Agenda and opportunities for cybersecurity collaboration Europe – Japan

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

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
### Key propositions for cybersecurity cooperation Europe - Japan

#### Human and technical cooperation

- **Cyber-threat information sharing**
- **Data sharing privacy and legal framework**
- **Cybersecurity training and awareness**
- **International communication**

#### SME-oriented

- Support of SMEs
- Support of big data, smart city and industry 4.0
- Support of robotics and AI in cybersecurity

#### Technical lead

- EUNITY

#### Key organizations for leading cybersecurity activities

- Selection of two permanent authorities that lead cybersecurity discussions
- Creation of joint activities, policies and networks of competences

### Summary of cybersecurity challenges Europe - Japan

#### Area: Legal and policy

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

**JAPAN**
- Lack of cybersecurity accelerators and academic cybersecurity centres;
- 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 standardization

**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 types of companies;
- Difficulties for organization to adopt cybersecurity naturally in their business;

### Cooperation opportunities

<table>
<thead>
<tr>
<th></th>
<th>Cyber-threat information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Difficulty to share information</td>
</tr>
<tr>
<td></td>
<td>No common legal framework</td>
</tr>
</tbody>
</table>

| **Scope** | Design and development of methodologies, tools and data format |
|  | Assurance of data exchange and harmonization of legal frameworks |

<table>
<thead>
<tr>
<th></th>
<th>Data sharing privacy and legal framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Administrative requests and complex additional work</td>
</tr>
<tr>
<td></td>
<td>Public and private partners under the same umbrella</td>
</tr>
</tbody>
</table>

| **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 |

<table>
<thead>
<tr>
<th></th>
<th>Cybersecurity training and awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Employees are usually considered the &quot;weakest part of the chain&quot;</td>
</tr>
<tr>
<td></td>
<td>Trainings should not only look at the Europe-Japan relationship</td>
</tr>
</tbody>
</table>

| **Scope** | Creation of coordinated training programs for legal, research, education and industry between the two regions |
|  | Courses for development of strong trained experts |

<table>
<thead>
<tr>
<th></th>
<th>Key organizations for leading cybersecurity activities in both areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Shared organizational and certification mechanisms</td>
</tr>
<tr>
<td></td>
<td>Permanent authority with scope and mandate on both territories</td>
</tr>
</tbody>
</table>

| **Scope** | Selection of two permanent authorities that lead cybersecurity discussions |
|  | Creation of joint activities, policies and networks of competences |

<table>
<thead>
<tr>
<th></th>
<th>Support of SMEs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Problems for finding the right cybersecurity tools</td>
</tr>
<tr>
<td></td>
<td>Difficulty to access common market</td>
</tr>
</tbody>
</table>

| **Scope** | Creation of a platform for SMEs for accessing cybersecurity solutions |
|  | Easy access to funding opportunities in both areas and as joint participation |

<table>
<thead>
<tr>
<th></th>
<th>IoT enhancement and usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Need for a common perspective for supporting capabilities of service providers</td>
</tr>
<tr>
<td></td>
<td>Technical regulations, universal protocols and standards</td>
</tr>
</tbody>
</table>

| **Scope** | Development of IoT cybersecurity information database and information sharing |
|  | Creation of common protocols and policies for trusted usage of IoT devices |

<table>
<thead>
<tr>
<th></th>
<th>Support of big data, smart city, and industry 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Digitally transforming businesses, impacting different critical areas</td>
</tr>
<tr>
<td></td>
<td>Need for common data systems that allow free exchange of information</td>
</tr>
</tbody>
</table>

| **Scope** | Creation of processes and tools for integrating cybersecurity |
|  | Research and integration of human-oriented approaches |

<table>
<thead>
<tr>
<th></th>
<th>Support of robotics and AI in cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Policy and legal systems are not mature enough yet</td>
</tr>
<tr>
<td></td>
<td>Need of ethical recommendations in the two regions</td>
</tr>
</tbody>
</table>

| **Scope** | Definition of common cybersecurity principles and rules for enabling a safe usage of AI in different technologies |