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[†]

Deliverable D5.5: Dissemination report year 2

Abstract: *This document contains the community engagement activities of the EUNITY project, including the dissemination activities for all EUNITY partners, for the year 2.*

Contractual Date of Delivery	May 2019
Actual Date of Delivery	May 2019
Deliverable Dissemination Level	Public
Editor	Despoina Antonakaki, Christos Papachristos, Sotiris Ioannidis
Contributors	All *EUNITY* partners
Quality Assurance	Christophe Kiennert

[†] The research leading to these results has received funding from the European Union H2020 Programme under grant agreement n° 740507.

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

Contents

1 Introduction

1.1 Introduction

This document contains the dissemination activities that target to spread information regarding the EUNITY project. This includes the community engagement activities of the EUNITY partners for the second year. We describe the visits of the partners within the scope of EUNITY project, along with the scope of the event, the purpose of the partner's visit, the participants and the accomplished goals.

2
Workshops

2.1 Organization of Workshops

During the second year of the EUNITY project, a second workshop was organised in Brussels on 24 January 2019, in conjunction with ECSO. A third workshop [1] was organized in Kyoto on 26 April 2019, gathering about 25 participants. In this document, we describe in detail the organization, content and methodology of the second workshop.

2.1.1 Workshop in Brussels

EUNITY, through Objective 1: *”Encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters relating to cybersecurity and privacy research and innovation issues”*, aims at the organization of at least two workshops. Here we describe the second workshop which was was organized by IMT, at, as the first one was analyzed in the ”Dissemination report Year 1”. The second workshop was organized by IMT in collaboration with ECSO and with the assistance of NAIST, at the L42 building in Brussels on 24 January, 2019. It should also be noted that Japanese representatives who took part in this workshop were also invited at the FIC 2019 held in Lille, France, on 22 and 23 January 2019. Though a EUNITY stand could not be obtained, we managed to organize panels on ”Feedbacks on the cybersecurity of big events” by Reiko Kondo (MIC), and on ”Cybers Security by design and IoT” by Youki Kadobayashi (NAIST).

[1] Program available at https://www.eunity-project.eu/en/workshops/3rd-eunity-workshop/

2.1.1.1 Organization

Local organization was assumed by ECSO who called on many industry representatives of ECSO. IMT and NAIST contributed to invite high-level speakers from the European Commission, Japanese representatives from (DG CNECT), and from Japan, including the Ministry of Internal Affairs and Communications (MIC)), or the Japan External Trade Organization (JETRO), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC). It was organized as a single track session with discussions concentrated among the speakers, but with participation from the audience. The morning session focused on comparing the European and Japanese cybersecurity ecosystems, from a business, and legal and policy points of view. The afternoon session concentrated on business solutions applied to selected verticals, namely health, findustry and academia. ance and energy sectors. Challenges in securing the supply chain were also presented. Finally, a last session tackled crucial challenge identified by EUNITY, such as training and awareness, and information sharing.

2.1.1.2 Objectives

The workshop is part of WP2 on "Dialogue and community interactions". The aim was to facilitate the exchange of good practices on cyber policy and investigate business opportunities in the context of the EU-Japan Trade agreement. The discussion helped identify where objectives or approaches of the European Union and Japan are close and where diverging if anycollaboration opportunities as well as gaps between the European Union and Japan. The workshop helped identify where cooperation could be strengthened beyond political aspects of cybersecurity, such as on aspects related to standards, certification, R&I, pilots for verticals.

Ultimately, the feedback gathered from the workshop interactions and discussions, the analysis of responses to the questionnaires distributed at the workshop, contributed to the definition of a joint agenda for research and business development.

2.1.1.3 Schedule

The second workshop's duration was one day. The workshop had three sessions. The first session included welcoming remarks from ECSO and EUNITY & Introduction, with chair: Hervé Debar (Telecom SudParis/EUNITY), Jakub Boratynski (DG CONNECT, European Commission) and Reiko Kondo (Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC)). The second session was on European and Japanese Ecosystems, with chair: Luigi Rebuffi, European Cyber Security Organisation (ECSO) and the third session was on Working Session on Business Solutions applied to selected vertical sectors, with chair: Nina Olesen, European Cyber Security Organisation (ECSO).

2.1.1.4 Attendance

Approximately, an amount of 63 people attended the workshop, including representatives from EUNITY, from ECSO, the DG CNECT, the Ministry of Internal Affairs and Communications, and the Japanese External Trade Office. Speakers on the European side were from the industry and had ECSO membership.

2.1.1.5 Exploitation

The results of the discussions and the responses to the questionnaire are provided in a specific section in the proceedings of the EUNITY European workshop.

2.2 Workshop Methodology

The methodology for building the workshop was manifold: liaising with the ECSO in order to highlight the EUNITY results, inviting high-level speakers from the European Commission and Japanese ministries, fostering dialogue to identify gaps and collaboration opportunities, and gathering feedback from the attendees.

2.2.1 Liaison with ECSO

One of the objectives of EUNITY is to reach out and collaborate with other CSAs and the Cybersecurity Public-Private Partnership. Through continuous interaction with ECSO we have been able to secure their organization of the workshop in Brussels to the condition of making it a joint event. By doing so, we ensured more visibility of the EUNITY outcomes and the possibility to reach out to the European Commission and invite high-level profiles.

2.2.2 Inviting high-level profiles

As indicated previously, the workshop being organized in Brussels, it allowed for people from DG CNECT to attend easily. In order to obtain some balance, we had to invite high-level profiles from Japan. Direct collaboration with EUNITY Japanese associated partners such as NAIST, allowed us to reach out to Ms. Reiko Kondo, from the Office of the Director-General for Cybersecurity, MIC. The presence of such high-profiles speaker gave more legitimity to the workshop and attracted more audience.

2.2.3 Fostering dialogue

Another objective of EUNITY was fulfilled by carefully choosing the topics of discussion to foster dialogue, identify gaps, and elicit synergies, through a dedicated discussion at the end of the morning session. The morning session was designed to help both regions understand each other's cybersecurity landscape, through their cybersecurity market and policy framework. The afternoon session focused on presenting more of the activities of ECSO, in particular sectorial and supply chain support. Additionally, a networking break offered more opportunities for attendees to connect, discuss, exchange.

2.2.4 Gathering feedback

Finally, another objective was achieved by directly engaging the attending community through a last session outlining 2 of the main challenges described in EUNITY, i.e., training and awareness on one hand, and information sharing on the other hand. This allowed to bootstrap the following discussion on potential cooperation between the two regions. Additionally, a questionnaire aimed at gathering feedback from several results of EUNITY presented in leaflet distributed at the event.

Below, we add the program of the workshop:

3 Workshop Program

3.1 Program Chairs

This chapter presents the program chairs, as well as the program of the workshop.
Session 1: Welcoming remarks from ECSO and EUNITY & Introduction
Chair: Hervé Debar (Telecom SudParis/EUNITY),
Jakub Boratynski (DG CONNECT, European Commission) and
Reiko Kondo (Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC)).
Session 2: European and Japanese Ecosystems
Chair: Luigi Rebuffi, European Cyber Security Organisation (ECSO)
Session 3: Working Session on Business Solutions applied to selected vertical sectors
Chair: Nina Olesen, European Cyber Security Organisation (ECSO)

3.2 Program

ECSO - EUNITY Workshop
24 January 2019, 10:00 - 17:00
L42 - Rue de la Loi 42, 1040 Brussels

REGISTRATION
09:30 - 10:00 Coffee and registration
INTRODUCTION
10:00 - 10:10 Welcoming remarks from ECSO and EUNITY
10:10 - 10:30 Expectations of the workshop

- EUNITY project expectations - Hervé Debar, Telecom SudParis/EUNITY
- DG CONNECT expectations - Jakub Boratynski, DG CONNECT/European Commission
- Japanese delegation expectations - Reiko Kondo, Office of the Director-General for Cybersecurity/Japan Ministry of Internal Affairs and Communications (MIC)

EUROPEAN AND JAPANESE ECOSYSTEMS - moderated by Luigi Rebuffi, European Cyber Security Organisation (ECSO)
10:30 - 11:00 Business approaches to cybersecurity

- European view on the Cybersecurity Market - Ulrich Seldeslachts, LSEC
- Japanese view on the Cybersecurity Market - Hiromichi Nakahara and Hiroo Inoue, Japan External Trade Organization (JETRO)

11:00 - 11:30 Introducing European cybersecurity ecosystem: from threats to industrial policy

- 2016 cybersecurity Public-Private Partnership (cPPP) and European Strategic Agenda on Research & Development: overview of the ecosystem and cyber technologies - Roberto Cascella, ECSO Secretariat
- EU strategy & legal response for strengthening cybersecurity: update on the European Commission 2017 Cyber Security Package and focus on 2018 initiatives - Jakub Boratynski, DG CONNECT/European Commission

11:30 - 12:00 Introducing Japanese cybersecurity ecosystems: legal and policy framework

- Cybersecurity Policy for Industry Sector in Japan - Hiromichi Nakahara and Hiroo Inoue, Japan External Trade Organization (JETRO)

- IoT Security Measures in Japan - Reiko Kondo, Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC)

12:00 - 12:30 Discussion on common approaches and possible synergies

12:30 - 13:30 Networking lunch

WORKING SESSION ON BUSINESS SOLUTIONS APPLIED TO SELECTED VERRTICAL SECTORS - moderated by Nina Olesen, European Cyber Security Organisation (ECSO)

13:30 - 14:15 Challenges and capabilities needs from the selected verticals

- Health sector - Julio Vivero, GMV
- Banking and Finance sector - Giorgio Cusm Lorenzo, Intesa Sanpaolo
- Energy sector - Mario Jardim, Schneider Electric

14:15 - 15:00 The answers from technology and trusted supply chain perspective

- Cybersecurity for the Internet of Things - Ana Ayerbe, Tecnalia
- Challenges of cybersecurity certification and supply chain management - Roberto Cascella, ECSO Secretariat

15:00 - 15:15 Networking coffee break

15:15 - 15:45 Training and awareness challenges

- Update on Training & Cyber Range activities in Europe - Nina Olesen, ECSO Secretariat
- Presentation on gap of cyber experts and skills in Japan Cybersecurity industries: Introducing Cyber Risk Intelligence Center, Cross Sectors Forum - Miho Naganuma, NEC Corporation

15:45 - 16:15 Information sharing challenges

- Multiscale approach to information sharing activities: The use case of the Basque Cyber Security Centre - Javier Dieguez, Basque Cybersecurity Centre
- Global Cooperation: Perspectives of Incident Response Practitioner - Koichiro Komiyama, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

16:15 - 17:00 Closing discussion on potential cooperation & next steps

Hervé Debar, Telecom SudParis/EUNITY

17:00 End of Meeting

4 KPIs for dissemination events

The partners of EUNITY have attended several networking events in order to share the goals of the project and identify common research directions.

Below a small summary of the events, in Table 4.1, includes the partner, the event, the date and the purpose of the visit. We have a detailed description in the next pages, where we also add how this visit contributed to the goal of EUNITY project; the type of participants, the number of EUNITY partners as well as, the overall number of participants that visited this event; and finally whether the initial intention to visit this event was accomplished and in what scale.

EUNITY partner	Event	Key Performance Indicator
1. KU Leuven	Does Privacy Remain in the Future Cyberworld, Luxembourg iTrust event, Luxembourg, 21 June 2018.	Workshop on cybersecurity. Bring research challenges to attention of experts. Goal accomplished.
2. FORTH	RAID International Symposium on Research in Attacks, Intrusions and Defenses, Heraklion, 10 - 12 September 2018	Workshop dedicated to the sharing of information in the field of intrusion-detection. Bring research challenges to attention of a broader audience. EUNITY was presented as poster. Goal accomplished.

3. FORTH	European Researchers' Night, 28 September 2018 - FORTH, Heraklion, Crete	Marie Sklodowska-Curie Actions that targets to bring scientific and research showcases to the attention of the broader audience. Goal accomplished
4. FORTH	ENISA NIS Summer school, Heraklion, 24 September 2018 - 28 September 2018	Summer school organized by ENISA to bring the Challenge of Changing Risk Landscape including the dynamics, the dependencies and the complexity inherent to Information Technology to attention of experts. Goal accomplished.
5. KU Leuven	EUROCRIM '18 - The cyberspace as a criminal enabler: new challenges and new policing approaches, Sarajevo, 29 August 2018 - 01 September 2018	Presentation of the project within cybercrime panel. Main goal outreach to criminologists on the legal comparative research conducted in EUNITY. Get updates on the most research and industry security challenges and needs.
6. NASK & ATOS	CyberSec Forum 2018, cyberwatching.eu Annual Event, Kraków, Poland, 8 October 2018	Presentation of the project findings in the "International cooperation and alignment on cybersecurity and privacy issues" session, panel discussion. Main goal – compare with US-EU (AEGIS) and internal EU (cyberwatching.eu, ECSO) viewpoints, promote the project.
7. KU Leuven	Victims of Cybercrimes: Legal Aspects on Protection and Liabilities (Public Policy lessons from DANTE and EUNITY projects) - Hebrew University of Jerusalem, 15 October 2018	Presentation of the project within cybercrime panel with main goal to engage in networking activities with non-EU academics and outline the policy uptakes of the legal comparative analysis undertaken in EUNITY.

8. IMT	France-Japan workshop on cybersecurity, Tokyo, 29-30 October 2018	Bilateral workshop on cybersecurity. Enabled presentation of current status the project to gather feedback on deliverable D3.1 and enabled EUNITY participants to obtain information about Japanese presentation on these subjects, particularly on Society 5.0.
9. IMT, NAIST	France - Japan visits to METI-MIC-NEC, 31 October 2018 and 02 November 2018	Professor Kadobayashi (NAIST) and Professor Debar (IMT) made several visits to Japanese influential representatives on cybersecurity. Presented EUNITY findings with highlights on D3.1.
10. KU Leuven	Freedom and Security - Killing the zero sum process. #kill0sum. The Hague, 22-23 November 2018, Europol premises	The objectives included the sensibilization of law enforcement and security community on two major EUNITY legal topics (vulnerability policy and Cybersecurity Act) as well as the engagement with Japanese attendants (see prof. Miyashita) on the EUNITY project. Goal accomplished.
11. All partners	EUNITY ECSO Workshop,24 January 2019, Brussels	The objectives include the valorization and showcase of EUNITY project through networking and learning of Japanese policy landscape and the setting of contacts and roadmap for next valorization trip in Japan.

12. KU Leuven	A Comparative Study Between Japan and the European Union on Software Vulnerability Public Policies, ICCCIS 2019 : International Conference on Cyber Crime and Information Security - Tokyo, 22-23 April 2019.	The scope of the event was to provide an international academic audience with a number of insights on the results of the legal analysis undertaken in EUNITY.
13. IMT	France-Japan Workshop on Cybersecurity, Kyoto, 23-25 April 2019.	Bilateral workshop on cybersecurity. G. Blanc (IMT) presented early results of EUNITY to an audience of French and Japanese cybersecurity experts from academia and industry, as well as policy makers. The presented results included D3.1, D3.2, D4.1 and D4.2 as well as reports on the EUNITY workshops (D2.2 and D2.3).
14. KU Leuven	S. Fantin, Privacy and Cybersecurity in Europe: Policy, Legislation and Opportunities, academic lecture at University of Tokyo Information Technology Center, 24 April 2019	The scope of the event was to explain to a Japanese audience (particularly of security professionals) what are the main novelties in terms of EU law and policy which have an impact on their daily activities and operations.

15. KU Leuven	S. Fantin, EU Japan Privacy and Cybersecurity partnership: an EU policy perspective, academic lecture at NAIST - IPLab/Center for Cyber Resilience - Nara, 25 April 2019	The scope of the event was to provide Japanese cybersecurity researchers and students the perspective on GDPR and EU Cybersecurity policies from a legal standpoint, so to bridge the engineering approach with the legal one.
16. All partners	3rd EUNITY Workshop, 26 April 2019, Kyoto	Workshop oriented to Japanese associated partners and stakeholders. The workshop showcased the results from WPs 3 and 4, as well as Japanese research and education projects to selected Japanese cybersecurity specialists from academia, industry and government.

Table 4.1: Key performance indicators

4.1 Does Privacy Remain in the Future Cyberworld

4.1.1 Objectives

4.1.1.1 Scope of the event

Workshop on cybersecurity held in Luxembourg - iTrust event on June 21st, 2018.

4.1.1.2 Purpose of the visit

KUL visited the event in order to bring research challenges to attention of security experts, talk, research activities and dissemination of EUNITY results.

4.1.2 Participants

4.1.2.1 Type of participants

Industry sector (cybersecurity experts)

4.1.2.2 Number of participants

100 people.

4.1.3 Accomplished goals - Measurements

Work towards EUNITY dissemination, networking and EU research challenges in the area of cyber security. Goal accomplished.

4.2 RAID: International Symposium on Research in Attacks, Intrusions and Defenses

4.2.1 Objectives

4.2.1.1 Scope of the event

The International Symposium on Research in Attacks, Intrusions and Defenses took place in Heraklion, Crete on September 10th-12th, 2018. The event, formerly known as International Symposium on Recent Advances in Intrusion Detection (RAID), is an annual event and its main goal is to share advances concerning intrusion detection.

4.2.1.2 Purpose of the visit

FORTH visited this event. EUNITY was presented as a poster and a leaflet.

4.2.2 Participants

4.2.2.1 Type of participants

The type of participants were academics and cybersecurity professionals.

4.2.2.2 Number of participants

The event has reached 120 participants around the world.

4.2.3 Accomplished goals - Measurements

EUNITY was presented to the audience (as a poster). Bring research on topics covering on cybersecurity and criminology to the attention of international experts. Accomplished.

4.3 European Researchers' Night 2018

4.3.1 Objectives

4.3.1.1 Scope of the event

The European Researchers' Night 2018 in Crete, Greece took place on September 29th, 2018 with the main objective to bring scientific and research showcases to the attention of the broader audience.

4.3.1.2 Purpose of the visit

EUNITY was presented as a poster and a leaflet.

4.3.2 Participants

4.3.2.1 Type of participants

The type of participants mixed people from the research community, academia and broader audience.

4.3.2.2 Number of participants

The event has reached approximately 2000 participants.

4.3.3 Accomplished goals - Measurements

EUNITY main objectives and accomplishments were presented to the audience (as a poster). The main goal was to bring scientific and research showcases to the attention of the broader audience. Goal accomplished.

4.4 NIS: ENISA Summer School

4.4.1 Objectives

4.4.1.1 Scope of the event

The fifth Network and Information Security Summer School, took place in Crete, Greece, from 24 September - 28 September 2018. The main objective for this year was to delve into the challenge of the Changing Risk Landscape. This includes the dynamics, the dependencies and the complexity inherent to Information Technology.

4.4.1.2 Purpose of the visit

FORTH with ENISA co-organized this event. EUNITY was presented as a poster and a leaflet.

4.4.2 Participants

4.4.2.1 Type of participants

The type of participants were academics and cybersecurity professionals.

4.4.2.2 Number of participants

The event has reached 180 participants around the world.

4.4.3 Accomplished goals - Measurements

EUNITY was presented to the audience (as a poster). The main goal was to bring the challenge of the Changing Risk Landscape to the attention of international experts. Accomplished.

4.5 Presentation in EUROCRIM '18- Sarajevo/BiH

4.5.1 Objectives

4.5.1.1 Scope of the event

The EUROCRIM '18 conference took place in Sarajevo from August 29th, 2018 till September 1st, 2018. The scope of the visit was to present the EUNITY project within the cybercrime panel.

4.5.1.2 Purpose of the visit

KU Leuven visited this event as a presenter (S. Fantin).

4.5.2 Participants

4.5.2.1 Type of participants

The participants were from academia.

4.5.2.2 Number of participants

The number of participants reached approximately 1000k.

4.5.3 Accomplished goals - Measurements

International conference for thought leaders in criminology, where cybersecurity and privacy are becoming increasingly important and are allocated in a number of panels. Bring research challenges to attention of broader EU and international audience. Get updates on the most recent research and industry security challenges and needs. Goal accomplished.

4.6 Participation in cyberwatching.eu Annual Event during CyberSec Forum 2018

4.6.1 Objectives

4.6.1.1 Scope of the event

The CyberSec Forum 2018 took place in Kraków, Poland from October 8th to 9th, 2018. This large, international conference also hosted the cyberwatching.eu Annual Event, with the session “International cooperation and alignment on cybersecurity and privacy issues” on October 8th. The scope of the visit was to present the findings of EUNITY (with a strong focus on D3.1) and take part in the following discussion panel.

4.6.1.2 Purpose of the visit

NASK visited this event as a presenter and panelist (A. Kozakiewicz).
ATOS also participated in this event as attendant, joining the discussions about possible collaborations of Europe-Japan in cybersecurity.

Note that the visit was seen as a good low-cost opportunity, as the costs were shared with another project (SISSDEN), which was already scheduled to be presented on the next day in a closed session by the same person.

4.6.2 Participants

4.6.2.1 Type of participants

The participants were varied, including academia, defense, LEA, industry and government.

4.6.2.2 Number of participants

The number of participants of the conference as a whole reached approximately 1000, but the number of participants in the actual session was approximately 40.

4.6.3 Accomplished goals - Measurements

Main goals – promote the project, disseminate the findings of D3.1, gather direct feedback, compare and contrast with the viewpoints of AEGIS (EU-US), cyberwatching.eu (EU) and ECSO (EU). Goals were accomplished.

4.7 Presentation in Victims of Cybercrimes: Legal Aspects on Protection and Liabilities

4.7.1 Objectives

4.7.1.1 Scope of the event

The Victims of Cybercrimes: Legal Aspects on Protection and Liabilities (Public Policy lessons from DANTE and EUNITY projects) took place in the Hebrew University of Jerusalem, Israel on October 15th, 2018. The scope of the visit was to present the EUNITY project within the cybercrime panel.

4.7.1.2 Purpose of the visit

KU Leuven visited this event as a presenter (S. Fantin).

4.7.2 Participants

4.7.2.1 Type of participants

The participants were academics and cybersecurity professionals.

4.7.2.2 Number of participants

The number of participants reached 30 people.

4.7.3 Accomplished goals - Measurements

Conference on cybersecurity and criminology. Bring research challenges to attention of international experts. Goal accomplished.

4.8 France-Japan workshop on cybersecurity

4.8.1 Objectives

4.8.1.1 Scope of the event

The France-Japan workshop on cybersecurity is an annual event for the French and Japanese cybersecurity research communities. The community organized an intermediate workshop at Keio University, Tokyo, in October 29th and 30th 2018. This workshop was focused on two specific topics, “cybersecurity for IoT” the first day, and “cybersecurity and IA” on the second day. A third event on ethics of cybersecurity was organized by the same team, but it was not attended.

4.8.1.2 Purpose of the visit

The purpose of attending the event was twofold. First, it enabled a presentation of the current status of the project (on October 29th), to gather feedback on the contents of D3.1. To this purpose, a reduced slide deck presented the main highlights of the deliverable. Second, it enabled the EUNITY participant to obtain information about the Japanese presentation on these subjects, particularly on Society 5.0.

4.8.2 Participants

4.8.2.1 Type of participants

The workshop was a small, by invitation only event. Roughly 20 persons participated, 5 from Europe and 15 from Japan (although several participants from Japan represented French organizations such as CNRS or the French embassy in Japan).

4.8.2.2 Number of participants

Hervé Debar was the only IMT participant. Roughly 20 persons attended, mostly from academia. Two presentations were made by Japanese ministry representatives, and 2 from industry.

4.8.3 Accomplished goals - Measurements

The objectives of gathering information were fully achieved. Information gathered about the Japanese perspective will be folded into D4.1 and D4.2. The following points can be highlighted:

- The 4th plan of NICT (2016-2020) has cybersecurity at its core, to support sensing, research, integrated ICT and data in the future society. NICT is publishing a research map on 4 quadrants along 2 axis, “global versus local attacks”, and “passive versus active security tools”.

- Japan has published 21 concepts in the IoT Security Guidelines V1.0 [1]. They are associated with Consumer Device Security Guidelines

[1] http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf

(CCDS) v2.0, which includes information for industry sectors (automotive, etc.).

- Working draft ISO/IEC JTC1/SC27 provides guidelines on risks, principle and controls for security and privacy in IoT.
- Japan wants to address IoT Data, Open IoT platform, IoT standards and IoT security. The later focuses on security and privacy by design and the production of guidelines and standards.

4.8.4 Key Performance Indicator

The intention was fully accomplished.

4.9 Visits to Japanese influential representatives on cybersecurity

4.9.1 Objectives

4.9.1.1 Scope of the event

On October 31st and November 2nd, Professor Kadobayashi from NAIST and Professor Debar from IMT made several visits to Japanese influential representatives on cybersecurity. The following visits took place:

- October 31st, visit to the IPA center of excellence ICS CoE to visit this state of the art training center on cybersecurity.
- October 31st, visit to the Ministry of Industry (METI) cybersecurity division
- November 2nd, visit to the Ministry of Communication and Internal affairs (MIC) and NICT, to the director general for cybersecurity.
- November 2nd, visit to NEC head of cybersecurity lab, cybersecurity strategy HQ and regulatory research office.

4.9.1.2 Purpose of the visit

The visits had three purposes. First, they aimed at presenting the EUNITY findings, using the same set of slides representing highlights of D3.1. Second, they aimed at eliciting the point of view of Japanese officials and industry on cybersecurity topics. Third, discussions took place on joint topics of interest. Interestingly enough, several topics of interest came out regardless of the participants' origin: training and awareness, certification, information sharing.

4.9.2 Participants

4.9.2.1 Type of participants

Participants were high-level representatives from their organizations, in management positions.

4.9.2.2 Number of participants

Each meeting was attended by 4 to 6 Japanese representatives.

4.9.3 Accomplished goals - Measurements

The following topics were discussed during the meetings:

Japanese vision of Society 5.0. As explained in D3.1, Japan has defined Society 5.0 as the future state of evolution. In this society, digital and physical components are intimately linked, so that there are seamless interactions between objects and humans. Therefore, the question of trust and cybersecurity is fundamental to the success of this evolution.

There is a horizontal expansion of cyber-risk in the supply chain, as outsourced compromised components may be installed in systems and products, with unintended effects such as backdoors or sending data back to the manufacturer. There is a vertical expansion of cyber risk, for example in the networked infrastructures of critical infrastructure providers, e.g. industrial control systems being affected by the same malicious code.

In society 5.0, traditional relationships between businesses and companies are also operated in cyberspace. Traditional risk management is relying on trust and accountability in companies. There are needs for trusted data to ensure that data circulates and is processed to create services, and there are needs for trusted transcription of data between the physical world and the cyber-world.

Cybersecurity is linked to industry expansion, and should be addressed by industry leaders. Hence, METI has established a Study Group on Industrial CyberSecurity. NEC is participating in the cross-sectors forum on cybersecurity human assets development (cf. training).

Training and awareness One of the fundamental issues recognized is the lack of skilled personnel. ICT companies can provide internal training to their workforce to increase the number of trained personnel. The ICT sector can provide services to end-user companies, but not train personnel, and not to the wider range of required skills that are important for end users, and for which ICT companies do not have the proper training forums.

The ICS CoE model for the development of cybersecurity expertise in Japan is particularly interesting. The center of excellence hosts a platform with several realistic industrial environments (manufacturing, transport, energy, etc.). Students are sent from companies for a one year training, including a lot of hands-on training, and project work related to their experience and background.

Certification of experts skills is difficult; there is a need for focused specification of skills, and also of an understanding of the job market. There should be skills maps and job profiles, with the associated training programs, to perform capacity building. Cybersecurity aspects should also be included in non-specialist job descriptions, to raise awareness.

Certification Cybersecurity requirements are sometimes too costly when taken in a generic and broad application sense. There is a need for international harmonization, and this has been discussed with DG CONNECT.

Software is increasingly included in big systems, so this is difficult to certify. There is a need for investment in certification capabilities, and the background of the EU in terms of formal methods for example, or the example of companies such as Quarkslab, is very appreciated. This could be an area for joint R&D. On the other hand, Japan has a strong industrial base and experience in the combination IT+OT.

The notion of self-certification was also discussed, similar to the US approach. However, there is uncertainty as to the level of cybersecurity that this will effectively provide. There should be some alignment of these capabilities.

HD: the capabilities for certification in the EU are different amongst member states.

SMEs SMEs do not have the means to protect themselves. A potential solution is to use insurance mechanisms, companies, to provide affordable cybersecurity services to SMEs, in a manner that is focused on their needs and related to the risk that they effectively incur. Another idea is to have a collaboration platform to exchange information regularly between companies.

Information sharing There is a desire to transfer cybersecurity knowledge to other countries, particularly in the ASEAN region, to build a trusted supply chain. There is a concern with privacy, related to the GDPR.

HD: in the first workshop, JPCERT also mentioned training, particularly in Africa, as a good example of cooperation.

International interactions and sourcing The international ecosystem is strongly present in the discussions, despite the fact that Japanese companies seem concentrated on their home market. METI in particular indicated multiple visits and discussions on cybersecurity with the EU and specific countries over 2018, to discuss policy issues. The main source of cybersecurity technology seems to be the US and Israel. There is a strong desire for presence in Asian countries (e.g. Vietnam, etc.) to maintain the regional influence of Japan in front of major players such as China.

HD: I believe that this is mostly because the European companies known in Japan (Thales, Airbus, etc.) have the image of integrators and are not identified as product vendors.

4.9.4 Key Performance Indicator

These meetings were of very high quality, with many interactions. The information gathered are incorporated in D4.1 and D4.2. The EUNITY project acknowledges and thanks Professor Kadoayashi from NAIST for his support in organizing these meetings.

4.10 Freedom and Security - Killing the zero sum process

4.10.1 Objectives

4.10.1.1 Scope of the event

The workshop took place in the Hague on 22-23 November 2018 in the Europol premises.

4.10.1.2 Purpose of the visit

Engage with law enforcement and policy experts about cybersecurity and privacy legal issues touched in EUNITY, particularly with a focus to the need for cross-border cooperation in research and enforcement of privacy and cybersecurity policies.

4.10.2 Participants

4.10.2.1 Type of participants

Law enforcement, policy professionals (industry, governments and institutions), academia. Reach: Europe and global.

4.10.2.2 Number of participants

The number of participants were around 300.

4.10.3 Accomplished goals - Measurements

Objectives: 1. Sensibilization of law enforcement and security community on two major EUNITY legal topics (vulnerability policy and Cybersecurity Act); 2. Engage with Japanese attendants (see prof. Miyashita) on the EUNITY project. Goal accomplished.

4.11 EUNITY ECSO Workshop.

4.11.1 Objectives

4.11.1.1 Scope of the event

The workshop took place in Brussels on 24 January 2019. The aim was to facilitate the exchange good practices on cyber policy and investigate business opportunities in the context of the EU-JAPAN Trade agreement.

4.11.1.2 Purpose of the visit

4.11.2 Participants

4.11.2.1 Type of participants

The participants originated from academia, industry and SMEs.

4.11.2.2 Number of participants

Approximately, an amount of 63 people attended the workshop.

4.11.3 Accomplished goals - Measurements

The objectives include the valorization and showcase of EUNITY project through networking and learning of Japanese policy landscape and the setting of contacts and roadmap for next valorization trip in Japan. Additionally, a questionnaire was distributed to receive feedback from the attendees and in particular, Japanese ones, with respect to the European approaches presented at the workshop.

4.12 A Comparative Study Between Japan and the European Union on Software Vulnerability Public Policies, ICCCIS 2019

4.12.1 Objectives

4.12.1.1 Scope of the event

International Conference on Cyber Crime and Information Security - Tokyo (JP), 22-23/4/2019. The scope of the event was to provide an international academic audience with a number of insights on the results of the legal analysis undertaken in EUNITY.

4.12.1.2 Purpose of the visit

The purpose of the visit was to engage in an international academic conference during KULs visit in Japan. Additionally, KUL presented abstract and publication in conference proceedings.

4.12.2 Participants

4.12.2.1 Type of participants

International academic professors, senior and junior researchers.

4.12.2.2 Number of participants

The number of participants reached around 50 people.

4.12.3 Accomplished goals - Measurements

The goal was achieved insofar as the abstracts were presented to academic professionals out of the scope of EUNITY and unaware of the project itself. The presentations were awarded with the Best Presentation Award by WASET The KPI for this event was twofold: presentation to at least 10+ people conference (achieved), as well as publication of two abstracts on the conference proceedings (achieved)

4.13 5th France-Japan Workshop on Cybersecurity

4.13.1 Objectives

4.13.1.1 Scope of the event

The event is an annual research-oriented workshop on cybersecurity featuring plenary presentations of research results and topic-focused working groups where specific collaborations are built and developed. The event is alternatively held in France and in Japan.

4.13.1.2 Purpose of the visit

G. Blanc was invited by the steering committee to update the attendees on the results of EUNITY, and in particular on early information on D4.2, which is the Strategic Research and Innovation Agenda. Dissemination was also performed through the distribution of leaflets of D3.1 and D4.2.

4.13.2 Participants

4.13.2.1 Type of participants

Participants are mostly academics, with a small number of industrial and some policy maker or government-level representatives, such as the NISC, the IPA or the French Embassy in Japan.

4.13.2.2 Number of participants

The number of participants were around 50.

4.13.3 Accomplished goals - Measurements

The goal was to disseminate early results of EUNITY as other such roadmapping projects, such as SecUnity, were also featured during this event. A number of leaflets were also distributed to attendees.

[**Comment:***duplicate event (first was held at UT)*]

4.14 Privacy and Cybersecurity in Europe: Policy, Legislation and Opportunities, academic lecture at University of Tokyo (JP)

4.14.1 Objectives

4.14.1.1 Scope of the event

Fantin S., Privacy and Cybersecurity in Europe: Policy, Legislation and Opportunities, academic lecture at University of Tokyo (JP) Information Technology Center, 24/4/2019. [academic lecture] The scope of the event was to explain to a Japanese audience (particularly of security professionals) what are the main novelties in terms of EU law and policy which have an impact on their daily activities and operations.

4.14.1.2 Purpose of the visit

The purpose of the visit was to provide operational and policy information to Japanese experts on the results of the analysis undertaken within EUNITY, as well as engage in discussions on future challenges and opportunities on EU-JP relationships.

4.14.2 Participants

4.14.2.1 Type of participants

University of Tokyo personnel, academic staff and security experts from academia.

4.14.2.2 Number of participants

The number of participants were around 10.

4.14.3 Accomplished goals - Measurements

The goal was achieved insofar as the results from EUNITY reached a broader number of departments within the EUNITY partner University of Tokyo, so to enable the whole organization to benefit from the European research. Broadly, the aim was to foster trust between KUL and UniTokyo for further potential engagements.

The KPI for this event was based on the number of questions received on GDPR-related matters (at least 5), which was fully achieved.

4.15 Academic lecture at NAIST -iPLab/Center for Cyber Resilience, Nara (JP), 25/4/2019

4.15.1 Objectives

4.15.1.1 Scope of the event

Fantin S., Eu Japan Privacy and Cybersecurity partnership: an EU policy perspective, academic lecture at NAIST -iPLab/Center for Cyber Resilience - Nara (JP), 25/4/2019 (academic lecture) The scope of the event was to provide Japanese cybersecurity researchers and students the perspective on GDPR and EU Cybersecurity policies from a legal standpoint, so to bridge the engineering approach with the legal one.

4.15.1.2 Purpose of the visit

The purpose of the visit was to engage with NAIST in a twofold way: by actively giving an academic lecture, as well as by visiting the research center and learning more on the research undertaken by associates of the IPLab, in order to explore further possibilities of collaboration.

4.15.2 Participants

4.15.2.1 Type of participants

NAIST personnel, NAIST students and young researchers

4.15.2.2 Number of participants

The number of participants reached approximately 30 people.

4.15.3 Accomplished goals - Measurements

The broader goal for this event was to engage with EUNITY partner NAIST and take part in its daily activity of lecturing and researching. This enabled fostering trust amongst partners KUL and NAIST for potential further collaboration.

The KPI for this event was based on the number of questions received on GDPR-related matters (at least 5), which was fully achieved.

4.16 3rd EUNITY Workshop in Kyoto, 26/04/2019

4.16.1 Objectives

4.16.1.1 Scope of the event

A third workshop was organized as a courtesy to Japanese associated partners to disseminate early results of EUNITY and getting latest feedbacks before submitting the final deliverables. Time was dedicated to discuss future project opportunities.

4.16.1.2 Purpose of the visit

EUNITY partners presented the results of the project from both research and innovation, education and training, legal and policy, as well as industry and standardization perspectives. These presentations were confronted to Japanese approaches in terms of capacity building and new frontiers in cybersecurity research. The main goal was to collect feedback from the attendees and to initiate new collaborations for future projects or cybersecurity initiatives. A specific session closing the event was featured to discuss future collaboration avenues. A number of leaflets covering D3.1, D3.2, D4.1 and D4.2 were also distributed.

4.16.2 Participants

4.16.2.1 Type of participants

Attendees were cautiously selected among active cybersecurity stakeholders in Japan from both academia and industry, several of them actually chairing at industry associations such as ISACs, Keidanren or CRIC CSF.

4.16.2.2 Number of participants

20+ attendees outside of EUNITY partners.

4.16.3 Accomplished goals - Measurements

This workshop is not part of the Document of Work, but was organized with the idea to touch base once more with the Japanese community, offering them an early peek into EUNITY results, getting their feedback on whether it aligned with their expectations, before getting into talks around what could be the next steps. The small number of attendees provided a comfortable venue to discuss future R&I opportunities, and some contacts were established, although not many joint calls will be proposed towards the end of Horizon 2020 framework programme.

5 ICS-CoE visit in Europe

5.1 Visit to France

19 trainees from the ICS-CoE, accompanied by two members of staff from NAIST visited France on September 18th and 19th. The trainees were mainly employees from critical infrastructure operators, and in particular from the energy sector, but the delegation also comprised people working at technology vendors or cybersecurity companies. On September 18th, the delegation was hosted at IMT/Tlcom ParisTech where they attended several talks around the security of critical infrastructures with a focus on industrial control systems offered by IMT/Tlcom SudParis for the research aspect, and by Sentryo for the operational aspect, and by the French National Cybersecurity Agency (ANSSI) for the policy and strategy aspects. On September 19th, the delegation visited the Nano-Innov location in Palaiseau, close from Paris, where they were hosted by both IRT System X and CEA. They were introduced to the CHESS Platform developed and maintained by IRT System X and they attended several demonstrations of cybersecurity measures on physical use cases emulated in the CHESS Platform. CEA presented their works to perform operation cybersecurity using advanced reasoning while EDF, the historical French energy provider, introduced research and development in securing IoT components, as carried out at their R&D laboratory.

6 Publications

Two abstracts were published in the conference IRC/ICCCIS 2019 : International Conference on Cyber Crime and Information Security - Tokyo (JP), 22-23/4/2019. IRC 2019

- Fantin, Stefano; 2019. Fantin S., Japanese and EU Legal Frameworks on Data Protection and Cybersecurity: Asymmetries From a Comparative Perspective , IRC/ICCCIS 2019 : International Conference on Cyber Crime and Information Security - Tokyo (JP), 22-23/4/2019. IRC 2019 - International Research Conference Proceedings; 2019 Publisher: World Academy of Science, Engineering and Technology

- Fantin, Stefano; 2019. Fantin S., A Comparative Study Between Japan and the European Union on Software Vulnerability Public Policies, ICCCIS 2019 : International Conference on Cyber Crime and Information Security - Tokyo (JP), 22-23/4/2019. International Research Conference Proceedings 2019; 2019 Publisher: World Academy of Science, Engineering and Technology

7 Website and Social Networks

7.1 EUNITY website

This chapter describes the EUNITY website [1], the Twitter [2] and the LinkedIn account[3]. All results, publications and news are published in these sources, along with general information about the project participants, the project goals, tools or other deliverables.

The main homepage provides general information and the objectives of the project, as well as the latest streamline of EUNITY Twitter account. The “partners” tab lists the partners that constitute “The EUNITY Consortium”, along with a brief description and a link about them. The “Publications” and ”News” section will be continuously updated with the project deliverables, the publications, technical reports, articles, posters and generally dissemination activities as results of the EUNITY project. Information about the events organized by the project is be available in the “Workshops” tab, and finally a contact page is available from which anyone can send a message through the “Contact Us”tab.

7.2 EUNITY on Twitter

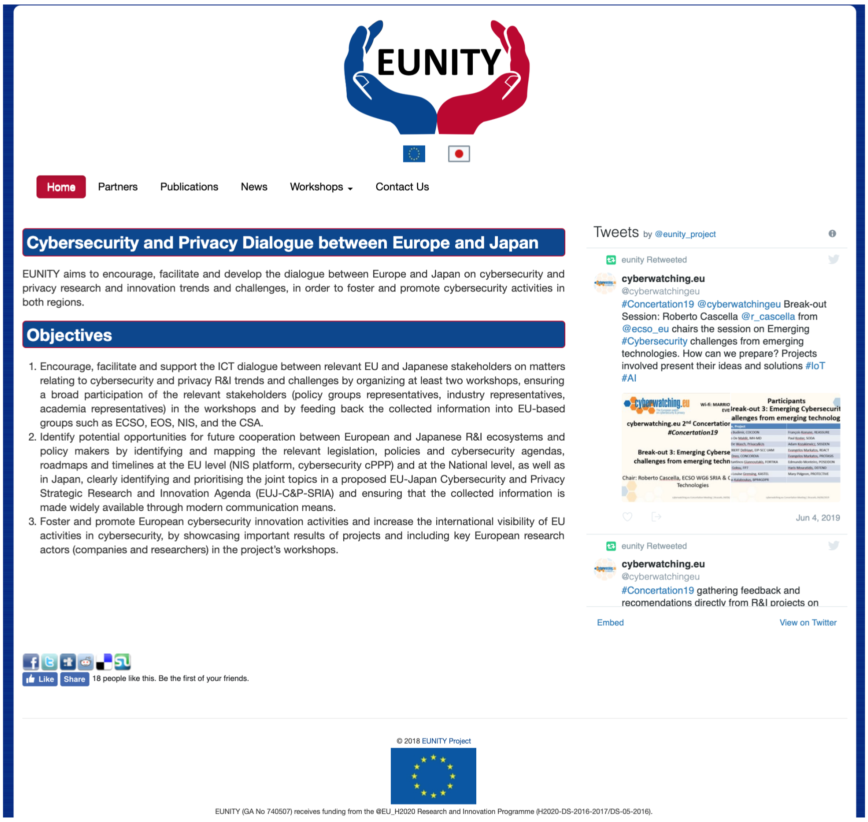
Currently EUNITY preserves an online presence in Twitter. The Twitter account has 173 followers, originating from partners and related contacts, experts in cybersecurity and dissemination agencies, 70 followings and 300 tweets posted with project tweets and tweets of general interest in Cyber Security, as well as tweets in Japanese.

The Twitter profile of EUNITY provides a continuous stream of information and updates concerning the news and development of the project. The

[1] Available at http://www.eunity-project.eu

[2] Available at https://twitter.com/EUNITY_project

[3] https://www.linkedin.com/in/eunity-project/



Cybersecurity and Privacy Dialogue between Europe and Japan

EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions.

Objectives

1. Encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters relating to cybersecurity and privacy R&I trends and challenges by organizing at least two workshops, ensuring a broad participation of the relevant stakeholders (policy groups representatives, industry representatives, academia representatives) in the workshops and by feeding back the collected information into EU-based groups such as ECSO, EOS, NIS, and the CSA.
2. Identify potential opportunities for future cooperation between European and Japanese R&I ecosystems and policy makers by identifying and mapping the relevant legislation, policies and cybersecurity agendas, roadmaps and timelines at the EU level (NIS platform, cybersecurity cPPP) and at the National level, as well as in Japan, clearly identifying and prioritising the joint topics in a proposed EU-Japan Cybersecurity and Privacy Strategic Research and Innovation Agenda (EUJ-C&P-SRIA) and ensuring that the collected information is made widely available through modern communication means.
3. Foster and promote European cybersecurity innovation activities and increase the international visibility of EU activities in cybersecurity, by showcasing important results of projects and including key European research actors (companies and researchers) in the project's workshops.

Tweets by @eunity_project

eunity Retweeted

cyberwatching.eu
@cyberwatchingeu
#Concertation19 @cyberwatchingeu Break-out Session: Roberto Cascella @r_cascella from @ecso_eu chairs the session on Emerging #Cybersecurity challenges from emerging technologies. How can we prepare? Projects involved present their ideas and solutions #IoT #AI

cyberwatching.eu
cyberwatching.eu 2nd Concertation
#Concertation19
Break-out 3: Emerging Cyberse
challenges from emerging techn
Chair: Roberto Cascella, ECSO WG6 SRIA & C
Technologies
Participants
Break-out 3: Emerging Cybersecurit
allenges from emerging technolog

Jun 4, 2019

eunity Retweeted

cyberwatching.eu
@cyberwatchingeu
#Concertation19 gathering feedback and recomendations directly from R&I projects on

18 people like this. Be the first of your friends.

© 2018 EUNITY Project

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

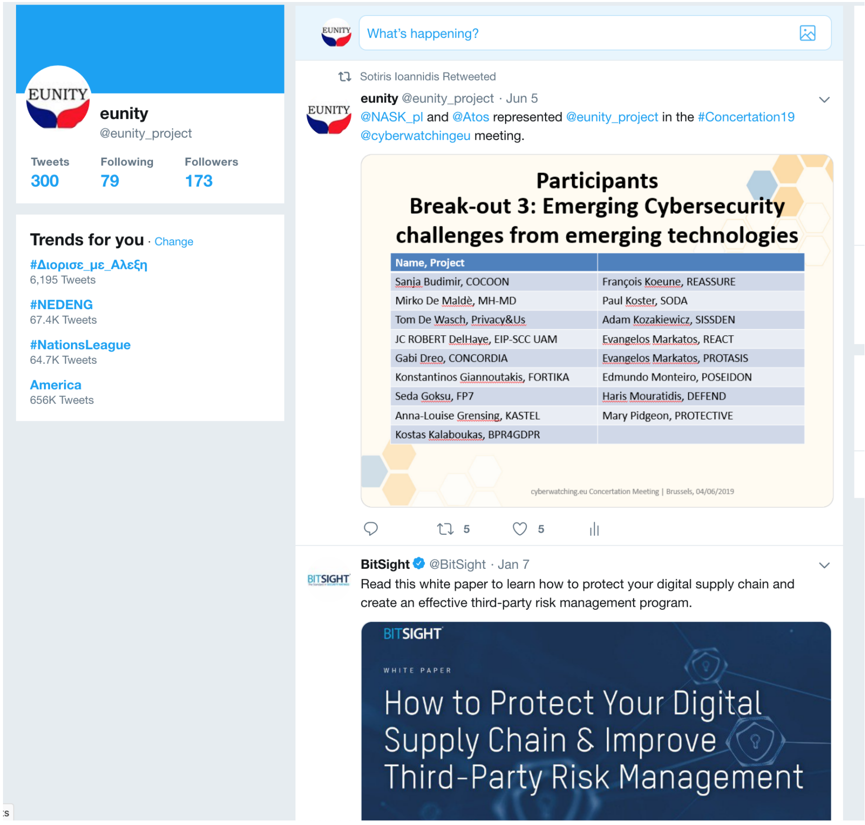
Figure 7.1: The Homepage of EUNITY website

Twitter timeline is also available through the website of EUNITY project in the form of *news feed*.

7.3 EUNITY on LinkedIn

EUNITY project is also present in LinkedIn [4]. The project account is connected to partners, correlated projects and cybersecurity experts. The account along with Twitter, publishes and reposts news about the project and general cybersecurity news.

[4] https://www.linkedin.com/in/eunity-project/



eunity
@eunity_project

Tweets 300 · Following 79 · Followers 173

Trends for you · Change

#Διοριοε_με_Αλεξη
6,195 Tweets

#NEDENG
67.4K Tweets

#NationsLeague
64.7K Tweets

America
656K Tweets

Sotiris Ioannidis Retweeted

eunity @eunity_project · Jun 5
@NASK_pl and @Atos represented @eunity_project in the #Concertation19 @cyberwatchingeu meeting.

Participants
Break-out 3: Emerging Cybersecurity challenges from emerging technologies

Name, Project	
Sanja Budimir, COCOON	François Koeune, REASSURE
Mirko De Maldè, MH-MD	Paul Koster, SODA
Tom De Wasch, Privacy&Us	Adam Kozakiewicz, SISSDEN
JC ROBERT DelHaye, EIP-SCC UAM	Evangelos Markatos, REACT
Gabi Dreo, CONCORDIA	Evangelos Markatos, PROTASIS
Konstantinos Giannoutakis, FORTIKA	Edmundo Monteiro, POSEIDON
Seda Goksu, FP7	Haris Mouratidis, DEFEND
Anna-Louise Grensing, KASTEL	Mary Pidgeon, PROTECTIVE
Kostas Kalaboukas, BPR4GDPR	

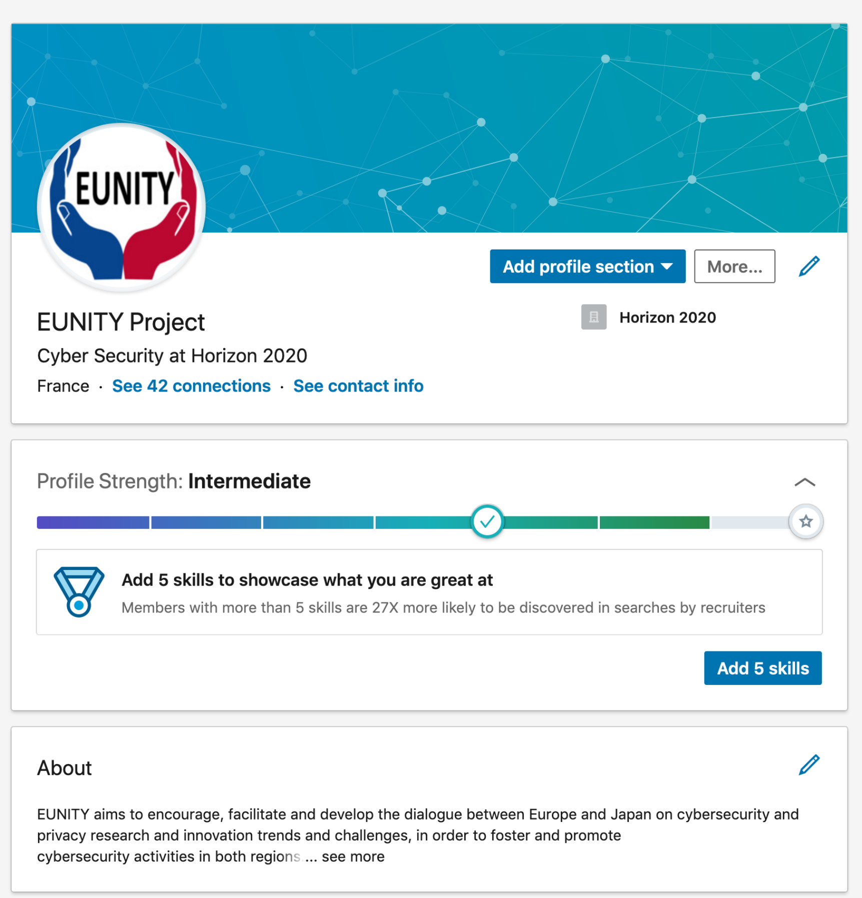
cyberwatching.eu Concertation Meeting | Brussels, 04/06/2019

5 5

BitSight @BitSight · Jan 7
Read this white paper to learn how to protect your digital supply chain and create an effective third-party risk management program.

BITSIGHT
WHITE PAPER
How to Protect Your Digital Supply Chain & Improve Third-Party Risk Management

Figure 7.2: Twitter profile of EUNITY



EUNITY Project

Cyber Security at Horizon 2020

France · See 42 connections · See contact info

Horizon 2020

Profile Strength: **Intermediate**

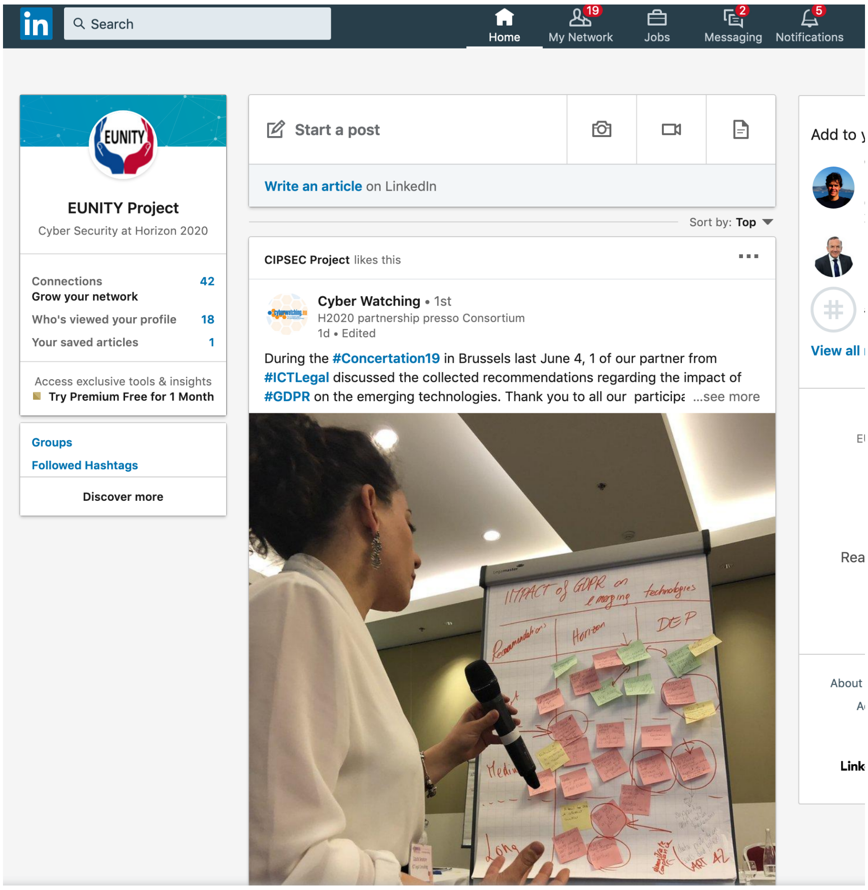
Add 5 skills to showcase what you are great at

Members with more than 5 skills are 27X more likely to be discovered in searches by recruiters

About

EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions ... see more

Figure 7.3: Twitter profile of EUNITY



EUNITY Project
Cyber Security at Horizon 2020

Connections Grow your network	42
Who's viewed your profile	18
Your saved articles	1

Access exclusive tools & insights
Try Premium Free for 1 Month

Groups
Followed Hashtags
Discover more

Write an article on LinkedIn

Sort by: Top

CIPSEC Project likes this

Cyber Watching • 1st
H2020 partnership presso Consortium
1d • Edited

During the #Concertation19 in Brussels last June 4, 1 of our partner from #ICTLegal discussed the collected recommendations regarding the impact of #GDPR on the emerging technologies. Thank you to all our participa ...see more

Figure 7.4: Twitter profile of EUNITY

8 Future projects with Japanese partners

As analyzed in the EUNITY deliverable “D5.2 Management report P1”, the EUNITY project will maintain its main dissemination portals (website, Twitter and LinkedIn), in order to keep the community informed on Europe-Japan activities. Additionally, after the EUNITY project will end, the partners intend to submit to the Cyberwatching.eu CSA small briefs, similar to the summary presentation of the EUNITY deliverable “D3.1: Preliminary version of the Cybersecurity Research Analysis Report for the two regions” that has been used to present the current status of the project for meetings. Also, the partners plan to provide regular updates to ECSO on the status of relationships with Japan and continue the communication to the ICT-03 pilot projects since EUNITY partners are involved in several of the pilot projects (SPARTA, CONCORDIA, Cybersec4EU).

1. How to initiate a potential collaboration between EU and Japan?. In order to initiate a collaboration with Japan the communication can be achieved via diverse channels like direct dialogues, forums, congress addresses and online communication. Additionally, the potential partners can meet in forums organized by cybersecurity organizations, like the European Cyber Security Organisation (ECSO) or ENISA and cybersecurity-related projects connecting the two regions. The Japanese cybersecurity community will be informed on the update and progress on the European cybersecurity strategic agenda, the related projects and calls, as well as the funding and the upcoming problems, by either the ECSO events or the direct communication of older project partners. The involving parties may originate from academia and research (identified by an RTO or universities), industry (industry, association of industry, clusters or SMEs) and policy makers (identified by national agencies like ANSSI, BSI or local organizations). The key Organisations and Networks in Japan include the JETRO - Japan External

Trade Organisation[1], the EEN Japan[2] and the European Business Council in Japan[3]. In addition, embassies of EU member states in Japan have been playing significant role in reaching out to potential collaborators in Japan, by organizing events, exhibits and workshops toward key Japanese stakeholders in policy, industry and research. Also the partnership board of ECSO implements the interaction with the European policy maker.

2. Who to contact for information on a potential collaboration between EU and Japan?. In Europe the main cybersecurity organizations except from the European Commission corresponding project calls and partners, are the European Union Agency for Network and Information Security (ENISA) and European Cyber Security Organisation (ECSO). In Japan the EU-Japan Centre for Industrial Cooperation[4], established under the joint initiative of the European Commission (DG Enterprise and Industry) and the Japanese Ministry of Economy, Trade and Industry (METI) provides information about the EU and Japan through its partnership with the Enterprise Europe Network Service. In addition, Keidanren (Japan Business Federation) maintains liaison offices overseas, which can be a contact point to its broad industrial membership. On cybersecurity matters, Cyber Risk Intelligence Center (CRIC) organizes Cross Sectors Forum where industry verticals exchange their views on strategic cybersecurity issues, which was our contact point on industry aspects.

3. Where to apply for funding in EU? The available funding mechanisms in Europe are the European Commission, including the Horizon 2020/FPs: the framework programmes for Research and Technological Development, open competitions, the European special programs such as CEF Connecting Europe Facility, the ENISA-European Union Agency for Network and Information Security, the European Strategy Forum for Research Infrastructures (ESFRI), the European Structural and Investment Funds (ESIF) as well as the international joint programs including the ERANETs and the joint Framework Programme networks. Additionally, there are the intergovernmental networks (e.g. COST) and the National Strategic Reference Framework (NSRF).

4. Where to apply for funding in Japan? The available funding mechanism in Japan include the Japanese Ministry of Internal Affairs and Communications (MIC). The Japan Society for the Promotion of Science (JSPS), is an independent funding agency with main goal to promote science. Specifically the JSPS 192 subcommittee on cybersecurity works as an information exchange hub, targeted to cybersecurity stakeholders from the private or public sector or the academia. JSPS 192 subcommittee on cybersecurity will reach researchers, industry and policy makers in the region. Both JSPS and

[1] https://www.jetro.go.jp/en/

[2] http://www.een-japan.eu/

[3] https://www.ebc-jp.com/

[4] http://www.eu-japan.eu/

National Institute of Information and Communidations Technology (NICT) operates fellowship programs to invite foreign researchers to Japan, which can be used as a funding instrument to build professional network further. Historically, MIC and NICT ran the Japanese part of EU-Japan joint calls in the FP7 and Horizon 2020 which Japanese consortium applied. Also, Japan Student Services Organization (JASSO) operates mobility programs for higher education institutions, which can be used to further develop collaborations among research institutions among EU and Japan, in a spirit similar to the Erasmus program.

5. Are there older collaboration partnership between the two regions?

The partners of EUNITY consortium (IMT, ATOS, NASK, FORTH and KUL) along with six Japanese associate partners (NAIST, UT, JAIST, Meiji, JPCERT, NTT) have a long-standing history of collaboration, since they have worked together in highly successful FP7 NECOMA project, which carried out joint research on cybersecurity and created solid and trust-based professional relationships.

NECOMA (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis) was funded by the European Commission and the Japanese Ministry of Internal Affairs and Communications and lasted from 2013-2016. The CIRRUS (Certification, InteRnationalisation and standaRdization in cloUd Security), initiated in 2012, included among the partners a Japanese agency IPA, belonging to Ministry of Economy, Trade and Industry.

9
Conclusions

9.1 Conclusions

This deliverable contains all the community engagement activities of EUNITY partners, for the second year of EUNITY project. The report includes all the relevant activities undertaken within the project scope to spread the project information to different types of audiences. The description of each event includes the scope of the event, the purpose of the partner's visit, the participants (type and number) as well as the accomplished goals and measurements.

10
Glossary

Name	Explanation
ACL	Access Control List
ANSSI	National Cybersecurity Agency of France (EN)
BSI	Federal Office for Information Security (EN)
CA	Certification Authority
CERT	Computer Emergency Response Team
CERTCOOP	Trans-European and Greek CERTs collaboration project
CIPSEC	Enhancing Critical Infrastructure Protection with innovative SECurity framework
CNR	Consiglio Nazionale delle Ricerche
cPPP	contractual Public Private Partnership
CRISP	Evaluation and Certification Schemes for Security Products
CSA	Coordination and Support Actions
CSIRT	Computer Security Incident Response Team
DHS	Department of Homeland Security
DOTS	DDoS Open Threat Signaling
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Network and Information Security
EOS	European Organisation of the Sawmill Industry
ESORICS	European Symposium on Research in Computer Security
ETSI	European Telecommunications Standards Institute
FG-DLT	Focus Group on Application of Distributed Ledger Technology
FSE	Fast Software Encryption
GDPR	General Data Protection Regulation
GRNET	Greek Research and Technology Network
HTTP	Hyper Text Transfer Protocol
ICISSP	International Conference on Information Systems Security and Privacy
ICS-CoE	Industrial Cybersecurity Center of Excellence

Name	Explanation
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IODEF	Incident Object Description Event Format
IPA	Information-technology Promotion Agency
ISG	Industry Specification Group
ISI	Information Security Indicators
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication
JSPS	Japan Society for the Promotion of Science
KIISE	Korean Institute of Information Scientists and Engineers
KPI	Key Performance Indicator
METI	Ministry of Economy, Trade and Industry
MEXT	Ministry of Education, Culture, Sports, Science and Technology
MIC	Ministry of Internal Affairs and Communications
MILE	Managed Incident Lightweight Exchange
NEDO	New Energy and Industrial Technology Development Organization
NFV	Network Functions Virtualization
NGO	Non-Governmental Organization
OASIS	Organization for the Advancement of Structured Information Standards
RAID	International Symposium on Research in Attacks, Intrusions and Defenses
RFC	Request For Comments
RTO	Research and Technology Organisation
SCOPE	Strategic Information and Communications R&D Promotion Programme
SDN	Software Defined Network
SEMS	Security for Embedded and Mobile Systems
SG	Study Group
SIEM	Security Information and Event Management
SISSDEN	Secure Information Sharing Sensor Delivery Event Network
SME	Small Medium Enterprises
SOC	Security Operating Center
STIX	Structured Threat Information Expression
STREP	Specific Targeted Research Projects
TAXII	Trusted Automated Exchange of Indicator Information
UoP	University of Patras
WG	Working Group
WP	Work Package