Institute of Science and Technology NAIST

東京大学 THE UNIVERSITY OF TOKYO

明治大学 MEIJI UNIVERSITY

JAIST JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

JPCERT CC Japan Computer Emergency Response Team Coordination Center JPCERT コーディネーションセンター

NICT National Institute of Information and Communications Technology

Institut Mines-Télécom

Atos

FORTH

NASK

KU LEUVEN

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

Analysis of cybersecurity gaps and challenges of Europe-Japan

www.eunity-project.eu

Cybersecurity challenges in EU-Japan

Legal and policy challenges

Europe
- Cyber defense: lack of cooperation with police and third parties
- Criminal law: different law provisions and treaties amongst national entities
- AI, IoT, software: lack of security. Need for certification

Japan
- Increase number of specialized agencies. Lack of cybersecurity start-ups and researches for legal and policy topics
- Cross-fertilization: need to interoperate additional features of IT systems

Research and innovation challenges

Europe
- Current threats: web-based attacks, spam, ransomware, botnets, ransomware evolution
- New frontiers: AI, IoT, Blockchain and cryptocurrencies
- Trust management in the digital society

Japan
- Cryptocurrencies: lack of expertise
- Cybersecurity education: lack of a crosscutting program for universities and research centers covering different areas
- Cybersecurity research: need to integrate non-technical fields in research areas

Industry and standardization challenges

Europe
- Global cybersecurity and ICT market dominated by global suppliers from outside Europe
- European industrial policies not yet addressing specific cybersecurity issues
- Establishing standards and processes for deploying new technologies or business models

Japan
- Low mobility of experts across technology suppliers and adopters
- Making latest technology offers available to all type of companies (large, medium, small)
- Difficult for organizations to adopt cybersecurity naturally in their business

Perspective of collaboration EU-Japan

Legal and policy opportunities

- Common privacy framework for enabling personal data exchange
- Data protection framework for police and law enforcement cooperation
- Harmonization of IoT certifications for security standards
- Collaboration at governance level (European and Japan centralized institutions)
- Support of training for best practices and business optimization in public and private domains

Research and innovation opportunities

- Joint education programs (online and on-site) together with exchange programs for students and employees
- Creation of international cyber-exercises
- Joint portal for sharing information about research and development projects in both areas
- Development of common cybersecurity intelligence and information exchange protocols and tools
- Creation of joint EU-Japan programs for conducting R&D&I projects on common topics

Industry and standardization opportunities

- International cooperation for studying cybersecurity challenges and flow of cybersecurity information across borders
- Networks for exchanging knowledge and training for improving cybersecurity culture in companies
- Common data system between both regions for big data and IoT
- Develop a joint roadmap with a common process and priorities for ongoing international standardization work
- Joint collaboration for markets of cybersecurity solutions for SMEs