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 D5.3: Dissemination report year 1

Abstract: *The dissemination report will describe the community engagement activities of the project during year 1 and the Japanese research activities landscape.*

Contractual Date of Delivery	May 2018
Actual Date of Delivery	May 2018
Deliverable Dissemination Level	Public
Editor	Despoina Antonakaki, Christos Papachristos, Sotiris Ioannidis
Contributors	All *EUNITY* partners
Quality Assurance	Gregory Blanc

[†] 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

The main objectives of the dissemination report is to summarize all the relevant activities that aim at spreading information, concerning EUNITY project. These activities include the organization of at least two workshops, and the gathering and compilation of feedback via questionnaires and social media. This report will include the community engagement activities only for the first year. We also refer briefly to the Japanese research activities landscape.

The first admission of the privacy rights in Japan were formed in the jurisprudence in the Utage no Ato case[1]. After that, the Act on Personal Information was announced in 2013 [2], but was effectively applied in 2005. The concept of privacy in Japan has been reformed since that, including the Diet [3], that has two parts: the basic principles (chapters 1 to 3), and the general obligations (chapters 4 to 6), and other steps [4], [5], until it was shaped in its final form in 2017 [6].

Currently the financing mechanisms in cybersecurity research in Japan include: the Ministry of Internal Affairs and Communications (MIC) including the Strategic Information and Communications R&D Promotion Pro-

[1]Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. International Data Privacy Law, 1(4), 229-238. http://dx.doi.org/10.1093/idpl/ipr019

[2]Carol Lawson, Japans New Privacy Act in Context, 29 U.N.S.W.L.J. 88 (2006)

[3]The equivalent for the parliamentary bodies of Japan

[4]Miyashita, H. (2011). The evolving concept of data privacy in Japanese law. International Data Privacy Law, 1(4), 229-238. http://dx.doi.org/10.1093/idpl/ipr019; Hiroshi Miyashita, Changing Privacy and Data Protection in Japan (2009) 10 The Sedona Conference Journal 277, 278.https://search.proquest.com/docview/1564009526?accountid=17215

[5]Harriet Pearson, Julie Brill, Mark Parsons and Hiroto Imai (Hogan Lovells) for Lexology, Changes in Japan Privacy Law to Take Effect in Mid-2017; Key Regulator Provides Compliance Insights (1.2.2017)

[6]M. Harada, Japan: Personal data protection. (2017). International Financial Law Review, Retrieved from https://search.proquest.com/docview/1872090298?accountid=17215

gramme (SCOPE) and the National Institute of Information and Communications Technology (NICT); the Ministry of Economy, Trade and Industry (METI) including the New Energy and Industrial Technology Development Organization (NEDO) and the Information-technology Promotion Agency (IPA);and the Ministry of Education, Culture, Sports, Science and Technology (MEXT) including the Japan Society for the Promotion of Science (JSPS).

The main goals of the Cybersecurity strategy in Japan are to provide a free, fair, and secure cyberspace; guarantee of free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders.

The ongoing arrangements on the budget that are provided to cybersecurity include: IoT security; critical infrastructure protection and the protection of government agencies; investment onto national R&D agencies; capacity building and R&D; and investments toward the Tokyo 2020 Olympic and Paralympic games. The IT security market in Japan was around 979 billion yen for 2017, (7.6 billion Euro) [7] and is expected to reach close to 1 trillion yen for 2018.

A more extended analysis is available in EUNITY deliverable 3.1, as well as the analysis of the European cybersecurity research activity landscape.

[7] According to the JNSA IT Security Market Analysis Report 2016,

2 Workshops

2.1 Organization of Workshops

2.1.1 Workshop in Tokyo

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 first workshop, as the second will be analyzed in the "Dissemination report Year 2". The first workshop was organized by IMT, at the Takeda Hall, in the University of Tokyo, Asano Campus, on 11-12 October, 2017.

2.1.1.1 Organization

Local organization was assumed by both The University of Tokyo and the Nara Institute of Science and Technology. Particular efforts were made by Japanese partners to attract and invite a balanced mix of people, including not only researchers and industry representative, but also policy makers, end-users and experts in law and privacy. The workshop, which was carried out over a period of 2 days, covered the main domains of interest that concern the Europe-Japan dialogue on cybersecurity, namely research & innovation and education, market and standards, law and privacy, awareness and incident response. It was organized in pairs of sessions in which, the first one presented the current situation of each topic with perspectives from both Europe and Japan, and the second one, organized as a break-out session, focused on discussions on these topics, with regards to what was presented. These break-out sessions were animated by the EUNITY partners, and often featured a questionnaire, prepared by the topic leaders (NASK for

CERT, ATOS for industry, KUL for privacy, and FORTH for R&I), to support the interactions.

2.1.1.2 Objectives

The workshop is part of WP2 on "Dialogue and community interactions". In particular the first workshop's objectives are as follows:

- inform the Japanese community about cybersecurity in Europe, in particular:
  - research and innovation activities
  - roadmaps
- gather feedback from the Japanese community on:
  - the relevance of the European cybersecurity and privacy objectives
  - the importance of these objectives in Japan
  - the identification of missing activities that are important in Japan

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

2.1.1.3 Schedule

The first workshop's duration was two days. The first day featured an introductory session where Hervé Debar (IMT), the EUNITY coordinator, introduced the EUNITY project to the attendees, jointly with Youki Kadobayashi (NAIST), who leads the consortium of Japanese associated partners. Two sessions followed on the topic of CERTs, with invited presentations highlighting challenges of information exchange and coordination at a global level on both Europe and Japan sides. The first day closed with a focus on industry, exposing the state of the market in Europe, the main challenges, with respect to the certification of products in Europe, and an overview on the coordination activities between different business sectors in Japan.

The second day started with a presentation of the cybersecurity landscape in Europe. It then focused on policy and legal matters in the morning: impacts of the different regulations from Europe (including NIS directive and GDPR), and data protection in Japan. The afternoon was dedicated to presenting the EUNITY take on research & innovation gap analysis between Europe and Japan, and particularly the past efforts from Europe to build roadmaps for cybersecurity R&I. The session explained to the attendees the

EUNITY methodology to identify common ground of interest, and gaps that could complete both Europe and Japan research agendas, eventually leading to reinforced collaboration.

2.1.1.4 Attendance

The workshop welcomed more than 60 attendees over the 2 days, including representatives from EUNITY, cybersecurity experts from industry, academia and CERTs seeking cooperation between Europe and Japan, representatives of policy makers and some end-users from the industry (television, automotive).

2.1.1.5 Exploitation

The results of discussions and the responses to the questionnaires will be exploited in the gap analysis and research agenda produced by WP3 and WP4, respectively.

Below, we add the program of the workshop:

EUNITY Project Workshop – October 11-12, 2017

[Cybersecurity and Privacy Dialogue between Europe and Japan]

Horizon 2020 – The EU Framework Programme for Research and Innovation
DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation
Scope 2: International dialogue with Japan

Location

Takeda Hall, the University of Tokyo
Address : 2-11-16 Yayoi, Bunkyo-Ku, Tokyo, 113-8658 Japan
Subway station: Nezu (subway code: C14) or Todaimae (subway code: N12)

Dates

From Wednesday, October 11 to Thursday, October 12, 2017

Agenda

October 11, 2017: 9:00 – 17:30

09:00 - 09:15	Registration
09:15 - 10:45	Session 1 *(chair: Hervé Debar, IMT and Youki Kadobayashi, NAIST)*
	Introduction
	TF-CSIRT (Baiba Kaskina, CERT.LV)
	JPCERT capability building (Takayuki Uchiyama, JPCERT/CC)
10:45 - 11:00	(coffee break)
11:00 - 12:00	Session 2: CERT (Workshop format) *(chair: Pawel Pawlinski, CERT Polska)*
	Information sharing
	Operations
	Cyber-security monitoring
	Incident coordination
12:00 - 13:30	(lunch break)
13:30 - 14:00	Session 3: CERT (continued)
	Wrap-up (Pawel, Pawlinski, CERT Polska)
	Task Force Software Vulnerability Disclosure in Europe (Afonso Ferreira, IRIT)
14:00 - 15:30	Session 4: Industry *(chair: Pedro Soria, ATOS)*
	Strategic agenda / ECSO by Hervé Debar, IMT
	Market situation and ECIL recommendations (Pedro Soria and Alicia Garcia, ATOS)
	Introductions of CRIC Cross Sectors Forum (Hiroshi Takechi, NEC/CSF)

Standards / ECSO/WG1 by Hervé Debar, IMT
15:30 - 16:00 (coffee break)
16:00 - 17:30 Session 5: Industry (Workshop Format) *(chair: Pedro Soria, ATOS)*
Cyberwatching.eu by Nicholas Ferguson (Trust-IT services, Cyberwatching.eu coordinator)

October 12, 2017: 9:00 – 17:30

09:00 - 09:15 Registration
09:15 - 10:45 Session 6: Landscapes *(chair: Hervé Debar, IMT)*
Restitution of 1st day (Hervé Debar, IMT)
The Cybersecurity Policy Landscape in Europe: Legislation and Research (Afonso Ferreira, IRIT)
(EC/MIC Project Officers)

10:45 - 11:00 (coffee break)
11:00 - 12:00 Session 7: Legal and Policy (Workshop format) *(chair: Stefano Fantin, KU Leuven)*
European privacy landscape: GDPR and others (Stefano Fantin, KU Leuven)
Japanese Landscape on Data Protection (Hiroshi Miyashita, Chuo Univ.)
Regulation
Privacy

12:00 - 13:30 (lunch break)
13:30 - 14:00 Session 8: Legal and Policy (continued)

14:00 - 15:30 Session 9: Research & innovation (Workshop format) *(chair: Sotiris Ioannidis, FORTH)*
ECSO WG6 / SRIA (Hervé Debar, IMT)

EU-JP joint call (Daisuke Inoue, NICT)

15:30 - 16:00 (coffee break)
16:00 - 17:30 Session 10: Wrap-up / summary

2.2 Workshop Methodology

In this subsection, we attempt to describe the methodology for organizing a successful workshop in Japan.

2.2.1 Building upon successful collaboration

This subject of international dialogue with Japan on cybersecurity is not new. In 2012, Europe and Japan launched a joint call, *FP7-ICT-2013-EU-Japan: ICT EU – Japan Coordinated Call* to develop international reseach collaboration on ICT technologies. International cooperation activities in this call had three main objectives: (i) to jointly respond to major global technological challenges by developing interoperable solutions and standards, (ii) to jointly develop ICT solutions to major global societal challenges, and (iii) to improve scientific and technological cooperation for mutual benefit. Six common topics of interest have been jointly selected by the European Commission and the Japanese Ministry of Internal Affairs and Communication (MIC). Among these topics of common interest, we could already find one on *Cybersecurity for improved resilience against cyber threats*. As a result, six FP7 Specific Targeted Research Projects (STREPs) have been jointly selected for funding, one for each topic.

The project selected on the topic of cybersecurity was the FP7 STREP NECOMA[1] project. NECOMA ran from June 1st, 2013 to March 30th, 2016. It carried research on (i) gathering cybersecurity-related datasets, (ii) proposing analysis techniques and tools for these datasets, and (iii) designing and experimenting with techniques to protect end users and large networking infrastructures from these threats. It produced several strong deliverables with high visibility, such as Deliverable 3.1 *Policy Enforcement Point Survey*, which was downloaded several hundred times from the project's website. It jointly organized two scientific workshops, one in Europe and one in Japan, both co-located with prestigious conferences (ESORICS 2014 and RAID 2015). Another important event was the NECOMA business meeting organized in 2014 at the University of Tokyo, where project partners presented their results and interacted with Japanese business partners to elicit common areas of interest. There was also shared interest in standardization activities, at ISO, ETSI and the IETF. In the end, exchange of personel and joint work on scientific subjects led to strong publications and results.

It has been the experience of the NECOMA project that the research activities that we have led together were in response to similar problems, and led to similar solutions. While NECOMA was a STREP project, and thus carrying out research, its success highlights the fact that, as researchers as well as individuals, we share common interests, objectives and cybersecurity is-

[1] http://www.necoma-project.eu/, http://www.necoma-project.jp

sues. Beyond this initial experience, sharing research roadmap information is thus a key goal in achieving cybersecurity innovations that benefit both regions on a more global scale. The EUNITY project has been inspired by the common work led by most of the partners during the NECOMA project. NECOMA has been considered particularly successful in terms of collaboration and common work between Japan and Europe on the topic of cybersecurity. EUNITY builds upon this successful collaboration and extends it in order to cover the topics and constituencies of the workshop.

2.2.2 Reaching out to core constituencies

Our targeted community include the policy makers, the industry, the government, the academia, the CSIRTs/CERTs, the standardization and certification bodies, the SMEs, the technology providers and the software vendors.

Since the planning phase of the project, we planned to address the various constituencies that are parties to the cybersecurity research activities. The three core constituencies identified are researchers, industry and policy makers. In the cybersecurity cPPP, researchers are identified through organizations classified as RTO or universities. Industry is identified either as large industry, professional organization (association of industries, either at the European level (e.g., EOS) or national level (e.g., ACN)), clusters or SMEs. Policy makers are identified through national agencies (e.g., ANSSI, BSI) or local organization (e.g., regions). The interaction with European policy makers will happen through the partnership board of ECSO.

In Japan, the JSPS subcommittee 192 on cybersecurity had these three core constituencies, thus it was feasible to reach researchers, industry and policy makers. In addition, the project successfully recruited Japanese associate partners from academic institutions, private industry and public specialized agencies, thus these associate partners further assisted in communicating with these three core constituencies.

2.2.3 Leveraging professional network

It is crucial to leverage professional network in order to get involvement of key cybersecurity professional in both regions. In Europe, the partners of EUNITY are active participants of the cybersecurity cPPP, helping national agencies and local organizations, and interact with European policy makers through ECSO.

In Japan, the associate partners are also active participants of the JSPS subcommittee 192 on cybersecurity, helping national agencies, and interacting with Japanese policy makers through specialized agencies as well as government subcommittees. In order to further develop and maintain good collaboration between EU and Japan, it is essential to build on this network of trust among professionals.

3 KPIs for dissemination events

In order to create opportunities for sharing and research directions, as well as to identify common research paths, the partners of EUNITY project have attended several networking events. We briefly summarize these efforts below, including: the objectives of the event; the purpose of the visit for the corresponding EUNITY partner who participated and how this 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.

We refer briefly to the KPIs for the dissemination events of the EUNITY partners in Table 3.1 and we analyze them, in details, in the next pages.

EUNITY partner	Event	Key Performance Indicator
IMT	ECSO WG6, Brussels, January 31st, 2018	Goals: raise awareness of the activities of EUNITY and initiate discussions with the other CSAs on future joint actions. The presentation of EUNITY was made available to all ECSO WG6 registered members.
IMT	ECSO WG2, Brussels, May 2nd, 2018	Goals: raise awareness of the EUNITY activities. As ECSO WG2 is seeking to develop interactions with foreign cybersecurity markets, particularly with Japan, they value EUNITY for the insights the project can bring with respect to the Japanese cybersecurity market.

KU Leuven	Cyber Security Round Table, Brussels, September 27th, 2018	Goal: get a first-hands explorative attendance and discover research topics, that were included in the EUNITY deliverables.
IMT	Fourth French-Japanese Cybersecurity Workshop, Annecy May 15th to 18th, 2018	WP3 aims at eliciting common topics of interest. As the French-Japanese workshop on Cybersecurity is a place where French and Japanese cybersecurity researchers seek to collaborate, it is ideal in surveying what are the current and future topics of common interest for both France (and then Europe) and Japan.
IMT & ATOS	Horizon 2020 - CSA Cyberwatching.eu, Brussels, 26th April 2018	WP2 on community engagement and WP4 on strategic research agenda requires interaction with other CSA projects for dissemination purposes. During the concentration meeting, EUNITY was given a spot for presenting its preliminary results, and future achievements.
KU Leuven	Updating the European Cyber Security Strategy: Partnerships for Prevention and Preparedness, Brussels, 3rd October 2017	Goal: need to understand the state of play of the cyber security research market and the economic value of it. The accomplished objectives included gaining the background information for the Tokyo project meeting.
NASK	Motorola Solutions Innovation Showcase, , 25 October 2017 in Krakow	Goal: build interest in EUNITY and notify about upcoming workshop in the EU. The resulting discussion and contacts made can be considered potentially valuable.
KU Leuven	Postquantum Cryptography, RSA conference, San Francisco, CA, February 14-17, 2017	Goal: Bring research and standardization challenges to attention of broader audience. Goal accomplished.

KU Leuven	The Future of Information Security,ICISSP 2017, Porto, February 20-22, 2017.	Goal: Bring research challenges to attention of audience of experts. Goal accomplished.
KU Leuven	Privacy and Security Challenges for the IoT, Workshop on Security for Embedded and Mobile Systems (SEMS), Paris, April 30, 2017.	Goal: Bring research and standardization challenges to attention of experts. Goal accomplished.
KU Leuven	The Future of Security and Privacy, Imec Technology Forum, Antwerp, May 16-17, 2017.	Goal: Bring research challenges to attention of broader audience. Goal accomplished.
KU Leuven	Does Privacy Remain in the Future Cyberworld ,Luxembourg iTrust event, Luxembourg, June 21, 2017.	Workshop on cybersecurity. Bring research challenges to attention of experts. Goal accomplished.
KU Leuven	The Future of Security and Privacy, Dcypher Event, Utrecht, Oct 4, 2017	Conference on cybersecurity. Bring research challenges to attention of experts and policy makers. Goal accomplished.
KU Leuven	The Future of Security and Privacy, Belgian Cybersecurity Convention, Mechelen, October 25, 2017.	Discuss cybersecurity challenges with nuclear industry. Goal accomplished.

KU Leuven	Visit to Fast Software Encryption (Tokyo), research lab of Hitachi in Yokohama and Kanai University in Osaka, March 2016	Networking. Explore further collaboration in cybersecurity. Goal accomplished.
KU Leuven	The 6th IEEE International Conference on Big Data and Smart Computing, Kyoto, 27.02.19	Presentation of comparative study on EU-Japan in cyber security laws and policies tbd Presentation at 20+ attendance panel.

Table 3.1: Key performance indicators

3.1 European Cyber Security Organisation - WG6

3.1.1 Objectives

3.1.1.1 Scope of the event

The event was an ECSO WG6 physical meeting in Brussels on January 31st, 2018. ECSO (European Cyber-Security Organization) is the European cPPP on cybersecurity. Working group 6 (WG6) is in charge of defining the strategic research agenda for ECSO. It discussed and provided input to the H2020 2018-2020 work-programme and is currently discussing the 2030 outlook for the next "Horizon Europe" research framework. WG6 is chaired by Fabio Martinelli (CNR), Volkmar Lotz (SAP) and Fabio Cocurullo (LEONARDO).

3.1.1.2 Purpose of the visit

A presentation was given in the context of a joint presentation of the three CSAs on cybersecurity.

The main objective of the visit was to raise awareness of the activities of EUNITY within the ECSO research community, specifically targeting the experts working on the ECSO research agenda. This addresses the needs of both industry and academia.

A secondary objective was the discussions with the other CSAs on future joint actions.

3.1.2 Participants

3.1.2.1 Type of participants

WG6 gathered over 300 experts, both from academia and industry.

3.1.2.2 Number of participants

Hervé Debar from IMT was the only participant and presenter. KUL and FORTH were also represented.

The WG6 meeting was attended by roughly 60 experts from industry and academia over Europe.

3.1.3 Accomplished goals - Measurements

3.1.3.1 Key Performance Indicator

ECSO WG6 meetings are usually attended by 60 to 80 persons. To this extend, this meeting reached its full objectives. The presentation of EUNITY was made available to all ECSO WG6 registered members (over 300 persons in 230 organizations).

3.2 European Cyber Security Organisation - WG2

3.2.1 Objectives

3.2.1.1 Scope of the event

The event is an ECSO WG2 physical meeting in Brussels, May 2nd, 2018.

ECSO (European Cyber-Security Organization) is the European cPPP on cybersecurity.

Working group 2 (WG2) is in charge of developing the market strategy for European products and fostering international collaboration to disseminate these products. It aims at facilitating private and public investment in the cybersecurity market, with both main trade partners (US, China, Brazil and Japan) and developing countries.

3.2.1.2 Purpose of the visit

A presentation was given in the context of a WG2 board meeting where survey results and strategies were discussed.

The main objective of the visit was to raise awareness of the activities of EUNITY within the ECSO business community, specifically targeting ECSO industry partners that are interested in the Japanese cybersecurity market.

3.2.2 Participants

3.2.2.1 Type of participants

This WG2 gathered mainly industry participants.

3.2.2.2 Number of participants

Gregory Blanc from IMT was the only participant and presenter.

The WG2 meeting was attended by more than 20 people from ECSO industry partners.

3.2.3 Accomplished goals - Measurements

3.2.3.1 Key Performance Indicator

One of the objectives of EUNITY is to promote European cybersecurity products. As ECSO WG2 is seeking to develop interactions with foreign cybersecurity markets, and in particular with Japan, they value EUNITY for the insights the project can bring with respect to the Japanese cybersecurity market.

3.3 Cyber Security Round Table, Brussels

3.3.1 Objectives

3.3.1.1 Scope of the event

The event was a Cyber Security Round Table on 27.09.2017 in Brussels. The scope of the event was to investigate insightful research topics on cyber security and the protection of critical infrastructures.

3.3.1.2 Purpose of the visit

KU Leuven participated in the Cyber Security Round Table in order to gain a clear idea on what domains are now explored in European cyber security research.

3.3.2 Participants

3.3.2.1 Type of participants

This round table meeting brought together EU policy makers, academic experts, and public & private sector representatives from Operational and IT backgrounds, leading cyber security authorities and some of the worlds most influential IT solution providers. In offering a variety of perspectives and

recommendations through a series of open discussions, the goal was to examine the ongoing challenges in effectively managing cyber security, exploring practical solutions, reaching an EU-wide consensus and implementing a forward action plan.

The participants were from academia and research professionals from industry.

3.3.2.2 Number of participants

The number of persons reached approximately 100 and one EUNITY partner from KU Leuven.

3.3.3 Accomplished goals - Measurements

3.3.3.1 Key Performance Indicator

The initial intention of our visit was to get a first-hands explorative attendance with the aim of drafting a first Table of Content in the Policy Section of D3.1. The accomplished objectives included the research topics discovery for the Table of Content drafted and the Table of Content Policy Section D3.1 completed. The participation at the event was 50 attendees. Accomplished.

3.4 Fourth French-Japanese Cybersecurity Workshop

3.4.1 Objectives

3.4.1.1 Scope of the event

The event is an annual workshop for French and Japanese researchers on the topic of cybersecurity, held from May 15th to 18th, 2018.

The French-Japanese Cybersecurity workshop is a bilateral workshop articulated around 8 working groups, tackling diverse cybersecurity fields. IMT is co-chairing WG7 on network security.

The workshop aims at fostering collaborations between France and Japan. The workshop meets once to twice a year, and presents results of ongoing collaborations, as well as future research avenues.

3.4.1.2 Purpose of the visit

A presentation was given in the context of a plenary session during the four-day workshop.

The main objective of the visit was to raise awareness of the activities of EUNITY within the European and Japanese cybersecurity research communities.

A secondary objective was to survey the research ongoing between the two countries and elicit common topics from the attendees.

3.4.2 Participants

3.4.2.1 Type of participants

This workshop mainly gathered academic participants, as well as a smaller number of industry and policy maker participants.

3.4.2.2 Number of participants

Gregory Blanc from IMT was the only participant and presenter.

The workshop was attended by more than 60 people, with 2/3 of them being from academia.

3.4.3 Accomplished goals - Measurements

3.4.3.1 Key Performance Indicator

WP3 aims at eliciting common topics of interest. As the French-Japanese workshop on Cybersecurity is a place where French and Japanese cybersecurity researchers seek to collaborate, it is ideal in surveying what are the current and future topics of common interest for both France (and then Europe) and Japan.

3.5 Horizon 2020 - CSA Cyberwatching.eu Concentration Meeting

3.5.1 Objectives

3.5.1.1 Scope of the event

The event is a concertation meeting organized by the Horizon 2020 CSA Cyberwatching.eu project.

Cyberwatching.eu is the Scope 1 CSA project from the H2020-DS-SC7-2016 call.

Cyberwatching.eu is a four-year project dedicated to survey cybersecurity and privacy R&I initiatives across Europe, and promote European products, firstly from SMEs, in order to provide them access to the markets, by building a catalogue of products, services and software.

3.5.1.2 Purpose of the visit

A presentation was given in the context of the Concertation meeting which gathered 50 H2020 projects on the topics of cybersecurity and privacy in order to foster collaboration and networking, as well as inform both Cyberwatching.eu and attending projects on future project outcomes (products, services, software).

The main objective of the visit was to raise awareness of the activities of EUNITY within the H2020 cybersecurity and privacy project community.

A secondary objective was to meet with other CSA partners such as Cyberwatching.eu and AEGIS, the EU-US dialogue project on cybersecurity and privacy.

3.5.2 Participants

3.5.2.1 Type of participants

The Concertation meeting gathered mainly industry (SMEs) and academic participants.

3.5.2.2 Number of participants

Gregory Blanc from IMT was the only participant and presenter. ATOS also attended the event.

The Concertation meeting was attended by more than 60 people, with around 25 academics, and more than 35 industry people. A small number of EU policy makers also attended the events, sitting on panel discussions.

3.5.3 Accomplished goals - Measurements

3.5.3.1 Key Performance Indicator

WP2 on community engagement and WP4 on strategic research agenda requires interaction with other CSA projects for dissemination purposes. During the concentration meeting, EUNITY was given a spot for presenting its preliminary results, and future achievements.

3.6 Updating the European Cyber Security Strategy: Partnerships for Prevention and Preparedness

3.6.1 Objectives

3.6.1.1 Scope of the event

The event "Updating the European Cyber Security Strategy: Partnerships for Prevention and Preparedness" was held in Brussels, on 3/10/2017.

This symposium provided businesses, local actors, industry regulators, intelligence agencies, police, technology specialists, academics and other key stakeholders with a timely and invaluable opportunity to engage with European cybersecurtity policies, collectively enhance our defences to malicious actors and address the root causes of vulnerability to cyber threats. The scope of the event was to update on the European strategy, the state of the research market and the main stakeholders.

3.6.1.2 Purpose of the visit

KU Leuven participated in this events because of their need to understand the state of play of the cyber security research market and the economic value of it.

3.6.2 Participants

3.6.2.1 Type of participants

The event attracted participants originated from business, EU Commission, lawyers, academia and NGOs.

3.6.2.2 Number of participants

The number of persons reached approximately 20, including two persons from KU Leuven.

3.6.3 Accomplished goals - Measurements

The initial intention of our visit was to get an update regarding the legal and policy novelties, which was successfully accomplished.

3.6.3.1 Key Performance Indicator

The initial intention included legal and policy novelties updates which were achieved, as well as background information for the Tokyo project meeting. Participation at policy event with 20+ attendance. Accomplished.

3.7 The 6th IEEE International Conference on Big Data and Smart Computing

3.7.1 Objectives

3.7.1.1 Scope of the event

The 6th IEEE International Conference on Big Data and Smart Computing was held in Kyoto 27/02/2018.

The goal of the International Conference on Big Data and Smart Computing (BigComp), initiated by KIISE (Korean Institute of Information Scientists and Engineers), is to provide an international forum for exchanging ideas and information on current studies, challenges, research results, system developments, and practical experiences in these emerging fields.

3.7.1.2 Purpose of the visit

KU Leuven participated in this events because of the their presentation of comparative study on EU-Japan in cyber security laws and policies.

3.7.2 Participants

3.7.2.1 Type of participants

The event attracted participants originated from business, EU Commission,lawyers, academia and NGOs.

3.7.2.2 Number of participants

The number of persons reached approximately 1000 persons.

3.7.3 Accomplished goals - Measurements

Accomplished objectives of our visit included the dissemination and presentation of EUNITY at the audience.

The conference was located in Japan and the topic was Big Data and security. This link a potential intervention in such event with the EUNITY project to the extent that it creates a possibility to foster EU-JP relationships and spread the EU privacy mindset amongst Japanese stakeholders and partners.

3.7.3.1 Key Performance Indicator

The presentation was held to more that 20 attendees.

3.8 Motorola Solutions Innovation Showcase

3.8.1 Objectives

3.8.1.1 Scope of the event

The Motorola Solutions Innovation Showcase is a regular internal event of the Polish campus of Motorola Solutions, attended by over 100 engineers and managers. The main goal of the event is internal cross pollination, but external keynote speakers are invited to widen the scope.

Motorola is a significant global industrial player. This year, the Polish event was visited by high-ranking regional and global officials of the company, increasing the effect of any presentation. Raising awareness of EUNITY and the upcoming European workshop was therefore considered useful.

3.8.1.2 Purpose of the visit

Adam Kozakiewicz was invited as a keynote speaker to the Motorola Symposium, in order to present NASK research activity, focusing on the SISSDEN project, that he coordinates. Since sufficient time was allocated, an additional short presentation of EUNITY was included. The goal of that presentation was to build interest in EUNITY and notify about upcoming workshop in the EU (at that time tentatively planned in Greece).

Since the event was mainly a NASK and SISSDEN presentation, costs of the event were not billed to EUNITY, apart from the time needed to prepare for presentation (1 person-hour).

3.8.2 Participants

3.8.2.1 Type of participants

The Motorola Solutions Innovation Showcase Industry attracted persons from engineering staff and management.

3.8.2.2 Number of participants

The EUNITY project was represented by one person from NASK while the overall number of participants during the presentation was around 80.

3.8.2.3 Accomplished goals - Measurements

As a main outcome of our presence in this meeting was a short discussion about the global differences in privacy regulations, as part of the discussion with Motorola management post-presentation.

3.8.2.4 Key Performance Indicator

Given the very minimal costs, any generated interest would be considered cost-effective. The resulting discussion and contacts made can be considered potentially valuable.

3.9 Postquantum Cryptography, RSA conference

The conference took place in San Francisco, CA, February 14-17, 2017.

3.9.1 Objectives

3.9.1.1 Scope of the event

The event was in San Francisco, CA on February 14-17 2017. Discussion on international research and standardization in Post-quantum cryptography.

3.9.1.2 Purpose of the visit

KU Leuven visited this event as a panel chair.

3.9.2 Participants

3.9.2.1 Type of participants

Academia and industry.

3.9.2.2 Number of participants

One (1) person participated from KU Leuven and 4 other panel members and 150 people in audience.

3.9.2.3 Accomplished goals - Measurements

Largest global industry conference on cybersecurity. Bring research and standardization challenges to attention of broader audience. Accomplished.

3.10 The Future of Information Security,ICISSP 2017, Porto.

3.10.1 Objectives

3.10.1.1 Scope of the event

Keynote on research challenges in information security.

3.10.1.2 Purpose of the visit

KU Leuven visited this event as a speaker on February 20-22, 2017

3.10.2 Participants

3.10.2.1 Type of participants

Academia and industry.

3.10.2.2 Number of participants

One (1) person participated from KU Leuven and approximately 100 people in audience.

3.10.2.3 Accomplished goals - Measurements

Scientific conference in the area of cybersecurity. Bring research challenges to attention of audience of experts. Accomplished

3.11 Privacy and Security Challenges for the IoT, Workshop on Security for Embedded and Mobile Systems (SEMS)

3.11.1 Objectives

3.11.1.1 Scope of the event

Keynote on research and standardization challenges related to IoT security in Paris on April 30, 2017.

3.11.1.2 Purpose of the visit

KU Leuven visited this event as a speaker.

3.11.2 Participants

3.11.2.1 Type of participants

Academia and industry.

3.11.2.2 Number of participants

1 person from KU Leuven + 60 people in audience

3.11.2.3 Accomplished goals - Measurements

Scientific workshop with international experts in IoT security. Bring research and standardization challenges to attention of experts. Accomplished

3.12 The Future of Security, CRISP Event

3.12.1 Objectives

3.12.1.1 Scope of the event

Keynote on research and standardization challenges related to IoT security

3.12.1.2 Purpose of the visit

KU Leuven visited this event as a speaker in Darmstadt on May 15, 2017.

3.12.2 Participants

3.12.2.1 Type of participants

Academia and industry.

3.12.2.2 Number of participants

One (1) person participated from KU Leuven and 120 people in audience

3.12.2.3 Accomplished goals - Measurements

This is a scientific conference in the area of cybersecurity and privacy. Bring research challenges to attention of experts. Accomplished

3.13 The Future of Security and Privacy, Imec Technology Forum

3.13.1 Objectives

3.13.1.1 Scope of the event

Keynote on research challenges in cybersecurity security and privacy.

3.13.1.2 Purpose of the visit

KU Leuven visited this event as a speaker in Antwerp on May 16-17, 2017.

3.13.2 Participants

3.13.2.1 Type of participants

The type of participats was mixed, most of them were from industry.

3.13.2.2 Number of participants

Five (5) persons participated from KU Leuven and 800 people in audience.

3.13.2.3 Accomplished goals - Measurements

International conference for thought leaders in semiconductor industry, where cybersecurity and privacy are becoming increasingly important. Bring research challenges to attention of broader EU and international audience. Get updates on the most research and industry security challenges and needs. Accomplished.

3.14 The Future of Security and Privacy, Dcypher Event

3.14.1 Objectives

3.14.1.1 Scope of the event

The "Future of Security and Privacy, Dcypher Event" was held in Utrecht on Oct 4, 2017. Keynote on research challenges in cybersecurity and privacy

3.14.1.2 Purpose of the visit

KU Leuven visited this event as a speaker.

3.14.2 Participants

3.14.2.1 Type of participants

The type of participats was mixed, most of them were from industry.

3.14.2.2 Number of participants

One (1) person participated from KU Leuven and 400 people in audience.

3.14.2.3 Accomplished goals - Measurements

Conference on cybersecurity. Bring research challenges to attention of EU and international experts and policy makers. Get updates on the most research and industry security challenges and needs. Accomplished.

3.15 Visit to Fast Software Encryption

3.15.1 Objectives

3.15.1.1 Scope of the event

The Visit to Fast Software Encryption (Tokyo), research lab of Hitachi in Yokohama and Kanai University in Osaka happened in March 2016.

The aim of the visit was to discuss future research collaborations in cryptography and cybersecurity.

3.15.1.2 Purpose of the visit

KU Leuven visited this event as a program co-chair of Fast Software Encryption. Session chair.

3.15.2 Participants

3.15.2.1 Type of participants

Mix.

3.15.2.2 Number of participants

From FSE originated 160 people and from Hitachi the discussion took place between 6 researchers. In Kansai University there was a discussion with 20+ researchers with visits to several labs.

3.15.2.3 Accomplished goals - Measurements

Networking. Explore further collaboration in cybersecurity. Accomplished.

4

Publications in conferences and journals

The publication of scientific works is included in the main goals of EUNITY project. Below we present all the studies published in the first year of the project.

- Yuji Sekiya, ”The Detection Possibility of Cyber-threats using Big Data Analysis and Machine Learning”, The 2017 International Data Mining and Cybersecurity Workshop, November 2017 (invited talk).
- Keiichi Shima, Daisuke Miyamoto, Hiroshi Abe, Tomohiro Ishihara, Kazuya Okada, Yuji Sekiya, Hirochika Asai, Yusuke Doi, ”Classification of URL bitstreams using Bag of Bytes” , First International Workshop on Network Intelligence (NI2018), February 20-22, 2018 (Workshop).
- Ryo Nakamura, Yuji Sekiya, Daisuke Miyamoto, Kazuya Okada, Tomohiro Ishihara, ”Malicious Host Detection by Imaging SYN Packets and A Neural Network”, Proceedings of IEEE International Symposium on Networks, Computers and Communications (ISNCC2018), Rome, Italy, June 2018 (Workshop).

5 Dissemination through standards activities

EUNITY project has been participating in several standards activities which we summarize below. This effort includes participation in the European Telecommunications Standards Institute (ETSI), in the Internet Engineering Task Force (IETF), and in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

5.1 Standard bodies

5.1.1 European Telecommunications Standards Institute (ETSI)

5.1.1.1 Objectives

5.1.1.1.1 Scope of the event Hervé Debar is vice-chair of the ETSI Information Security Indicators (ISI) Industry Specification Group (ISG). This standards group aims at defining a framework to evaluate and benchmark the performance of Security Information and Event Management (SIEM) and Security Operating Center (SOC) environments. One of the activities of the group is to specify the relationship with the various incident exchange formats, so that indicators can be exchanged between SOCs. The ISI group is an industry-driven initiative, backed by major European players from various sectors, such as Thales (group secretary), Airbus, Telecom Italia, BNP Paribas, La Banque Postale. National agencies such as the French ANSSI and the German BSI also provide funding to support participants.

5.1.1.1.2 Purpose of the visit ISI events are held 4 times a year at various locations in Europe. As usual with standards meetings, attendance to a suite of events is required in order to have an effective impact on the standards.

The purpose of the events was to discuss the inclusion in the ETSI ISI 003 specification of the Managed Incident Lightweight Exchange (MILE) IETF WG format (RFC7970), Incident Object Description Event Format (IODEF) version 2. One of the Request for Comments (RFC), the "MILE implementation report" (RFC 8134) was edited by Daisuke Miyamoto from NAIST, one of the EUNITY Japanese partners. This work enabled IMT to raise awareness of the MILE format in the ISI group, and to specify the appropriate format to describe ETSI ISI indicators in the MILE/IODEFv2 syntax. This is particularly strategic for Europe and Japan, as the main competing format (STYX/TAXII) is backed by the US Department of Homeland Security (DHS), chairman of the related OASIS working group. This is thus offering an open, standards-backed alternative to Europe and Japan based SOC operators to measure and document the performance of their SOCs.

5.1.1.2 Participants

5.1.1.2.1 Type of participants Participants are mostly from industry and RTO organizations.

5.1.1.2.2 Number of participants Hervé Debar from IMT is the only participant. Events gather 4 to 8 people typically.

5.1.1.3 Accomplished goals - Measurements

5.1.1.3.1 Key Performance Indicator The KPI was the inclusion of a description of the indicators in an ETSI specification. The objective has been met.

5.1.2 Internet Engineering Task Force (IETF)

5.1.2.1 Objectives

5.1.2.1.1 Scope of the event IETF delivers broad array of key standards for establishing and improving cybersecurity and privacy in the cyberspace, such as standards for securing domain names, e-mail messages as well as standards for incident reporting. In addition to standards pertaining to cybersecurity and communication privacy, IETF also delivers infrastructure technologies for 5G networks.

5.1.2.1.2 Purpose of the visit Infrastructure technologies for 5G, such as IPv6 and SDN were of common interest to the EUNITY partners, in addition to standards for incident reporting, secure domain names and secure messaging. In order to comprehend the broad array of its standardization

activities and analyze their impact to cybersecurity and privacy, participation to IETF meetings are considered essential.

5.1.2.2 Participants

5.1.2.2.1 Type of participants IETF meetings are largely comprised of industry experts who actively contribute to standardization in the field of networking protocols, network applications, and network security. There are also some participation from government agencies as well as academia, who also actively contribute to variety of standardization activities.

5.1.2.2.2 Number of participants Three (3) experts from EUNITY Japanese partners (The University of Tokyo and NICT) participated in the IETF meetings in Singapore, November 2017 as well as in London, March 2018 in order to progress work in the areas of infrastructure technologies and cybersecurity. Typically, more than 1,000 experts from more than 50 countries participate in each IETF meeting for five days.

5.1.2.3 Accomplished goals - Measurements

Possible goals in the participation to standardization activities can be: 1) understanding its activities and analyzing their impact, 2) identify relevant work, 3) contribute to the drafting and editing, 4) contribute to deliberations through voting, review and feedback, 5) undocumented dialogue with stakeholders, and 6) requirements analysis and gap analysis. Since EUNITY Japanese partners have been participating in the IETF meetings for several years, the scope of the work within the context of EUNITY project is 2) identification of relevant work.

5.1.2.3.1 Key Performance Indicator The KPI was identification of relevant ongoing work that will have significant impact to the cybersecurity and privacy in near future. These IETF participation provided valuable information on its standardization status, as well as, ongoing activities on SDN and security-related working groups, thus the objective has been met. More specifically, DDoS Open Threat Signaling (DOTS) WG aims to standardize realtime information sharing for DDoS among detection and mitigation devices. In the Network Functions Virtualization research group, European research activities on 5G testbeds are presented. We plan to keep up with the standardization trends on network infrastructure and security through ongoing participation to key IETF working groups.

5.1.3 International Telecommunication Union Telecommunication Standardization Sector (ITU-T)

5.1.3.1 Objectives

5.1.3.1.1 Scope of the event ITU-T Study Group 17 delivers several key standards for understanding and improving cybersecurity and privacy, such as the definition of cybersecurity, public-key infrastructure, identity management and so on. SG17 operates under the high-level mandate of ITU, which is the specialized agency of the United Nations.

5.1.3.1.2 Purpose of the visit The objective of the visit was identification and analysis of new study activities that may have profound impact to cybersecurity and privacy in near future. Since the September 2017 meeting, new study activities on the security of DLT have started under the SG17, in coordination with the Focus Group on Application of Distributed Ledger Technology (FG DLT), which is intended to augment the Study Group work programme by providing an alternative working environment for the quick development of specifications in the focus areas.

5.1.3.2 Participants

5.1.3.2.1 Type of participants ITU-T SG17 meetings are comprised of representatives from Member States, subject-matter experts from specialized agencies, national labs and enterprises, as well as invited academic experts.

5.1.3.2.2 Number of participants Two (2) experts from Japanese partners (NAIST and NICT) participated in the ITU-T Study Group 17 meetings in Geneva, where they contributed to the standardization activities in the areas of cybersecurity and DLT (Distributed Ledger Technology). The SG17 meetings were held twice at ITU premises in Geneva, in September 2017 and March 2018, where 150 delegates from more than 35 countries participated in the deliberation and editing sessions for 8 days. In addition to these plenary meetings, several interim meetings for DLT security were held in Seoul, Tokyo and Beijing, which typically consisted of approximately 10 participants. In addition to face-to-face meetings, the group liaises with ISO TC307, ISO/IEC JTC1 SC27 as well as FG DLT in order to inform and coordinate their work.

5.1.3.3 Accomplished goals - Measurements

In this particular study period (2017-2020), a number of new study activities are proposed, including the DLT security Question [1] , which one of the EUNITY Japanese partner serves as a co-rapporteur. These new study activities will also inform the subsequent deliverables of EUNITY.

5.1.3.3.1 Key Performance Indicator The KPI was identification of relevant new study activities that will have significant impact to cybersecurity and privacy in near future. As DLT security has been identified as the new study activity of critical importance to EUNITY partners, the objective has been met. Current work items on DLT security within SG17 includes threat models, new security capabilities for DLT platforms, security consideration of DLT applications, as well as new security services on top of DLT.

[1] SG17: https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q14.aspx

6 ICS-CoE mission visits to Europe

Taking into account the utmost importance of cybersecurity in the critical infrastructure sectors, the government of Japan has recently established Industrial Cybersecurity Center of Excellence (ICS-CoE) under IPA, the specialized IT agency of METI (Ministry of Economy, Trade and Industry).

As part of its capacity building programme, NAIST team had planned to lead participants from industry in Japan to visit EUNITY partners as part of an open communication and collaboration dialogue. The participants gained knowledge from European cybersecurity initiatives, regulations, standards, and research activities, obtained insights into business and technology ecosystems, and initiated a professional network with cybersecurity experts and stakeholders in Europe.

6.1 Visits to France

As for the first visits, 14 delegates from critical infrastructure sectors visited Paris, France from the 26th to 28th of September, 2017. On September 26th, EUNITY partners from NAIST visited IRT SystemX [1]. They observed cybersecurity initiatives for smart meters and automotive vehicles.

The NAIST team visited Telecom ParisTech on September 27, 2017 where the EUNITY partners in IMT introduced them to the case studies of cyber-physical systems and security research activities, supported under Horizon 2020. Another partner also provided lectures on cybersecurity research in Europe, including the viewpoints of standards and legislation. On the last day, they had the opportunity to discuss with the French government agency and industrial sectors. ANSSI (French national cybersecurity agency) presented cybersecurity issues on the industrial control systems, and Quarkslab

[1] IRT SystemX: https://www.irt-systemx.fr/

provided a case studies of a French-Japanese collaborative project for automotive cybersecurity.

6.2 Visits to Greece

FORTH facilitated a two-day visit in Athens, Greece on 5th to 6th of December 2017, from four (4) stakeholders from Japan who came to meet stakefolders from Greece. During the first day of their visit Japanese members had the opportunity to meet members from GRNET [2] (The Greek Research and Technology Network), University of Patras [3], AEGIS IT Research [4] and FORTH. Cyber security experts and the Head of the GRNET CERT were present (GRNET was the host of the meeting) in the presentations and the discussions. GRNET presented the secure cloud infrastructure that they offer to the Minitry of Education of Greece and the ARIS supercomputing system as well as the measures taken to secure all those infrastructures. FORTH, UoP and AEGIS participants introduced a series of cybersecurity related projects like CIPSEC [5] SMESEC [6] and CERTCOOP [7] projects and how these projects address the cybersecurity aspects. Projects results and approaches were disseminated to the Japanese ICS-CoE members. Those projects are related to critical infrastructures, cyber security for SMEs and a Greek network of CERTs respectively. FORTH also supported the arrangement of a visit and linked the ICS-CoE members to ENISA on December 6th, and the participants observed the essence of ENISA activities, including NIS Directive, GDPR, and guidelines for Smart Airport, Smart Car, IoT, and critical infrastructure systems. The next visit was in Prague, Czech Republic from 7th to 9th in order to attend the OASIS Borderless Cyber cybersecurity conference.

[2] GRNET: https://grnet.gr/en/
[3] UoP: https://www.uop.gr/en/
[4] AEGIS: http://aegisresearch.eu/
[5] CIPSEC: https://www.cipsec.eu
[6] SMESEC: https://www.smesec.eu
[7] CERTCOOP: https://www.certcoop.eu

7 Website and Social Networks

7.1 EUNITY website

This section describes, in brief, the EUNITY website. A more detailed report is available in deliverable D5.1. The website [1], along with the EUNITY Twitter account [2] consist the main channels of communication with the public. All results, publications and news will be available through 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”tabs lists the partners that constitute“The EUNITY Consortium”, along with a brief description and a link about them. The“Publications” section will be continuously updated with the project deliverables, the publications, technical reports, articles and posters as results of the EUNITY project. Information about the events organized by the project will be available in the“Events”tab, and finally a contact page is available from which anyone can send a message through the“Contact Us”tab.

7.1.1 Updates on the EUNITY website

The EUNITY website has been updated as shown in 7.2 with more features that a user can experience while entering in the first web page.

While viewing from top to bottom a visitor can observe the following information:

- HTTPS protocol has been enabled. The website is able to use a secure communication protocol (HTTPS protocol), while communicating with the visitors.

[1] Available at http://www.eunity-project.eu
[2] Available at https://twitter.com/EUNITY_project

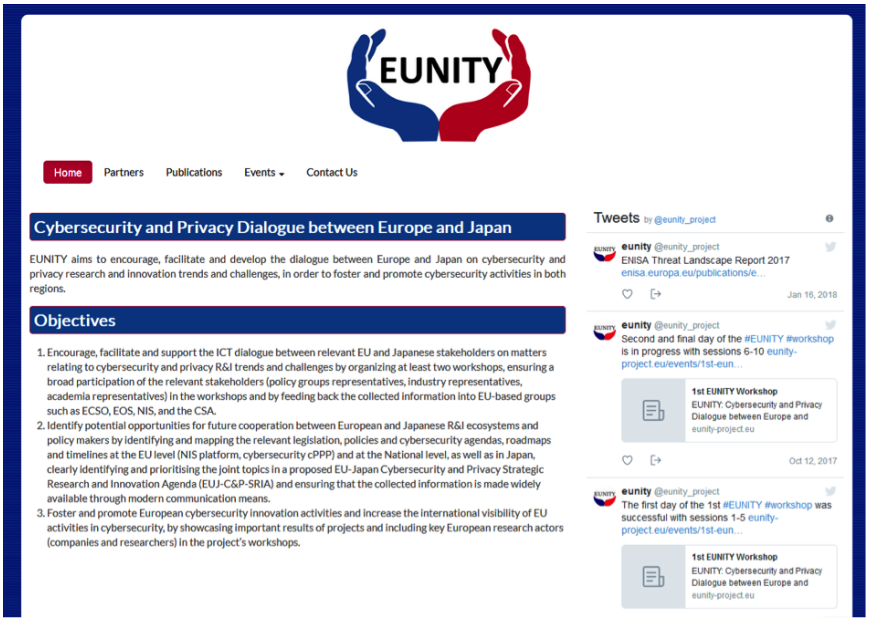

Figure 7.1: The Homepage of EUNITY website

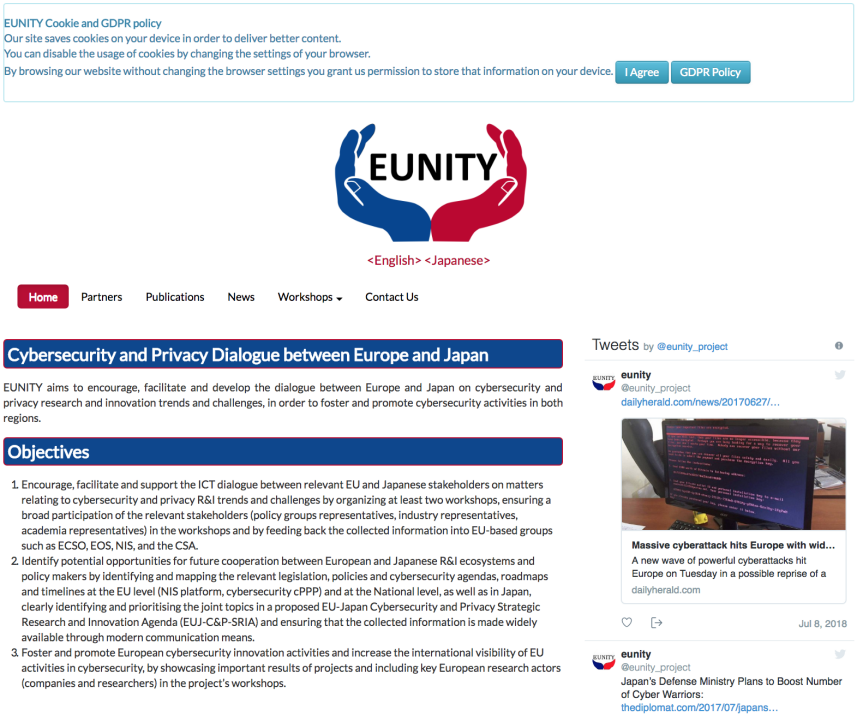

Figure 7.2: The updated EUNITY front page

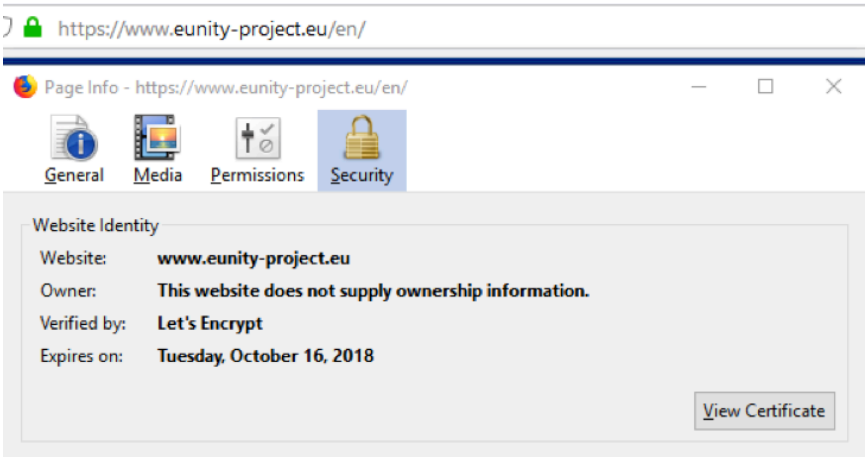

Figure 7.3: The EUNITY website uses a LetsEncrypt certificate for secure information exchange

- The EUNITY website has been using a Lets Encrypt[3] certificate to secure the information exchange performed. Lets Encrypt is a free, automated, and open certificate authority (CA), see Figure 7.3.
- The first thing that a visitor notices in the first web page of the project is the regulation regarding the cookie usage and the GDPR privacy policy of the website. The visitor is able to view more information about the privacy policy by pushing the GDPR policy button.
- While the initial version of the website was developed in English, the updated version of the website has included a Japanese version as well Figure 7.4. The user can switch between the two languages according to his/her preferences.
- The main menu of the website has been changed to include a News section and the Workshops to be organized by the EUNITY project and are now under a specific Workshops section. The News section, among other, will include all the EUNITY related dissemination events that the partners will participate.
- The live feed from the tweets (at the right part of the webpage) is (and will be) continuously updated with EUNITY related information,

[3] https://letsencrypt.org/

that is going to be shared with the website visitors and the Twitter followers. In Figure 7.2 can be seen the latest tweets performed.

Figure 7.4: The Japanese version of the website is ready and will be populated with more content to inform the JP audience as well.

The EUNITY web server is protected through a host level firewall and an Access Control List (ACL) firewall, that is enabled in FORTH's router allowing communication only to ports 80 and 443 (HTTP and HTTPS respectively). Moreover, the server is running a stable release of the Django-CMS framework, in order to serve the EUNITY website.

7.2 EUNITY on Twitter

Currently EUNITY preserves an online presence in Twitter.

The Twitter profile of EUNITY provides a continuous stream of information and updates concerning the news and development of the project. The timeline is also available through the website of EUNITY project in the form of *news feed*.

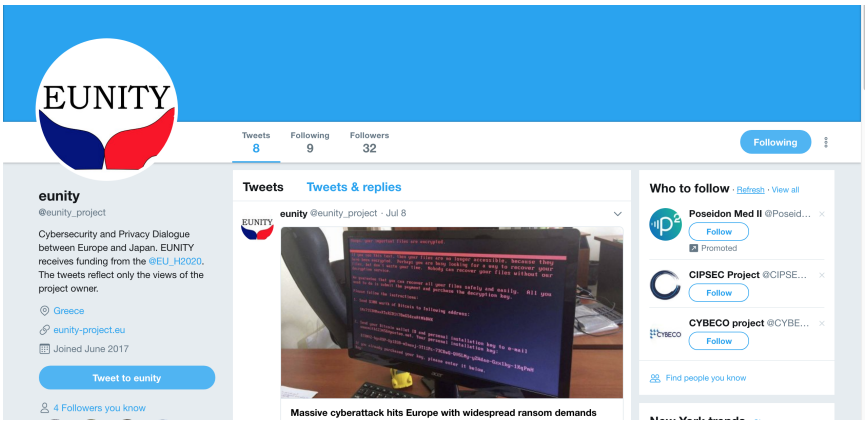

Figure 7.5: Twitter profile of EUNITY

8 Future activities

8.1 Future activities

The report included dissemination activities already performed. Besides those activities we have identified some activities for the future that we believe that will provide better disseminate to the project outcomes. We have already connected the twitter account with some other cybersecurity related twitter accounts from projects and the European Commission. The process is ongoing and we will connect to other accounts as soon we find them. We also plan to explore the LinkedIn social media accounts to identify possible groups and project that are of EUNITY interest and related to Cybersecurity in both regions. In order to boost the visibility of the website and the project as a whole we plan to compile a simple to read introduction webpage which will include information regarding GDPR and the relative Japanese Act. The information may be similarities and differences so that the visitor can obtain a quick view of the two Regulations.
EUNITY project will be also promoted and disseminated (e.g via a poster or an one-page leaflet) at the upcoming CIPSEC and SMESEC workshop that will be held in Heraklion on September and collocated with the RAID2018 [1] conference. FORTH and ATOS are partners in those projects. KUL partner is also planning to make a presenation at ISSE 2018 [2] in Brussels. It will be a keynote presentation on recent developments in cryptography. It is expected to be followed by a mixed audience (e.g academia, industry, policy makers) of approximately 150 people. With this activity we plan to bring research challenges to attention of EU and international experts and policy makers. EUNITY partners are exploring the possible upcoming venues and dates for the second EUNITY workshop. The second EUNITY workshop will be held in Europe.

[1] RAID2018: https://www.raid2018.org/
[2] ISSE2018: https://www.isse.eu.com//

9 Conclusions

9.1 Conclusions

The EUNITY Dissemination report detailed the first 12 months of activity of the project. The document describes all the relevant activities undertaken within the project scope, to spread the project information to different types of audiences. These activities include the organization of the first EUNITY workshop that was held in Tokyo, where gathering of information and assemblance of feedback via questionnaires took place. This report includes the community engagement activities for the first year of the project. The report will be updated at the end of the project where we will include the dissemination activities carried out in the second year of the project.

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