Project Details :

Start date: **June 1st 2017**

Duration: **24 Months**

Contact:

Prof. Herve Debar (herve.debar@telecom-sudparis.eu)

@eunity_project

www.eunity-project.eu

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016).

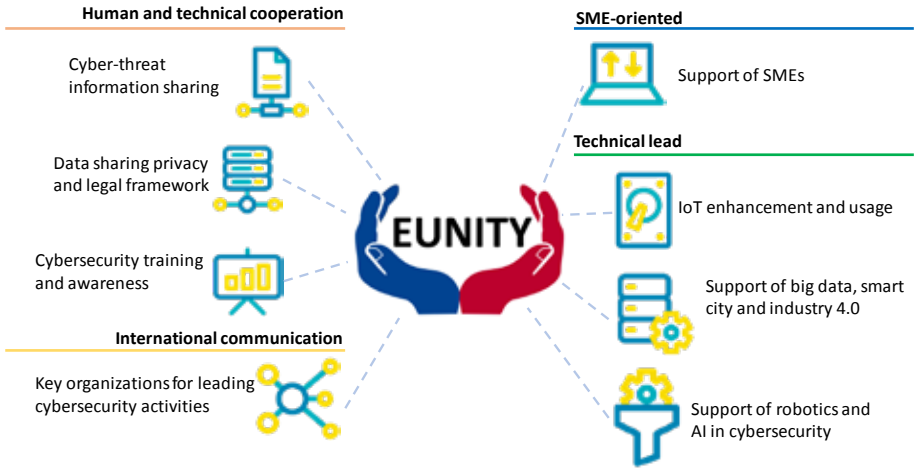
EUNITY

Cybersecurity and Privacy Dialogue between Europe and Japan

Agenda and opportunities for cybersecurity collaboration Europe – Japan

www.eunity-project.eu

Key propositions for cybersecurity cooperation Europe - Japan



Summary of cybersecurity challenges Europe - Japan

Area — Legal and policy

EUROPE
- Cyber-defence: lack of cooperation with policy and third parties;
- Criminal law: different law provisions and treaties;
- AI and IoT software: lack of security and need for certification

JAPAN
- Lack of cybersecurity accelerators and academic cybersecurity centres;
- Lack of contractual public-private partnership;
- Cross fertilization: need to interoperate additional features of IT systems;

Area — Research and innovation

EUROPE
- Growth of spam, web-based attacks, ransomware and botnets;
- New frontiers of R&I: cryptocurrencies, blockchain, IoT and AI;
- Threats to trust management in the digital society;

JAPAN
- Cybersecurity integration with different areas of expertise (e.g. human, design, etc.)
- Holistic security expertise;
- Cybersecurity education;

Area — Industry and standartization

EUROPE
- Cybersecurity market controlled by global suppliers with headquarters outside of Europe;;
- European industrial policies not yet addressing specific cybersecurity issues;
- Established standards and processes for deploying business models or new technologies;

JAPAN
- Low mobility of experts across technology suppliers and adopters;
- Making latest technology offers available to all type of companies;
- Difficulties for organization to adopt cybersecurity naturally in their business;

Cooperation opportunities

I	Cyber-threat information sharing
Context	Difficulty to share information No common legal framework
Scope	Design and development of methodologies, tools and data format Assurance of data exchange and harmonization of legal frameworks
II	**Data sharing privacy and legal framework**
Context	Administrative requests and complex additional work Public and private partners under the same umbrella
Scope	Creation of tools and processes in a common platform for European and Japanese Definition of privacy-preserving and data-centred security for data sharing
III	**Cybersecurity training and awareness**
Context	Employees are usually considered the “weakest part of the chain” Trainings should not only look at the Europe-Japan relationship
Scope	Creation of coordinated training programs for legal, research, education and industry between the two regions Courses for development of strong trained experts
IV	**Key organizations for leading cybersecurity activities in both areas**
Context	Shared organizational and certification mechanisms Permanent authority with scope and mandate on both territories
Scope	Selection of two permanent authorities that lead cybersecurity discussions Creation of joint activities, policies and networks of competences
V	**Support of SMEs**
Context	Problems for finding the right cybersecurity tools Difficulty to access common market
Scope	Creation of a platform for SMEs for accessing cybersecurity solutions Easy access to funding opportunities in both areas and as joint participation
VI	**IoT enhancement and usage**
Context	Need for a common perspective for supporting capabilities of service providers Technical regulations, universal protocols and standards
Scope	Development of IoT cybersecurity information database and information sharing Creation of common protocols and policies for trusted usage of IoT devices
VII	**Support of big data, smart city, and industry 4.0**
Context	Digitally transforming businesses, impacting different critical areas Need for common data systems that allow free exchange of information
Scope	Creation of processes and tools for integrating cybersecurity Research and integration of human-oriented approaches
VIII	**Support of robotics and AI in cybersecurity**
Context	Policy and legal systems are not mature enough yet Need of ethical recommendations in the two regions
Scope	Definition of common cybersecurity principles and rules for enabling a safe usage of AI in different technologies