Analysis of challenges and opportunities for cooperation EU-Japan

Gregory Blanc (IMT) on behalf of Jose Francisco Ruiz (Atos)

European Commission

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016).
The information reflects only the views of the project owner.

Table of contents

- Introduction
- Challenges and recommendations Europe - Japan
- Opportunities for cooperation
- On-going work
- Conclusions

Introduction

- **Objective:** increase cooperation of cybersecurity activities between Europe and Japan

- **Output:** strategic research and innovation agenda

Introduction

- Key questions:
  - What are the needs?
  - What is the status of cybersecurity in Europe and Japan?
  - What are the existing mechanisms?
  - What is missing?
  - How can cooperation between both areas be improved?

Introduction

First key activity

- Research and identify status, gaps and challenges in Europe and Japan

- **Three different areas**:

Legal and policy

Research and innovation

Industry

Introduction

Second key activity

- Identify gaps and challenges in Europe and Japan

Different needs

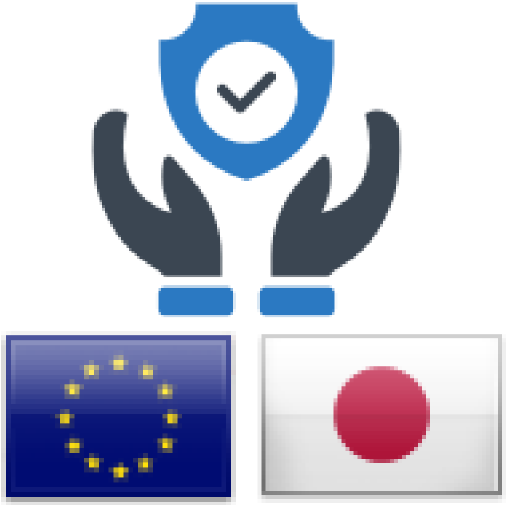
Diverse specializations of cybersecurity

Particular cybersecurity situations (e.g. geopolitical, industry, citizens, etc.)

Introduction

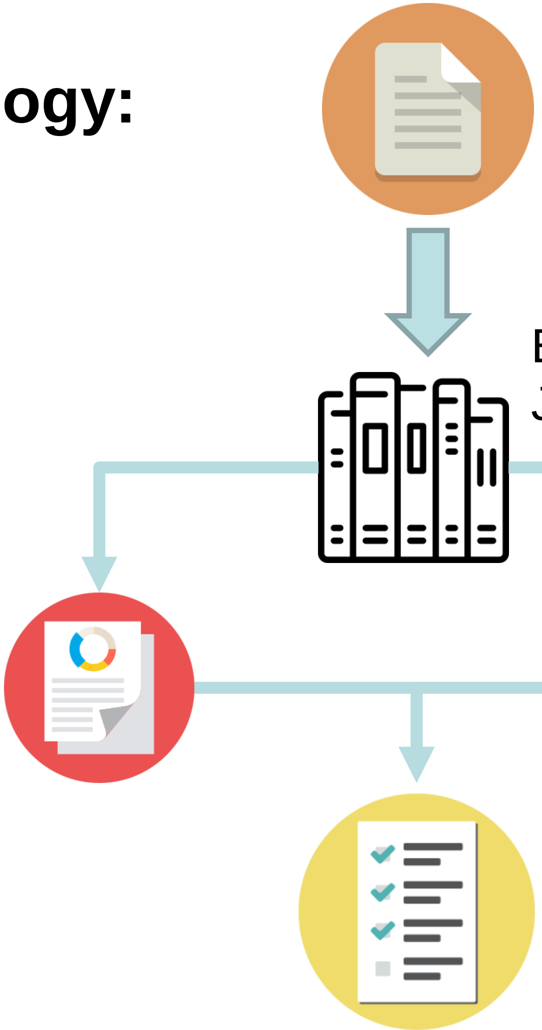
Third key activity

- Opportunities for cooperation in Europe and Japan
- Study from Europe and Japan perspective



Introduction

Methodology:



Cybersecurity research analysis for the two regions

European and Japanese knowledge

European report

Japanese report

Collaboration and challenges Europe - Japan

Europe
Legal and policy - Challenges

- Cybersecurity is a cross-cutting topic
- Laws and policies **must harmonize**
- **GDPR**
- Software vulnerabilities
- Europe needs an **institution that takes the lead in most** cyber security challenges
- **Cross-border nature** of online crimes leads cyber defense to be at a **structural disadvantage**

Europe

Legal and policy - Recommendations

- **Coordination of** legal and policy effort
- **Collaborative channel** between security researchers, CERTs and software producers
- **Competence hub** with leading tasks on policy and law making
- **Harmonization** of criminal law provisions and treaties
- Improving **police cooperation**

Japan

Legal and policy - Challenges

- Japan has a **limited number** of specialized agencies with **limited number** of workforce
- **Cybersecurity investment** in the private sector is much larger than that of public sector
- **Society 5.0**

Japan

Legal and policy - Recommendations

- Introducing **policy instruments** to facilitate innovations in cybersecurity
- Cybersecurity is only **one desirable characteristic of IT** (scalability, agility, etc.)
- **Develop cybersecurity policy programs** that deal with particular platforms
- Elaborate a **public-private partnership**

Europe

Research and innovation - Challenges

- Malware
  - New malware attacks have reached **22 million samples** in the first quarter of 2017
- Ransomware Evolution
- **Cyber threat environment** is even more **complex** (and evolving)
- **Criminals using analytics** for attacking
- **SMEs lack in preparedness** for cyber attacks

Europe

Research and inn. - Recommendations

- **Regulations and state support**
- Need of a **methodology for transparency**
- Work on the **defense strategy, training programs and better adaptation of ICT**
- Work along with **technical, research and educational resolutions**
- **Funding** is of great need in the training of cybersecurity programs
- **Gap** of national educational programs

Japan

Research and innovation - Challenges

- **Lack of expertise** on formal methods, system security and network security
- **Compartmentalized structure** of research
- A **crosscutting security education program is no longer funded**
- **Universities do not guarantee cross-fertilization**

Japan

Research and inn. - Recommendations

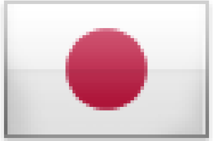
- Fund **programs** that **incentivize** academic entities to work with private sector
- **Incentives for students** for cybersecurity and privacy as their **topic of study** (realism of exercises)
- **Crosscutting** cybersecurity education programs

Europe Industry - Challenges

- **Global cybersecurity and ICT market** dominated by global suppliers from **outside** Europe
- European industrial **policies not yet addressing** specific cybersecurity issues
- **Fragmentation** of the European cybersecurity market
- Industrial infrastructures are **increasingly exposed** to cyber threats

Europe
Industry - Recommendations

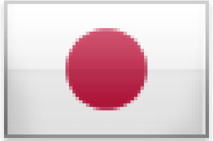
- **Address threats** to online platforms
- **Support small and medium enterprises** to be competitive in the digital economy
- Invest in the **use of cybersecurity technologies** in vertical sectors
- Cross-border exchange of information
- Need for **trust in industry and society**
- Secure communications in connected devices

Japan 

Industry - Challenges

- **Deep split** between technology suppliers and adopters
- **Low mobility** of cybersecurity experts across technology suppliers and adopters
- **Lack** of career path
- Most of the latest technology offerings are **only available**
  - Most of small and medium businesses **remain unprotected**

Japan



Industry - Recommendations

- **Cybersecurity adoption** addressed at industry associations
- Industry groups should analyze the root cause of **skepticism that hinder cybersecurity adoption**
- Focus in **economy of scale** and deliver affordable products and services SMEs
- Business partnerships and strategic agreements **among technology suppliers and adopters**

Europe - Japan
Strategic agenda

- Situation across the two regions is by nature substantially different
- Imminent issue of the privacy framework between Japan and the European Union
- Exchange of best practices
- Cyber-dialogue between Europe, Japan and NATO
- Intelligence sharing and participation in bilateral or multilateral counter terrorism platforms

Europe - Japan Strategic agenda

- Legal and policy:
  - Mutually accepted cybersecurity certification authorities
  - Sharing of best practices and business optimization
  - Training of judicial and legal professionals
  - Information sharing legal framework (support of GDPR)
  - Harmonization of criminal laws
  - Improve police cooperation

Europe - Japan Strategic agenda

- Research and innovation:
  - Joint education programs (online and on-site)
  - Exchange programs for students and employees
  - International cyber exercises
  - Development of new protocols and tools enabling exchange of information
  - Creation of joint EU-Japan programs which aim at conducting R&D&I projects

Europe - Japan Strategic agenda

- Industry:
  - Industrial revolution lead by robots
  - IoT joint work in EU-Japan
  - Mechanisms for international cooperation of cyber-intelligence
  - EU-Japan information sharing platform
  - Cybersecurity solutions for SMEs in EU-Japan
  - Cybersecurity to provide information for all levels of the organization (technical expert, CEO, etc.)

Europe - Japan
Beneficial aspects

- Optimization of grants usage
- Economic bootstrapping
- Co-development
- Market extension
- Institutionalization of funding strategy
- Cross-industry funding
- Workforce development

Europe - Japan
Beneficial aspects

- Cybersecurity guidelines
- Policy programs
- Public private partnership
- Joint industry/academia funding programs
- Human-centric approaches
- AI-driven cybersecurity research
- Considering SMEs
- Technology associations
- Incorporation of standards

On-going work

- Defining a strategic research and innovation agenda for the European Commission
- Guidelines for European and Japanese roadmaps
- Feedback of workshops, end-users, etc. help to shape the cooperation between both regions

Conclusions (I)

- Europe and Japan have specific needs that could be solved via cooperation
- The GDPR implies work on the Japanese side in order to have a common data-sharing framework
- Common funding programmes for research and innovation
- Exchange of students and employees for experience and expertise sharing

Conclusions (II)

- SMEs are part of the vital industry fabric
- Increase trust of cybersecurity for citizens
- Cyber-crime data sharing
- Enhance vertical domains with cybersecurity (e.g. IoT, 5G, etc.)
- Cyberattacks evolve continually, and so must do cybersecurity and cooperation

https://www.eunity-project.eu

https://twitter.com/eunity_project @eunity_project

https://www.linkedin.com/

Contact:

Project Coordinator

Prof. Hervé Debar

herve.debar@telecom-sudparis.eu

European Commission

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

The information reflects only the views of the project owner.