

H2020 FRAMEWORK PROGRAMME

H2020-DS-SC7-2016: DS-05-2016 EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation



Cybersecurity and privacy dialogue between Europe and Japan

D2.1: Community Engagement Report

Abstract: This document discusses the targeted community engagement and dialogue activities undertaken within the EUNITY project for engaging both the general public, and more particularly policy makers and relevant constituencies in preparation for the first EUNITY workshop in Tokyo, Japan on 11-12 October 2017. In this report, we focus on the concrete approaches applied in the form of information gathering, dissemination, data collection, and activities undertaken leading to the workshop in Japan. This document includes a collection of sources and cybersecurity related material, describing the current research scenarios in both regions.

Contractual Date of Delivery	31/01/2018
Actual Date of Delivery	01/06/2018
Deliverable Security Class	Public
Editor	KU Leuven
Contributors	All <i>EUNITY</i> partners
Quality Assurance	Athos, FORTH

The *EUNITY* consortium consists of:

Institut Mines-Telecom	Coordinator	France
FORTH	Principal Contractor	Greece
ATOS SPAIN SA	Principal Contractor	Spain
NASK	Principal Contractor	Poland
KATHOLIEKE UNIVERSITEIT LEUVEN	Principal Contractor	Belgium

Document Revisions & Quality Assurance

Revisions

Version	Date	By	Overview
3.0	01/06/2018	Elena Andreeva, KU Leuven	Final version
2.0	30/05/2018	Despoina Antonakaki, FORTH	Editorial corrections and suggestions on the content improvement throughout
1.0	20/05/2018	Pedro Soria-Rodriguez, Athos	Editorial corrections and suggestions on the content improvement in section 3.1
0.0.1	13/04/2018	Stefano Fantin, KU Leuven	Review
0.0.0	07/04/2018	Elena Andreeva, Stefano Fantin, KU Leuven	First draft

Table of Contents

DOCUMENT REVISIONS & QUALITY ASSURANCE	2
TABLE OF CONTENTS	3
1 INTRODUCTION.....	5
1.1 DOCUMENT OUTLINE	5
2 KNOWLEDGE DISSEMINATION	6
2.1 JAPANESE PARTNERS	6
2.1.1 <i>JSPS 192 subcommittee on cybersecurity:.....</i>	<i>6</i>
<i>JSPS is an information-exchange hub for cybersecurity stakeholders coming from academia, and the private and public sectors. They were informed about the forthcoming workshop in Japan in a timely manner, both online and in the form of direct dialogue and discussions.....</i>	<i>6</i>
2.1.2 <i>Forums: the Cross Sectors Forum of the Cyber Risk Intelligence Center, which was held in July, 2017 on ECSO and cybersecurity PPP and consisted of more than 1000 participants.....</i>	<i>6</i>
2.1.3 <i>E-mails: have been distributed to more than 50 key Japanese cybersecurity experts across academia, government agencies, industry research labs, cybersecurity service providers, product vendors and cybersecurity coordination organizations. The respective response has been above 50% with 31 of the contacted attending the first EUNITY Workshop in Japan.</i>	<i>6</i>
2.1.4 <i>Direct dialogue: in the form of working meetings both online and offline via:.....</i>	<i>6</i>
<ul style="list-style-type: none"> • <i>EUNITY Project Kick-off meeting (held in Brussels, July 2017);</i> • <i>Permanent communication on the progress of the preparatory work with the Japanese partners of the EUNITY consortium;</i> 	<i>6</i>
2.2 EUROPEAN PARTNERS.....	7
2.2.1 <i>ECSO involvement: to share information to the Japanese community via awareness raising of the cybersecurity strategic research agenda in Europe, the outcomes of recent EU cybersecurity related projects and calls, problems considered important for funding in the sector-specific area, long-term-directions and projection in the 2018-2020 cybersecurity space, together with the funding available landscape using both:.....</i>	<i>7</i>
2.2.2 <i>Direct communication: in the form of working meetings both online and offline with:.....</i>	<i>7</i>
<ul style="list-style-type: none"> • <i>Both Japanese and European EUNITY partners: to coordinate the organization of the two-days workshop meeting and approve each other's plans for their respective panels or seminars;.....</i> • <i>EU cybersecurity institutions: such as the Information Technologies Security Incident Response Institution in Latvia - CERT.LV, which is run by the agency of the University of Latvia: "Institute of Mathematics and Computer Science, University of Latvia", in cooperation with the Ministry of Transport of the Republic of Latvia. BaibaKaskina, the chair of TF-CSIRT and head of CERT.LV, was contacted to give a talk and participate in the workshop based on her very good knowledge of how the CSIRT environment works in the EU;.....</i> • <i>European think-tanks and interest groups: Dr. Afonso Ferreira (French CNRS) presented the Task-Force on software vulnerability disclosure held by CEPS (Centre for EU Policy Studies), for which he has been the rapporteur;.....</i> • <i>Japanese institutions and universities: KUL contacted and joined its forces with Prof. Hiroshi Miyashita, professor of Privacy Law at Chuo University of Tokyo for the exchange of information with regard to the respective data protection regimes.....</i> • <i>IMT had a talk introducing forthcoming EUNITY kick-off during the France-Japan symposium on cybersecurity, held in Tokyo, April 2017.....</i> 	<i>7</i>
3 KNOWLEDGE COLLECTION.....	8
3.1 PUBLIC DOCUMENTATION.....	8
3.2 DIRECT AND INDIRECT COMMUNICATION CHANNELS	9
3.2.1 <i>Meetings with the ECSO cabinet in Brussels have allowed the EUNITY European partners to gather material relevant for several of the presentations at the workshop.</i>	<i>9</i>
3.2.2 <i>Market studies about industry focused of research in cybersecurity, were used as the starting point for the EUNITY workshop questionnaires and the discussion session around industry. With this exercise we intended to derive a link between challenges in cybersecurity in company operations and how they focus and priorities in research to address such challenges.....</i>	<i>9</i>

3.2.3	<i>Joint collaboration for the preparation of the workshop questionnaires for each workshop session: CSIRTs, ECSO, Industry, and Privacy, Research & Innovation.</i>	9
4	WORKSHOP PREPARATION	10
4.1	ENGAGEMENT ROADMAP	10
4.1.1	<i>EUNITY Kick-off meeting (Brussels, July 2017): all partners had the opportunity to begin the project and to lay down the preliminary works related to community engagement. The line-up of stakeholders and constituencies was therefore validated, and a unitary strategy for outreach and public interaction was first agreed upon.</i>	10
4.1.2	<i>Continuous and iterative engagement within the Consortium: throughout a number of online meetings, the EUNITY partners kept each other aware of their own plans for community engagement. Furthermore, such series of meetings were set up to concretely roll out logistics and contents of the first Workshop in Tokyo. In such circumstances, all partners agreed on each other's program, while separately they conducted the necessary research in order to achieve the intended individual plans and joint results.</i>	10
4.1.3	<i>EUNITY Workshop Meeting (Tokyo, 11/12 October 2017): during the workshop, both Japanese and European partners had the chance to present to each other and to the registered audience their own research, based on the agreed strategy and peculiar partners' expertise. The workshop proliferated in various forms of engagement activities: presentations; panel discussions; workshop discussions; questionnaires and meetings.</i>	10
4.1.4	<i>Iteration of follow-up activities: after the workshop, the research as well as the community management and engagement continued by means of:</i>	10
	(a) <i>Analysis of the questionnaires that each partner and all participants in the Tokyo Workshop filled in. Answers were based on their specialization and gave the opportunity to have a high-level understanding of the state of play of both privacy and cybersecurity landscapes in Europe and Japan;</i>	10
	(b) <i>Coordination of online meetings amongst EUNITY Project Partners, with the aim of monitoring partners' research and community engagement activities in light of the scope of this project;</i>	10
4.2	WORKSHOP OBJECTIVES AND PROGRAM	11
4.2.1	Workshop Objectives	11
4.2.2	Workshop Program	11
5	CONCLUSIONS	13

1 Introduction

This document summarizes the various types of actions taken towards communicating the EUNITY project and the first EUNITY workshop in Japan in 2017 to the general public, the policy makers and various cybersecurity stakeholders, as well as the engagement of the latter in a dialogue and knowledge transfer. This workshop was organized by the EUNITY project, in collaboration with the JSPS subcommittee 192 on cybersecurity.

The content of this report is based largely on the answers of a questionnaire conducted among the EUNITY partners, following the workshop in Japan in October 2017.

The questionnaire was sent by KU Leuven, in its role of a leader of this deliverable, to collect the answers of the EUNITY partners on their preparatory works, leading to the workshop in Tokyo, Japan. EUNITY partners were asked to comment on the following questions:

1. Describe the preparation process that led you to the Tokyo workshop meeting. Emphasize your focus and specialization, the main themes, aims and purposes, background information, finalities, and expectations from the workshop.
2. Describe what your participation in the Tokyo meeting entailed (if you were presenting a panel, please describe the panel. If otherwise, please specify your contribution).
3. Enlist and explain the sources that served you as background documentation for the preparation of the Tokyo meeting (please also specify what documents, available on the SVN EUNITY repository, you made use of).

1.1 Document Outline

In the following chapters, we describe the EUNITY community engagement efforts undertaken and leading to the first joint EUNITY workshop in Japan, in October 2017.

In Chapter 2, we present the actions taken towards information dissemination by both the Japanese and European partners of the consortium.

Then, in Chapter 3, we describe how the information towards the organization of the first EUNITY workshop in Japan was collected. Next, in Chapter 4, we describe the preparation of the workshop itself, and we give a short outline of the contributions of our partners to the workshop program.

Finally, in Chapter 5 we summarize our results.

2 Knowledge Dissemination

In this section, we describe and summarize the results concerning the approaches taken towards effective community information dissemination. We make somewhat of an informal distinction between the steps taken by the EUNITY Japanese partners in the EUNITY consortium and the European ones, in order to allow drawing comparisons between the approaches taken by both sides later on. The partners of the EUNITY consortium reported their first efforts towards community engagement, in the form of information dissemination in June 2017.

2.1 Japanese Partners

Towards reaching out to a maximal number of relevant parties from both the general public and policy makers, the following channels and approaches for distributing information about the EUNITY project and the forthcoming workshop in Japan have been applied. Reaching out information both in person via direct dialogue, meetings, forum and congress addresses, and online in the form of e-mail, website, Twitter, Facebook and web coverage have been utilized. More concretely, the following communication approaches for collection information were reported:

2.1.1 JSPS 192 subcommittee on cybersecurity:

JSPS is an information-exchange hub for cybersecurity stakeholders coming from academia, and the private and public sectors. They were informed about the forthcoming workshop in Japan in a timely manner, both online and in the form of direct dialogue and discussions.

2.1.2 **Forums:** the Cross Sectors Forum of the Cyber Risk Intelligence Center, which was held in July, 2017 on ECSO and cybersecurity PPP and consisted of more than 1000 participants.

2.1.3 **E-mails:** have been distributed to more than 50 key Japanese cybersecurity experts across academia, government agencies, industry research labs, cybersecurity service providers, product vendors and cybersecurity coordination organizations. The respective response has been above 50% with 31 of the contacted attending the first EUNITY Workshop in Japan.

2.1.4 **Direct dialogue:** in the form of working meetings both online and offline via:

- EUNITY Project Kick-off meeting (held in Brussels, July 2017);
- Permanent communication on the progress of the preparatory work with the Japanese partners of the EUNITY consortium;
- EU and Japanese research institutions;
- European partners: a three-day meeting at IMT was held in March 2017. The meeting consisted of ten members of the EUNITY Japanese consortium. The goal was to collect information on ECSO and cybersecurity PPP initiative, among others. This in result has led to further spreading out the gathered information to the industry

stakeholders, by dispatching 14 industry cybersecurity trainees to Paris, France in September 2017.

2.2 European Partners

Towards the organization and preparation of the first EUNITY workshop in Japan, the efforts of the European partners have put a heavier emphasis on the reach out of the EU initiatives and policies in the cybersecurity domain to the Japanese public. The latter was naturally justified by the intent and location of the workshop in Tokyo, Japan. Most notably, the reported efforts of the EUNITY partners include:

2.2.1 **ECISO involvement:** to share information to the Japanese community via awareness raising of the cybersecurity strategic research agenda in Europe, the outcomes of recent EU cybersecurity related projects and calls, problems considered important for funding in the sector-specific area, long-term-directions and projection in the 2018-2020 cybersecurity space, together with the funding available landscape using both:

- WG1 (standards)
- WG6 (SRIA)

2.2.2 **Direct communication:** in the form of working meetings both online and offline with:

- Both Japanese and European EUNITY partners: to coordinate the organization of the two-days workshop meeting and approve each other's plans for their respective panels or seminars;
- EU cybersecurity institutions: such as the Information Technologies Security Incident Response Institution in Latvia - CERT.LV, which is run by the agency of the University of Latvia: "Institute of Mathematics and Computer Science, University of Latvia", in cooperation with the Ministry of Transport of the Republic of Latvia. BaibaKaskina, the chair of TF-CSIRT and head of CERT.LV, was contacted to give a talk and participate in the workshop based on her very good knowledge of how the CSIRT environment works in the EU;
- European think-tanks and interest groups: Dr. Afonso Ferreira (French CNRS) presented the Task-Force on software vulnerability disclosure held by CEPS (Centre for EU Policy Studies), for which he has been the rapporteur;
- Japanese institutions and universities: KUL contacted and joined its forces with Prof. Hiroshi Miyashita, professor of Privacy Law at Chuo University of Tokyo for the exchange of information with regard to the respective data protection regimes.
- IMT had a talk introducing forthcoming EUNITY kick-off during the France-Japan symposium on cybersecurity, held in Tokyo, April 2017

3 Knowledge Collection

The accumulation of relevant knowledge and information on cybersecurity policies and initiatives in both Europe and Japan has been the primary objective towards the preparation of the first EUNITY workshop in Japan in 2017. Various standard information collection channels were used, such as questionnaires, market studies, public policy documents, etc. Furthermore, one important result of our community interaction and knowledge dissemination about the forthcoming EUNITY workshop in Japan resulted in the accumulation of further information sources.

Most of the information collected towards the preparation of the workshop has been via publicly available sources and in a few cases to the EUNITY partners via forms of internal communication:

3.1 Public documentation

- The Directive on Security of Network and Information Systems (NIS Directive, EU, 2016/1148)
- ENISA guidelines and Japanese media articles on GDPR.

According to our analysis, the NIS directive and the ECSO ones were successful in garnering a lots of interested stakeholders.

- GDPR and the EU Privacy Reform Package as a principal background documentation;
- ECSO documentation and slides which were communicated during the general assembly in June, 2017;
- H2020 documents (freely downloadable):
The EU Framework Programme for Research and Innovation: ; “H2020 Work Programme 2018-2020” which includes all the research and funding opportunities provided by the European Commission, for the 2018-2020 period;
- EU cybersecurity initiatives - working towards a more secure online environment, European Commission, January 2017;
- Current And Emerging Challenges In Cybercrime And Cyberterrorism 10 -11 March 2016 Nieuwspoord International Press Centre Den Haag;
- Preliminary analysis of the result of CyberRAD project; <https://www.cyberroad-project.eu/en/publications>;
- Research and Development projects in the H2020 and FP7 EU framework:
 - EUINCOOP, <http://www.eunicoop.eu/>, and the computing systems roadmap produced between the EU and India regions;
 - CONNECT2SEA, <http://www.connect2sea.eu/> and the cybersecurity related roadmap produced between the EU and the Association of Southern Asian Nations (ASEAN) regions;
 - NECOMA, <http://necoma-project.eu/>, which was a joint cybersecurity project between EU and Japan;
 - CYBERSURE, <http://www.cybersure.eu/>, which is about cyber insurance policies for cybersystems;

- PROTASIS, <https://www.protasis.eu>, SYSSEC Network of Excellence (NoE) security project;

Alongside strictly legal papers, documents, project documentation and articles, a set of policy documents were analysed:

- PIPAME, La filiere industrielle Francaise de Sécurité (2015)
- EU Parliament, cybersecurity in the European Union and Beyond (Study for LIBE Committee)
- R. Dewar, Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union cybersecurity Policy (EUSA, Boston, 2015)

This had the objective of raising the discussion at a higher level, thus understanding the reasons and the rationale behind a given range of legislative choices.

3.2 Direct and indirect communication channels

- 3.2.1 **Meetings** with the ECSO cabinet in Brussels have allowed the EUNITY European partners to gather material relevant for several of the presentations at the workshop.
- 3.2.2 **Market studies** about industry focused of research in cybersecurity, were used as the starting point for the EUNITY workshop questionnaires and the discussion session around industry. With this exercise we intended to derive a link between challenges in cybersecurity in company operations and how they focus and priorities in research to address such challenges.
- 3.2.3 Joint collaboration for the preparation of the workshop **questionnaires** for each workshop session: CSIRTs, ECSO, Industry, and Privacy, Research & Innovation.

4 Workshop preparation

Towards the organization of the first EUNITY workshop in Tokyo, Japan all the EUNITY partners aligned their agenda, ideas and intents. We coordinated potential topics, forms of community engagement and subsequent organization for the two days workshop meeting and approved each other's plan for their respective panels or seminars.

4.1 Engagement roadmap

This section outlines the roadmap that was rolled out by EUNITY partners, in order to prepare them for the first Workshop Meeting in Tokyo (October 2017). All the efforts have been coordinated by the Project Leaders and saw the active participation of all project partners, united in a collective effort to engage with each other for the rolling out of a fruitful offline two-days meeting in the Japanese Capital city.

- 4.1.1 **EUNITY Kick-off meeting (Brussels, July 2017):** all partners had the opportunity to begin the project and to lay down the preliminary works related to community engagement. The line-up of stakeholders and constituencies was therefore validated, and a unitary strategy for outreach and public interaction was first agreed upon.
- 4.1.2 **Continuous and iterative engagement within the Consortium:** throughout a number of online meetings, the EUNITY partners kept each other aware of their own plans for community engagement. Furthermore, such series of meetings were set up to concretely roll out logistics and contents of the first Workshop in Tokyo. In such circumstances, all partners agreed on each other's program, while separately they conducted the necessary research in order to achieve the intended individual plans and joint results.
- 4.1.3 **EUNITY Workshop Meeting (Tokyo, 11/12 October 2017):** during the workshop, both Japanese and European partners had the chance to present to each other and to the registered audience their own research, based on the agreed strategy and peculiar partners' expertise. The workshop proliferated in various forms of engagement activities: presentations; panel discussions; workshop discussions; questionnaires and meetings.
- 4.1.4 **Iteration of follow-up activities:** after the workshop, the research as well as the community management and engagement continued by means of:
 - (a) Analysis of the questionnaires that each partner and all participants in the Tokyo Workshop filled in. Answers were based on their specialization and gave the opportunity to have a high-level understanding of the state of play of both privacy and cybersecurity landscapes in Europe and Japan;
 - (b) Coordination of online meetings amongst EUNITY Project Partners, with the aim of monitoring partners' research and community engagement activities in light of the scope of this project;
 - (c) Organization of a 3-day seminar in France in September 2017 for Japanese critical infrastructure cybersecurity trainees, with topics ranging from European and French cyberstrategy to SCADA security, to formal methods, to smart grid security;

- (d) Organization of a follow-up meeting to the 1st workshop in Tokyo, on January 17, 2018, to complete the collection of questionnaires responses and feedback from around 30 Japanese attendees.

4.2 Workshop Objectives and Program

We list the main objectives of the workshop in Japan and the corresponding actions towards their realization including the concrete program of the workshop and the respective roles of the individual partners.

4.2.1 Workshop Objectives

The main goal of the workshop in Japan was to inform the Japanese community about cybersecurity in Europe. More concretely, those include the European research and innovation activities, and roadmaps. Furthermore, the workshop focused on gathering feedback from the Japanese community on the relevance of the European objectives with regard to:

- The importance of these objectives in Japan;
- Missing activities that are important in Japan.

The main purpose of the workshop was to collect feedback information and understand gaps and differences between EU and Japan for research and business stakeholders in cybersecurity and privacy.

To meet these objectives, the EUNITY partners worked to gather relevant stakeholders in the first workshop in Japan, taking advantage of co-location with other events as much as possible. Thanks to the expertise of our members, we collected the appropriate existing research agendas, legislations and business practices in Europe and Japan and then analyzed the information collected to formulate recommendations, including business opportunities and a research agenda. A particular attention was brought to the similarities of the research and market strategies, as well as the differences that must be taken into account when addressing the Japanese market.

We worked closely with the European Cyber Security Organization association, the cybersecurity cPPP signatory with the Commission and tried to cover the broad range of constituencies of ECSO (large organizations, SMEs, public bodies, associations, clusters, RTOs) thanks to both the direct participation of its partners to ECSO and to their ties with industry associations, cluster and public bodies. The goal was to ensure that the most relevant and recent information available is on one hand, taken into account by the project, and on the other hand, is providing relevant information to interested parties in the EU.

4.2.2 Workshop Program

The workshop program was prepared in accordance with the main EUNITY project objectives as outlined above. The workshop was scheduled over two days with a total of 9 sessions. The Introductory and Landscape sessions 1 and 6, were chaired by prof. Hervé Debar, IMT, France.

CSISRT Sessions: 2 and 3 took a workshop format and were chaired by Pawel Pawlinski, CERT Polska, Poland. The CSIRT introductions were made by Baiba Kaskina (CERT.LV) and Takayuki Uchiyama (JPCERT/CC). After a questionnaire wrap-up performed by Pawel, the session was

closed by an invited talk, entitled Task Force Software Vulnerability Disclosure in Europe given by Afonso Ferreira (IRIT).

Industry Sessions: 4 and 5 were chaired by Pedro Soria-Rodriguez (ATOS) with Session 5 taking a Workshop Format. These sessions featured a number of invited talks, including an Introduction of CRIC Cross Sectors Forum by Hiroshi Takechi (NEC), and an introduction to the other CSA project, Cyberwatching.eu by its coordinator, Nicholas Ferguson (Trust-IT Services). ATOS also made a presentation on Market Situations and ECIL Recommendations.

Legal and Policy Sessions: 7 and 8 had also a Workshop format and were chaired by Mr. Stefano Fantin from KU Leuven, Belgium. These sessions featured an introduction by himself on the European privacy landscape including a segment on the forthcoming GDPR, and a presentation on the Japanese Landscape on Data Protection by Hiroshi Miyashita (Chuo University).

Research & Innovation Session: 9 was held in a Workshop format and chaired by Sotiris Ioannidis, FORTH, Greece. It included an ECSO presentation on the Strategic Research and Innovation Agenda by Hervé, and short talk on the forthcoming EU Japan joint collaborative call (EUJ-01-2018) given by Daisuke Inoue (NICT).

The final session 10 summarized the discussions and points of the workshop days.

5 Conclusions

In this document, we discussed the EUNITY community engagement towards the organization of the first EUNITY workshop in Japan. We presented the actions towards information dissemination and collection by both the Japanese and European partners of the EUNITY project. We also gave summary of the concrete actions for the preparation of the workshop.

We established a stronger and successful communication and collaboration between our European and the Japanese partners. Furthermore, both sides have been efficient facilitators of new contacts and communication opportunities.