Cybersecurity and privacy dialogue between Europe and Japan

A resume of the revised version of
the Cybersecurity Research Analysis Report for the two regions

Research and Innovation aspects

The goal of this resume is to give a quick glance at the picture of the cybersecurity and privacy in Europe and Japan in the context of research and innovation aspects, as it is more analytically shown in the report 3.2 of the EUNITY project. The report 3.2 analyses the priorities in both EU and Japan, in order to produce an overview on the status of cybersecurity and privacy research and innovation activities. Among others, the report focuses on the analysis of research agendas, programs, project calls, roadmapping and pilot projects as well as on showing the available mechanisms to finance cybersecurity research. The report describes the finance mechanisms of research and innovation in cybersecurity, in both regions, and the current role and activity of different units (SMEs, research institutions, CSIRTs, LEAs, etc.) in research and innovation. In the report we provide an overview of the main research directions in the field, we identify the strong and weak points in both regions to indicate the topics of common interest in which there are opportunities for cooperation and topics in which some aspects are covered asymmetrically, allowing greater synergy. We also analyse long-term research programs at the national and international level, in order to find thematic parallels between the EU and Japan, which may create opportunities for either co-financing of joint EU-Japan projects, or at least synchronization of efforts enabling cooperation.

Mechanisms to finance research

The report 3.2, in the chapter 3, among others, identifies and describes the mechanisms to finance cybersecurity research in the European Union and Japan. Table 1 summarizes the most important types of finance mechanisms or institutions financing research in cybersecurity in the European Union (on the international and national level) and Japan.

In the case of Member States of the European Union, there are a lot of financing mechanisms that support research and innovation in the field of cybersecurity. In addition to international funding, there are also national funding mechanisms that may vary depending on the partner country. However, on the Japanese side, we have three ministries that finance research and innovation in the field of cybersecurity and the Cross-ministerial Strategic Innovation Promotion Program (SIP) program released by CAO.

European Union	Japan
European Union, International	
• Framework Programmes (now Horizon 2020) - open competitions • Special programmes such as Connecting Europe Facility (CEF) - Cybersecurity calls • ENISA-European Union Agency for Network and Information Security • EUREKA	
EUNITY project partners' countries	
• national programmes • government, state programmes • regional programmes • national agencies • international, joint programming • structural measures, i.e. Operational Programmes • funding for research, in general to support PhD grants • other	• Ministry of Internal Affairs and Communications (MIC) • Ministry of Economy, Trade and Industry (METI) • Ministry of Education, Culture, Sports, Science and Technology (MEXT) • Cabinet Office (CAO)

Table 1 List of the financing mechanisms in the European Union and Japan

The main research directions in the field

A top-down approach is utilized in the analysis of the main research directions. It starts on the basis of strategic documents regarding cybersecurity, and in particular, Strategic Research and Innovations Agendas, and, on a limited scope, on the basis of national cybersecurity strategies. Although we try to take into account most of the important aspects of cybersecurity, a special emphasis is given to the research and innovation aspect. Then, the tactical aspects of implementation of the strategies are analysed, on the basis of programs and project calls regarding cybersecurity. Next, operational, aspects of cybersecurity are analysed, on the basis of the most important and recent projects in the area of cybersecurity. The special attention is paid to four EU pilot projects launched to prepare the European Cybersecurity Competence Network (namely: CONCORDIA, ECHO, SPARTA and CyberSec4Europe). There are also activities other than

This project has received funding from the European Union H2020 Programme under grant agreement No 740507

projects described, which are important from the perspective of research and innovation. Each analysis is performed at both the EU and Japan levels. Each analysis generally focuses on the EU perspective as a whole, but in some specific areas where it was especially relevant, we also considered the perspective of the individual Member States of the EU. The schematic overview of the analysis is presented in Figure 1.

The strong and weak points

The general overview of strong and weak points for both regions is provided in the report. The conclusions have been prepared on the basis of a number of sources of information. First of all, the outcomes of questionnaires collected during and after the project workshops have been deeply analysed. Secondly, the observations and experience of all partners of the consortium have been used to broaden the landscape of the problems indicated in questionnaires and highlight the common ones. Another very important source of information is the review of the strategies, projects and programs with regard to research and innovation in the area of cybersecurity and privacy, as well as relevant financing mechanisms. It is worth noting that in many aspects of research in cybersecurity and privacy, the strong and weak points are common for both regions. In case of significant differences, the most important distinctive features are provided. To sum up, the main strengths are: **establishment of the cybersecurity strategy** and **declared focus on cybersecurity and privacy**. Whereas the main weaknesses are the following: **opposition between industry and research**, **high-level cybersecurity's personnel shortage**, **lack of coordination of research actions on various levels**, and **lack of strong global cybersecurity enterprises and solutions originating in the EU and Japan**.

Areas which need the most collaboration

The areas which need the most collaboration in the field of cybersecurity are indicated:

- **education and awareness:**
  - education on various levels,
  - enhancing security awareness,
  - development of human resources,
  - promoting the exchange of personnel;
- **standards and regulations:**
  - harmonization on standards and regulations among government and industrial associations,
  - guidelines by industry sector,
  - sharing best practices regarding cybersecurity;
- **information sharing:**
  - sharing environments to monitor attacks,
  - sharing security intelligence among security vendors/organizations,
  - continuous information feeds on web sites, e.g. blogs or whitepapers,
  - continuous exposure in conferences/exhibitions,
  - continuous workforce activities, e.g. industry ISAC.

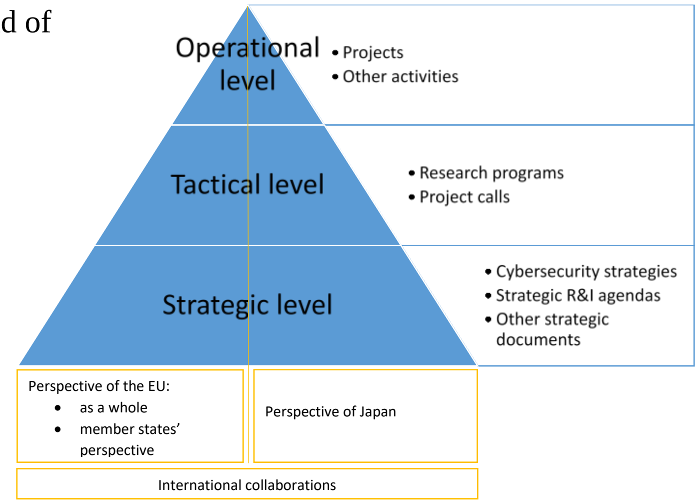

Figure 1 Schematic overview of the analysis

Other activities which could be performed together: maintain Interpol-like cooperation and non-aggression treaties, improve communication, information/data sharing, legal framework, harmonize legal and penal frameworks to ensure effective prosecution of cybercriminals, reduce administrative procedures, intensify collaboration between CERT/CSIRT teams, and promote joint initiatives (incl. meetings and workshops).

Certainly boosting the responsiveness of Europe as a whole and fostering cooperation and coordination in cybersecurity between Member States and Japan is a very important issue. There is a need of industry-government cooperation and global collaboration to exchange sensitive data and to enlarge the cooperation to as many countries and industry sectors as possible. Global collaboration should not only be horizontal, i.e. limited to state entities, nations and international organizations. Rather, global cooperation should be horizontal and vertical, i.e. also involving private entities and other stakeholders (academia for instance).

In the report one can also find other identified common interests between the EU and Japan and also the list of main strategic directions in institutions, the list of R&I cybersecurity priorities and current directions, and also identification of common threats related to cybersecurity and privacy.