures that ease the process of certification at the level of services and
  - (iv) develop mechanisms to better audit and analyse open source and/or open license software, and ICT systems with respect to cybersecurity and digital privacy.
- Trusted supply chains of ICT systems
- Designing and developing privacy-friendly and secure software and hardware

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (2)

- Cybersecurity/privacy audit, certification and standardisation
- Trusted supply chains of ICT systems
  - (i) develop advanced, evidence based, dynamic methods and tools for better forecasting, detecting and preventing propagated vulnerabilities,
  - (ii) estimate both dynamically and accurately supply chain cyber security and privacy risks,
  - (iii) design and develop security, privacy and accountability measures and mitigation strategies for all entities involved in the supply chain,
  - (iv) design and develop techniques, methods and tools to better audit complex algorithms (e.g. search engines), interconnected ICT components/systems
  - (v) devise methods to develop resilient systems out of potentially insecure components
  - (vi) devise security assurance methodologies and metrics to define security claims for composed systems and certification methods, allowing harmonisation and mutual recognition based on evidence and not only on trust.
- Designing and developing privacy-friendly and secure software and hardware

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (3)

- Cybersecurity/privacy audit, certification and standardisation
- Trusted supply chains of ICT systems
- Designing and developing privacy-friendly and secure software and hardware
  - (i) security and privacy requirements engineering (including dynamic threat modelling/ attack trees, attack ontologies, dynamic taxonomies and dynamic, evidence based risk analysis),
  - (ii) embedded algorithmic accountability (in order to monitor the security, privacy and transparency of the algorithms/software/systems/services),
  - (iii) system-wide consistency including connection between models, security/privacy/accountability objectives, policies, and functional implementations,
  - (iv) metrics to assess a secure, reliable and privacy-friendly development,
  - (v) secure, privacy-friendly and accountability-enabled programming languages (including machine languages), hardware design languages, development frameworks, as well as secure compilation and execution,
  - (vi) novel, secure and privacy-friendly IoT architectures

Joint topics with 5G

- ICT-18-2018: 5G for cooperative, connected and automated mobility (CCAM)
  - Security for automotive V2x
- ICT-19-2019: Advanced 5G validation trials across multiple vertical industries
  - Consistent deployment of cyber-security
- ICT-20-2019-2020: 5G Long Term Evolution
  - Trusted workload deployment
  - Secure provisioning and deployment
  - Trusted multi-tenancy

Joint topics with BDVA

- The areas of interest for collaboration between BDVA and ECSO can be summarised as follows:
  - Cyber security to make big data analytics resilient and robust: trustworthy data;
  - Big data analytics for cyber security to prevent, infer and detect potential attack;
  - Leverage big data techniques, artificial intelligence and cyber security for application areas and verticals: joint approach.
- ICT-12-2018-2020: Big Data technologies and extreme-scale analytics
  - Secure federated systems
- ICT-13-2018-2019: Supporting the emergence of data markets and the data economy
  - Trusted and secure platforms
  - Privacy-aware analytics
  - Personnal and Industrial data platforms
- ICT-26-2018-2020: Artificial Intelligence
  - SRIA for AI including cyber-security

Thank you for your attention

Questions ?