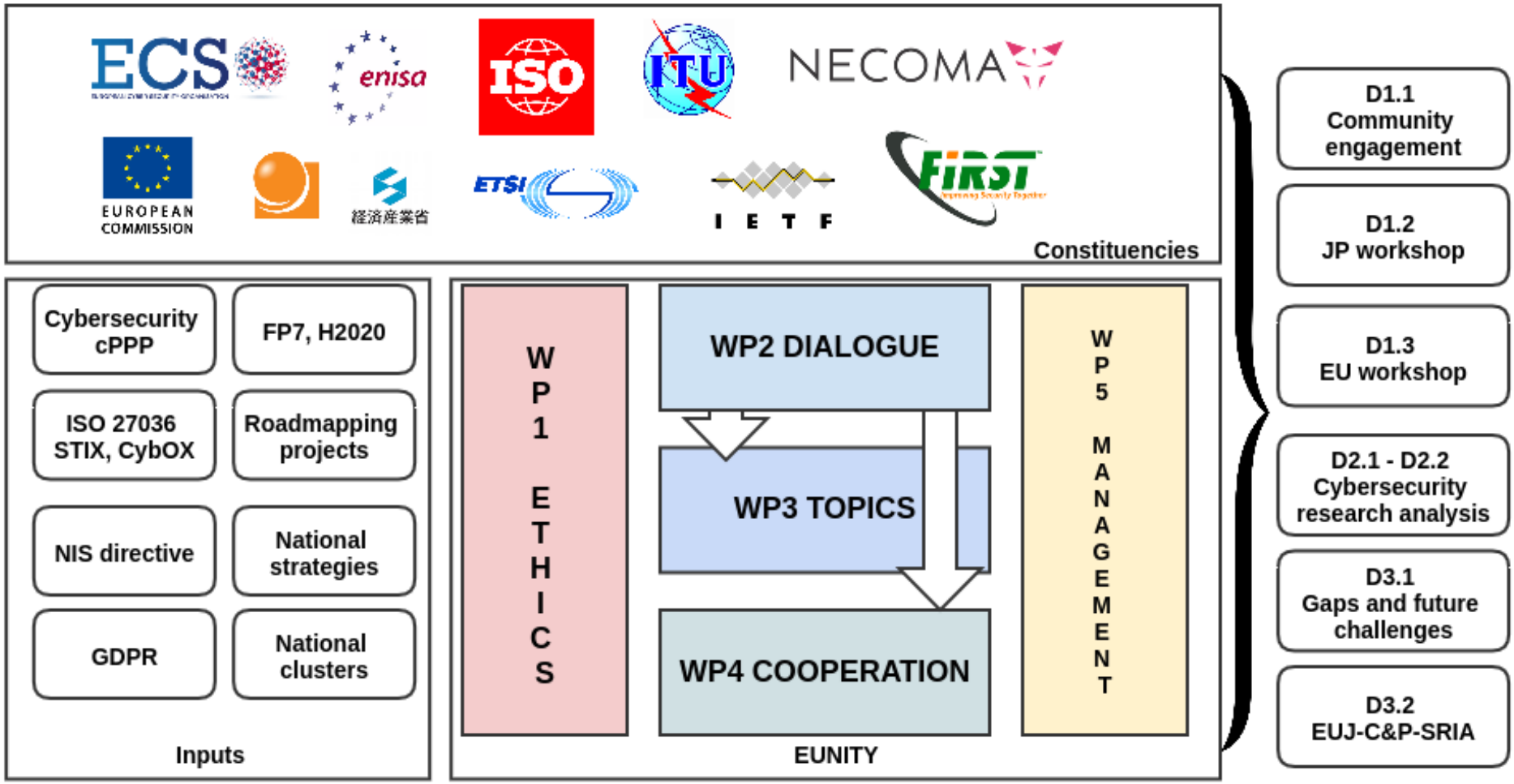
EUNITY Project Outcomes

Identified gaps, recommendations and roadmap

Gregory Blanc (IMT/Télécom SudParis)

5th France-Japan Cybersecurity Workshop
April 23rd, 2019 – Kyoto

Implementation



1st Year Main Results

- 1st EUNITY workshop (Oct. 2017)
  - Invited talks from Baiba Kaskina (CERT.LV) and Afonso Ferreira (CNRS)
  - ~60 participants incl. industry, academia, policy makers, CERT, end-users
- Visit of ICS-CoE in France, Greece
  - September and December 2017
  - Funding schemes in FR and EU
  - Smartgrid, SCADA and CPS security
  - Formal methods
- Links with ECSO, ENISA, ETSI, etc.
  - Presentation for ECSO WG2, WG6
  - Panel on certification at Cyberwatching.eu

1st workshop key highlights

- CERT
  - Similar expectations in both regions
    - Training actions undertaken by JPCert in Africa
- Industry
  - Strong SME ecosystem in Japan
  - Main issue is cost of solutions (and their operation)
    - Secondary issue is the ability to select and operate the proper tools.
- Legal and privacy
  - Different attitude towards legal processes: guidelines
  - Equivalent interest in privacy
  - Questions on the global reach of GDPR
    - Possibly better preparedness of US and JP companies than EU companies.
- Research
  - Topics of the 2017-2020 calls considered relevant

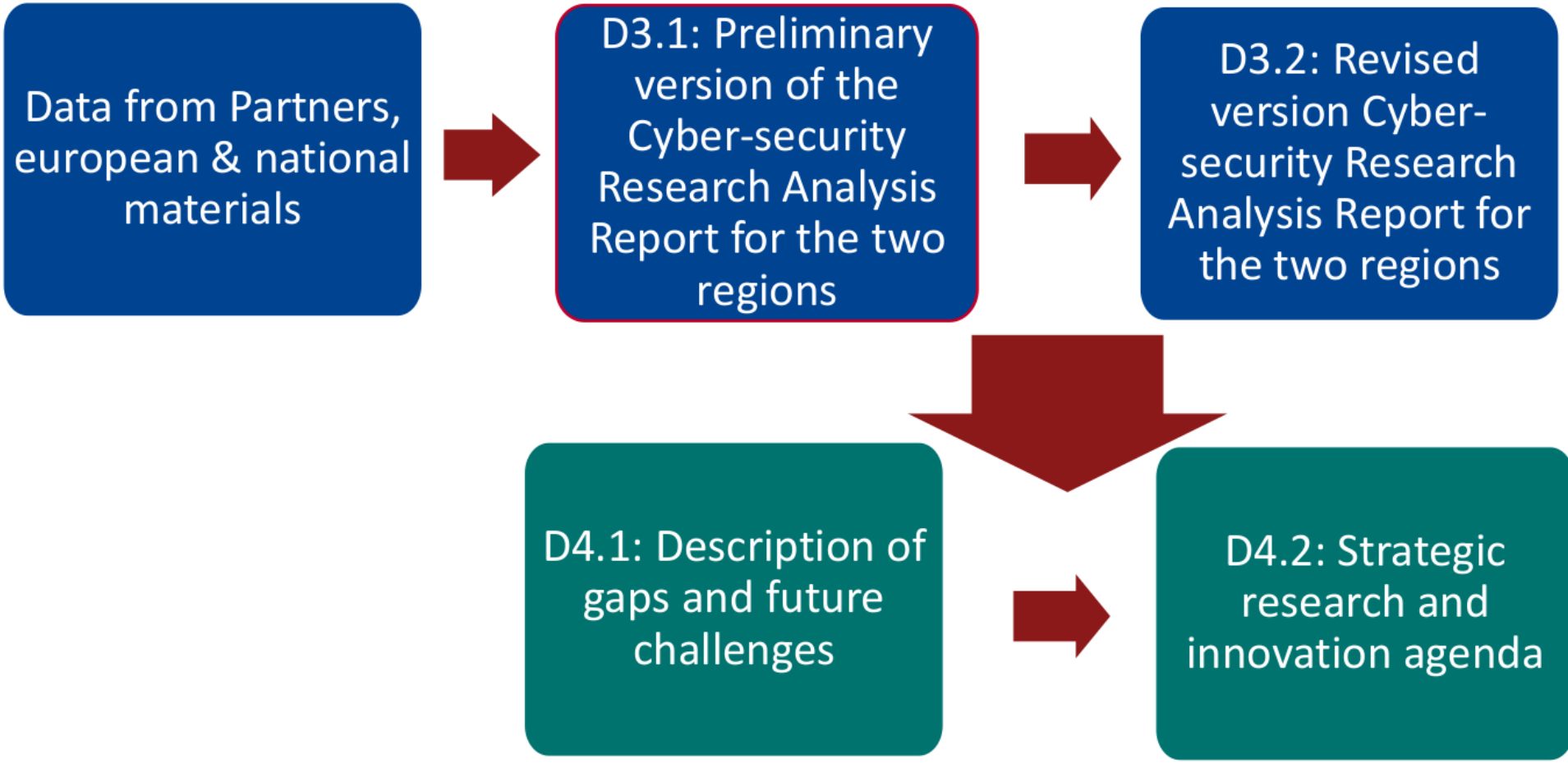
2nd Year Main Results

- 2nd EUNITY workshop (Jan. 2019)
  - Joint with ECSO, after appearance at FIC'19
  - 60+ participants incl. mainly industry and policy makers from ECSO and invited speakers from Japan (MIC, JETRO, CRIC-CSF, JPCERT)
- Visit of ICS-CoE in France (Sept. 2018)
  - ICS and CPS security
- Visit of FEPC in France (Feb. 2019)
  - Power grid security
- More integration w/ ECSO, liaison extension
  - Joint workshop, talks in WG2 and WG6
  - Participation in the EU Cybersecurity CCs
  - Joining the 5G Industry Alliance

Next Steps

- 3rd EUNITY workshop in Kyoto (Apr. 2019)
  - Research and innovation aspects
  - Education and training aspects
  - Future collaboration opportunities
- M24 deliverables
  - D2.2: 2nd workshop proceedings
  - D3.2: revised cybersecurity research analysis for the two regions
  - D4.2: strategic research and innovation agenda
- Final review in Brussels (June 24th, 2019)
- DG CNECT Policy Event (June 25th, 2019) – brief with AEGIS
- Dissemination in ECSO, and other PPPs as well as CCCs

EUNITY analysis data flow



EUNITY methodology

- Identification and description of **funding schemes**
- Overview of main directions and identification of **strong/weak point**
- Analysis of the current **role** of different units (SMEs, RTOs, etc.)
- Analysis of **long-term programs**

D3.1: Most important findings

- Despite **many similarities and overlaps** between the two regions, there are **legal and policy** gaps
- **Various** programs and institutions **funding R&I** in the field of cybersecurity and privacy
- Strong and weak points are often common to both regions
- Industry in both regions identified areas of **great interest**
  - e.g., **5G**, **Big Data**, **IoT**
  - **Organizations** to promote and address challenges
- Common research interests include (aside from crypto):
  - Privacy of Big Data
  - Availability and reliability of open data
  - Security of 5G communication networks and protocols
  - Legal aspects to enable technology developments

D3.2: Legal challenges and policy blockers

- Comparison of EU and JP legal frameworks
  - **Scope imbalance**: EU framework extends to orgs offering services in EU and targeting market behaviors
  - **Unaligned concept of PII**: EU takes a more protective and data-subject-driven perspective
  - **Extended information rights** in EU
  - **Significantly higher sanctionary regime**
  - **More advantageous liability regime** in JP
- Potential policy **blockers**
  - Processing of IP addresses
  - Concerns around the respect of the right to privacy in JP wrt to anti-terrorism laws (intelligence, investigation and prosecution)

D3.2: Areas of collaboration

- Education and awareness
  - At **various levels** (undergraduate, postgraduate, professional training, general public awareness)
  - Promotion of **personnel exchange**
- Standards and regulations
  - **Harmonization** among government and industrial associations
  - Guidelines by industry **sector**
  - Sharing cybersecurity **best practices**
- Information sharing
  - Sharing environments to **monitor** attacks
  - Sharing **intelligence** among vendors and security orgs
  - Continuous **exposure** in conferences/exhibitions
  - Continuous **workforce** activities, e.g., industry ISAC

D4.1: Gaps and challenges

- **Legal and policy**
  - EU: lack of cooperation with police, need for certification
  - JP: limited number of specialized agencies, need for cross-fertilization with other technology sectors
- **Research and innovation**
  - EU: AI, IoT, blockchain, cryptocurrencies; trust management in the digital society
  - JP: lack of cross-cutting education program; need to integrate non-technical fields in research
- **Industry and standardization**
  - EU: foreign-supplier dominated market; industrial policies not yet addressing cybersecurity issues
  - JP: low mobility between suppliers and adopters; lack of availability of recent technology to all businesses

D4.2: Collaboration perspectives

- Legal and policy
  - Common **privacy** framework (**data exchange**)
  - **Collaborative channel** between researchers, CERTs and software vendors
  - Common regulation for **certification** schemes
- Research and innovation
  - **Joint education** programs together with exchange
  - International **cyber-exercises**
  - Joint EU-Japan **R&D&I programs** for projects
  - Common **intelligence**, **information exchange** protocols
- Industry and standardization
  - Common **data systems** for Big Data and IoT
  - Common roadmap for **international standardization**
  - Joint collaboration for **marketing** cybersecurity solutions
  - Cooperation to study flow of information **across borders**

Changes in Horizon Europe

- Starts in 2021
- New priorities include **cybersecurity**, **AI**, **5G**, as well as **energy**
- Beware: increase in **dual funding**
    - European Defense Organization is partially funding projects, related to cyberdefence
- Work programme is still under development
- PPPs will terminate in 2020 (incl. CPPP)
  - New legislation will be proposed
  - Existing PPPs are transitioning

Stay tuned !

- Twitter
  - @eunity_project
- Web
  - www.eunity-project.eu
- Contact points
  - EU coordination : herve.debar@telecom-sudparis.eu
  - JP contact point : youki-k@is.naist.jp