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 D2.3: Workshop 1 proceedings

Abstract: *The proceedings will include on one hand the presentations and supporting documentation provided by the speakers, and on the other hand a report on the interactions and the feedback provided by the attendees.*

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, Paweł Pawliński

[†] 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 Front matter

1.1 Preface

The EUNITY project addresses scope 2 (international dialogue with Japan), of the objective DS-05-2016, of the Horizon 2020 work programme. Within these two years the project aims at developing and encouraging the dialogue between Europe and Japan on cybersecurity and privacy topics. The partners involved have a long-standing history of research on both topics at the European level, as well as cooperation with Japan. EUNITY has 3 main objectives:

1. Encourage, facilitate and support the ICT dialogue between relevant EU and Japanese stakeholders on matters concerning cybersecurity and privacy research and innovation issues;

2. Identify potential opportunities for future cooperation between European and Japanese research and innovation ecosystems; and

3. Foster and promote European cybersecurity innovation activities and increase the international visibility of EU activities in cybersecurity.

To meet these objectives, EUNITY will first gather relevant stakeholders in at least two workshops, one in each region (EU and JP), taking advantage of the co-location with other events as much as possible. Thanks to the expertise of its members, EUNITY project will collect the appropriate existing research agendas, legislations and business practices in Europe and Japan.

It will then analyze the information collected to formulate recommendations, including business opportunities and a research agenda. A particular attention will be brought to the similarities of the research and market strategies, as well as the differences that must be taken into account when addressing both markets. EUNITY will operate in close relationship with the European Cyber Security Organization association, the cybersecurity cPPP signatory and the European Commission. EUNITY will cover all the constituencies of ECSO (large organizations, SMEs, public bodies, associations, clusters, RTOs) thanks to both the direct participation of its partners to ECSO, and to their ties with industry associations, cluster and public bodies. This will ensure that the most relevant and recent information available is on one hand taken into account by the project and on the other hand is providing relevant information to interested parties in the EU. The EUNITY consortium is formed of 5 European partners (IMT, ATOS, NASK, FORTH and KUL) and six Japanese associate partners (NAIST, UT, JAIST, Meiji, JPCERT, NTT). These partners have a long-standing history of working together. In particular, most of them were involved in the highly successful FP7 NECOMA project, which carried out joint research on cybersecurity and created solid and trust-based professional relationships.

The EUNITY workshop held in Tokyo is a first step towards bringing together stakeholders and business and cybersecurity experts from the two regions to share information about existing research agendas, legislation and business practices in Europe and Japan. We are happy to announce that many people from Japanese industry, SMEs, government and academia responded positively to the call, accepted the invitation and participated in the event as speakers or participants. Approximately, an amount of 60 people attended the workshop. The workshop program consisted of nine (9) different sessions thus trying to cover as much aspects as possible. The program triggered lively discussions and feedback that have been included in this report in the respective section. Feedback was also received in a more structured format, via questionnaires that were compiled for each one of the sessions by the EUNITY partners and the session chairs. The participants provided their feedback on the respective questions after each session. The questionnaires helped us to gain more feedback on the participants' point of view on the respective aspects discussed in each session. Among other, the results obtained from the workshop included information related to the existing legislation between the two regions, the willingness of Japanese people to visit Europe and gain insight information on research initiatives and projects funded, the difficulties in collaboration when there is a need for security related information exchange, incident reporting and handling of security issues.

Tokyo, 11th-12th October 2017

The EUNITY Consortium

2 Workshop Program

2.1 Program Chairs

Below we present the program chairs as well as the program of the workshop.
Session 1: Opening. Chair: Hervé Debar, IMT and Youki Kadobayashi, NAIST
Session 2 & 3: CERT. Chair: Paweł Pawliński, CERT Polska
Session 4 & 5: Industry. Chair: Pedro Soria, ATOS
Session 6: Landscapes. Chair: Hervé Debar, IMT
Session 7 & 8: Legal and Policy. Chair: Stefano Fantin, KU Leuven
Session 9: Research & innovation. Chair: Sotiris Ioannidis, FORTH
Session 10 - Wrap-up/Summary.

2.2 Program

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

3 Presentations

3.1 Session 1: Opening

Chair: Hervé Debar, IMT and Youki Kadobayashi, NAIST

The workshop lasted two days. The first session, of the first day, was an introduction given by Hervé Debar (IMT), and Youki Kadobayashi (NAIST). Hervé Debar is the EUNITY coordinator and Youki Kadobayashi leads the consortium of Japanese associated partners.

3.1.1 EUNITY General Presentation

The original presentation is shown below.

EUNITY General Presentation

Hervé Debar

Télécom SudParis

EUNITY Coordinator

What is EUNITY

- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan

EU Project Objectives

(our project goals, supported by this workshop and your participation)

- Encourage exchange of views between Europe and Japan on cybersecurity and privacy research and innovation trends
- Raise awareness of the European cybersecurity and privacy research agenda in Japan, and disseminate the Japanese cybersecurity and privacy research agenda in Europe.
- Provide comparative analysis of Europe and Japan cybersecurity and privacy research agendas to highlight areas of future collaboration.
- Promote European cybersecurity and privacy research and innovation results.

EUNITY Areas of Interest

- Research community
- CERT community
  - Cyber-security pilar
- Standards community
  - Certification
- Business community
  - Developement of interoperable products and services
  - Trustworthy digital infrastructures
- Policy-makers community.
  - Strategy, regulations, funding

EUNITY Partners

In Europe

- Institut Mines-Telecom (France, Coordinator)
- Foundation for Research and Technology – Hellas (Greece)
- Atos Spain SA (Spain)
- Research and Academic Network (NASK, Poland)
- K U Leuven (Belgium)

In Japan

- Nara Institute of Science and Technology
- The University of Tokyo
- Meiji University
- Japan Advanced Institute of Science and Technology
- JPCERT Coordination Center
- National Institute of Information and Communications Technology
- NTT Secure Platform Laboratories

Working together since 2013

Objectives of the workshop

- Inform the Japanese community about cyber-security in Europe
  - Research and innovation activities
  - Roadmaps
- Gather feedback from the Japanese community on
  - The relevance of our objectives
  - The importance of these objectives in Japan
  - Missing activities that are important in Japan
- Ultimately, propose a joint research agenda for research and business development

3.1.2 JPCERT capability building (Takayuki Uchiyama, JPCERT/CC)

The presentation is not provided.

3.1.3 TF-CSIRT (Baiba Kaskina, CERT.LV)

The original presentation is shown below.

CSIRT collaboration in Europe

EUNITY Project Workshop

Cybersecurity and Privacy Dialogue between Europe and Japan

11-12 October 2017, Tokyo

Baiba Kaskina, TF-CSIRT Chair

Topics

- TF-CSIRT
  - Strategy
- Trusted Introducer
- CSIRT Maturity
- TRANSITS training
- NIS directive and CSIRT network
  - CEF funding
- Other cooperation groups
  - EGC
  - Regional
  - Bilateral
- Other players

TF-CSIRT

Task Force Computer Security Incident Response Teams

- Forum for exchanging experiences and knowledge in a trusted environment in order to improve cooperation and coordination
- 3 meetings a year
- Host organisation - GEANT
- All inclusive - Academic (NREN) – Governmental – Commercial
- CSIRT Services, common standards and procedures, joint initiatives
- Liaison with ENISA, FIRST, APNIC and others
- https://tf-csirt.org/
- Focus on European region (RIPE NCC service area), but not limited

TF-CSIRT – historical perspective

- Started in 2000 as mostly academic initiative
- Longest running task force at GEANT
- We just had 52nd meeting

TF-CSIRT – meetings

- 3 times per year
- 130 – 200 participants
- Community – 315 teams
- 2-3 days, social event
- Different location every time

TF-CSIRT – Steering Committee

- 5 elected members from the community (including the Chair) + representative from GEANT
- Term – 2 years, can be re-elected for another 2 years
- Elections for 2 members every year
- In the future
  - Term 3 years?
  - More members – 7+1 = 8?

TF-CSIRT

TF-CSIRT Strategy

- Formulated in 2017
- Mission, critical success factors, strategic aims, goals
- Authors – TF-CSIRT SC, GEANT, TI

TF-CSIRT Mission

The mission of TF-CSIRT is to facilitate and improve the collaboration between the European CSIRT community to make cyber space a better place.

Why Us?

TF-CSIRT operates with a European mindset, and strives to make it services and meetings inclusive, accessible, easy-to-reach, and affordable for all CSIRTS in Europe – regardless of sector. Through the Trusted Introducer service, TF-CSIRT can offer well-maintained and up-to-date information and provide teams with recognition status via its differentiated listing, accreditation and certification processes.

Critical Success Factors

1. Knowledge within and outside the community is leveraged to provide high quality training and trainers.
2. Live meetings happen.
3. A governance and financial models that are fit for purpose.
4. We provide a reliable infrastructure that meets community needs.
5. We drive projects with impact.
6. There is sustainable membership development and engagement.
7. We foster the “we feeling”.
8. There are trusted information and maturity processes.
9. TF-CSIRT has prestige and visibility.

Strategic Aims

1. Improve TF-CSIRT governance.
2. Leverage community knowledge.
3. Champion the prestige and visibility of TF-CSIRT.
4. Develop a future business and financial model.
5. Improve face-to-face engagement.
6. Improve internal organizational processes.
7. Safeguard and enhance the trusted infrastructure and maturity process.

TI – Trusted Introducer Service

The trusted backbone of infrastructure services and serves as clearinghouse for all security and incident response teams

- Maturity: Listing, Accreditation, Certification
- Team Directory: Public & Member access
- Closed meeting for the Accredited and Certified teams
- Open and Secure mailing lists
- Other services (member restricted)
- https://www.trusted-introducer.org/

CSIRT Maturity – 3 steps

1. Listed
2. Accredited
3. Certified

CSIRT Maturity – Listed teams

- Registration (only listed – 160 teams)
- Team exists – provides basic/substantial services
- Contact information
- Constituency
- To get listed – 2 sponsor teams needed

CSIRT Maturity – Accredited teams

- Full members of the community
- September 2017 – 155 teams
- Procedures in place
- RFC2350
- Accreditation takes 1-4 months
- Fees
    - 800 EUR/year – initial fee
    - 1200 EUR/year – annual fee

CSIRT Maturity – Certified teams

- Based in SIM3 (Security Incident Management Maturity Model) model
- SIM3 describes 45 parameters, divided over four categories: Organisation, Human, Tools, Processes
- Minimum score needs to be attained for each parameter
- 22 teams

CSIRT Maturity – why certify?

- Public Relation reasons – locally and internationally
- To evaluate CSIRT organization against international criteria
- An external drive to understand, document and put in order processes within the CSIRT team
- To establish or put in order auditing, accountability and reporting schemes
- To implement continuous improvement in a quality management framework

TRANSITS Training

CSIRT personnel training

- TRANSITS I: Operational, Organisational, Legal and Technical
- TRANSITS II: NetFlow Analysis, Forensics, Communication, CSIRT Exercises
- Over 1000 security professionals trained in Europe and more in other regions
- Knowledge exchange

NIS directive

Directive on security of network and information systems – Scope:

- National strategy on the security of network and information systems
- Cooperation Group
- CSIRTs network
- Security and notification requirements for operators of essential services and for digital service providers
- National competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems

NIS directive – CSIRT network

- Members:
  - CSIRTs
  - CERT-EU
  - Commission (observer)
  - ENISA (secretariat)
- Operational information exchange
- Discuss coordinated incident response
- Support member states in addressing cross-border incidents

CEF Funding

- “Core Service Platform” – MeliCERTes
- EU CEF framework (under SMART 2015/1089)
- Development timeframe 2017-2019
- Platform areas:
  - incident management: exchange of incident related data and security feeds
  - event management: exchange of threat/vulnerability related information
  - artefact analysis: exchange of artefact related information
  - secure communications: secure conferencing, “chat” and file sharing
  - contact management

European Government CSIRT group EGC

- Historical group
  - Austria - GovCERT Austria
  - Belgium - CERT.be
  - Denmark - CFCS-DK
  - Finland - NCSC-FI
  - France - CERT-FR
  - Germany - CERT-Bund
  - Netherlands - NCSC-NL
  - Norway - NorCERT
  - Spain - CCN-CERT
  - Sweden - CERT-SE
  - Switzerland - GovCERT.ch
  - United Kingdom - CERT-UK
  - United Kingdom - GovCertUK
  - EU institutions, agencies and bodies - CERT-EU

Other Cooperation

- Regional
  - Central European CSIRT group
  - Baltic CSIRTs
  - Nordic CSIRTs
- Bilateral

Other Players and Areas

- ENISA
- FIRST
- ITU

- Help to establish new CSIRT teams
- Training, materials
- Train the trainers
- Development of tools
- Best practices, benchmarking

Questions

Who?

What?

When?

Where?

3.2 Sessions 2 & 3: CERT

Chair: Paweł Pawliński, CERT Polska

The next two sessions, on the same day, were about the topic of CERTs, including invited presentations, highlighting the challenges of information exchange and the coordination, at a global level, on both Europe and Japan sides.

3.2.1 Session 2: CERT / CSIRT community (Paweł Pawliński, NASK / CERT.PL)

The second session of the first day started with a presentation from Paweł Pawliński (NASK / CERT.PL). The session focused on Cybersecurity operations & international cooperation. After the presentation, the audience formed small groups in order to discuss and fill the questionnaires provided by the EUNITY partners (Appendix A). The results of the questionnaires and the discussions are mentioned in chapter 4. The discussion focused on: Incident coordination, Information exchange, Joint initiatives, Exercises, Future plans.

3.2.2 Session 3: Task Force Software Vulnerability Disclosure in Europe (Afonso Ferreira, IRIT)

Chair: Paweł Pawliński, CERT Polska

The third session of the first day included a presentation from Afonso Ferreira (IRIT). Below we add the original presentation.

Task Force
Software Vulnerability Disclosure in Europe

Afonso Ferreira
French National Research Centre (CNRS)
Computer Science Research Institute at Toulouse (IRIT)
France

Quick background

- Researcher in Algorithms, Optimisation, Networks, Cybersecurity, Insurance, CPS
- Policy maker in Future and Emerging Technologies, Cybersecurity, Privacy at the European Commission (until end March 2017)
- Foresight designer and practitioner, mainly on the impact of the Digital Revolution and Digital Transformation
- Adviser to Institutions and to EU Projects

Vulnerability disclosure

The process by which someone shares information about a security vulnerability so that it can be mitigated or fixed

Types:

- Full disclosure
- Responsible disclosure
- Coordinated vulnerability disclosure
- No disclosure

Coordinated vulnerability disclosure

- Process of
  - Gathering information from vulnerability finders
  - Coordinating the sharing of that information between relevant stakeholders
  - Disclosing the existence of software vulnerabilities
  - Disclosing their mitigations to various stakeholders including the public

Finders: individuals or organisations that identify a potential software vulnerability in a product or service

Task Force
Software Vulnerability Disclosure in Europe

Sponsor:

- Centre for European Policy Studies – CEPS

Chair:

- Marietje Schaake, Member of European Parliament

Research Group:

- Romain Bosc, Rapporteur
- Afonso Ferreira, Rapporteur
- Lorenzo Pupillo, Coordinator
- Gianluca Varisco, Rapporteur

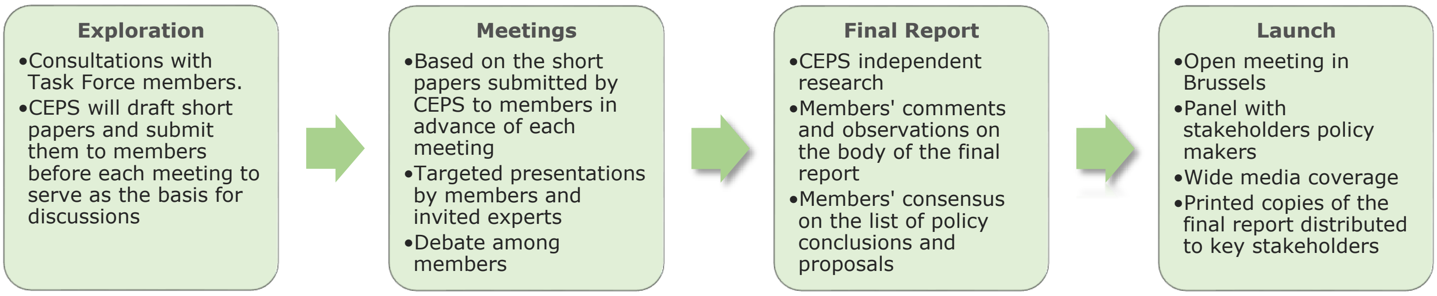
Members of the Task Force

- Private Sector: Airbus, Cloudflare, Enter, ETNO, ICANN, Mozilla, Microsoft, SAP

- European Institutions: Council of European Union, DG Connect, DG Home Affairs, JRC European Commission
- European Governments: Dutch National Cyber Security Center
- Civil Society: Access Now
- Advisory Committee:
  - Ross Anderson, Cambridge University;
  - Michael Daniel, Cyber Threat Alliance,
  - Allan Friedman, NTIA,
  - Andriani Ferti, Karatzas & Partners Law Firm,
  - Trey Herr, Belfer Center Harvard University,
  - Tim Watson, Warwick University.

In conversations with CERTs and ENISA

Methodology



Exploration

- Consultations with Task Force members.
- CEPS will draft short papers and submit them to members before each meeting to serve as the basis for discussions

Meetings

- Based on the short papers submitted by CEPS to members in advance of each meeting
- Targeted presentations by members and invited experts
- Debate among members

Final Report

- CEPS independent research
- Members' comments and observations on the body of the final report
- Members' consensus on the list of policy conclusions and proposals

Launch

- Open meeting in Brussels
- Panel with stakeholders policy makers
- Wide media coverage
- Printed copies of the final report distributed to key stakeholders

Events

First meeting

- Held on September 27th, 2017 in Brussels

Next meetings

- November 29th
- January 31st

- Questions?

- Want to contribute?

Afonso.Ferreira@irit.fr

3.3 Sessions 4 & 5: Industry

Chair: Pedro Soria, ATOS

The first day ended with an industry session that exposed 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 presentation by Hervé Debar, “European Cyber Security Organization (ECSO)”, included the definition of ECSO, as well as the ECSO General Structure and its working groups, including objectives and deliverables.

Below we add the original presentation.

European Cyber Security Organization (ECSO)

www.ecs-org.eu

Hervé Debar

Télécom SudParis

EUNITY Coordinator

What is EUNITY

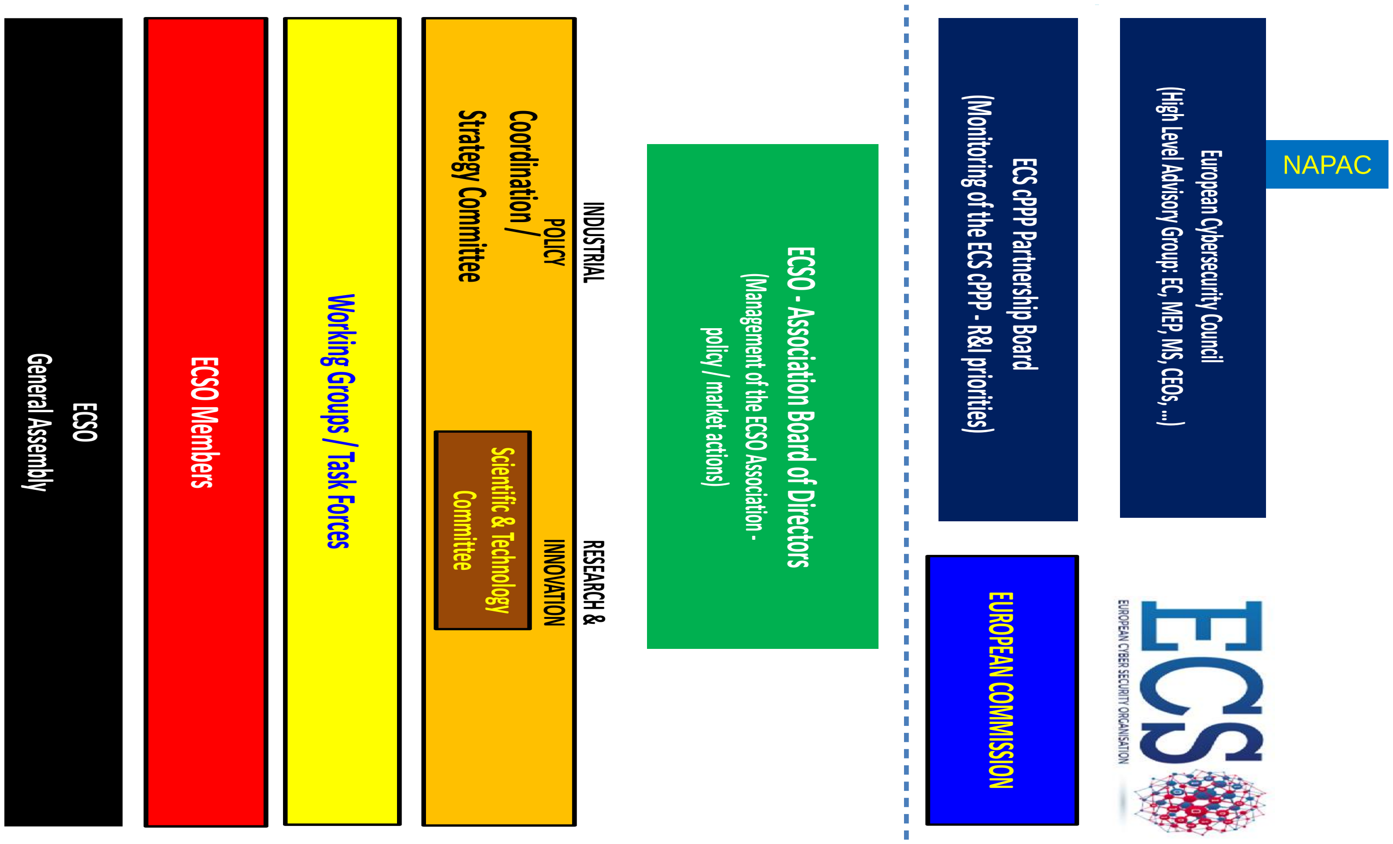
- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan
- Our goals:
  - Raise awareness of European views and activities on cybersecurity in Japan
  - Understand similar activities in Japan to complete European research roadmaps, e.g. with joint activities

What is ECSO

- Association established in Brussels
  - “Industry Proposal”
- Contractual Public-Private Partnership (cPPP)
  - Joint effort between the European Commission and the private sector
  - Leverage public research funding to develop business activity.
- Signed July 2016
  - Other cPPPs exist: DVA (big data); 5G (mobile 5G); EFFRA (smart industry), …
  - cPPP could evolve into a more ambitious structure (Joint Undertaking- like) following the recent EU cybersecurity strategy (Sept 2017)

ECSO Intro/L.Rebuffi

ECSO General Structure



ECSO
General Assembly

ECSO Members

Working Groups / Task Forces

INDUSTRIAL POLICY
Coordination / Strategy Committee

RESEARCH & INNOVATION
Scientific & Technology Committee

ECSO - Association Board of Directors
(Management of the ECSO Association - policy / market actions)

ECS cPPP Partnership Board
(Monitoring of the ECS cPPP - R&I priorities)

European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, ...)

NAPAC

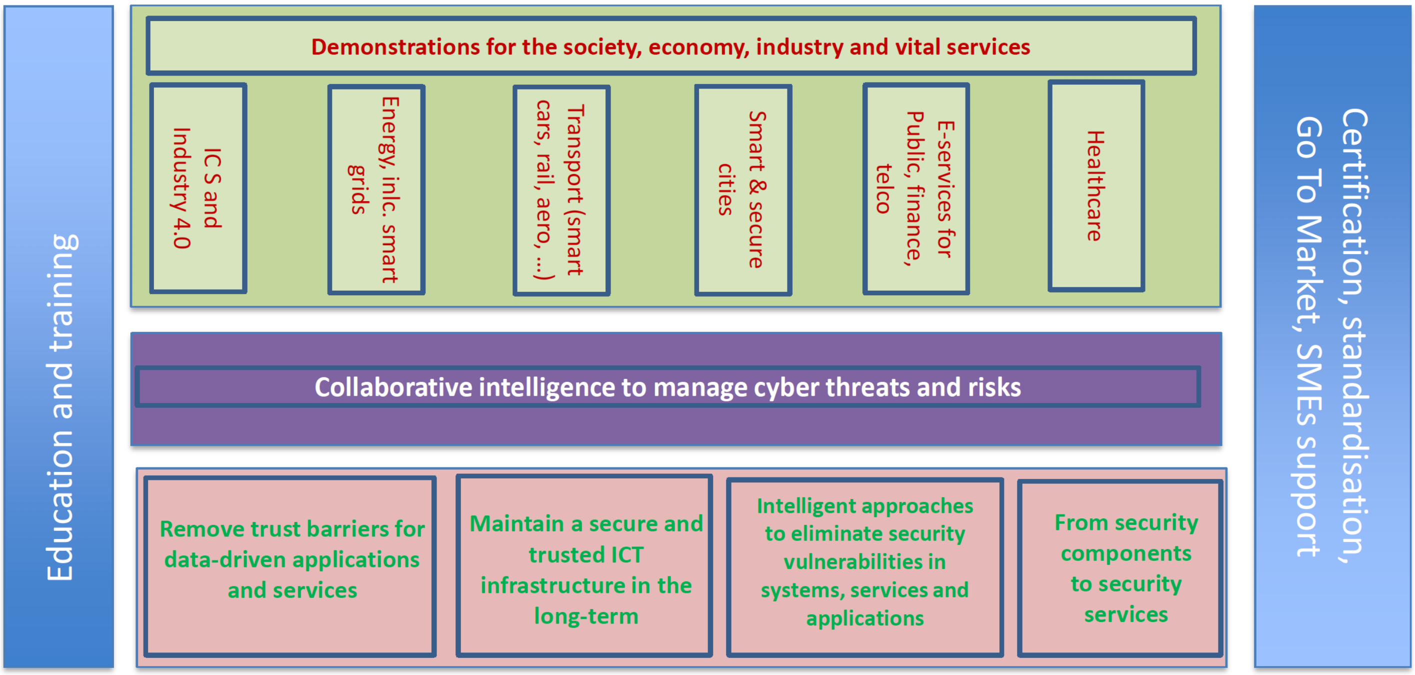
EUROPEAN COMMISSION

6 working groups

- WG1 (standards / certification / label / trusted supply chain)
- WG2 (market / funds / international cooperation / cPPP monitoring)
- WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities)
- WG4 (SMEs, Regions, East EU)
- WG5 (education, training, awareness, cyber ranges…)
- WG6 (SRIA)

- WG maturity is different. Initial activity has been more important in WG1 and WG6.

From basic R&I building blocks to products



Education and training

Demonstrations for the society, economy, industry and vital services

IC S and Industry 4.0

Energy, inlc. smart grids

Transport (smart cars, rail, aero, …)

Smart & secure cities

E-services for Public, finance, telco

Healthcare

Collaborative intelligence to manage cyber threats and risks

Remove trust barriers for data-driven applications and services

Maintain a secure and trusted ICT infrastructure in the long-term

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

From security components to security services

Certification, standardisation, Go To Market, SMEs support

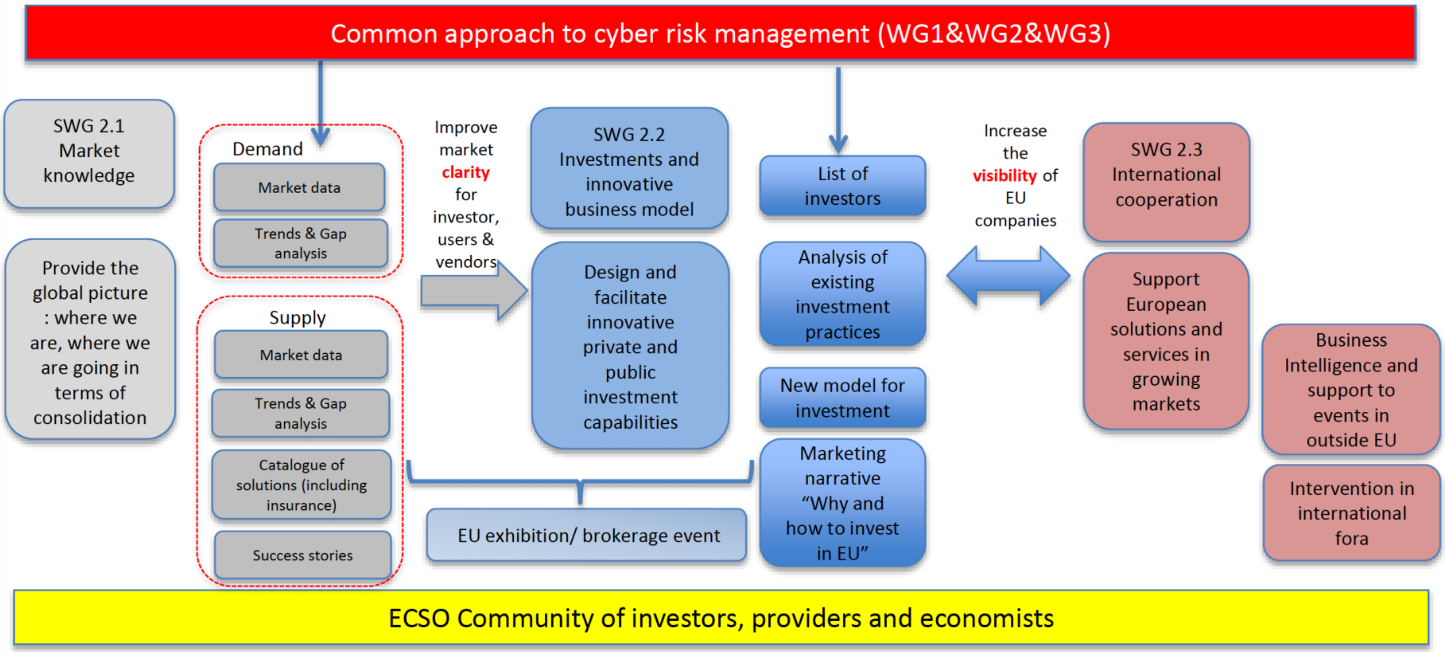
WG1 – Standardisation, certification, labelling & supply chain management

- Mission and Objectives: The WG will focus its work around the following topics:
  - EU ICT security certification framework (liaise with the Commission and contribute to the European ICT security certification framework proposal which is foreseen to be published by the end of 2017).
  - Standards for interoperability
  - EU cybersecurity labelling
  - Increased digital autonomy
  - Testing and validation of the supply / value chain in Europe
- Cooperations:
  - CEN/CENELEC (already defined)
  - ETSI (planned)

WG1 Initial Activities

- Initial activities focus on
  - the overview of existing cybersecurity standards and certification schemes relevant for the activities of WG1 (SOTA – which will be public and evolve every 3 – 4 months),
  - and the identification of the challenges relevant for the industrial sector (COTI – which will remain an internal document).
- They will be used as basis for ECSO recommendations for EU certification in the Meta – Framework document.

WG2 Objectives and Deliverables


Common approach to cyber risk management (WG1&WG2&WG3)
SWG 2.1 Market knowledge
Provide the global picture : where we are, where we are going in terms of consolidation
Demand
Market data
Trends & Gap analysis
Supply
Market data
Trends & Gap analysis
Catalogue of solutions (including insurance)
Success stories
Improve market clarity for investor, users & vendors
SWG 2.2 Investments and innovative business model
Design and facilitate innovative private and public investment capabilities
EU exhibition/ brokerage event
List of investors
Analysis of existing investment practices
New model for investment
Marketing narrative "Why and how to invest in EU"
Increase the visibility of EU companies
SWG 2.3 International cooperation
Support European solutions and services in growing markets
Business Intelligence and support to events in outside EU
Intervention in international fora
ECSO Community of investors, providers and economists

WG3 - Verticals

- Identification of user/market needs
- Assess vertical sectors challenges and impact
  - Understand market needs (e.g. demand driven requirements, threats, functional requirements, ecosystem impact etc.)
  - Influence EU instruments on research and/or policy issues by input to other ECSO WG's and other means as appropriate in the scope/constitution of ECSO
  - Drive well founded sector impact into other ECSO WGs
- WG3 planning for 2017
  - Current SOTA drafts describe the sector and its challenges well
  - Further in depth refinements on vertical based SOTA's plus transversal aspects to continue
  - Interactions with vertical organisations, ENISA, Europol and adjacent ECSO WG's (1,2,5,6)
- Need for more users and operators

WG3 – Which verticals ?

- SWG 3.1: Industry 4.0 and ICS
- SWG 3.2: Energy (oil, gas, electricity), and Smart Grids
- SWG 3.3: Transportation (road, rail, air, sea, space)
- SWG 3.4: Financial Services, ePayments and Insurance
- SWG 3.5: Public Services, eGovernment, Digital Citizenship
- SWG 3.6: Healthcare
- SWG 3.7: Smart Cities and Smart Buildings (convergence of digital services for Citizens) and other Utilities
- SWG 3.8: Telecom, Media and Content

WG4 – SMEs and Regions Vision on SMEs

- Boost the demand for SMEs solution
  - European cyber security SMEs HUB to help SMEs consolidation
  - Create a “Made in the EU/EU trusted solution” label
  - Measures for enhanced SME participation in public procurement
  - Foster clusters cooperation
- Adapt Cyber certification to SME needs
  - Proportionality of verification processes to suit the size and complexity of the company
  - Reduce the level of formalism required to micro and small businesses
  - Develop implementation guides specific to SMEs
  - Allow gradual approach and self-certification
  - Reduce cost for certification renewal
- EU Funding for R&I&D of solutions that effectively reach the market
  - Requirements for minimum participation of SMEs in H2020 projects
  - Review and simplify the SME Instrument
  - Design of a EU model for investment

WG4 Initial Activities

- SMEs:
  - discussions on other forms of support to SMEs other than R&D (e.g. EU regional funds);
  - SME hub;
  - Cooperation with large companies;
  - certification issues / labelling;
  - workforce.
- Regional aspects:
  - cooperation with “EU Regions“(DG REGIO + DG CNECT + DG JRC, DG GROW, ECSO members and regions not ECSO members):
    - identification of regional and structural funds for cybersecurity;
    - gathering of Regions to better target these resources.
  - East EU aspects to be developed soon.

WG5 – Education and Training

- Purpose and Approach:
  - Increase education and skills on cyber security products and safe use of IT tools in Member States for citizens' individual and professionals.
  - Cyber security training and exercise ecosystem leveraging upon cyber range environments
  - Awareness-raising and basic hygiene skills
- SubWG's:
  - SWG5.1 Cyber range environments and technical exercises
  - SWG5.2: Education and professional training
  - SWG5.3: Awareness

WG5 Initial Activities

- SubWG meetings ongoing to define detailed needs / objectives / actions.
- Just started the EHR-4CYBER Network
  - (to promote and harmonise education and training and develop job creation)

WG5 - Creation of an EU Cybersecurity Human Resources Network to develop education, training and jobs: EHR-4CYBER

- Europe urgently needs a larger number of skilled cyber experts: the European Commission estimates that by 2020, 900.000 new jobs will be needed in Europe in the cybersecurity sector.
- This need is recognised by large companies to increase their business activity and competitiveness, by SMEs that look for a fast growth, by public administrations that need to protect public services from threats leveraging upon experts that are increasingly attracted by the salary of the private sector, by RTOs and Universities that need to keep high profile researchers attractive to the private sector facilities and of course by users / operators that need to develop a consistent internal panel of experts to run cybersecurity solutions for protection of their activity.
- Initial investments from the private sector are already done independently: such a platform could create a synergetic effect across ECSO members and provide European / national public administrations and decision makers (politicians) with a very strong message on the need for an effective financial support and incentives for developing cybersecurity competence in order to feed as soon as possible the need for jobs with European manpower, allowing also the possibility to retain them.
- This platform would discuss and work on a benchmarking system, foster collaboration through the exchange of best practices, look towards harmonisation of education and training procedures across Europe, develop and harmonise certification for diploma and specialties, as well as foster the recruitment process of cybersecurity specialists.

WG6 – Strategic Research and Innovation Agenda (SRIA)

- Technical areas, Products, Services
- Objectives
  - Coordination of results and expectations from EC R&I projects
  - Coordination of cybersecurity activities across cPPPs and EIT
  - Support cPPP implementation and H2020 cybersecurity projects
  - Detailed suggestions for the WorkProgramme 2018 - 2020 using an updated and focussed SRIA

Thank you for your attention

Questions ?

The presentation of “ECSO WG1 Standardization and Certification” by Hervé Debar included the definition of EUNITY, the ECSO WG1’s structure, the ECSO’s recent events, the WG1’s Calendar, the basic R&I building blocks and the products, as well as some key issues. Below we add the original presentation.

ECSO WG1
Standardization and Certification

Hervé Debar

Télécom SudParis

EUNITY Coordinator

What is EUNITY

- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan
- Our goals:
  - Raise awareness of European views and activities on cybersecurity in Japan
  - Understand similar activities in Japan to complete European research roadmaps, e.g. with joint activities

What is ECSO

- Association established in Brussels
  - “Industry Proposal”
- Contractual Public-Private Partnership (cPPP)
  - Joint effort between the European Commission and the private sector
  - Leverage public research funding to develop business activity.
- Signed July 2016
  - Other cPPPs exist: DVA (big data); 5G (mobile 5G); EFFRA (smart industry), …
  - cPPP could evolve into a more ambitious structure (Joint Undertaking- like) following the recent EU cybersecurity strategy (Sept 2017)

ECSO Intro/L.Rebuffi

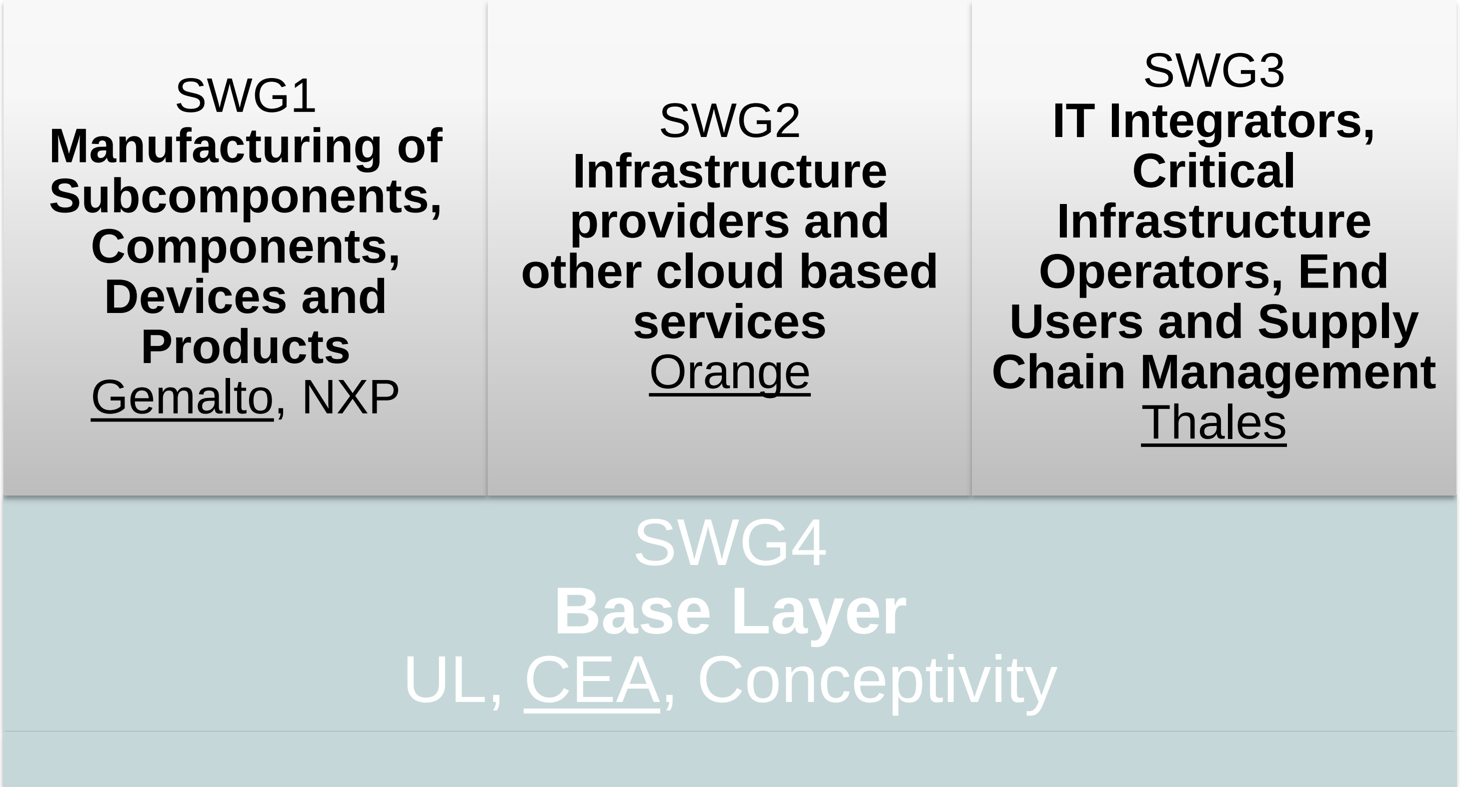
6 working groups

- WG1 (standards / certification / label / trusted supply chain)
- WG2 (market / funds / international cooperation / cPPP monitoring)
- WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities)
- WG4 (SMEs, Regions, East EU)
- WG5 (education, training, awareness, cyber ranges…)
- WG6 (SRIA)

WG1 – Standardisation, certification, labelling & supply chain management

- Mission and Objectives: The WG will focus its work around the following topics:
  - EU ICT security certification framework (liaise with the Commission and contribute to the European ICT security certification framework proposal which is foreseen to be published by the end of 2017).
  - Standards for interoperability
  - EU cybersecurity labelling
  - Increased digital autonomy
  - Testing and validation of the supply / value chain in Europe
- Cooperations:
  - CEN/CENELEC (already defined)
  - ETSI (planned)

WG1 Structure



SWG1
Manufacturing of Subcomponents, Components, Devices and Products
Gemalto, NXP

SWG2
Infrastructure providers and other cloud based services
Orange

SWG3
IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management
Thales

SWG4
Base Layer
UL, CEA, Conceptivity

Roughly 80 ECSO members

WG1 Structure

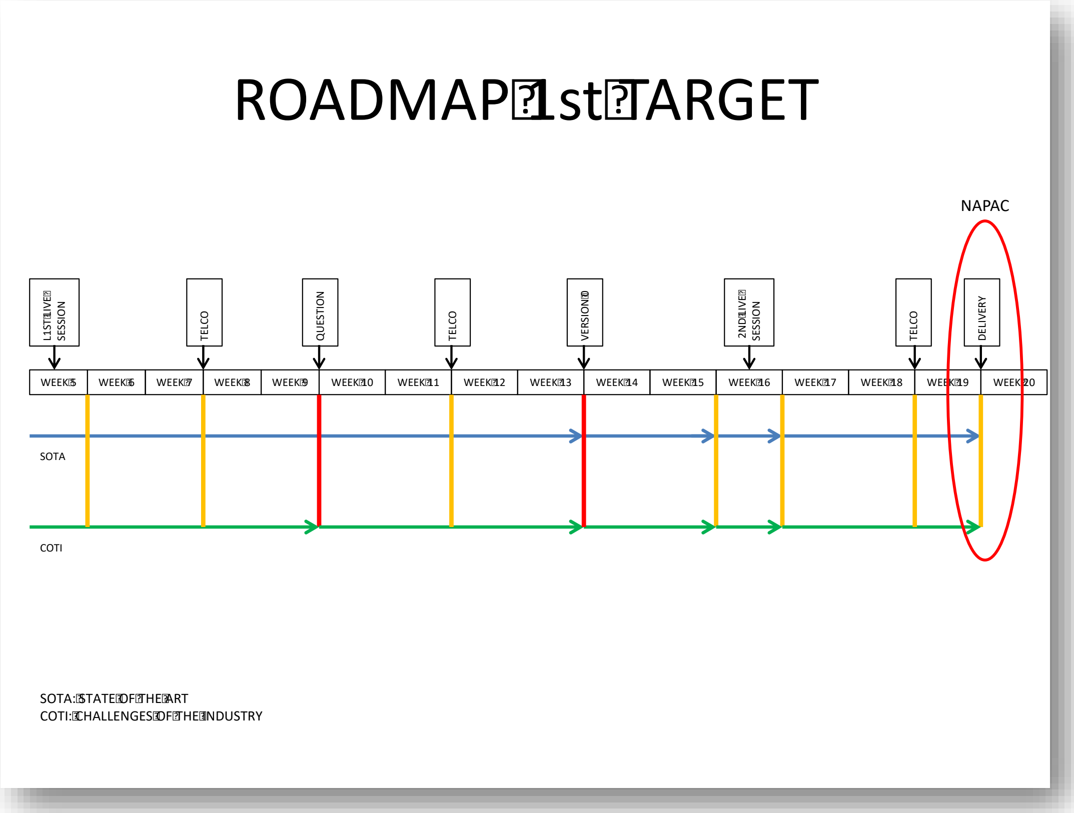
- SWG 1.1. “Manufacturing of Subcomponents, Components, Devices and Products”
  - Manufacturing of cyber secure products (from IC components up to cars, aircraft and others that require the integration of several components) including the respective supply-chain during integration of components.
  - Software as a product is also covered by this SWG.
- SWG 1.2. “ICT infrastructure providers and other cloud based services”
  - Delivering of cyber secure services but with a big effort on the privacy of data handling in Telco or other ICT infrastructure providers, but also cloud -based ones.
- SWG 1. 3. “IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management”
  - Organizations and their IT infrastructure, end users and the organizational and IT infrastructure changes needed to have a market of companies and suppliers able to deliver their services (ICT or non) to citizen in a secure way.
- SWG 1.4. “Base Layer”
  - Delivering required specific capabilities to other SWGs as advanced research, definition of common terms, structures and procedures.

RECENT EVENTS

- NAPAC Contributions and recommendations
  - on meeting logistics
  - on security certification specificities and vertical end-users / consumers
  - on market analysis
- SOTA – WG 1.4
  - objective: collect a raw list of existing standards / certification / labels
  - 180+ pages
  - split product / infrastructure / systems and services
  - ranking / scoring not done yet
- COTI – WG 1.1, 1.2, 1.3
  - objective: collect partner positions on general issues
  - 150+ inputs
  - integration in progress
  - contribution of the member states not identified yet

ECSO France

WG1 Calendar



ROADMAP 1st TARGET

NAPAC

1ST LIVE SESSION

TELCO

QUESTION

TELCO

VERSION 0

2ND LIVE SESSION

TELCO

DELIVERY

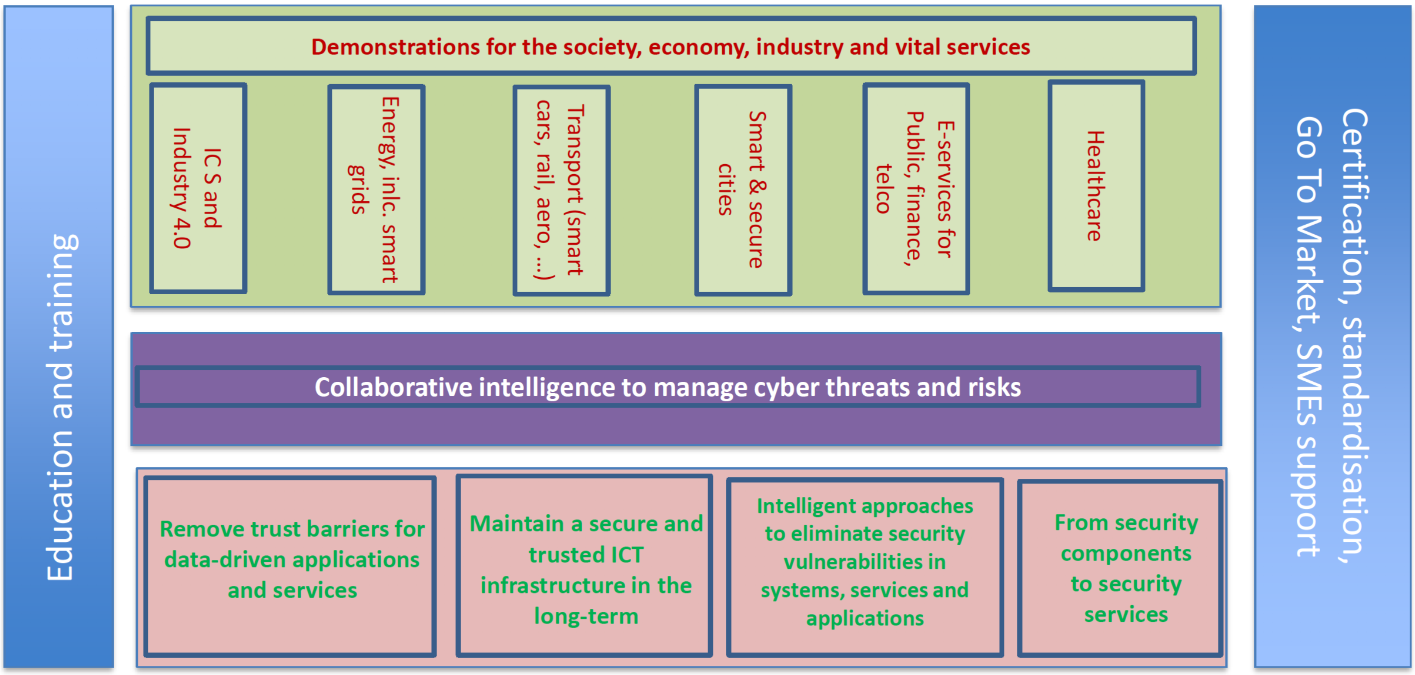
WEEK 5	WEEK 6	WEEK 7	WEEK 8	WEEK 9	WEEK 10	WEEK 11	WEEK 12	WEEK 13	WEEK 14	WEEK 15	WEEK 16	WEEK 17	WEEK 18	WEEK 19	WEEK 20

SOTA

COTI

SOTA: STATE OF THE ART
COTI: CHALLENGES OF THE INDUSTRY

From basic R&I building blocks to products



Education and training

Demonstrations for the society, economy, industry and vital services

IC S and Industry 4.0

Energy, inlc. smart grids

Transport (smart cars, rail, aero, …)

Smart & secure cities

E-services for Public, finance, telco

Healthcare

Collaborative intelligence to manage cyber threats and risks

Remove trust barriers for data-driven applications and services

Maintain a secure and trusted ICT infrastructure in the long-term

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

From security components to security services

Certification, standardisation, Go To Market, SMEs support

Key issues

- Cross-certification between European countries

- Certifications for SMEs
  - As product developers
  - As users

- With the new strategy Europe wants to set up an ambitious EU Certification Framework which structure and process is under discussion between Commission, Member States and Private Sector (and in particular ECSO).

Thank you for your attention

Questions ?

The session of “Industry considerations” by ATOS mentioned the cybersecurity market situation, including challenges and opportunities, priorities in industry, who leads cybersecurity practice (from SMEs to large businesses), as well as industry recommendations. Below we add the original presentation by Pedro Soria and Alicia Garcia (ATOS).

1st EUNITY Workshop

Tokyo

Oct 11th-12th 2017

Session: *Industry considerations*

Atos

Session Agenda

- Market situation & ECIL recommendations
- Cyberwatching introduction
- Japan cybersecurity capacity building TF.
- Standards / ECSO WG1
- SMEs & cybersecurity / ECSO WG4

EUNITY

Cybersecurity Market Situation

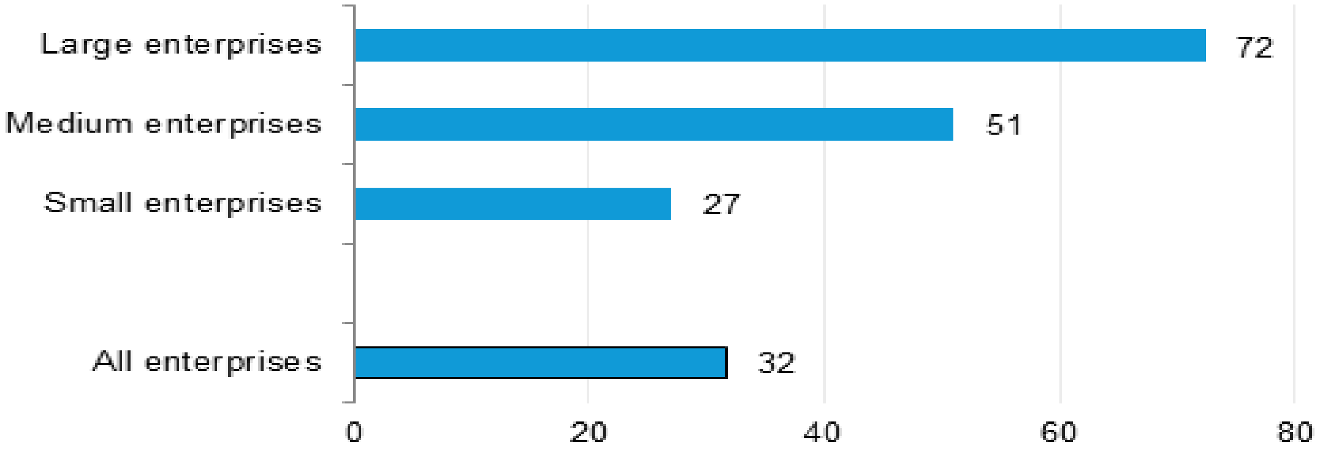
Session: Industry considerations

Pedro Soria-Rodríguez, Atos

From challenge to opportunity

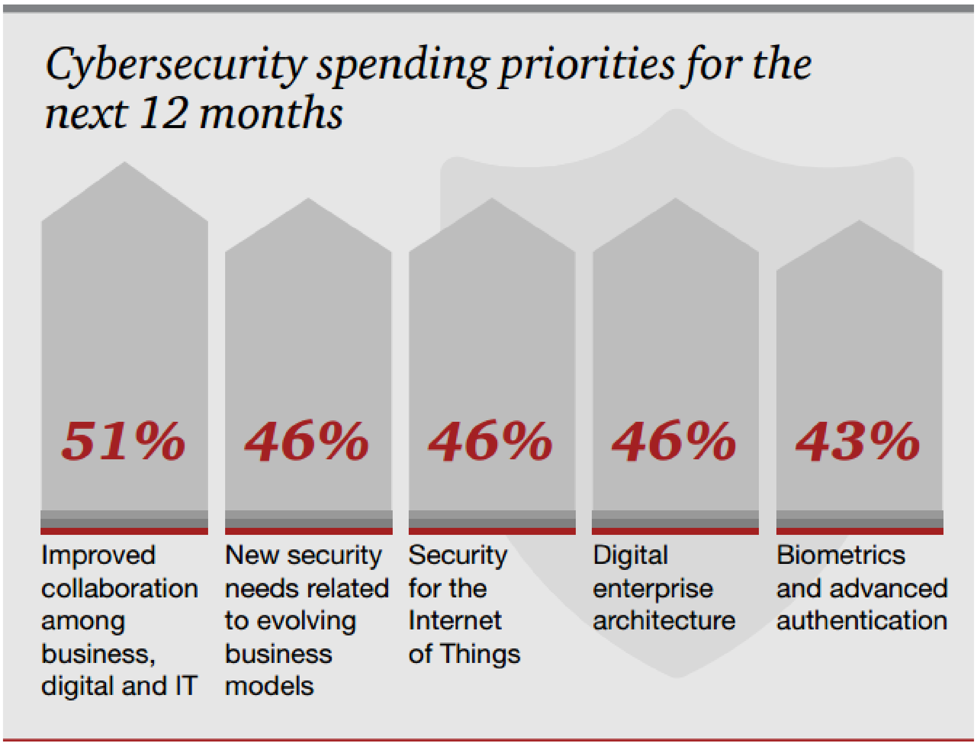
- Transformation in mindsets
- Cybersecurity regarded from a “need” or a “cost” to an opportunity.
- Transformation still to translate into action:

% of companies (globally) with formal ICT security policy defined



Cybersecurity priorities in industry

Cybersecurity spending priorities in 2017



Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

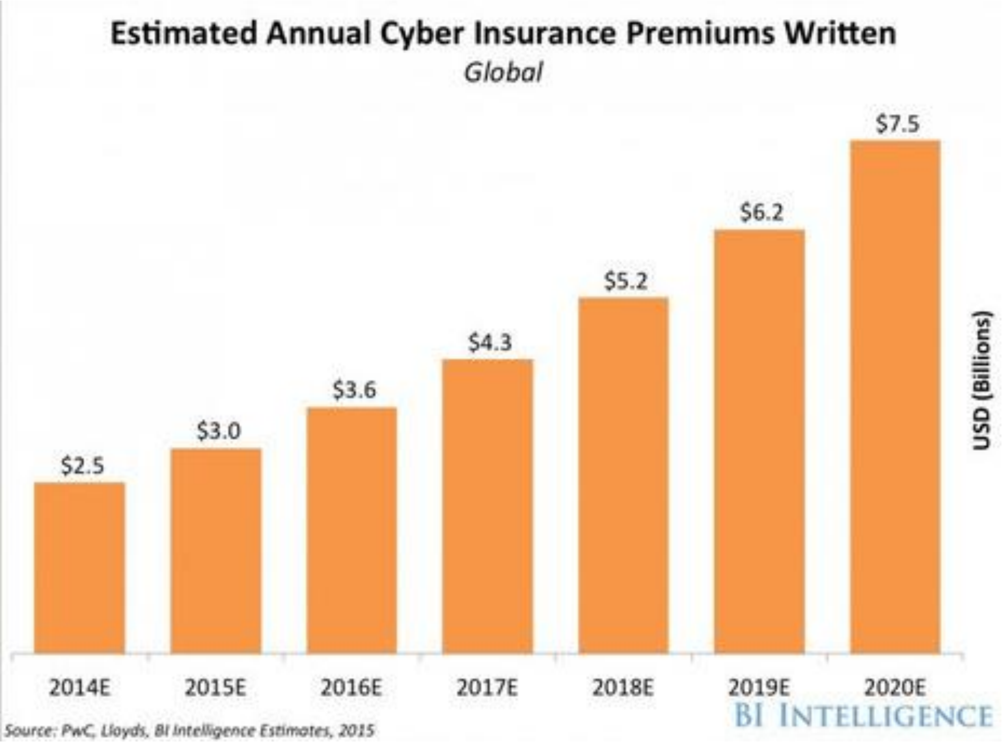
Who leads cybersecurity practice...

- Not SMEs:

Estimated number of SMEs in the European Union	**23 million. 99 out of every 100** European businesses are SMEs. With an increasing number expected to become digital businesses, many will need to ensure they are safe on line.
Typical company size	Roughly 93% of SMEs are micro (< 10 employees) 6% employ between 11 and 49 people. 1% of the SMEs are medium employing between 50 and 249 people.
Priorities	Focusing on core business. No resources for cybersecurity considerations
Level of IT expertise	Fewer than 20% of SMEs in Europe have an IT manager.
Jobs & Growth	SMEs employ 2 in every 3 employees.

Who leads cybersecurity practice...

- Large businesses: Do have resources and security policies in place but…



Source: PwC, Lloyds, BI Intelligence Estimates, 2015

Industry recommendations

Session: Industry considerations

Alicia García Medina, Atos

ECIL

09/2014 Com. **Kroes**, responsible for the **Digital Agenda** in Europe, wish a small size working group of **European Industry** as consultant, with the focus on **Cybersecurity**;

10/2014 Com. **Kroes** talks with **High Levels** from dedicated **companies**;

11/2014 Com. **Kroes** retired; President Juncker nominate Com. **Oettinger**;

03/2015 Com. Oettinger initiate a **Round Table** with EU companies in dedicated important **market domains**:
- Automotive, Telecom, Network Infrastructure, IT-Service, Aircraft Industry, Finance Sector, Cyber Lab's and Semiconductor Industry

and from a **broad range of countries**:
- Spain, France, Sweden, Estonia and Germany

(Atos, Airbus, BBVA, Cybernetica, Deutsche Telecom, Ericsson, Infineon, Thales)

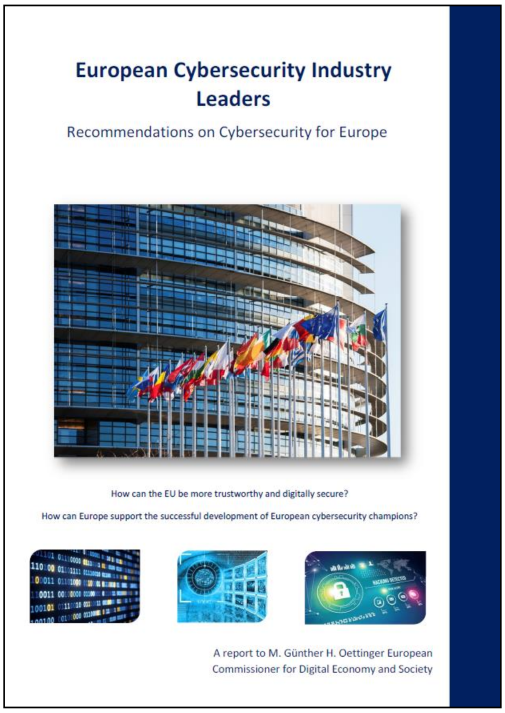
Naming: **E**uropean **C**ybersecurity **I**ndustry **L**eadership = ECIL

Recommendations from industry

ECIL Report

Recommendation on Cybersecurity in Europe:

- How can the EU be more **trustworthy** and **digitally secure**?
  - Cybersecurity **monitoring** and **advising**
  - Additional **regulatory** measures
- How can EU support the successful development on European **Cybersecurity Champions**?
  - Certification pillar: **legislation**, **standardization** and **labeling**
  - **Cooperation** between MS
  - Supporting **ecosystem** for Cybersecurity
  - Initiatives towards **market consolidation**



European Cybersecurity Industry Leaders

Recommendations on Cybersecurity for Europe

How can the EU be more trustworthy and digitally secure?

How can Europe support the successful development of European cybersecurity champions?

A report to M. Günther H. Oettinger European Commissioner for Digital Economy and Society

Recommendations

- **Public – private** sector **cooperation** must **be reinforced**;
- Sustainable implementation of **CSIRTs** network (as defined in NIS);
- An efficient and valuable **incident sharing/reporting mechanism**;
- Regular **awareness campaigns** for **customers**;
- Foster **certification** and **labelling**;
- Regulatory **sandboxing**;
- **Encryption** should continue to gain more and **more momentum**
- Raising **awareness** and **transparency** for **consumer**;
- **SME´s** transparency become paramount;
- Statement on the new **ENISA-Mandate**;

EUNITY

Thank you
Any questions?

Contact:

Alicia García Medina, alicia.garcia@atos.net
Pedro Soria-Rodríguez, pedro.soria@atos.net

Atos

References:
Wiser Market Watch Report,
https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders

The European cybersecurity PPP's presentation referred to the key objectives of the commission in cybersecurity, why do we need a PPP on cybesecurity, the aims, the budget and the support. Finally the PPP presentation referred to the model, the ECSO membership base, and its working groups. Below we add the original presentation about the European Cybersecurity PPP.

ABOUT THE EUROPEAN CYBERSECURITY PPP

ECS
EUROPEAN CYBER SECURITY ORGANISATION

KEY OBJECTIVES OF THE COMMISSION IN CYBERSECURITY

1- Increase cybersecurity capabilities and cooperation
2- Making the EU a strong player in cybersecurity
3- Mainstreaming cybersecurity in EU policies

WHY DO WE NEED A PPP ON CYBERSECURITY?

The cybersecurity market, one of the fastest growing markets in the ICT sector, yields huge economic opportunities.

It suffers from :

- Lack of funding
- Fragmentation of the European cyber industry
- Gap between R&D and market deployment
- Strong dependence on non-EU providers
- Lack of standards

Strengthening the EU's cybersecurity industry will allow European businesses to seize these opportunities and reinforce trust of citizens and businesses in the digital world, contributing to the goals of the Digital Single Market Strategy.

Europe needs high-quality, affordable and interoperable cybersecurity products and solutions.

ABOUT THE EUROPEAN CYBERSECURITY PPP

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

AIM

1. Foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right for privacy.

2. Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).

3. Coordinate digital security industrial resources in Europe.

BUDGET

The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4 years). Cybersecurity market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total of €1800 mln.

SUPPORT

European Cyber Security Organisation – ECSO Association has been created to engage with the EC in this PPP.
ECSO is open to any stakeholder (public / private; user / supplier) allowed to participated in H2020 projects.

ABOUT ECSO: A UNIQUE MODEL

ON CONTENT

The ECSO approach is going beyond the work of a typical Association supporting a cPPP.
it tackles, on top of Research & Innovation issues, all those topics that are linked to the market development and the protection of the development of the Digital Single Market, in the frame of the European Cybersecurity Strategy.

ECSO working groups are dealing with the different aspects of what we call "cybersecurity industrial policy": standardisation and certification; investments (link across public and private funds);international cooperation; needs of the different vertical market sectors; support to SMEs; regional / local aspects; education, training, awareness and cyber ranges; R&I / capability development priorities.

GOVERNANCE: A PPP WITHIN A PPP

A peculiarity of ECSO is to **include among its members (also at Board of Directors level) high representatives and experts from national and regional public administrations**. This approach is fundamental in a sector dealing with "security" as application of cybersecurity is and will remain a sovereign issue.

The presence at decision level (Board) and at working level (working groups) of **representatives from public administrations increases the quality of the ECSO recommendations** to the European and national institutions, thanks to a "pre-digested" dialogue and consensus between public and private experts. This will allow a faster decision making by public bodies and a viable implementation by the private sector of the decisions taken (regulations, standards etc.).

For this reason **ECSO itself is a public – private body**, creating a **new and dynamic multi-stakeholder dialogue**, preparing for the future evolutions and needs in this sector, as envisaged in the EU cybersecurity strategy.

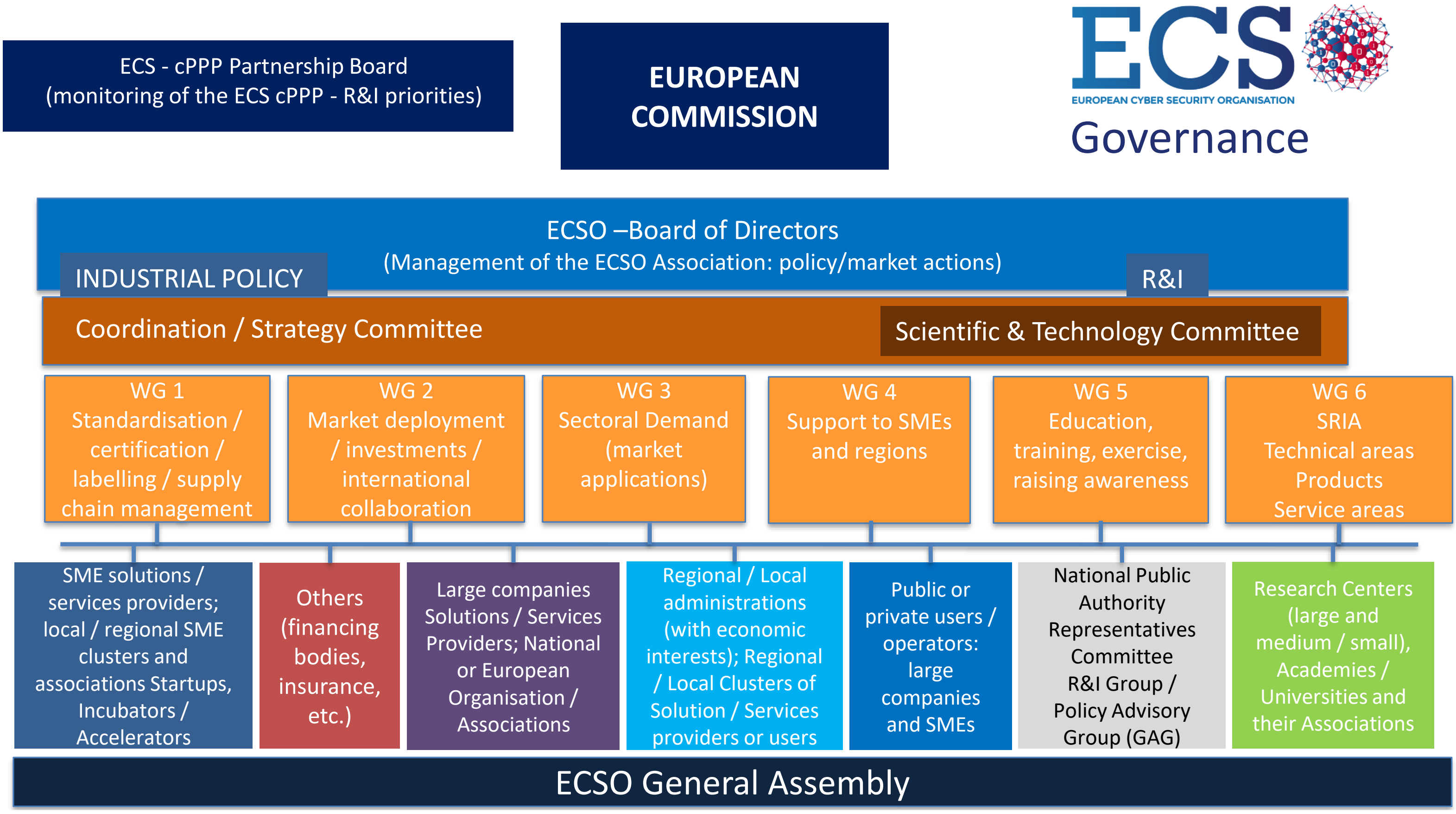
ECSO MEMBERSHIP BASE

At the time of the signature ceremony of the PPP contract (5th July 2016), ECSO counted 132 founding members. Now we are **218 organisations from 28 countries and counting (already 3 new requests)**

- Associations : 21
- Large companies and users: 70
- Public Administrations: 15
  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK + observers at NAPAC (BG, DK, HU, IE, LT, LU, LV, PT, RO, SE, SI, MT, …)
- Regional clusters: 3
- RTO/Universities: 55
- SMEs: 54

Looking for increased membership from users / operators

AUSTRIA	6	LATVIA	1
BELGIUM	11	LITHUANIA	1
BE - EU ASSOCIATIONS	10	LUXEMBOURG	4
CYPRUS	4	NORWAY	4
CZECH REP.	2	POLAND	7
DENMARK	3	PORTUGAL	5
ESTONIA	7	ROMANIA	1
FINLAND	8	SLOVAKIA	3
FRANCE	23	SPAIN	28
GERMANY	19	SWEDEN	1
GREECE	4	SWITZERLAND	4
HUNGARY	2	THE NETHERLANDS	14
IRELAND	3	TURKEY	2
ISRAEL	2	UNITED KINGDOM	9
ITALY	30		



ECS

EUROPEAN CYBER SECURITY ORGANISATION

Governance

ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN COMMISSION

ECSO –Board of Directors
(Management of the ECSO Association: policy/market actions)

INDUSTRIAL POLICY

R&I

Coordination / Strategy Committee

Scientific & Technology Committee

WG 1
Standardisation / certification / labelling / supply chain management

WG 2
Market deployment / investments / international collaboration

WG 3
Sectoral Demand (market applications)

WG 4
Support to SMEs and regions

WG 5
Education, training, exercise, raising awareness

WG 6
SRIA
Technical areas
Products
Service areas

SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators

Others (financing bodies, insurance, etc.)

Large companies Solutions / Services Providers; National or European Organisation / Associations

Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users

Public or private users / operators: large companies and SMEs

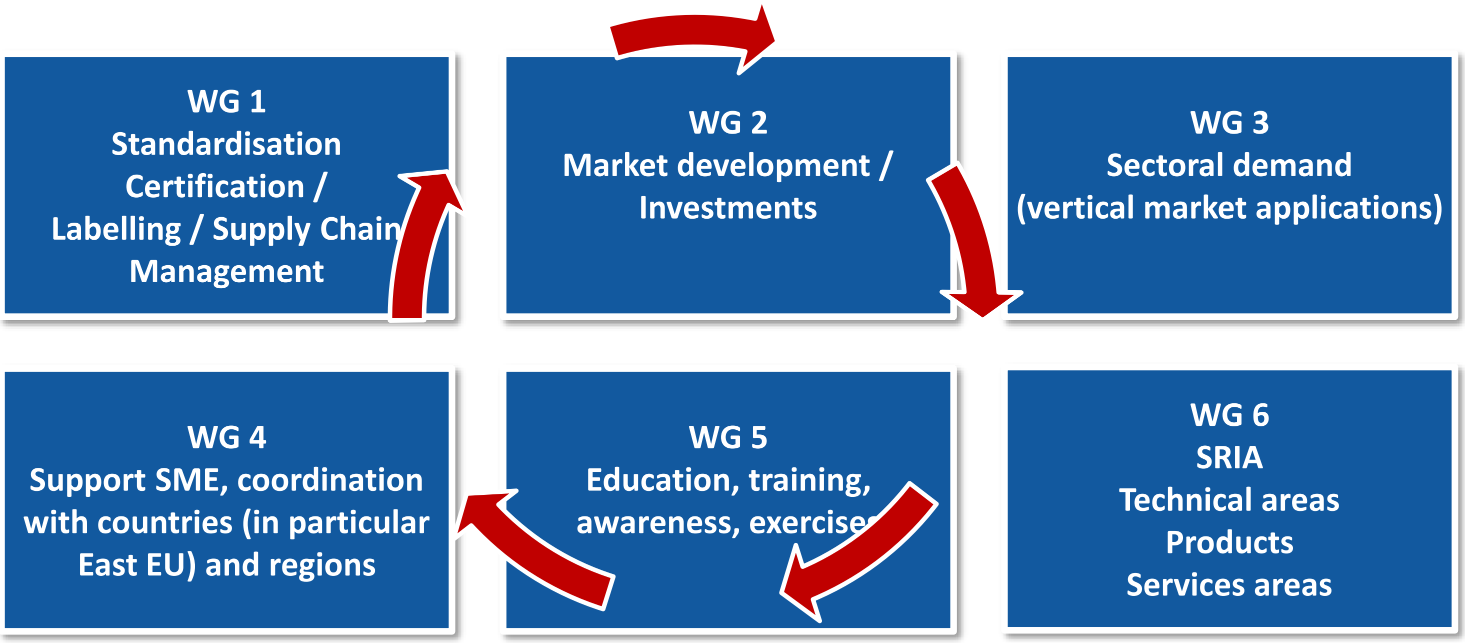
National Public Authority Representatives Committee
R&I Group / Policy Advisory Group (GAG)

Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO General Assembly

WORKING GROUPS & TASK FORCES

ECS
EUROPEAN CYBER SECURITY ORGANISATION



WG 1
Standardisation
Certification /
Labelling / Supply Chain
Management

WG 2
Market development /
Investments

WG 3
Sectoral demand
(vertical market applications)

WG 4
Support SME, coordination
with countries (in particular
East EU) and regions

WG 5
Education, training,
awareness, exercises

WG 6
SRIA
Technical areas
Products
Services areas

The presentation of CRIC Cross Sectors Forum (CSF) included an overview about CSF, the sectors forum, the motivation of collaboration, the activities and results on 1st period and current, the top layers meeting and the future work plan. Below we add the original presentation by Hiroshi Takechi (NEC / CSF).

Introduction of “CRIC Cross Sectors Forum(CSF)”

Wednesday, 11th October, 2017
CRIC Cross Sectors Forum

Agenda

1. Cross Sectors Forum’s Overview
2. Activities and Results on 1st period and Current
3. Top layers meeting
4. Future work plan

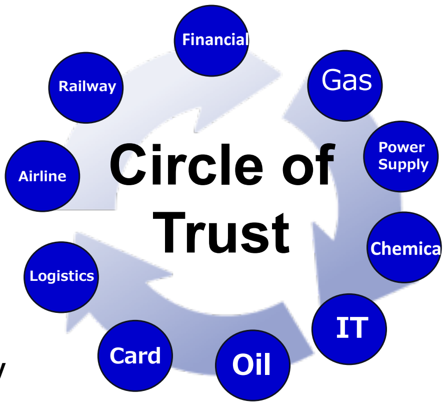
1. Cross Sectors Forum’s Overview

CRIC Cross Sectors Forum

Cyber Risk Intelligence Center Cross Sectors Forum - CRIC CSF"

- URL: http://cyber-risk.or.jp/
- Launched in June 2015
- Trigger to Launched：Advisory Board of Cybersecurity in ”Keidanren”
- Published a cybersecurity policy proposals to the Japanese government in February 2015
- More than 30 companies mainly from 13 Critical Infrastructure Industries (e.g. Finance, Airline, Railway, Power, Energy etc)

ANA
DNP (Printing)
Fujitsu
Hitachi
JAPAN POST HOLDINGS
JX Holdings
KDDI
KDDI Research
Mitsubishi Corp.
Mitsubishi Electronics
Mitsubishi Heavy Industry
Mizuho Financial Group
NEC
NHK
NTT

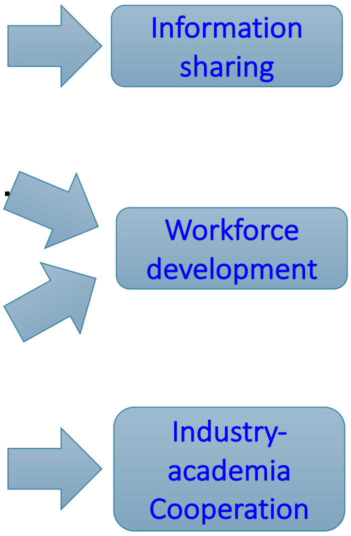


NYK Line (Transportation)
Nikkei Newspaper
Nippon Express Company
Nippon TV
Nissei (Life Insurance)
Panasonic
Pasona (Staffing)
SONY
Sumitomo Chemical
TBS
Tokyo Gas
Toshiba
Toyota
Yamato Holdings
etc.

Motivation of Collaboration

- Readiness enhancement and workforce development are common challenges among industries.
- It is impossible to protect everything by a single company.
- Collaboration beyond sectors is imperative.

- Need the opportunity for sharing information that companies want to know/are worried about, but they can’t ask/don’t know who knows.
- Need the definition of security workforce to clarify industry needs for effective recruitment and education.
- Expected cost reduction by sharing workforce development programs and tools.
- Develop professionals who match the needs from industries by educating promising students (e.g. university students) who are interested in security.



Information sharing

Workforce development

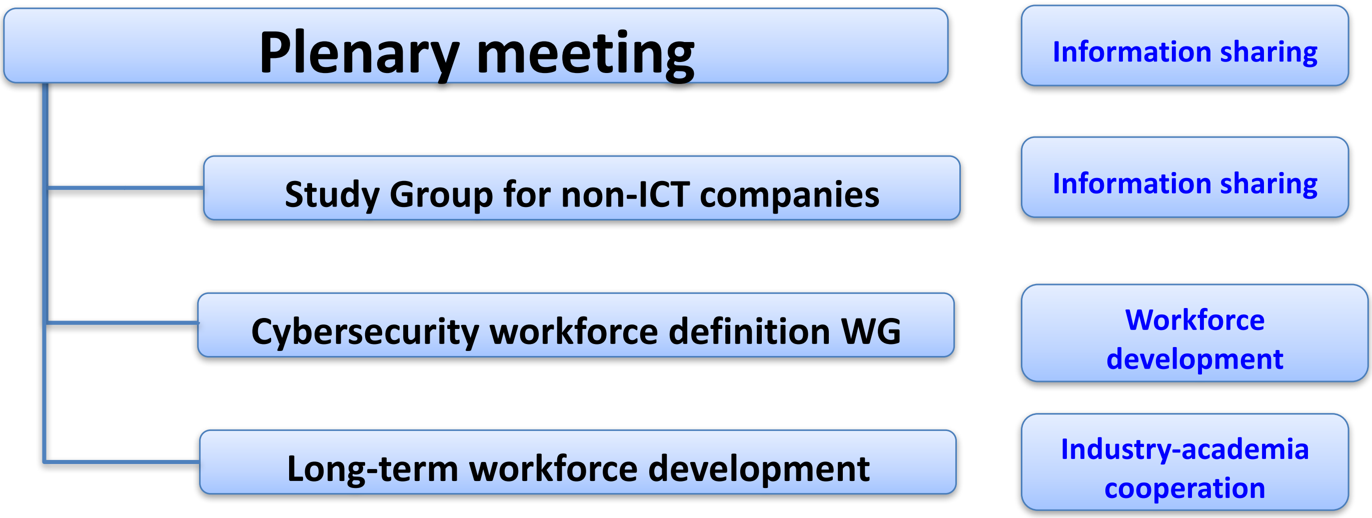
Industry-academia Cooperation

2. Activities and Results on 1st period and Current

Working Groups in 1st period

(June 2015 – September 2016)

- Set the following groups and promote “Information Sharing”, “Workforce Development”, and “Industry-Academia Cooperation”
- It is important to construct “Circle of Trust” because enhancing cybersecurity readiness is imperative.



Plenary meeting

Study Group for non-ICT companies

Cybersecurity workforce definition WG

Long-term workforce development

Information sharing

Information sharing

Workforce development

Industry-academia cooperation

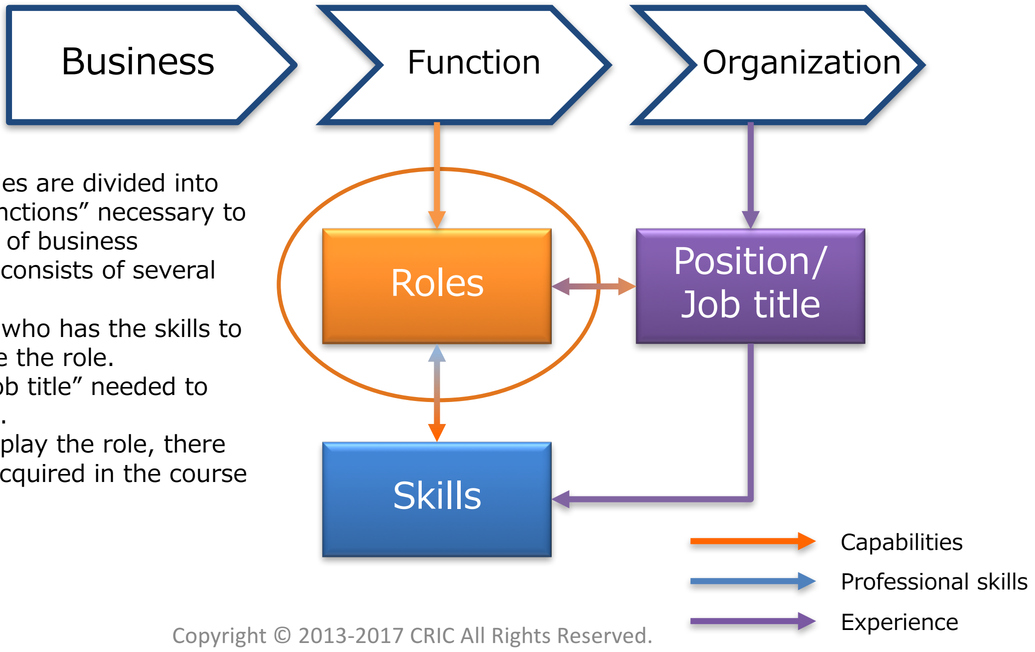
Key considerations on Workforce definitions

The Forum considers the characteristics and circumstances of Japanese companies to make our workforce definitions practical.

Wide variety industries	We build our forum to cover Japanese wide variety industries.
Specific characteristics of Japanese companies	We carried out the discussion on Japanese companies' culture and practices by specifically clarify that the typical structure of Japanese companies
Balance between core business role and security role	Security related roles must be considered in conjunction with the core business roles.

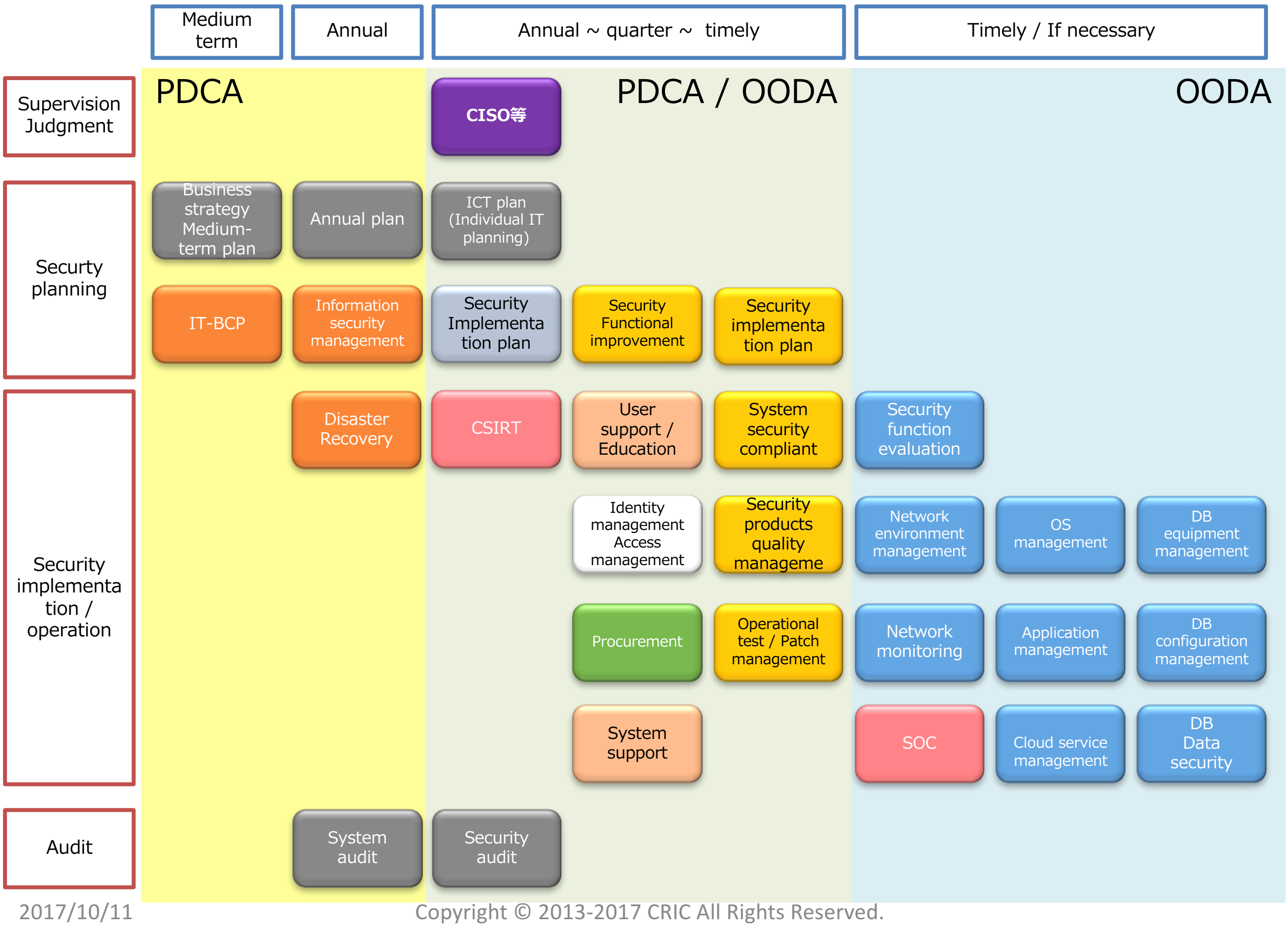
Relationship between Organization and Workforce

- Security workforces of user companies are different from that of security vendors regarding its roles, career and capabilities.
- **Excellent workforce is the workforce that can fulfill the role.** Company have to provide the environment on which they can use their capability to play the role.
- In our approach, the relationship of "Roles", "Position/Job title", and "Skill" is below;



- Company activities are divided into some of the "Functions" necessary to achieve the goal of business
- Each "Function" consists of several "Roles".
- Assign a person who has the skills to be able to realize the role.
- Give "Position/Job title" needed to perform the role.
- Require skills to play the role, there are skills to be acquired in the course to play the role.

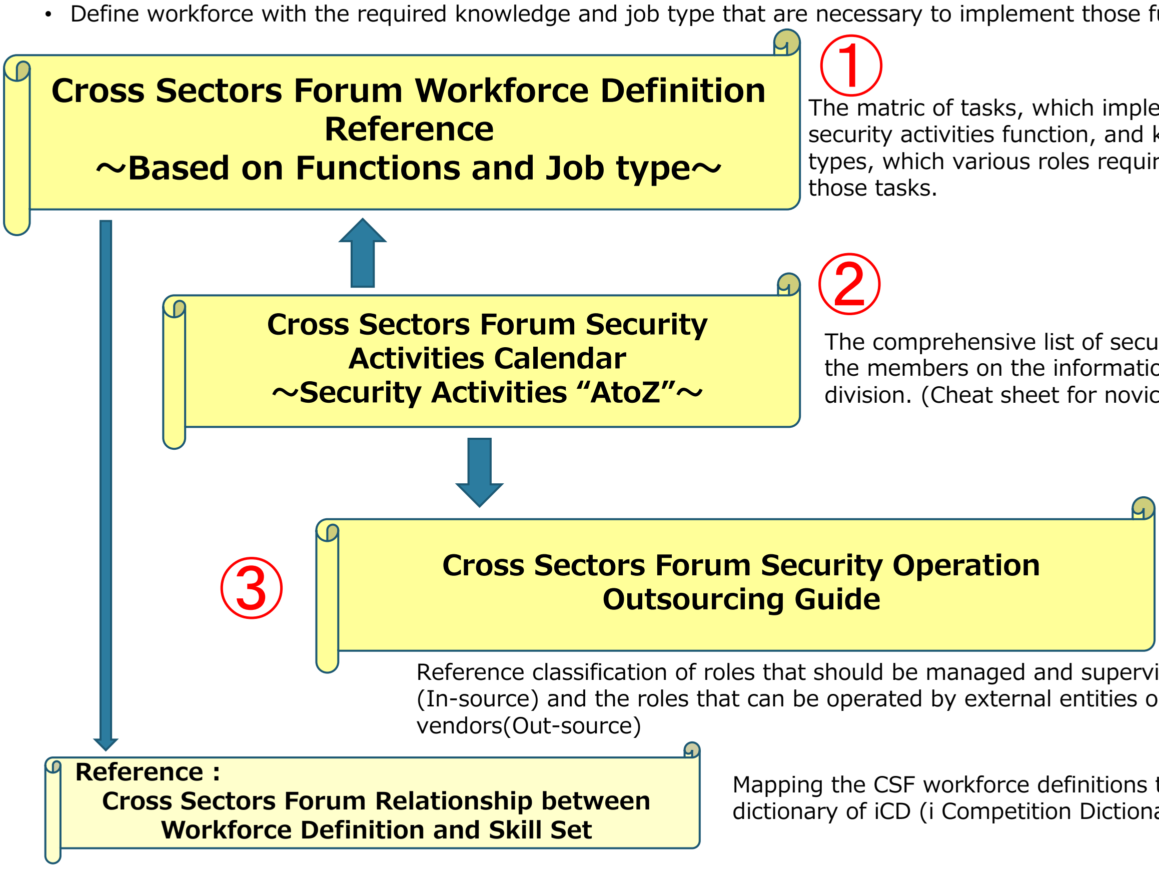
Function definition of cyber security measures



	Medium term	Annual	Annual ~ quarter ~ timely			Timely / If necessary		
	PDCA			PDCA / OODA				OODA
Supervision Judgment			CISO等					
Securty planning	Business strategy Medium-term plan	Annual plan	ICT plan (Individual IT planning)					
	IT-BCP	Information security management	Security Implementation plan	Security Functional improvement	Security implementation plan			
Security implementation / operation		Disaster Recovery	CSIRT	User support / Education	System security compliant	Security function evaluation		
				Identity management Access management	Security products quality manageme	Network environment management	OS management	DB equipment management
				Procurement	Operational test / Patch management	Network monitoring	Application management	DB configuration management
				System support		SOC	Cloud service management	DB Data security
Audit		System audit	Security audit					

Outputs of Cross Sectors Forum (1st period)

- The Scope of the 1st period is the information systems division in the Japanese user companies.
- Identify the required Cybersecurity related functions in the scope
- Define workforce with the required knowledge and job type that are necessary to implement those functions



Cross Sectors Forum Workforce Definition Reference
～Based on Functions and Job type～

①
The matric of tasks, which implement cyber security activities function, and knowledge and job types, which various roles require to achieve those tasks.

Cross Sectors Forum Security Activities Calendar
～Security Activities “AtoZ”～

②
The comprehensive list of security activities for the members on the information system division. (Cheat sheet for novice CISOs)

③
Cross Sectors Forum Security Operation Outsourcing Guide

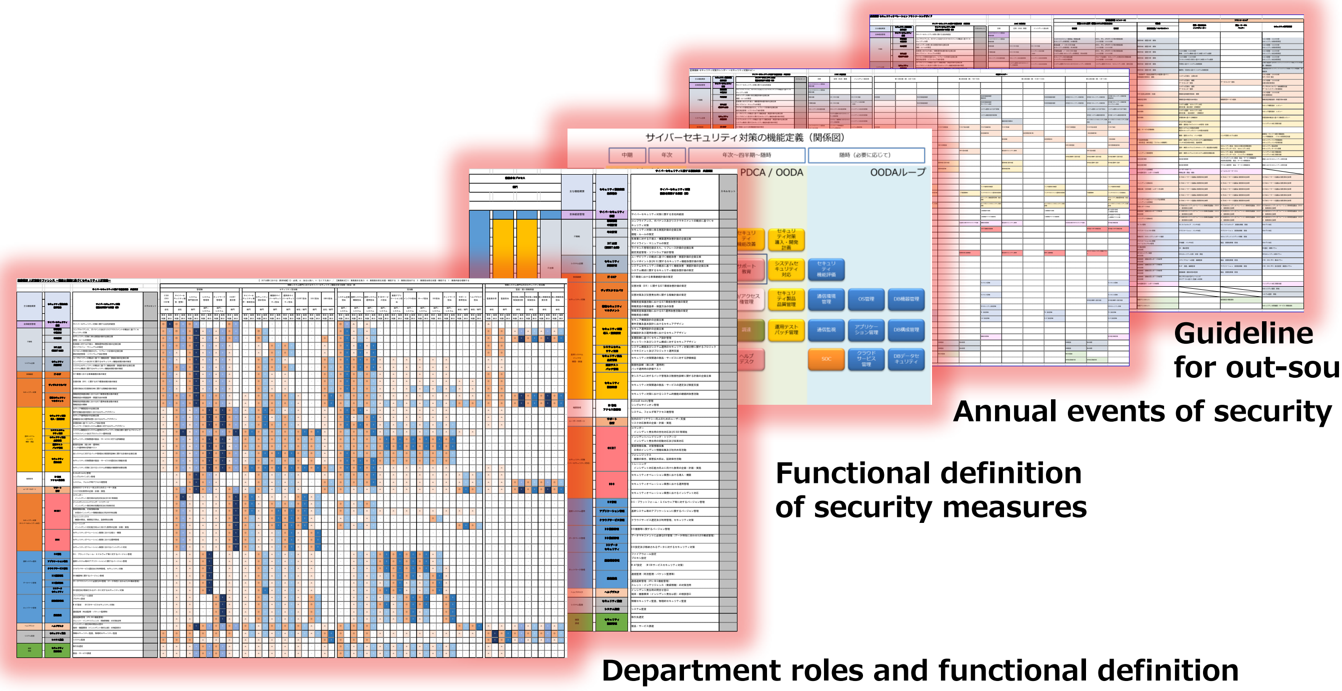
Reference classification of roles that should be managed and supervised in-house (In-source) and the roles that can be operated by external entities or security vendors(Out-source)

Reference :
Cross Sectors Forum Relationship between Workforce Definition and Skill Set

Mapping the CSF workforce definitions to the skill dictionary of iCD (i Competition Dictionary, IPA)

Cross-sectors collaboration for Cybersecurity Workforce Development

- **Cybersecurity workforce definition for Japanese companies.**
- **Sharing into industry organizations and government organizations.**



Guideline for out-sourcing

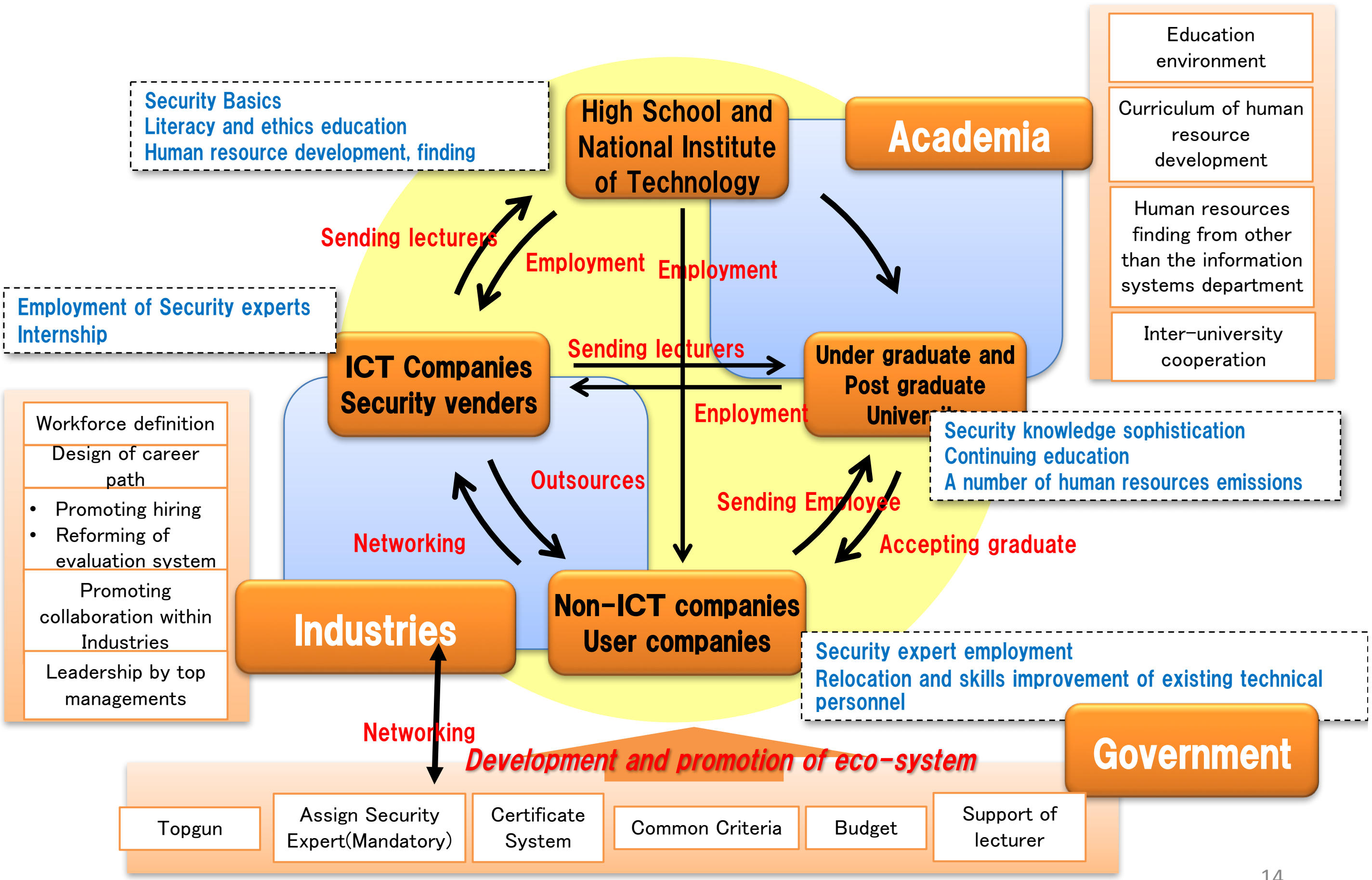
Annual events of security

Functional definition of security measures

Department roles and functional definition

References of workforce definition

Eco-System for Cyber Security Workforce Development



Security Basics
Literacy and ethics education
Human resource development, finding

High School and National Institute of Technology

Academia

Education environment

Curriculum of human resource development

Human resources finding from other than the information systems department

Inter-university cooperation

Sending lecturers

Employment

Employment

Employment of Security experts
Internship

ICT Companies Security venders

Sending lecturers

Employment

Under graduate and Post graduate Univer

Security knowledge sophistication
Continuing education
A number of human resources emissions

Workforce definition

Design of career path

- Promoting hiring
- Reforming of evaluation system

Promoting collaboration within Industries

Leadership by top managements

Outsources

Networking

Sending Employee

Accepting graduate

Industries

Non-ICT companies User companies

Security expert employment
Relocation and skills improvement of existing technical personnel

Networking

Development and promotion of eco-system

Government

Topgun

Assign Security Expert(Mandatory)

Certificate System

Common Criteria

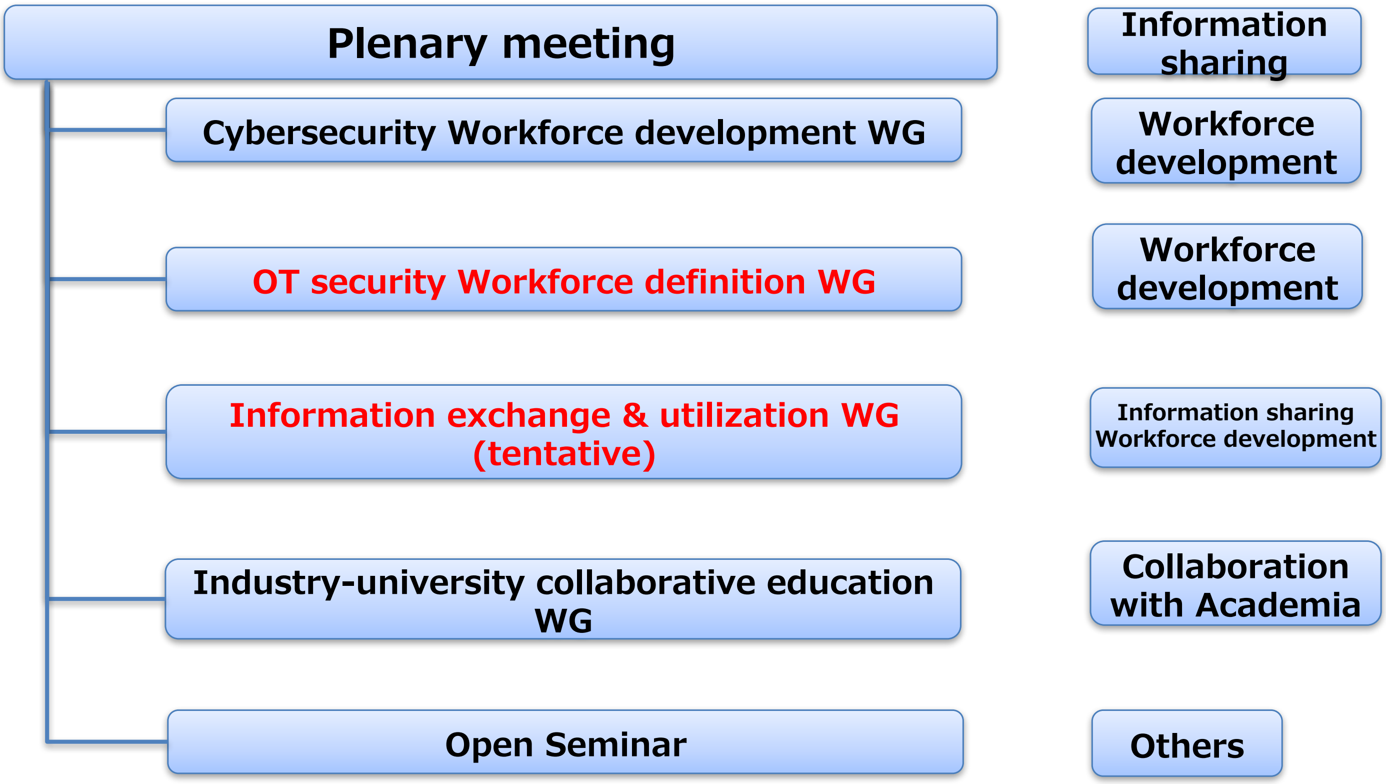
Budget

Support of lecturer

New structure of WG in 2nd period

(October 2017 – September 2018)

- 2017/4/1 Transition to a consortium with corporate status (established under the existing group "Cyber Risk Intelligence Center (CRIC)")

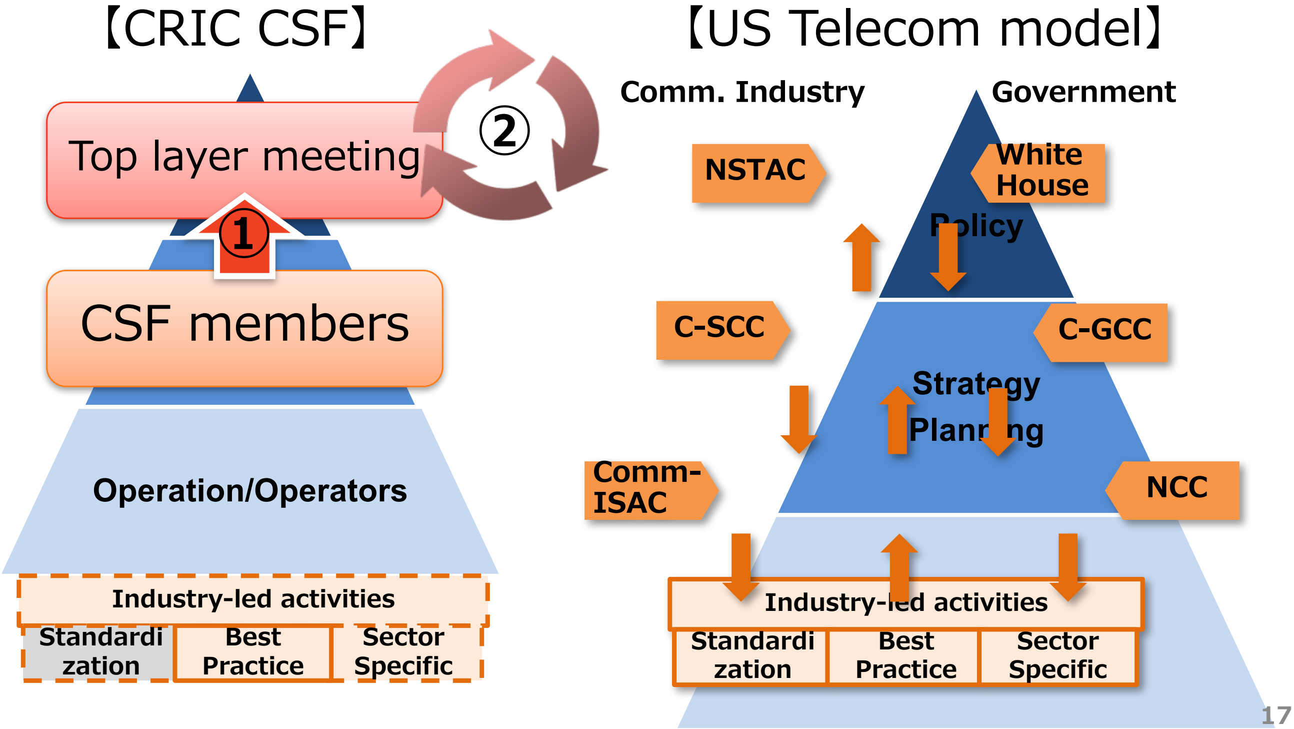


Plenary meeting	Information sharing
Cybersecurity Workforce development WG	Workforce development
OT security Workforce definition WG	Workforce development
Information exchange & utilization WG (tentative)	Information sharing Workforce development
Industry-university collaborative education WG	Collaboration with Academia
Open Seminar	Others

3. Top Layers Meeting

Background of the top tier meeting

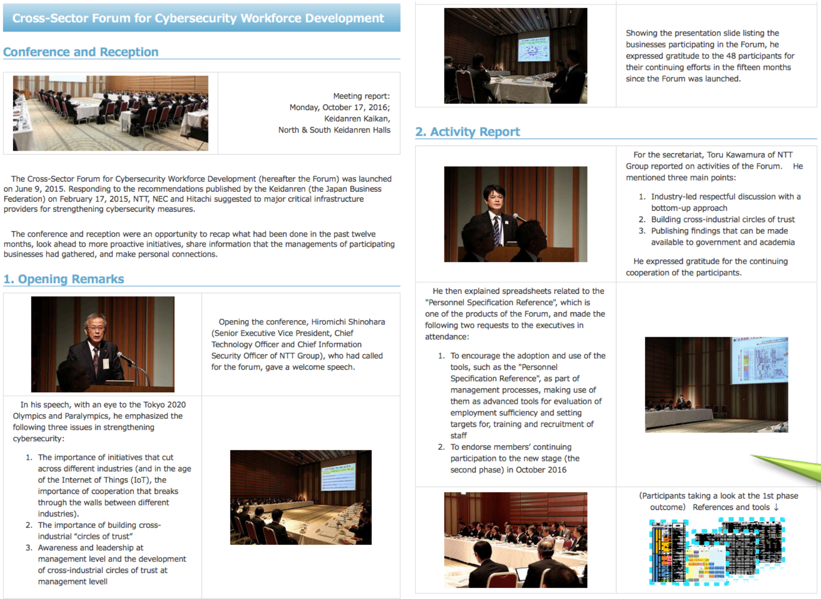
- The involvement of the top tier and management person is essential.
- Reference the US telecommunications industry to strengthen collaboration across industries
  ①Gain support from the management with the understanding of management
  ②Establishment of Trusted Network in cross-industry management



1st TOP layer meeting

Focus points

① Confirm the necessity of working across industries (cooperation beyond industries is necessary as a response to the IoT era when all are connected, etc.)
② Promotion of CSF initiatives (importance of building trust circle, etc.)
③ Understanding of management and leadership (Establishment of Trusted Network among cross-industry management)



Cross-Sector Forum for Cybersecurity Workforce Development

Conference and Reception

Meeting report:
Monday, October 17, 2016;
Keidanren Kaikan,
North & South Keidanren Halls

The Cross-Sector Forum for Cybersecurity Workforce Development (hereafter the Forum) was launched on June 9, 2015. Responding to the recommendations published by the Keidanren (the Japan Business Federation) on February 17, 2015, NTT, NEC and Hitachi suggested to major critical infrastructure providers for strengthening cybersecurity measures.

The conference and reception were an opportunity to recap what had been done in the past twelve months, look ahead to more proactive initiatives, share information that the managements of participating businesses had gathered, and make personal connections.

1. Opening Remarks

Opening the conference, Hiromichi Shinohara (Senior Executive Vice President, Chief Technology Officer and Chief Information Security Officer of NTT Group), who had called for the forum, gave a welcome speech.

In his speech, with an eye to the Tokyo 2020 Olympics and Paralympics, he emphasized the following three issues in strengthening cybersecurity:

1. The importance of initiatives that cut across different industries (and in the age of the Internet of Things (IoT), the importance of cooperation that breaks through the walls between different industries).
2. The importance of building cross-industrial "circles of trust"
3. Awareness and leadership at management level and the development of cross-industrial circles of trust at management levell

Showing the presentation slide listing the businesses participating in the Forum, he expressed gratitude to the 48 participants for their continuing efforts in the fifteen months since the Forum was launched.

2. Activity Report

For the secretariat, Toru Kawamura of NTT Group reported on activities of the Forum. He mentioned three main points:

1. Industry-led respectful discussion with a bottom-up approach
2. Building cross-industrial circles of trust
3. Publishing findings that can be made available to government and academia

He expressed gratitude for the continuing cooperation of the participants.

He then explained spreadsheets related to the "Personnel Specification Reference", which is one of the products of the Forum, and made the following two requests to the executives in attendance:

1. To encourage the adoption and use of the tools, such as the "Personnel Specification Reference", as part of management processes, making use of them as advanced tools for evaluation of employment sufficiency and setting targets for, training and recruitment of staff
2. To endorse members' continuing participation to the new stage (the second phase) in October 2016

(Participants taking a look at the 1st phase outcome) References and tools ↓

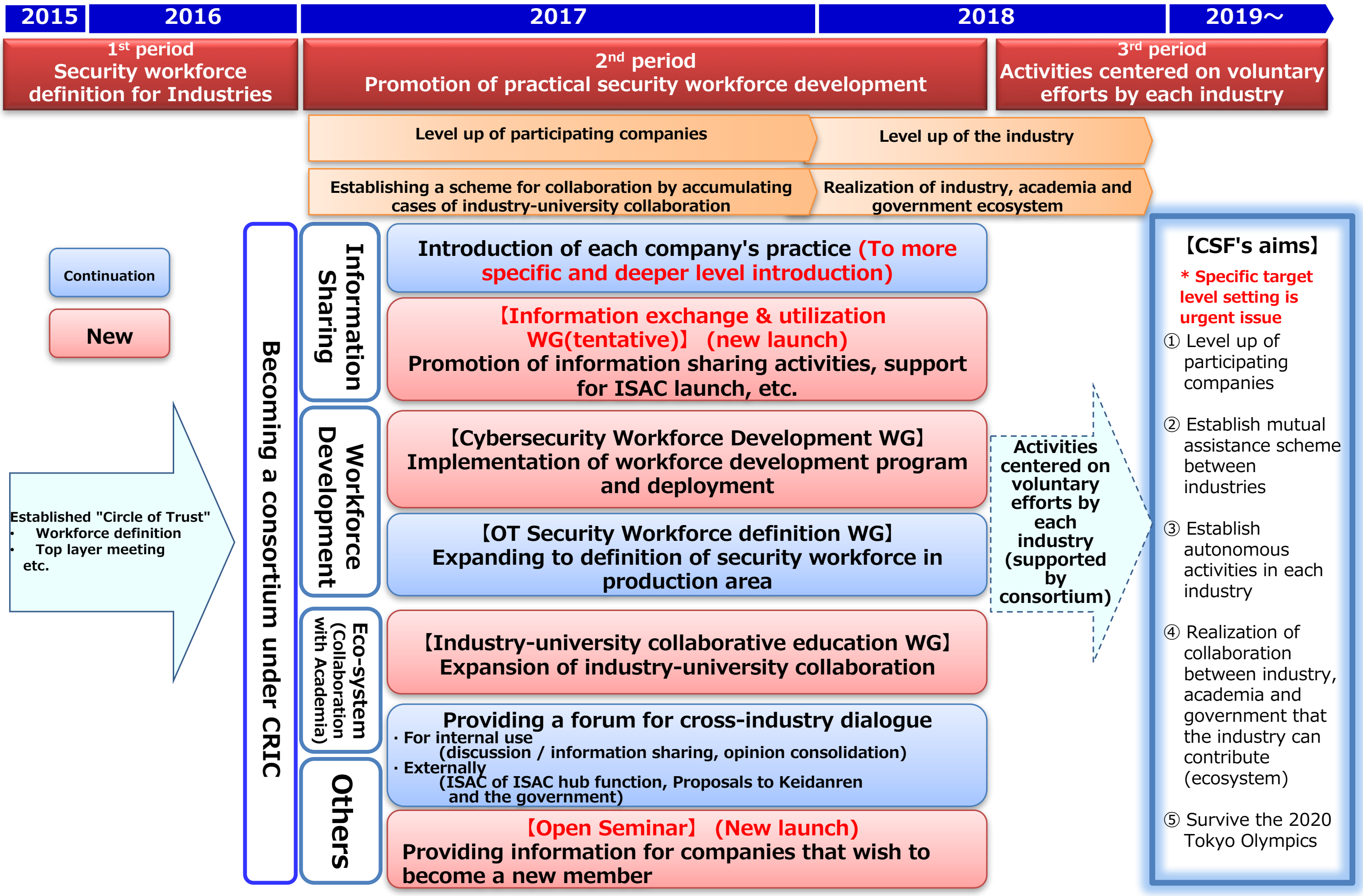
Top layer meeting scene

Publish a report to broadly share the summary of the meeting

http://cyber-risk.or.jp/sansanren/conference_20161017_en.html

4. Future work plan

Future Activities Plan



2015 | 2016 | 2017 | 2018 | 2019～

1st period
Security workforce definition for Industries

2nd period
Promotion of practical security workforce development

3rd period
Activities centered on voluntary efforts by each industry

Level up of participating companies

Level up of the industry

Establishing a scheme for collaboration by accumulating cases of industry-university collaboration

Realization of industry, academia and government ecosystem

Continuation

New

Established "Circle of Trust"
- Workforce definition
- Top layer meeting

etc.

Becoming a consortium under CRIC

Information Sharing

Introduction of each company's practice (To more specific and deeper level introduction)

【Information exchange & utilization WG(tentative)】 (new launch)
Promotion of information sharing activities, support for ISAC launch, etc.

Workforce Development

【Cybersecurity Workforce Development WG】
Implementation of workforce development program and deployment

【OT Security Workforce definition WG】
Expanding to definition of security workforce in production area

Eco-system (Collaboration with Academia)

【Industry-university collaborative education WG】
Expansion of industry-university collaboration

Others

Providing a forum for cross-industry dialogue
- For internal use
  (discussion / information sharing, opinion consolidation)
- Externally
  (ISAC of ISAC hub function, Proposals to Keidanren and the government)

【Open Seminar】 (New launch)
Providing information for companies that wish to become a new member

Activities centered on voluntary efforts by each industry (supported by consortium)

【CSF's aims】

＊ Specific target level setting is urgent issue

① Level up of participating companies

② Establish mutual assistance scheme between industries

③ Establish autonomous activities in each industry

④ Realization of collaboration between industry, academia and government that the industry can contribute (ecosystem)

⑤ Survive the 2020 Tokyo Olympics

Thank you

The last presentation was “Cyberwatching.eu” by Nicholas Ferguson (Trust-IT services, Cyberwatching.eu coordinator). The presentation referred to the challenges, the observatory, the catalogue of services, the marketplace, the SME End-User Club, and the collaborations.

Below we add the original presentation of Cyberwatching.eu: “Bringing EU Cybersecurity & privacy research results closer to the market”, by Nicholas Ferguson (Trust-IT services, Cyberwatching.eu coordinator).

cyberwatching.eu

The European watch
on cybersecurity & privacy

Bringing EU Cybersecurity & privacy research results closer to the market

EU-Unity Workshop | 11 October 2017, Tokyo, Japan

Nicholas Ferguson, Trust-IT Services &
Coordinator, Cyberwatching.eu

www.cyberwatching.eu
@cyberwatching.eu
info@cyberwatching.eu

Funded by the European Commission
Horizon 2020 – Grant # 740129

cyberwatching.eu
The European watch
on cybersecurity & privacy

ICT - A land of opportunity but…

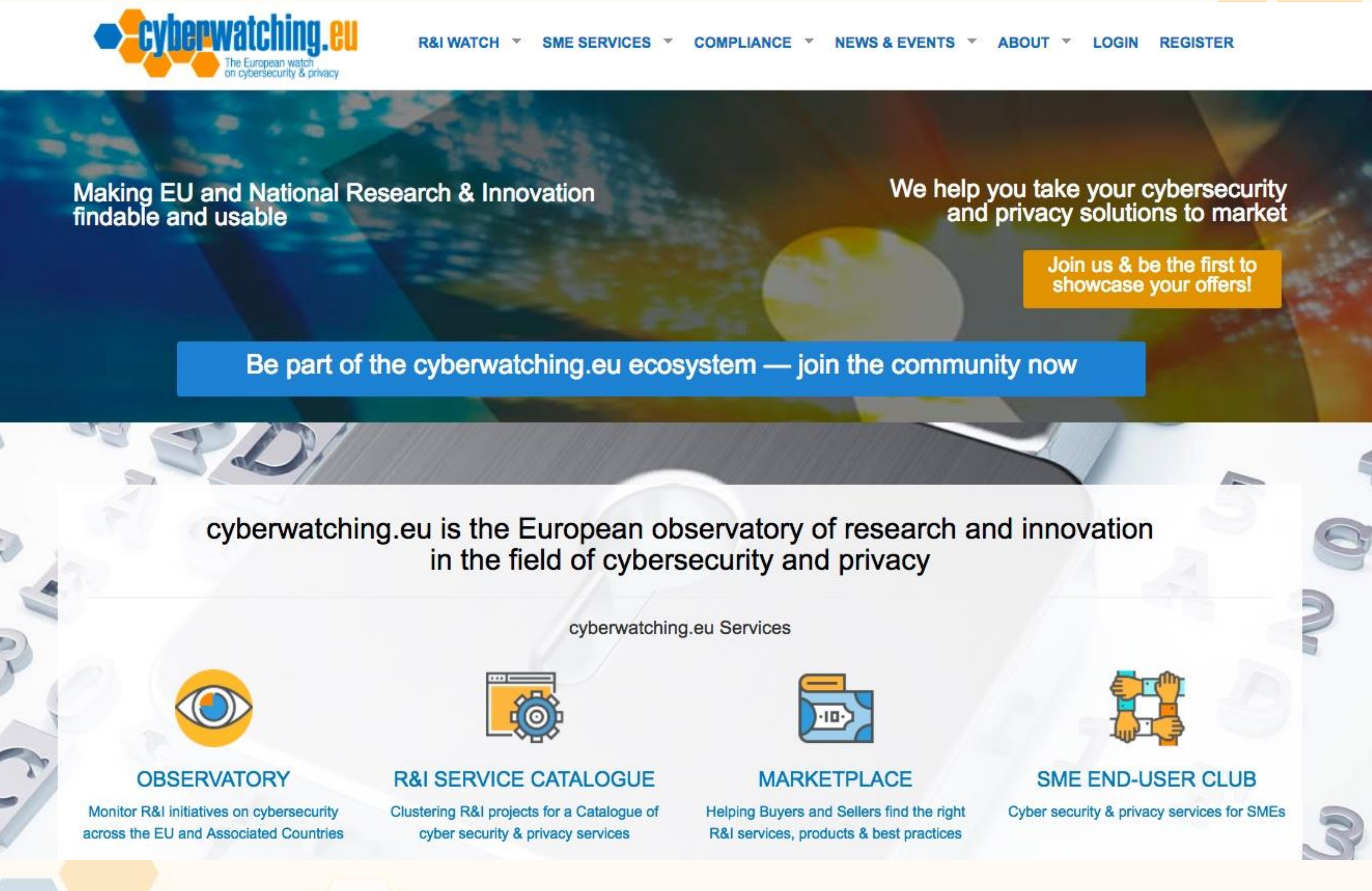
SMEs

- Lack of awareness of socio-economic impact
- Lack of resources, skills and expert knowledge
  - Risk management
  - What do I do?
  - Legal implications of a data breach?
- So many products, so little money!

Research & Innovation

- Cyber security is a pillar of the EC's Digital Single Market
- Massive EU & national funding in R&I
- Services targetting vertical sectors & SMEs
- Limited results reaching market = limited impact on SMEs

Cyberwatching.eu: Bringing R&I closer to end-users



R&I WATCH ▾ SME SERVICES ▾ COMPLIANCE ▾ NEWS & EVENTS ▾ ABOUT ▾ LOGIN REGISTER

Making EU and National Research & Innovation findable and usable

We help you take your cybersecurity and privacy solutions to market

Join us & be the first to showcase your offers!

Be part of the cyberwatching.eu ecosystem — join the community now

cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy

cyberwatching.eu Services

OBSERVATORY

Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

R&I SERVICE CATALOGUE

Clustering R&I projects for a Catalogue of cyber security & privacy services

MARKETPLACE

Helping Buyers and Sellers find the right R&I services, products & best practices

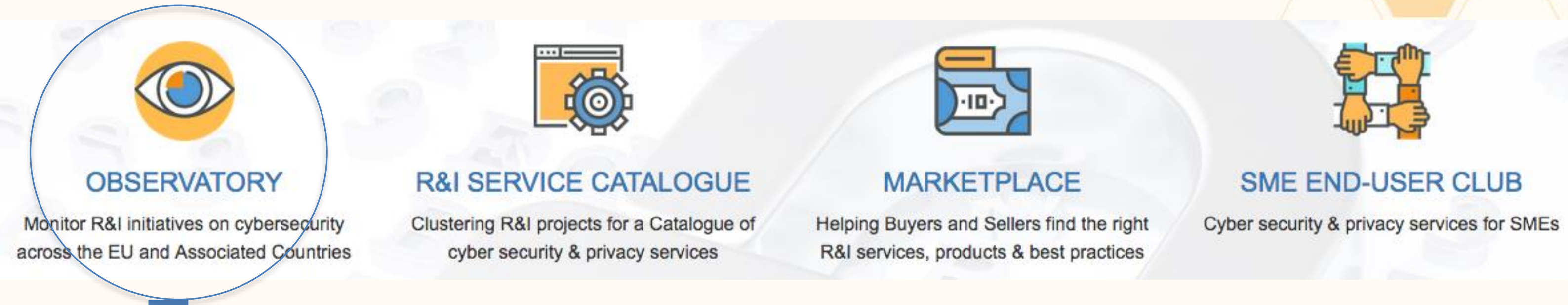
SME END-USER CLUB

Cyber security & privacy services for SMEs

Our main assets are:
Observatory, Service catalogue, Marketplace and SME end-user club

cyberwatching.eu
The European watch on cybersecurity & privacy

Asset #1 – Observatory



OBSERVATORY

Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

R&I SERVICE CATALOGUE

Clustering R&I projects for a Catalogue of cyber security & privacy services

MARKETPLACE

Helping Buyers and Sellers find the right R&I services, products & best practices

SME END-USER CLUB

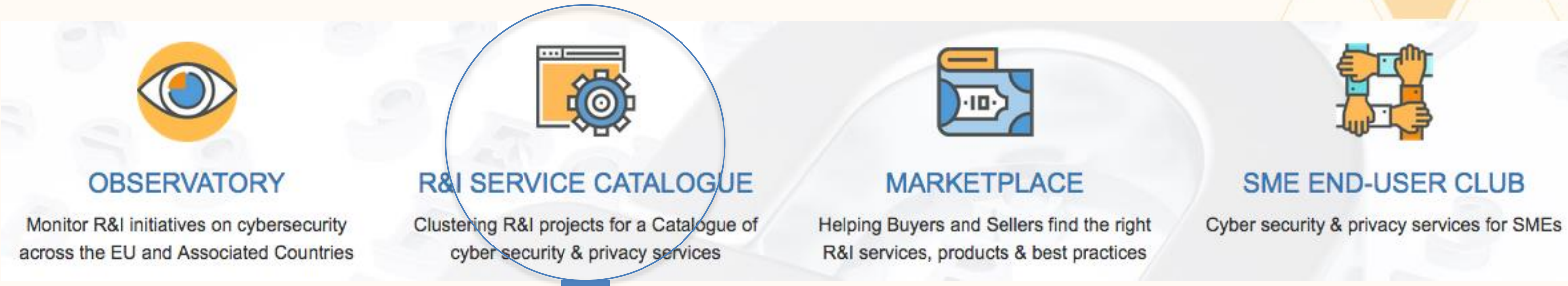
Cyber security & privacy services for SMEs

- **Monitor all cybersecurity and privacy R&D initiatives** across EU and at National level – Already 150+ identified
- Clustering projects based on cybersecurity taxonomy & PCA
- Cluster events on TRL analysis & (re-)usability of research results
- Synergies & convergence for future funding opportunities

A European technology radar

cyberwatching.eu
The European watch
on cybersecurity & privacy

Asset #2 – Catalogue of Services



Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

Clustering R&I projects for a Catalogue of cyber security & privacy services

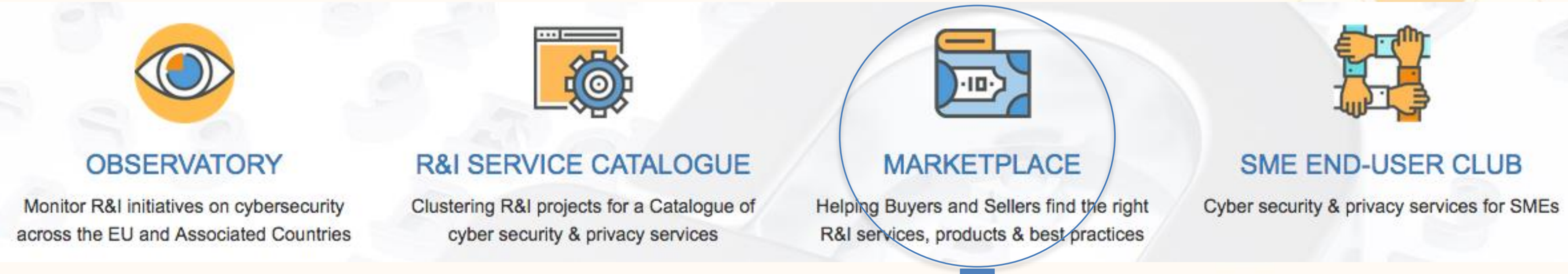
Helping Buyers and Sellers find the right R&I services, products & best practices

Cyber security & privacy services for SMEs

- Online catalogue of **R&I projects and services**
- Single access point for all EU & National projects
- Service-oriented offers: user needs, pain points, changing people's lives, target stakeholders, mapped & to taxonomy

Make your Cybersecurity & privacy results more findable & accessible
Submit your project: http://bit.ly/2xiQh17

Asset #3 – Marketplace



OBSERVATORY

Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

R&I SERVICE CATALOGUE

Clustering R&I projects for a Catalogue of cyber security & privacy services

MARKETPLACE

Helping Buyers and Sellers find the right R&I services, products & best practices

SME END-USER CLUB

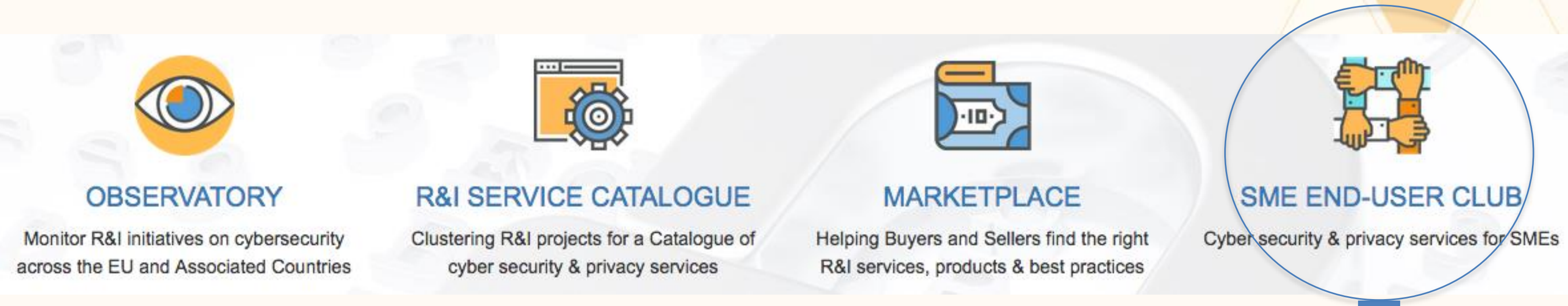
Cyber security & privacy services for SMEs

- A Marketplace of **cybersecurity & privacy "services"**
- **Suppliers**: R&I projects with results for testing, validation or adoption.
- **Users**: SMEs find new solutions and services
- **The win-win** mechanism can take place both at research synergy level and at commercial level, in developing new business opportunities

Connecting research results with both the supply and demand side of the cybersecurity & privacy industry

cyberwatching.eu
The European watch on cybersecurity & privacy

Asset #4 – SME End-User Club



OBSERVATORY

Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

R&I SERVICE CATALOGUE

Clustering R&I projects for a Catalogue of cyber security & privacy services

MARKETPLACE

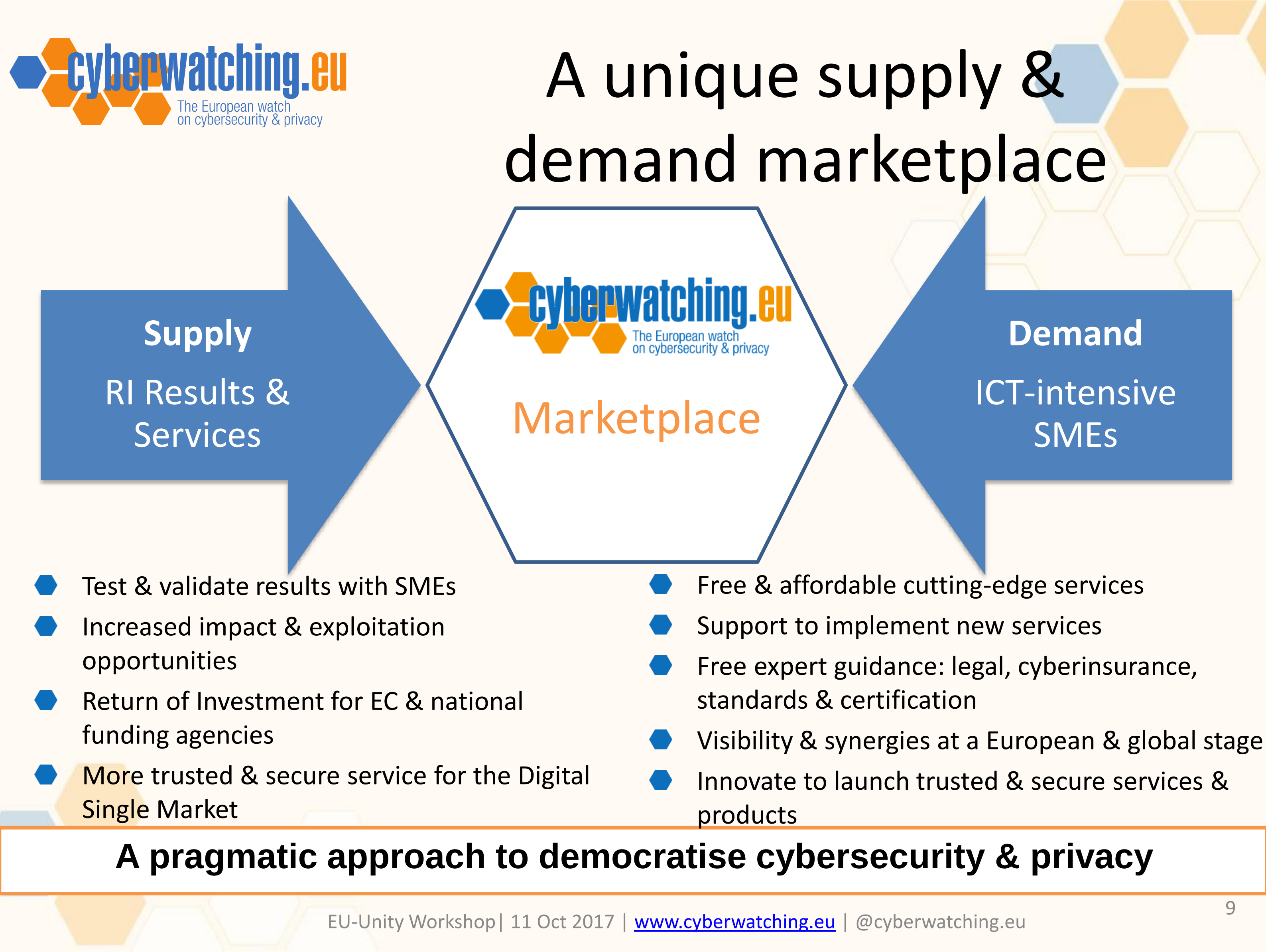
Helping Buyers and Sellers find the right R&I services, products & best practices

SME END-USER CLUB

Cyber security & privacy services for SMEs

- Prime and guided access to Marketplace: Affordable & free cyber security & privacy services
- Free events, guides and discounted consultancy on legal, cyber insurance and standards & certification
- EU-wide collaboration opportunities with SMEs & R&I funding

Ensuring that the EU research investments actually address real users' needs in an effective way
Sign up today: http://bit.ly/2i28Xvi



A unique supply & demand marketplace

Supply

RI Results & Services

Marketplace

Demand

ICT-intensive SMEs

- Test & validate results with SMEs
- Increased impact & exploitation opportunities
- Return of Investment for EC & national funding agencies
- More trusted & secure service for the Digital Single Market

- Free & affordable cutting-edge services
- Support to implement new services
- Free expert guidance: legal, cyberinsurance, standards & certification
- Visibility & synergies at a European & global stage
- Innovate to launch trusted & secure services & products

A pragmatic approach to democratise cybersecurity & privacy

cyberwatching.eu
The European watch
on cybersecurity & privacy

Collaboration

ECS
EUROPEAN CYBER SECURITY ORGANISATION

EUNITY

aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

- Cybersecurity taxonomy
- Mapping & clustering R&I initiatives
- International collaboration
- Policy alignment
- Joint workshops & annual events (Spring 2018)
- Standards & certification
- SME engagement

Thank you for your attention! Questions?

Contact

Nick Ferguson, Project Coordinator
Trust-IT Services Ltd – www.trust-itservices.com
n.ferguson@trust-itservices.com

cyberwatching.eu
The European watch on cybersecurity & privacy

www.cyberwatching.eu
@cyberwatching.eu
info@cyberwatching.eu

3.4 Session 6: Landscapes

Chair: Hervé Debar, IMT

This session was focused on the cybersecurity policy landscape in Europe (Legislation and Research).

3.4.1 The Cybersecurity Policy Landscape in Europe: Legislation and Research (Afonso Ferreira, IRIT)(EC/MIC Project Officers)

Initially the "Cybersecurity Policy" by Afonso Ferreira included an introduction about the Computer Science Research Institute at Toulouse and the EU Cybersecurity Strategy as a play in two acts.

Below we add the original presentation.

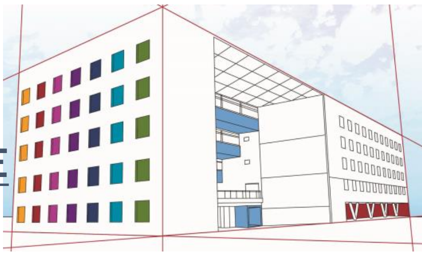
The Cybersecurity Policy Landscape in Europe: Legislation and Research

Afonso Ferreira
French National Research Centre (CNRS)
Computer Science Research Institute at Toulouse (IRIT)
France

Quick background

- Researcher in Algorithms, Optimisation, Networks, Cybersecurity, Insurance, CPS
- Policy maker in Future and Emerging Technologies, Cybersecurity, Privacy at the European Commission (until end March 2017)
- Foresight designer and practitioner, mainly on the impact of the Digital Revolution and Digital Transformation
- Adviser to Institutions and to EU Projects

INSTITUT DE RECHERCHE EN INFORMATIQUE DE TOULOUSE (Computer Science Research Institute at Toulouse)



More than 700 researchers

7 main areas of research

- Information analysis and synthesis
- Indexing, and information search
- Interaction, Cooperation, self-Adaptation through Experimental Studies
- Reasoning and decision
- Modelling, Algorithms and High Performance Computing
- Architecture, systems and networks
- Safe software development

Four strategic axes of impact:

- Information systems for health and ageing well
- Big data
- Ambient socio-technical systems
- Critical embedded systems

Several application areas

- Aeronautics and space industry, telecommunication, multimedia, health, transport, engineering, semantic web, security, handicap

You can skip this ad in 5s

The EU Cybersecurity Strategy

A Play in Two Acts

Act I

EU Cybersecurity Strategy February 2013

Strategic priorities

Achieve cyber resilience

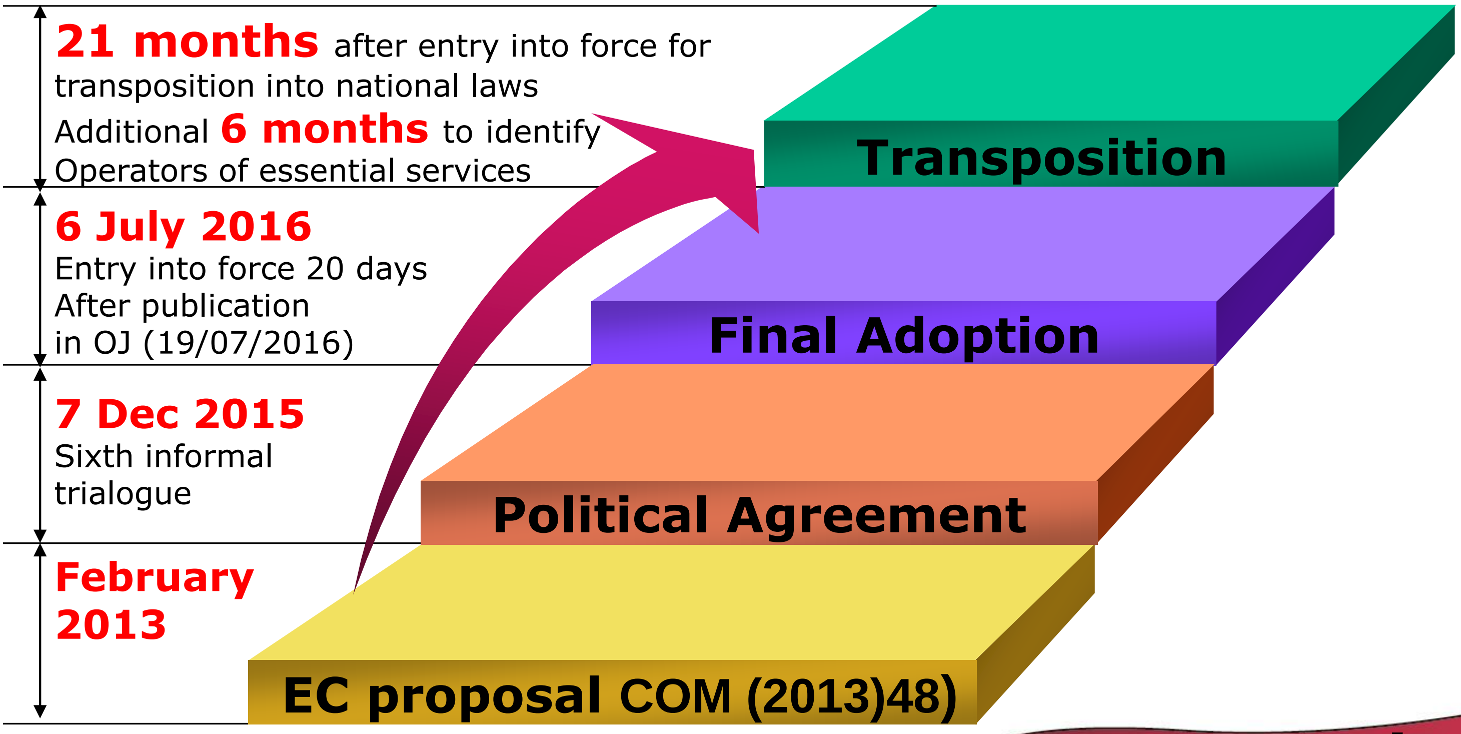
Drastically reduce cybercrime

Develop cyber defence policy

Develop industrial and technological resources

Establish international cyberspace policy

The NIS Directive: from proposal to transposition



21 months after entry into force for transposition into national laws
Additional **6 months** to identify Operators of essential services

Transposition

6 July 2016
Entry into force 20 days
After publication
in OJ (19/07/2016)

Final Adoption

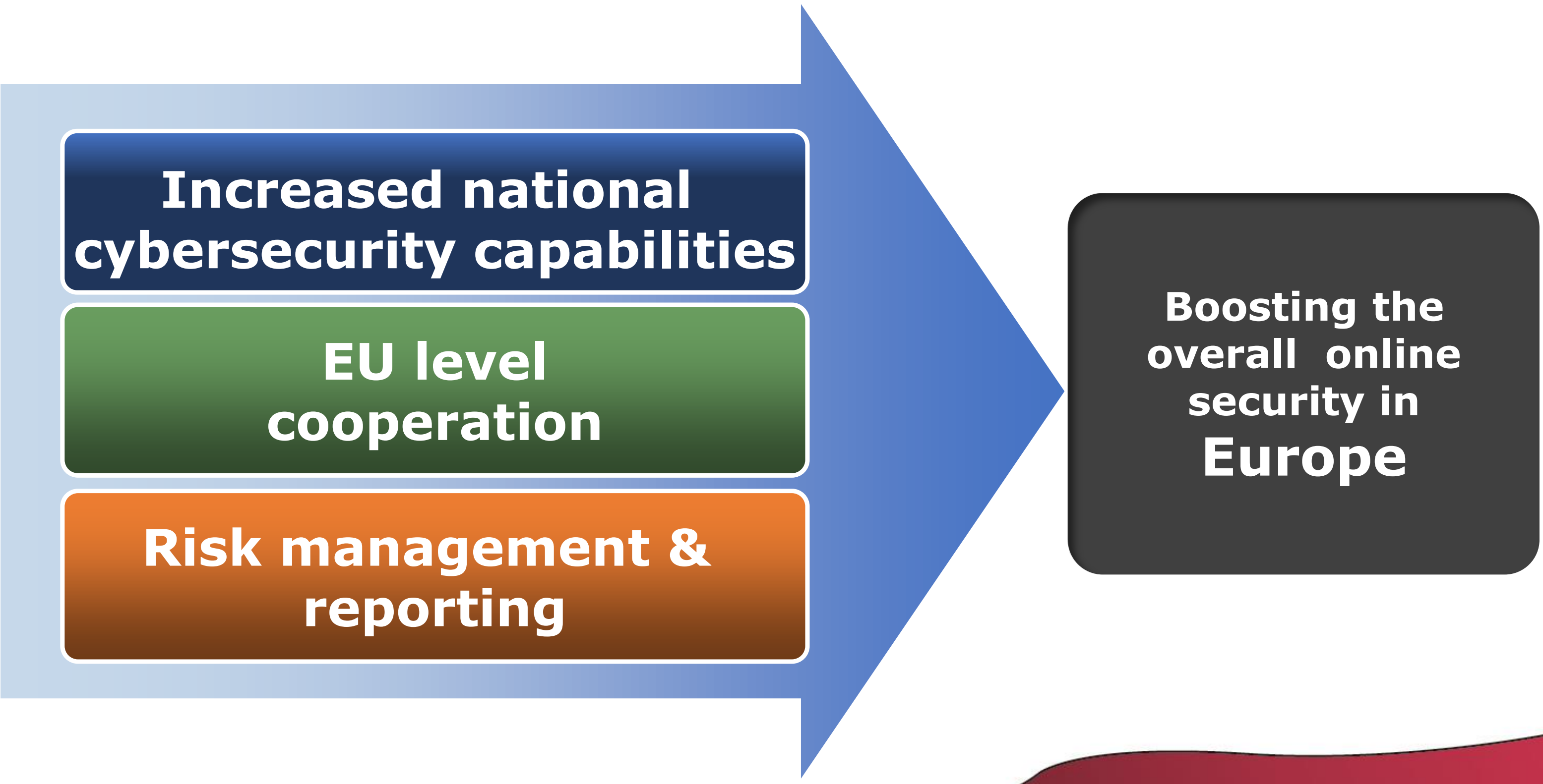
7 Dec 2015
Sixth informal
trialogue

Political Agreement

February 2013

EC proposal COM (2013)48)

July 2016
First comprehensive EU cybersecurity legislation: The NIS Directive



Increased national cybersecurity capabilities

EU level cooperation

Risk management & reporting

Boosting the overall online security in Europe

Capabilities

All Member States to have in place

- NIS National strategy
- NIS competent national authority
- Computer Security Incident Response Team (CSIRT)

Cooperation

Cooperation Group

what: strategic cooperation

who: MSs, EC, ENISA

CSIRT network

what: operational cooperation

who: national CSIRTs,CERT-EU, ENISA

Security and notification requirements

Operators of essential services

- Energy: electricity, gas and oil
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructure
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registers

Security and notification requirements

Digital Services Providers (DSPs)

Online market places

Cloud computing services

Search engines

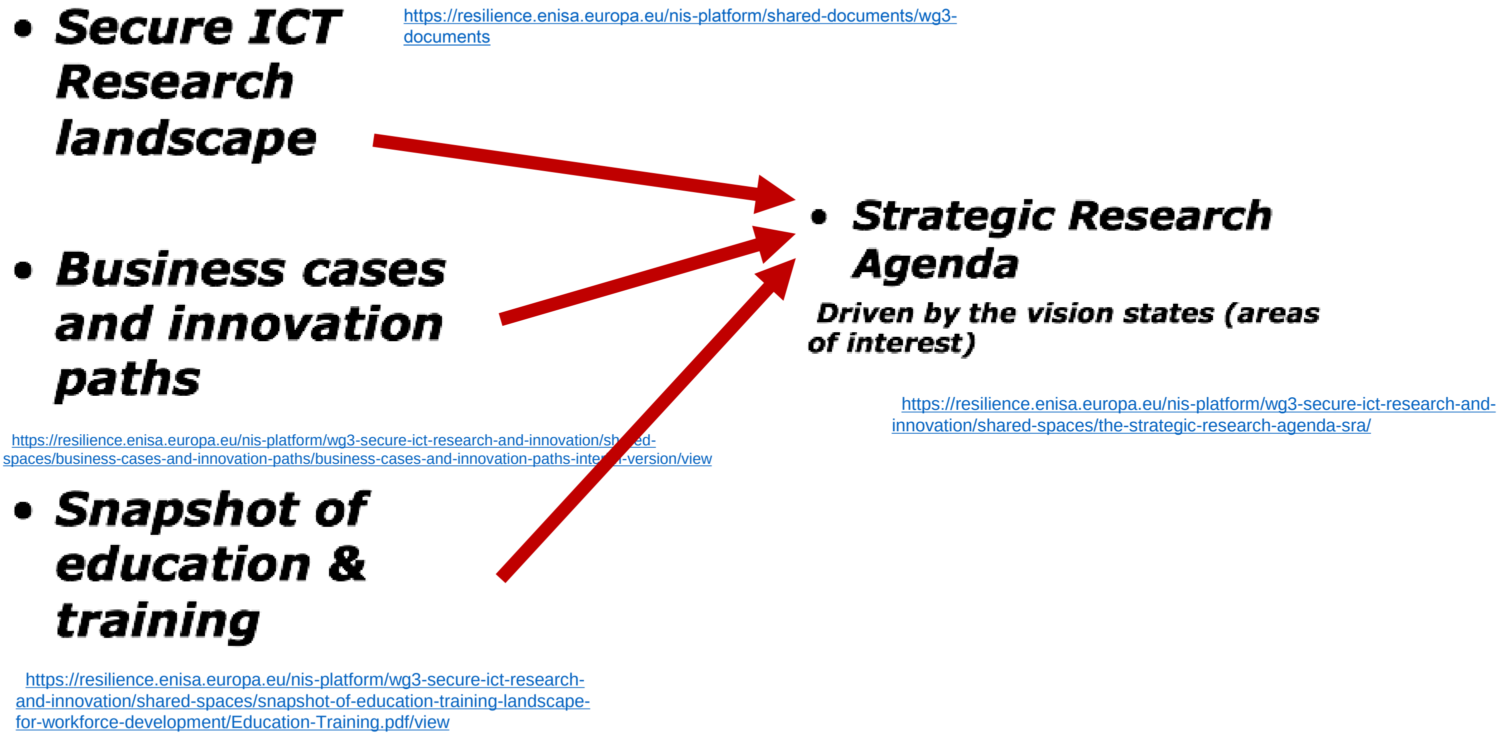
Develop Industrial and Technological Resources: Research Policy

© Dreamstime

The Working Group 3 on Secure ICT Research and Innovation

(Launched September 2013)

WG3 Main deliverables



- ***Secure ICT Research landscape***

https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents

- ***Business cases and innovation paths***

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/business-cases-and-innovation-paths/business-cases-and-innovation-paths-interim-version/view

- ***Snapshot of education & training***

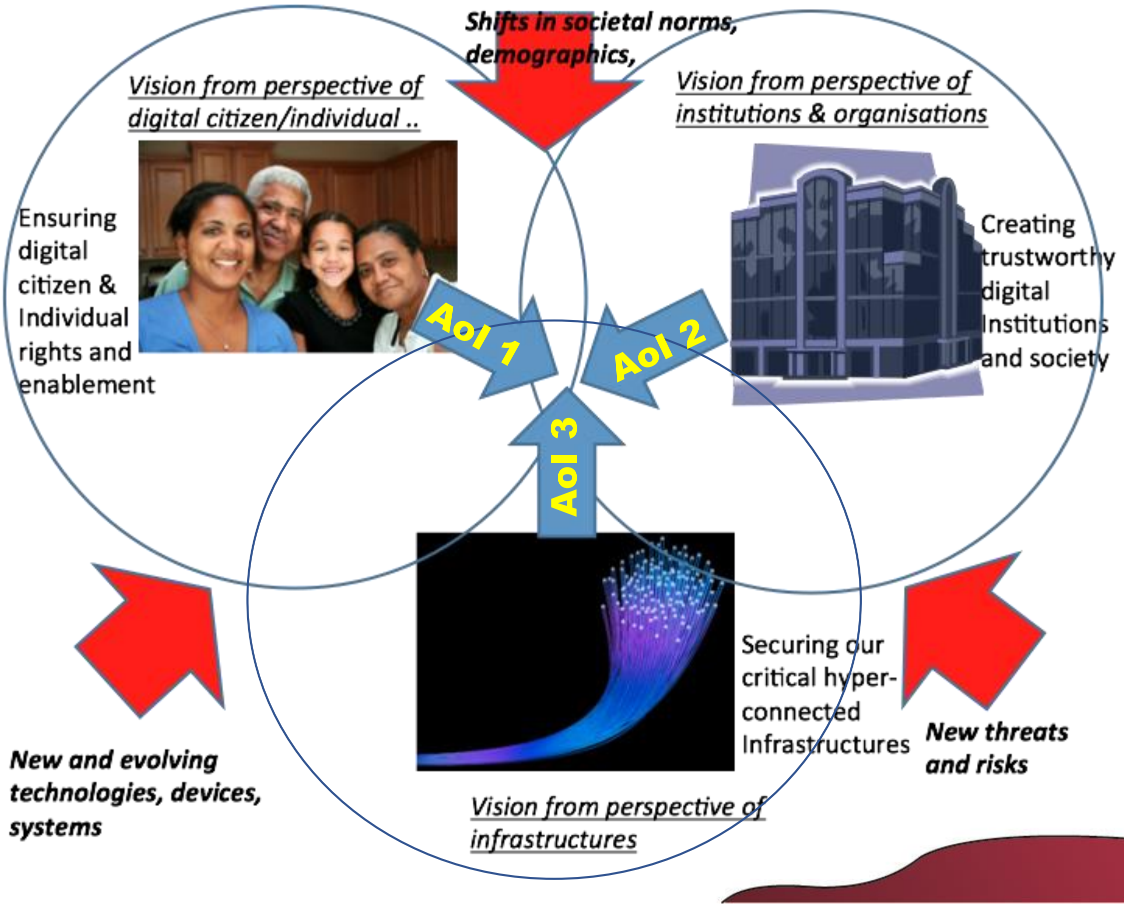
https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/snapshot-of-education-training-landscape-for-workforce-development/Education-Training.pdf/view

- ***Strategic Research Agenda***

Driven by the vision states (areas of interest)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/the-strategic-research-agenda-sra/

Methodology of the Strategic Research Agenda



Shifts in societal norms, demographics,

Vision from perspective of digital citizen/individual ..

Ensuring digital citizen & Individual rights and enablement

Vision from perspective of institutions & organisations

Creating trustworthy digital Institutions and society

Securing our critical hyper-connected Infrastructures

Vision from perspective of infrastructures

New and evolving technologies, devices, systems

New threats and risks

Common focus summary

Fostering assurance

- Security Engineering
- Certification
- Cyber Insurance

Focussing on data

- Data protection
- Data provenance
- Data-centric security policies
- Operations on encrypted data
- Economic value of personal data

Preserving privacy

- Privacy Enhancing Technologies
- Privacy-aware security mechanisms
- ID management

Protecting ICT Infrastructure

- Networks
- Cloud
- Mobile
- IoT, others

Managing cyber risks

- Dynamic, composable risk assessment
- Integrated risk metrics and indicators
- Managing complexity and system evolution

Education and awareness

- Multi-disciplinary focus
- Responsiveness to changes
- End-to-end skill development
- Continuous awareness

Standardization and Interoperability

- Crypto ("everywhere")
- Certification, assurance, risk, security metrics/indicators
- Information sharing

Enabling secure execution

- Secure platforms
- Intrusion Prevention/Detection
- Secure operating Systems

Increasing trust

- Dynamic trust assessment
- Computational Trust Models
- Trust and big data

Achieving user-centricity

- Focus on user centric design and engineering
- Usability of security mechanisms

Contractual Public-Private Partnership

Mobilising public & private resources to boost cybersecurity industry

1.8 € billion for 4-years

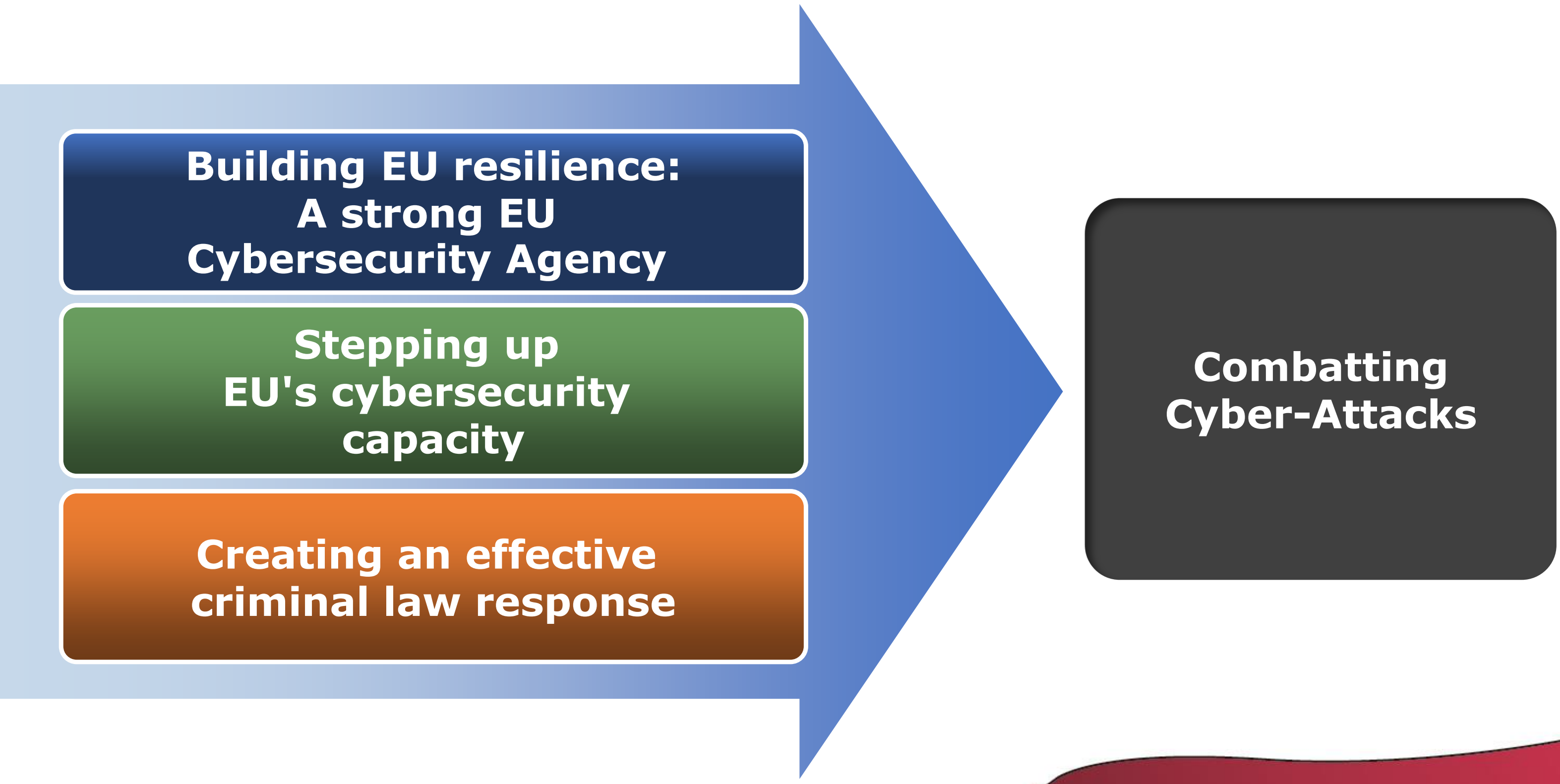
The WG3 SRA: The cornerstone of ECSO

End of Act I

Act II

September 2017:

Renewed Cybersecurity Strategy for the EU



Building EU resilience: A strong EU Cybersecurity Agency

Stepping up EU's cybersecurity capacity

Creating an effective criminal law response

Combatting Cyber-Attacks

A strong EU Cybersecurity Agency

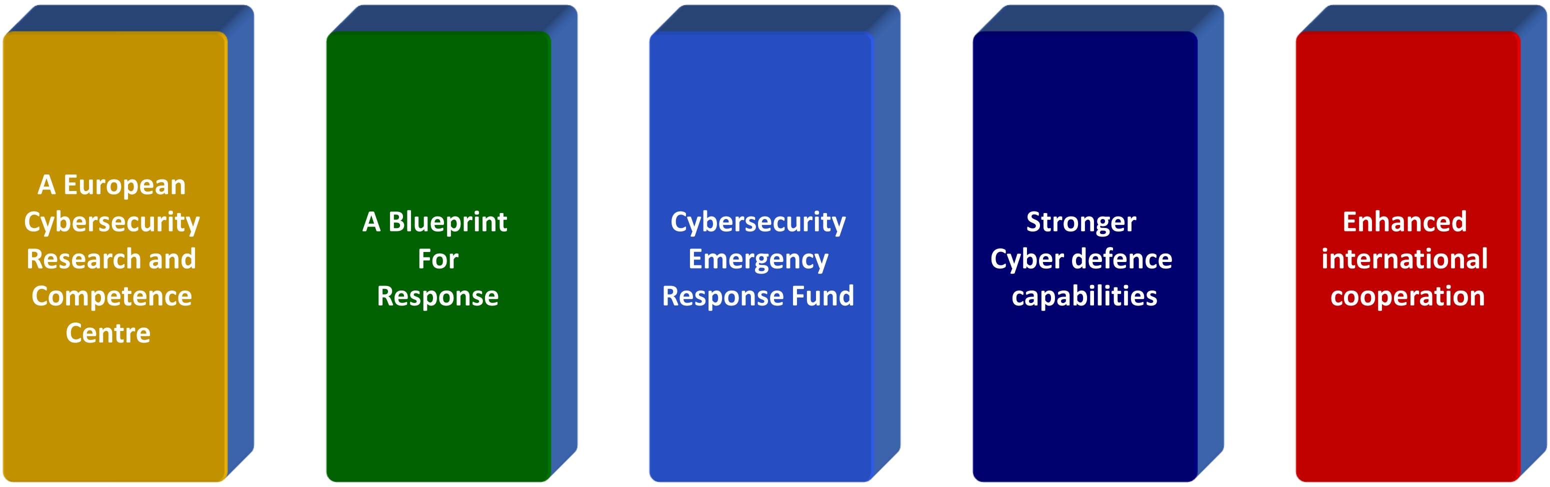
Building up on ENISA's success

Pan-European cybersecurity exercises

Information Sharing and Analysis Centres

EU-wide certification framework

Stepping up the EU's cybersecurity capacity



A European Cybersecurity Research and Competence Centre

A Blueprint For Response

Cybersecurity Emergency Response Fund

Stronger Cyber defence capabilities

Enhanced international cooperation

Creating an effective criminal law response

Against cyber criminals

Detection

Traceability

Prosecution

The End
Or is this just the beginning...?

Thanks for your attention!

- Questions?

Afonso.Ferreira@irit.fr

3.5 Sessions 7 & 8: Legal and Policy

Chair: Stefano Fantin, KU Leuven

This session focused on the European privacy landscape, including as well some background and context, the definition of GDPR, international transfers and NIS Conclusions, and the Japanese Landscape.

3.5.1 European privacy landscape: GDPR and others (Stefano Fantin, KU Leuven)

Below we add the original presentation.

European privacy landscape:

GDPR and others

EUNITY Project meeting
Tokyo, 11/12 October 2017

KU Leuven
Centre for IT & IP Law (CiTiP) – imec

Stefano Fantin

Policy Researcher

www.law.kuleuven.be/citip

Summary

Background and context

What is GDPR?

International transfers and NIS

Conclusions

Japanese Landscape

Background and context

The Digital Single Market

Announced in 2015 with the purpose of fostering the role of the EU as a global leader in the digital economy.

Aims at creating **the right environment and conditions for digital networks and services***.

Developing stronger data protection rules is part of such a policy area.

State of the European Union 2017

(Strasbourg, 13/09/2017)

Two out of five* Commission's priorities for the next year explicitly mention privacy and data protection as a main driver.

The General Data Protection Regulation and EU privacy reform

To start with:

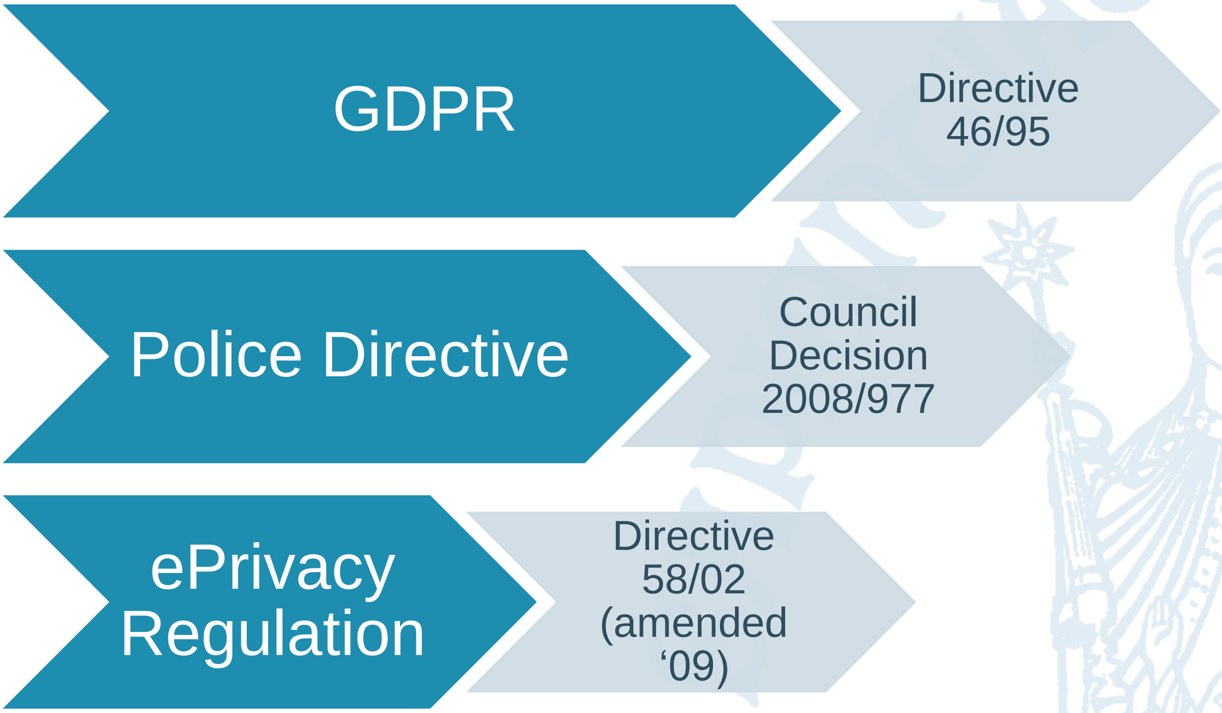
It is not **only** about GDPR!

The new reform is more comprehensive:

- GDPR
- Directive on data protection in the Police and Justice Sector (“Police Directive”)
- Proposal for a new ePrivacy Regulation (currently work in progress)

What do we leave behind?

The three acts of the reform repeal previous legal texts:



GDPR

Directive 46/95

Police Directive

Council Decision 2008/977

ePrivacy Regulation

Directive 58/02 (amended ‘09)

Let’s talk about GDPR

Among the main themes…

- Technology neutral
- Risk-based approach
- Significant increase of sanctions cap
- It is a Regulation!

Application and scope

It will apply as of **May 25th, 2018.**

It will apply to the processing of personal data:

- **by** controllers established in the EU (regardless of whether the processing takes place in the Union or not).
- **of** data subjects who are in the Union by a controller or processor not established in the Union

(GDPR, Art.3)

More protective towards individuals' rights

Right to access

Right to transparent information

Right to rectification

Right to object

Right to be forgotten*

Right to data portability*

(GDPR, Ch. III)

More reactivity required

In the event of a **data breach**, organizations need to:

- Inform the data subject if there’s a high risk
- Notify the breach to the data protection authority
- React promptly (72 hours)

(GDPR, Art. 34)

More accountability and transparency requirements for data controllers

Obligation to keep records of processing activities and to appoint a Data Protection Officer *(Art.30 and 37)*

Stricter rules on consent, lawful processing, data minimization and purpose limitation *(Art. 5, 6 and 7)*

Data protection by design and by default* *(Art.25)*

More security

Demonstrating compliance with GDPR through security of personal data processing and of the systems;

Controllers will have the obligation to implement technical and organizational security measures such as PETs (encryption, pseudonymisation) and other actions aimed at ensuring CIA. *(Art. 32)*

Such measures will have to be duly documented *(R78, 81 and 83)*

Consent by children

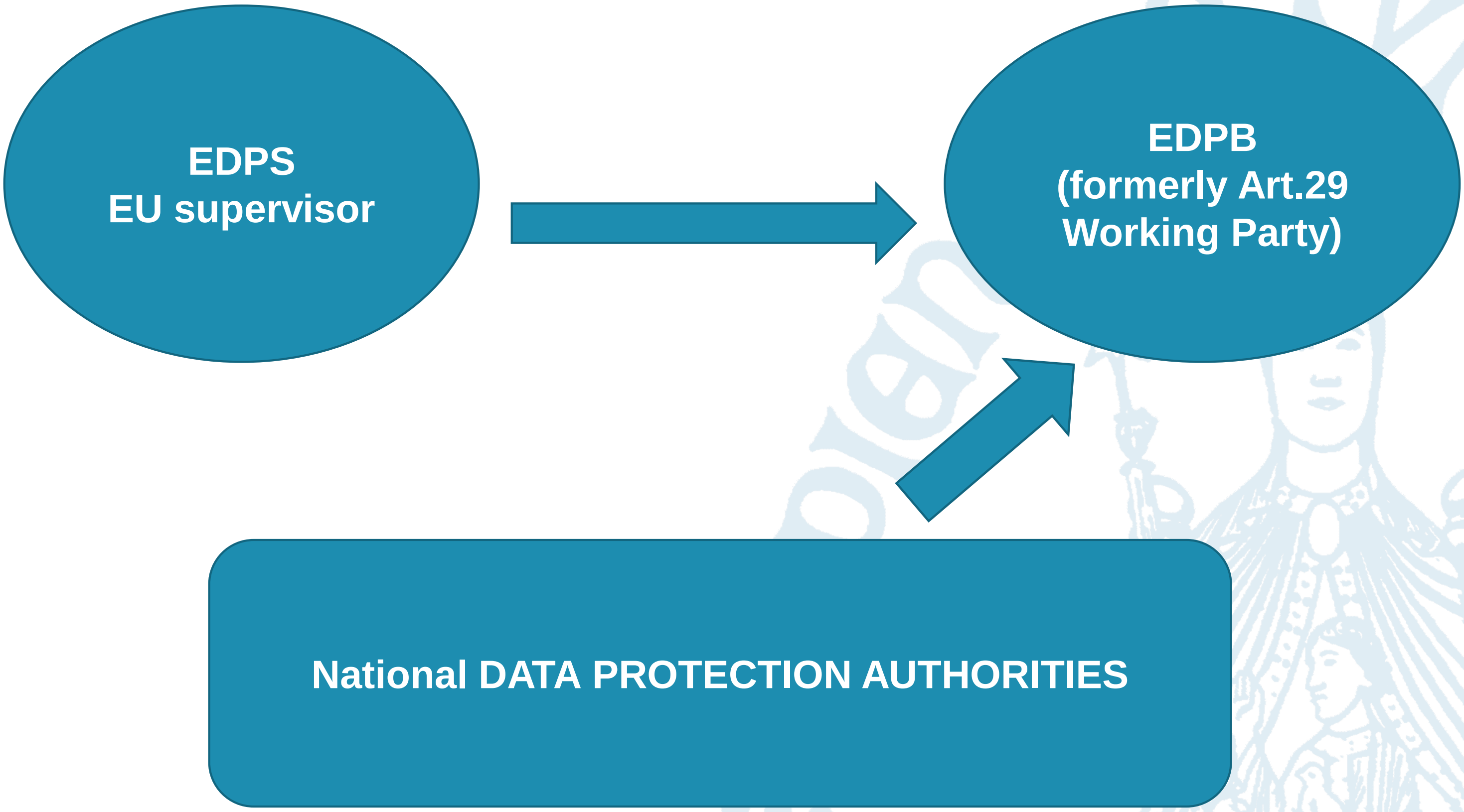
art 8 GDPR

Consent by children under 16 must be given by parent.

BUT Member States may lower the age to 13.

- So far, the UK & Ireland: 13, Spain: 14
- Other MS with plans to change age: Sweden & Poland

Key regulatory bodies: the model as from May 2018



EDPS
EU supervisor

EDPB
(formerly Art.29 Working Party)

National DATA PROTECTION AUTHORITIES

GDPR readiness

Are organizations ready?

Not fully: two examples…

- In the United Kingdom, 33% of Local Government Authorities still don’t do privacy impact assessments (source: ICO, 3/2017).

- Globally, 47% of companies claim that all of their critical data is securely stored (source: NTT, 8/2017).

International transfers

State of play

The EU is **not only** reviewing its internal data protection rules.

↓

This is in fact a crucial period for several relationships with international **partners** with regard to cross-border personal data flows.

Some examples…

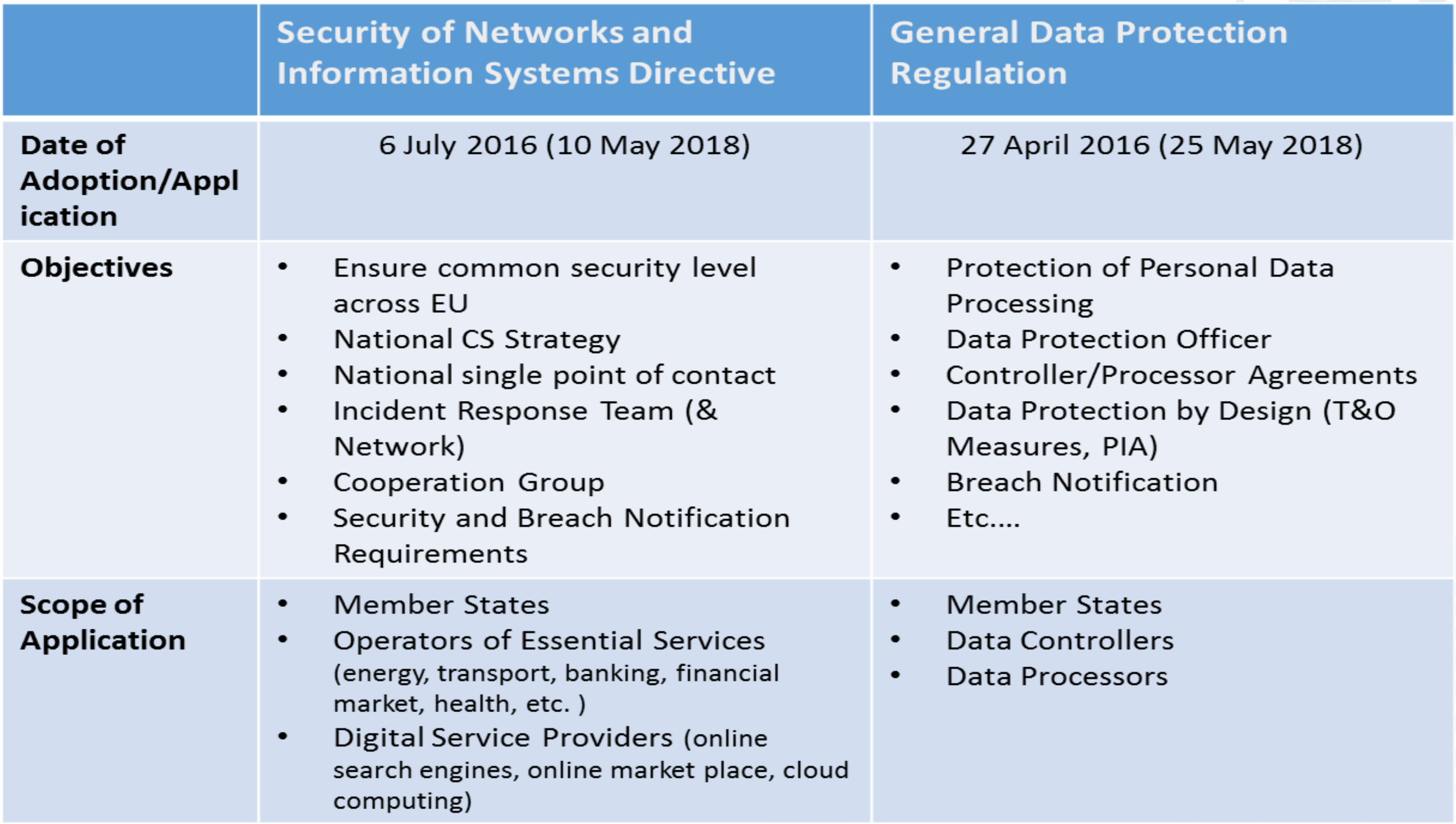
United States: Privacy Shield is suffering delays in its full implementation after its first EU review

United Kingdom: GDPR standards will still apply regardless of its withdrawal from the EU (“Brexit”)

Japan and South Korea: ongoing negotiations with the European Commission aimed at an adequacy decision

GDPR and NIS Directive

GDPR and NIS Directive



	Security of Networks and Information Systems Directive	General Data Protection Regulation
Date of Adoption/Application	6 July 2016 (10 May 2018)	27 April 2016 (25 May 2018)
Objectives	• Ensure common security level across EU • National CS Strategy • National single point of contact • Incident Response Team (& Network) • Cooperation Group • Security and Breach Notification Requirements	• Protection of Personal Data Processing • Data Protection Officer • Controller/Processor Agreements • Data Protection by Design (T&O Measures, PIA) • Breach Notification • Etc….
Scope of Application	• Member States • Operators of Essential Services (energy, transport, banking, financial market, health, etc.) • Digital Service Providers (online search engines, online market place, cloud computing)	• Member States • Data Controllers • Data Processors

Post-Scriptum: the NIS Directive

The different legal instruments used to codify reveal two major considerations:

- Different stages of progress at EU policy level between privacy and cyber security
- Different strategies. Cyber security in the EU requires active intervention by Member States: it aims at boosting cooperation, rather than imposing strict and readily-enforceable rules (different from GDPR).
- Different models: PPPs (public-private partnership) vs EDPB (regulatory/advisory intergov. authority)

Conclusions

GDPR is part of a broader EU policy initiative:

- It is part of the **DSM** strategy
- It is a milestone of a bigger **reform package**
- It influences the setting up of **international** personal data transfers
- It is about protecting **individuals**
- It aims at shifting corporate behaviors into a more transparent **mentality**

EUNITY

Thank you.

Reach out at the following contacts:

Stefano Fantin
stefano.fantin@kuleuven.be

KU Leuven Centre for IT & IP Law
(CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip

3.5.2 Japanese Landscape on Data Protection (Hiroshi Miyashita, Chuo University)

The next presentation by Hiroshi Miyashita included a number of privacy infringement cases in Japan, involving ICT technologies such smart cards, facial recognition or data brokerage. It also compares the EU GDPR and the Japanese Privacy Act, giving a broad picture of the legal system, with some particular insights into the reform of the Privacy Law in Japan and the definition of personal information. The presentation also highlights several current and future challenges, including the process of ensuring the use of personal information under the proper conditions, the strengthening of the protection of personal information (data brokerage measures), the establishment of a personal information protection commission and its supervision, the global harmonization, and data breach cases.

Below we add the original presentation.

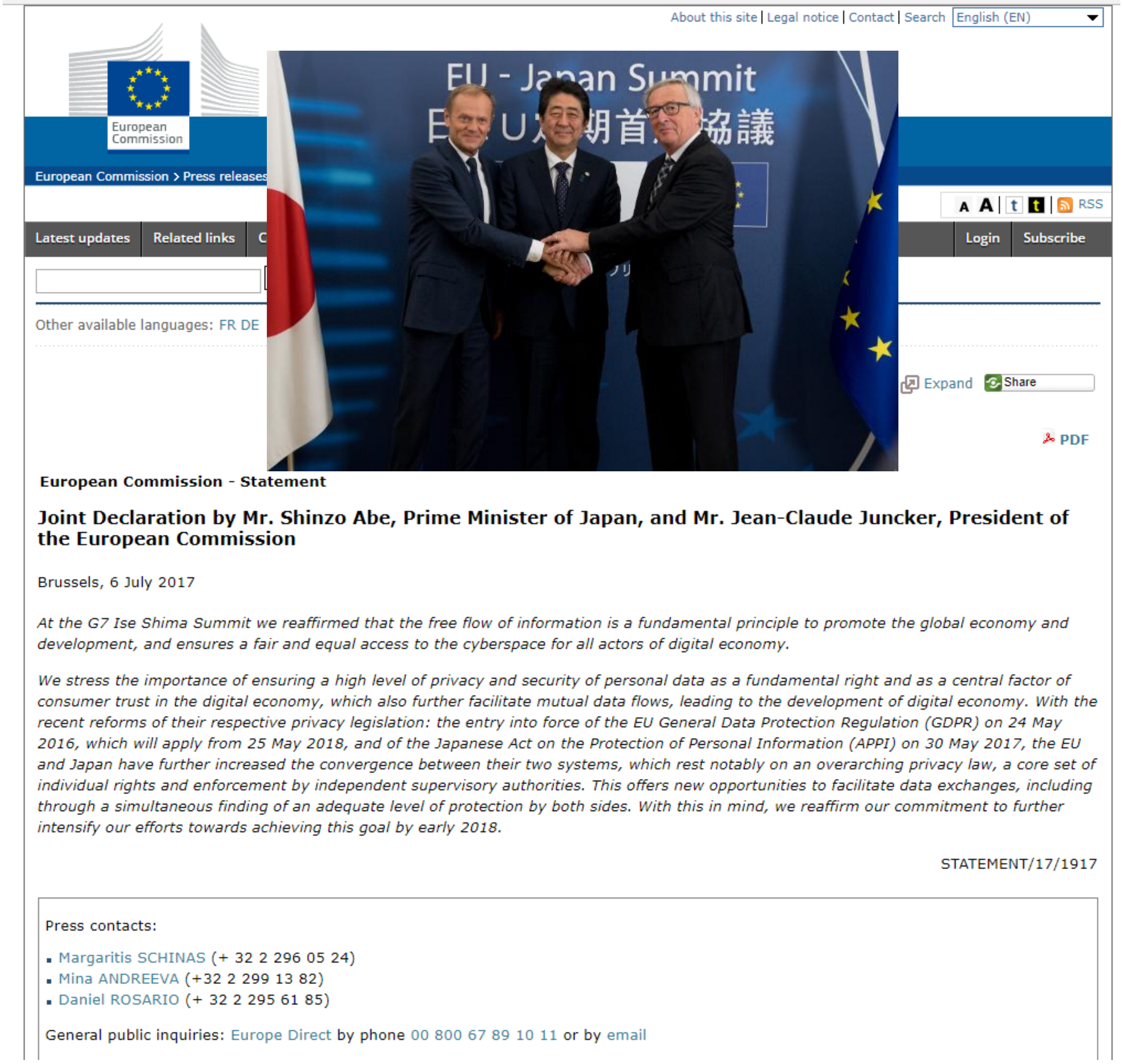
Legal and Policy: Privacy
EUNITY Project Workshop

12 October 2017

Hiroshi Miyashita

Associate Professor of Law (LL.D.)

Chuo University


About this site | Legal notice | Contact | Search | English (EN)
European Commission
European Commission > Press releases
EU - Japan Summit
A A t t RSS
Latest updates
Related links
Login
Subscribe
Other available languages: FR DE
Expand
Share
PDF

European Commission - Statement

Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission

Brussels, 6 July 2017

At the G7 Ise Shima Summit we reaffirmed that the free flow of information is a fundamental principle to promote the global economy and development, and ensures a fair and equal access to the cyberspace for all actors of digital economy.

We stress the importance of ensuring a high level of privacy and security of personal data as a fundamental right and as a central factor of consumer trust in the digital economy, which also further facilitate mutual data flows, leading to the development of digital economy. With the recent reforms of their respective privacy legislation: the entry into force of the EU General Data Protection Regulation (GDPR) on 24 May 2016, which will apply from 25 May 2018, and of the Japanese Act on the Protection of Personal Information (APPI) on 30 May 2017, the EU and Japan have further increased the convergence between their two systems, which rest notably on an overarching privacy law, a core set of individual rights and enforcement by independent supervisory authorities. This offers new opportunities to facilitate data exchanges, including through a simultaneous finding of an adequate level of protection by both sides. With this in mind, we reaffirm our commitment to further intensify our efforts towards achieving this goal by early 2018.

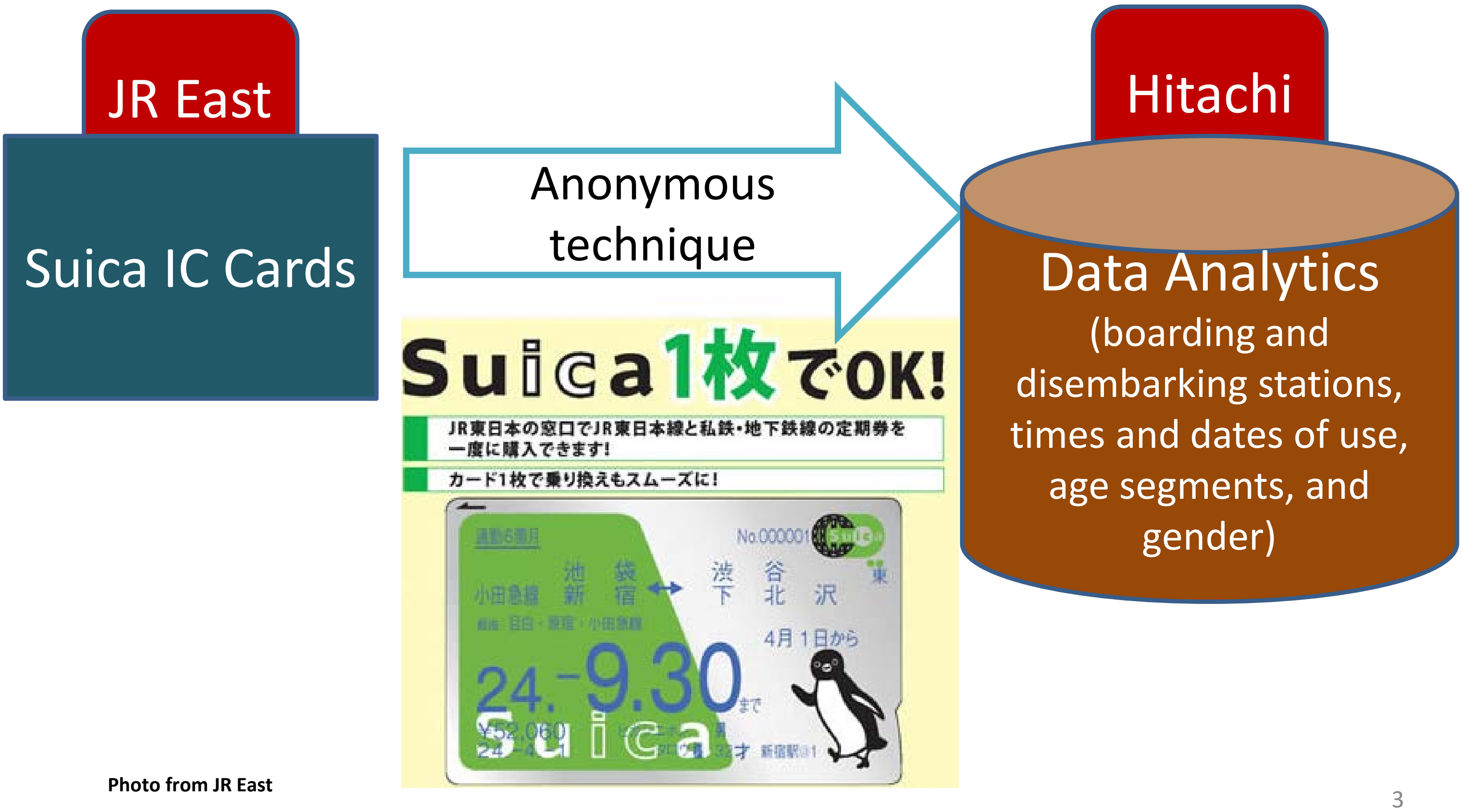
STATEMENT/17/1917

Press contacts:

- Margaritis SCHINAS (+ 32 2 296 05 24)
- Mina ANDREEVA (+32 2 299 13 82)
- Daniel ROSARIO (+ 32 2 295 61 85)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

1-1. IC Public Transportation Cards sold in an Anonymous Form



JR East

Suica IC Cards

Anonymous technique

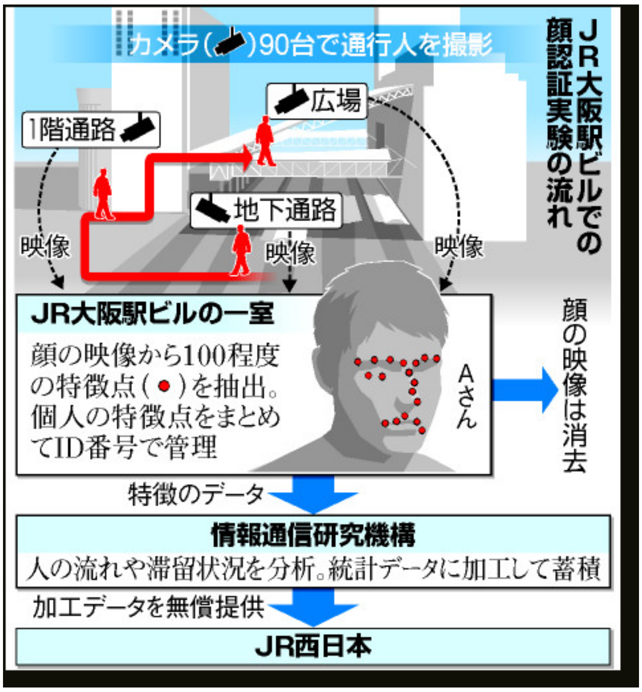
Hitachi

Data Analytics (boarding and disembarking stations, times and dates of use, age segments, and gender)

Suica1枚でOK!
JR東日本の窓口でJR東日本線と私鉄・地下鉄線の定期券を一度に購入できます!
カード1枚で乗り換えもスムーズに!
4月1日から
24.-9.30
Suica

Photo from JR East

1-2. Facial Recognition and CCTV in Osaka Station



顔の映像から100程度の特徴点(●)を抽出。個人の特徴点をまとめてID番号で管理

人の流れや滞留状況を分析。統計データに加工して蓄積

National Institute of Information and Communications Technology prepared for the experiment on the facial recognition CCTVs, but canceled in March 2014.

Photos from Asahi Newspaper, January 6, 2014

1-3. Data Broker
35 million personal information sold

- 35.04 million costumer personal data (name, birthdate, address, email address ect (no credit card information)) in Benesse Corp. was sold by the employee to the 3 data brokers.
- Benesse submitted the report to the Ministry of Economy, Trade and Industry (July 2014/ October 2014), which was appointed by the Prime Minister to investigation.
- Benesse voluntarily paid 500 yen gift cards.
- Class action lawsuit was brought by several parents.

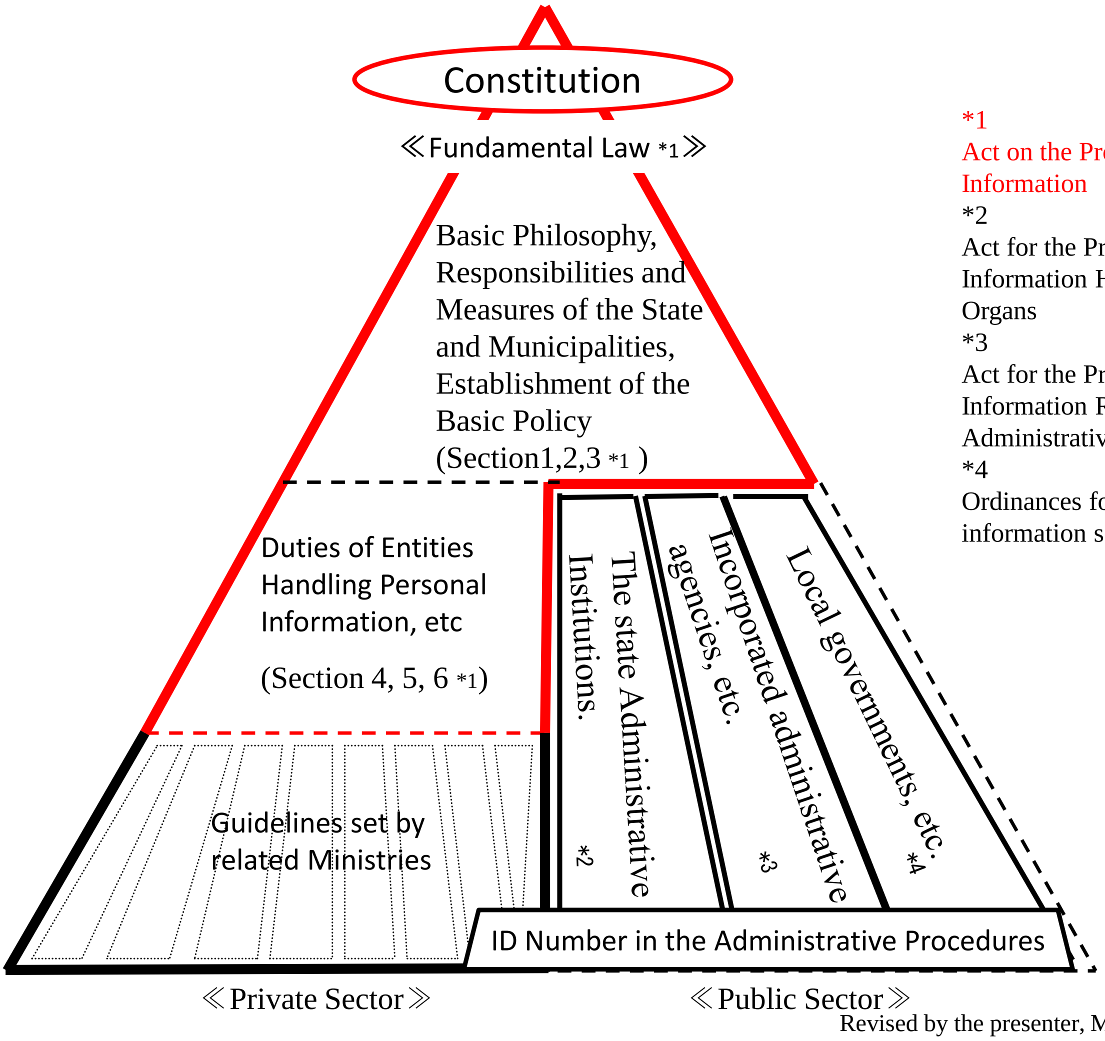
Photo by Asahi Newspaper

Press Release: Notice and Apology Regarding Leakage of Customers' Personal Information in English
http://www.benesse-hd.co.jp/en/about/release_20140709.pdf
http://blog.benesse.ne.jp/bh/en/ir_news/m/2014/09/10/uploads/news_20140910_en.pdf

Comparison: EU GDPR and the Japanese Act

GDPR		Japanese Act
extraterritorial (offering goods or services / monitoring behaviour)	territorial scope	extraterritorial (offering goods or services)
any information relating to an identified or identifiable natural person / psedonymisation / genetic, biometric data	definition	information relating to a living individual which a specific individual can be identified (easily collated with other information)/ personal identifier / anonymous processing information
lawfulness of processing / conditions for consent/ conditions of child's consent / special categories of personal data	principles	information with special care
Information to data subject / access, rectification, erasure (right to be forgotten) / data portability / profiling	rights	disclosure, rectification, cease / explanation of reason (provided in the obligations chapter)
data protection be design / representatives / processing records / data breach notification & communication / impact assessment / data protection officer / codes of conduct	obligations	purpose limitation / proper collection / security / supervision over employee and trustee (processor) /transfer to the third party /opt-out notification / records keeping of sending and receiving / anonymous processing information
adequacy / appropriate safeguards / binding corporate rules / derogations	international transfer	equivalence / commission's rule or consent
independence / investigative, corrective & advisory powers / lead authority / cooperation and consistency (one-stop shop) / European Data Protection Board	independent supervisory authorities	Independence / order, recommendation, guidance & report collection, onsite inspection / delegation of powers to the competent Minister in an emergence / accreditation
lodge a complaint / effective judicial remedy / compensation and liability	remedies, liability	fee for disclosure exhaustion & two weeks waiting requirement
up to 20,000,000 EUR (10,000,000EUR) or 4 % (2%)of annual turnover	penalties	database stealing: up to 500,000 yen (4,200 EUR) or one year imprisonment failure of recommendation, order & report : up to 300,000 yen or six months imprisonment
freedom of expression / official documents / employment / archiving, scientific, historical purposes	specific situation	exemptions for press / writer / academic institution / religious body

Picture of the Legal System



Constitution

≪Fundamental Law *1≫

Basic Philosophy, Responsibilities and Measures of the State and Municipalities, Establishment of the Basic Policy (Section1,2,3 *1)

Duties of Entities Handling Personal Information, etc

(Section 4, 5, 6 *1)

Guidelines set by related Ministries

The state Administrative Institutions. *2

Incorporated administrative agencies, etc. *3

Local governments, etc. *4

ID Number in the Administrative Procedures

≪Private Sector≫

≪Public Sector≫

*1
Act on the Protection of Personal Information

*2
Act for the Protection of Personal Information Held by Administrative Organs

*3
Act for the Protection of Personal Information Retained by Incorporated Administrative Agencies, etc.

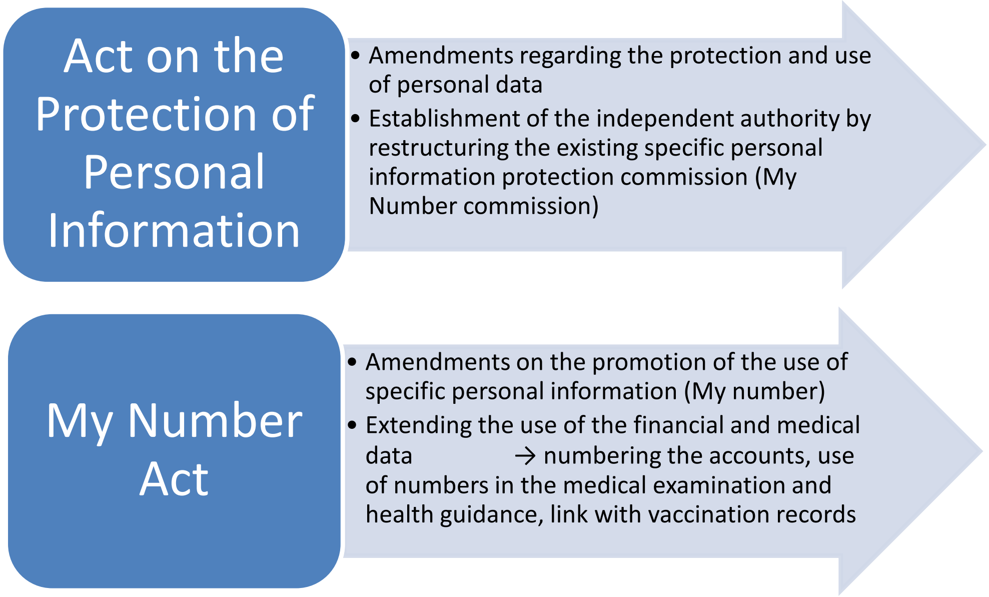
*4
Ordinances for the protection of personal information set by each municipalities

Revised by the presenter, Materials by Consumer Affairs Agency

2-1. Points of the Privacy Law Reform in Japan

- 2007/6 The Quality-of-Life Council decided not to amend the law
- 2011/8 The Consumer Commission pointed out the challenges on privacy
- 2013/12 The Law Reform Plan adopted by the Cabinet (IT Strategic Headquarter)
- 2014/6 Policy Outline of the Institutional Revision for Utilization of Personal Data
- 2014/12 The Amendment Outline of the Bill
- **2015/3 The Cabinet Decision on the Amendment on the Acts**

Purpose of Law Reform: To create innovation and new services and realize the promotion of safety of the people by protecting personal information and fostering the use of personal data and to extend the use of My Numbers administration



Act on the Protection of Personal Information

- Amendments regarding the protection and use of personal data
- Establishment of the independent authority by restructuring the existing specific personal information protection commission (My Number commission)

My Number Act

- Amendments on the promotion of the use of specific personal information (My number)
- Extending the use of the financial and medical data → numbering the accounts, use of numbers in the medical examination and health guidance, link with vaccination records

Points on the Amendments

1. **Clarification on the definition of personal information**

- Adding certain categories such as facial recognition data
- Sensitive data – opt-out prohibition

2. **Ensuring the use of personal information under the proper conditions**

- Use of anonymous data
- Personal information policy

3. **Strengthening the protection of personal information (data broker measures)**

- Ensuring traceability (obligation of checking and recoding the transfer)
- Criminal sanction of processing under illegitimate purposes

4. **Establishment of Personal Information Protection Commission**

- Independent Personal Information Protection Commission (restructuring current Specific Personal Information Protection Commission) with on-site inspection

5. **Global harmonization**

- Extra-territorial scope and information sharing with the foreign authorities
- Data transfer restriction to the third countries

6. **Other issues**

- Registration of opt-out and publication by the Commission
- Relaxation of the purpose limitation requirement
- SME: the Act should apply to businesses which handle no more than 5,000 personal information

59 Articles with 6 chapters → 78 Articles with 7 chapters

Clarification on the definition of personal information

- Personal Information (Art. 2-1) Information that is identifiable of the individuals by names, birthdate and the other descriptions including the documents, drawings, electromagnetic records or voices, motions and the other means

- Personal Identifiers (Art. 2-2) letters, numbers, marks and the other codes which fall in 1) characteristics of the part of body for the purpose of use of electronic machines, which is identifiable for the individual or 2) the individual user or purchaser designated, written, or recorded in the service use or the sales

  * IP address, device ID, mobile phone numbers, customer ID – not generally fall in

- Sensitive Personal Information (Personal Information with the Special Care) (Art. 2-3)
  Personal information including race, religious brief, social status, medical records, criminal offences, the facts of victims of criminal offences, which require the special care for not causing the injurious discrimination, bias and the other disadvantages.

Ensuring the use of personal information under the proper conditions

- Anonymous Processing Data (Art. 2-9) – personal information which is not able to identify the individual and is not able to restore by 1) deleting the descriptions containing the personal information or 2) deleting all the personal identifiers containing the personal information

- Anonymous Processing Information Entities (Art. 2-10) – Entities that use the anonymous processing database (easily searchable for the anonymous processing information in the aggregation of information by the electronic machines)

*The expert technological working group report (10 December 2013)

There is no generic means to process any personal information into the identifiable non-specified information or non-identifiable non-specified information. Even in the case of anonymous measures for providing the third party, it is impossible to always delete the identification and specification and to make general standards on the anonymous measures.

Strengthening the protection of personal information (data broker measures)

- Obligation to Keep Records (Art. 25) Personal information handling entities must keep the records of date of providing personal data and names of its third party based on the Commission's rule. This record must retain the period which the Commission decides.

  1 year: repeatedly and continuously / contractual proof
  3 years: except for the above

- Check of Receiving Information (Art. 26) – When the personal information handling entities receive the information from the third party, the entities must check 1) names and address (and the representatives of the corporation) and 2) the context of acquiring the personal data. The entities must keep the records of the dates of receiving personal data. This record must retain the period which the Commission decides.

- Criminal Sanction on the Illegal Database Provision (Art. 83) Personal Information handling entities or its employees shall be punished up to 1 year imprisonment and 500,000 yen fine when he or she provides or steals the personal information database in his or her business use for the purpose of acquiring an illegal profit.

Establishment of Personal Information Protection Commission

- Chapter 5
- **Establishment** (Art.50)- PIPC shall be established under the jurisdiction of the Prime Minister (based on Art 49-3 Establishment of the Cabinet Office Act)
- **Mission** (Art.51) – ensure the proper handling of personal information, taking into account the effective use of personal information
- **Task** (Art. 52) – 1) make and promote the Basic Policy

  2) supervision on the use of My Number

  3) impact assessment of my number

  4) public relations and education

  5) necessary study

  6) international cooperation

  7) other tasks provided by laws
- **Independency** (Art. 53) – The President and the Commissioners of the Commission shall act independently
- **Organisation** (Art.54) – Commission shall consist of the President and 8 Commissioners (4 part-time); PM will appoint with consent of both Houses in the Diet; Commissioners shall include experts from academia, consumer organisation, IT technologist, My number administration, businesses, and local organisation
- **Term** (Art. 55)- 5 year; can be reappointed
- **Guarantee of Status** (Art. 56)- President and Commissioners will not dismissed except for insolvency, action against this Act, imprisonment, and being mentally or physically disabled
- **Expert Committee** (Art. 60)- Commission can establish the Expert Committee (part-time) to the examine the technical issues
- **Secretariat** (Art. 61) – Commission shall establish the Secretariat
- **Report to the Diet** (Art. 70)- Commission shall annually report the implementation status to the Diet
- **Penalty** (Art. 73) – Commissioners shall be penalized up to 2 year imprisonment or 1 million yen if he or she leaks the confidential matters.

Supervision by Personal Information Protection Commission

- Chapter 4 –Section 3
- **Report and On-Site Inspection** (Art. 40)- Commission shall have powers to submit reports or materials and conduct on-site inspection against the personal information operators and the anonymous information operators.
- **Instruction and Advice** (Art.41)- Commission can make instruction and advice
- **Recommendation and Order** (Art. 42) – Commission can make recommendation and order
- **Limits of Powers** (Art. 43) – Commission shall not interfere with freedom of expression, academic freedom, freedom of religion and freedom of political activities.
- **Delegation of Powers** (Art.44) – Commission can delegate its powers to the Competent Minister in emergent and selective cases. The Competent Minister must report of the result to the Commission.
- **Request from the Competent Minister** (Art. 45) – Competent Minister can request the Commission to take necessary measures

Global Hamonisation

International Harmonisation (Art. 6) – Government shall take necessary measure to ensure the international harmonisation with the foreign governments

Data Transfer Restriction (Art. 24) – Personal data cannot be transferred to the third party (except for those which prepares for the system in the Commission's standard) foreign countries (except for those which the Commission found the equivalent level of protection of our country in the protection of personal rights and interest). This restriction does not apply when obtaining the consent of data subjects.

Information Sharing with the Foreign Counterparts (Art. 78) - Commission can provide information to the foreign counterparts when it is necessary for conduct its tasks. Information sharing is limited to use for the purpose of conducting the task of the foreign counterparts and not to use for the criminal investigations unless Commission's approval.

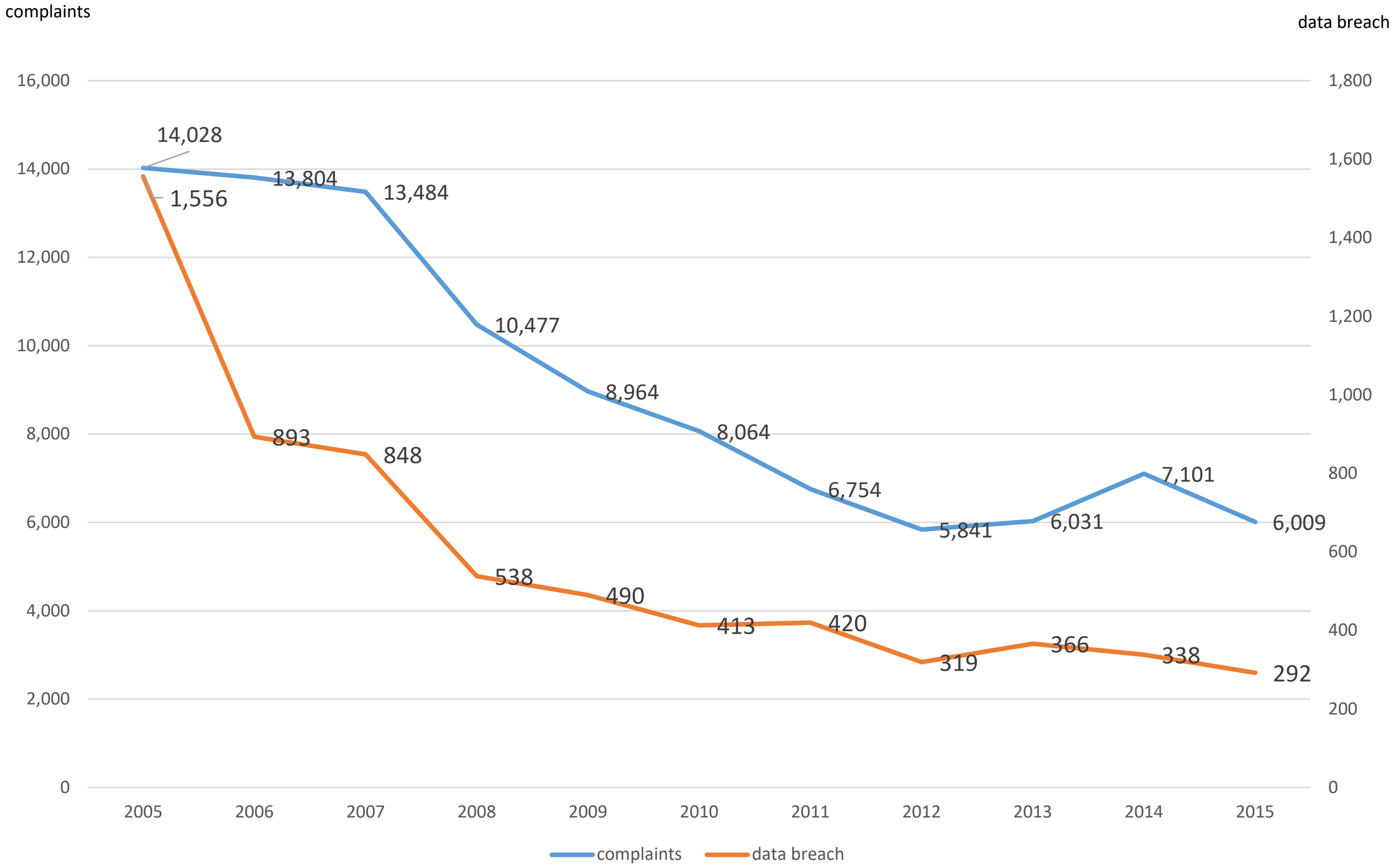
Other Issues

- Opt-out Notification and Publications (Art 23-4) Personal information handling entities can use opt-out only when it notifies or publicises the data subjects and notifies to the Commission. The Commissions shall publicise the items of the opt-out notifications

- Purpose Limitation (Art 15) duly relevant to the original purpose in changing the purpose; “duly ” was erased

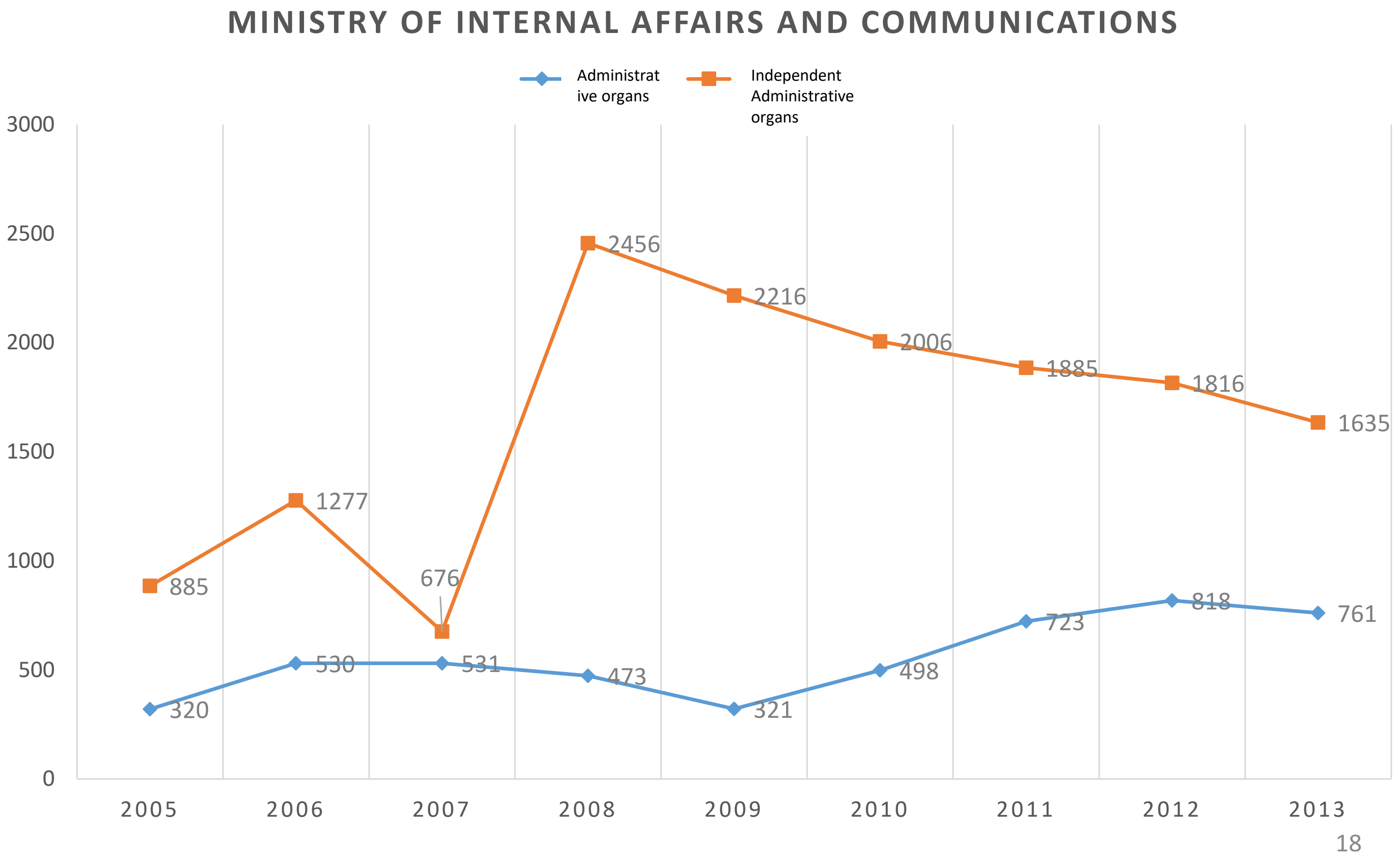
- Small-Medium Enterprise Exemptions – The existing 5,000 personal data requirement will be abolished

Data Breach Cases in the Private Sector



Source from the annual report of Personal Information Protection Commission

Data Breach Cases in the Public Sector



Cyber Attack Case

Japan Pension Service (June 2015)

- The national pension system hacked: 1.25 million items of personal information stolen (pension IDs, names, addresses and birth dates)

  - 8/5/2015 Two target emails sent to two open email addresses

  - 18-19/ 5/2015 A series of target emails attack (101 emails)

  - 20/5/2015 Target emails (5 emails)

Ad hoc committee's report
(21 August 2015)

1) A lack of preparation of the human and organizational measures(rotation personnel change)

2) A lack of information security system (unclear responsibility and power in an emergency)

3) A lack of sense of personal information protection (no passwords for the shared folders)

4) Inadequate risk assessment and audit

Legal and Policy: Privacy
EUNITY Project Workshop

12 October 2017

Hiroshi Miyashita

Associate Professor of Law (LL.D.)

Chuo University

3.6 Session 9: Research & innovation

Chair: Sotiris Ioannidis, FORTH

This session 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. It 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. Below we add the presentation by Dr. Sotiris Ioannidis.

EUNITY Project Workshop [Cybersecurity and Privacy Dialogue between Europe and Japan]

Session 9: Research and Innovation

Dr. Sotiris Ioannidis

FORTH

What is EUNITY

- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan

Contents

- Roadmaps and collaboration actions/projects
- Research problems and EU agenda on cybersecurity and privacy
- Mechanisms for realization
- Education

Contents

- Roadmaps and collaboration actions/projects
- Research problems and EU agenda on cybersecurity and privacy
- Mechanisms for realization
- Education

Prior work: FORWARD

- Research Challenges
  - The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of Cyber-threats defenses, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures
- Research Roadmap
  - The **FORWARD Whitebook** is the main result of the project. It contains detailed and concrete scenarios of how adversaries can leverage the emerging threats identified by the FORWARD project working groups to carry out their malicious actions. These scenarios illustrate future dangers and provide arguments to policy makers that are needed to support research in critical areas

SEVENTH FRAMEWORK PROGRAMME
Information & Communication Technologies
Secure, dependable and trusted Infrastructures

COORDINATION ACTION
Grant Agreement no. 216331

forward

Managing Emerging Threats in ICT Infrastructures

Deliverable D3.1:
White book: Emerging ICT threats

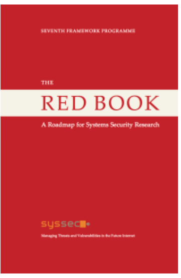
Contractual Date of Delivery	31/12/2009
Actual Date of Delivery	17/01/2010
Deliverable Security Class	Public
Editor	FORWARD Consortium
Contributors	FORWARD Consortium
Quality Control	FORWARD Consortium

The FORWARD Consortium consists of:

Technical University of Vienna	Coordinator	Austria
Institut Eurecom	Principal Contractor	France
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
ICS/FORTH	Principal Contractor	Greece
IPP/BAS	Principal Contractor	Bulgaria
Chalmers University	Principal Contractor	Sweden

Prior work: SYSSEC

- Research Challenges for Europe and India
  - a **Network of Excellence** in the field of Systems Security for Europe to play a leading role in changing the rules of the game.
- Research Roadmap
  - The **SysSec Red Book** is a Roadmap in the area of Systems Security, as prepared by the SysSec consortium and its constituency. For preparing this roadmap a Task Force of young researchers with proven track of record in the area was assembled and collaborated with the senior researchers of SysSec



SEVENTH FRAMEWORK PROGRAMME

THE

RED BOOK

A Roadmap for Systems Security Research

syssec

Managing Threats and Vulnerabilities in the Future Internet

Prior work: EUINCOOP

- Research Challenges for Europe and India
  - describes the computing systems research challenges that are shared by Europe and India, along with the trends, strategies and opportunities in each region that are behind the research challenges.
- Research Roadmap
  - summarizes the initial research report based on analysis, experts opinion and first brokerage event with further review and feedback from the community of experts

Prior work: CONNECT2SEA

- Report on horizontal pilot actions, with assessment and feedback to the policy recommendations toward SEA-EU cooperation in Cybersecurity.

Prior work: NECOMA

NECOMA

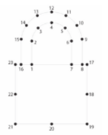
- NECOMA was a EU-JP collaboration project. It addressed the aspect of
  - **data collection,**
  - **threat data analysis and**
  - **develop and demonstrate new cyberdefense mechanisms**.

The goals were achieved by leveraging past and current work on the topic with the goal to expand these existing mechanisms and orient them towards threat data analysis.

Ongoing work: CYBERSURE

- **CyberSure** is a programme of collaborations and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance policy for cyber systems. The purpose of creating such policies will be to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches in them.

Ongoing work: PROTASIS



PROTASIS: Connecting the dots...

- PROTASIS aims to expand the reach of SysSec to the international community via a joint research program in the area of **Systems Security** spearheaded by the need to develop a computing infrastructure that will be trusted by the citizens and the organizations they use it.

Contents

- Roadmaps and collaboration actions/projects
- Research problems and EU agenda on cybersecurity and privacy
- Mechanisms for realization
- Education

Horizon 2020: Work Programme 2018-2020 (draft) (1/2)

- Indicative calls addressing directly the Security&Privacy aspect (pre-analysis results)
  - ICT-08-2019: Security and resilience for collaborative manufacturing environments
  - SU-ICT-01-2018: Dynamic countering of cyber-attacks
  - SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems
  - SU-ICT-03-2020: Advanced cybersecurity and digital privacy technologies
  - SU-ICT-04-2019: Quantum Key Distribution testbed
  - EUJ-01-2018: Advanced technologies (Security/Cloud/IoT/BigData) for a hyper-connected society in the context of Smart City

Horizon 2020: Work Programme 2018-2020 (draft) (2/2)

- Indicative calls including the Security&Privacy (S&P) aspect (pre-analysis results)

  - ICT-01-2019: Computing technologies and engineering methods for cyber-physical systems of systems (S)
  - ICT-02-2018: Flexible and Wearable Electronics (S&P)
  - ICT-07-2018: Electronic Smart Systems (ESS) (S&P)
  - ICT-09-2019-2020: Robotics in Application Areas (S&P)
  - ICT-10-2019-2020: Robotics Core Technology (S)
  - ICT-15-2019-2020: Cloud Computing (S&P)
  - ICT-18-2018: 5G for cooperative, connected and automated mobility (CCAM) (S)
  - ICT-20-2019-2020: 5G Long Term Evolution (S)
  - ICT-27-2018-2020: Internet of Things (S&P)

Contents

- Roadmaps and collaboration actions/projects
- Research problems and EU agenda on cybersecurity and privacy
- Mechanisms for realization
- Education

Means

- Structured workshops – networking events (like this one) ☺
- Strategic research agenda analysis from roadmapping projects
- European Commission open calls and directives (e.g H2020, GDPR etc)

Workshops

- Participants
  - Representatives of EUNITY

  +

  - Cybersecurity experts from industry, academia and CERTs seeking cooperation between EU and JP

  +

  - Representatives of policy makers

Roadmap: Methodology/Sources

- Identification of data
  - EU and JP Cybersecurity Work Programmes/priorities/initiatives
- Preliminary analysis of data
- Creation of a “cybersecurity matrix“ for EU and JP priorities

- Sources
  - Horizon 2020 Work Programme
  - Project roadmaps and research directions
  - Major research centers priorities
  - Activities of SMEs, CSIRTs, LEAs
  - Long-term research programmes on national and international levels

Research Roadmap Elements

Motivations

- Context
- Challenges or needs
- Targets or planned achievements

Technologies

- Structure
- Definition or descriptions
- Desired Advances

Actions

- Stakeholders
- Policies
- Programmes
- Initiatives

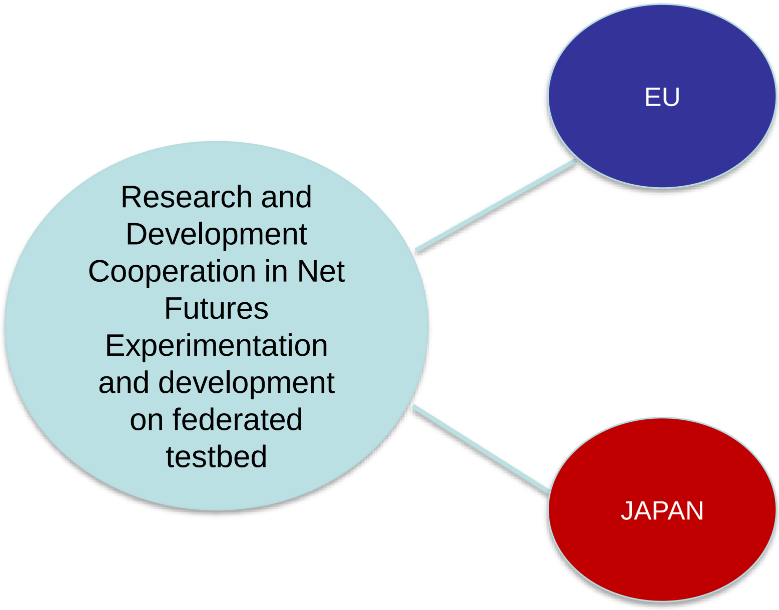
Consensus Process

- Committees
- Collaborative Projects
- Networks of Excellence

JP-EU priorities comparison

- EU cybersecurity priorities/calls/initiatives that seem to match with some of the JP priorities
- JP Priorities **not** Matched with EU Priorities
- JP priorities that do not clearly fit with EU ones

Comparison example



Research and Development Cooperation in Net Futures Experimentation and development on federated testbed

EU

JAPAN

Comparison: Cybersecurity priorities (1/2)

EU	JAPAN
• European Research Infrastructures, and e-Infrastructures • Information and Communication Technologies • EU-Brasil/Japan • Nanotechnologies, Advanced Materials, Advanced Manufacturing and Processing, and Biotechnology • Innovation in SMEs • Societal Challenges - Secure, Clean and Efficient Energy • Smart, Green and Integrated Transport • Secure societies – Protecting freedom and security of Europe and its citizens • Call – Digital Security: Cybersecurity, Privacy and Truste	• Priority 1 • Priority 2 • Priority N

Comparison: Cybersecurity priorities (2/2)

EU	JAPAN
• European Research Infrastructures, and e-Infrastructures • Information and Communication Technologies •Smart Cyber-Physical Systems •Smart System Integration •Customised and low power computing •Smart Networks and novel Internet Architectures •Advanced Cloud Infrastructures and Services •Boosting public sector productivity and innovation through cloud computing services •Advanced 5G Network Infrastructure for the Future Internet •Internet of Things and Platforms for Connected Smart Objects •Cybersecurity, Trustworthy ICT •Research & Innovation Actions •Security-by-design for end-to-end security •Cryptography •Activities supporting the Cryptography Community	• Given the cyberspace crime is mostly cross-country, therefore the government should actively cooperate with foreign parties and focus to protect national interests. • Protect national critical infrastructure and improve the security of cyberspace individually and collectively • Applying risk management approach for assessing, prioritising and providing resources for cybersecurity activities. Early warning systems and rapid recovery • Protect national critical infrastructure and improve the security of cyberspace • Gov-CSIRTs

Contents

- Roadmaps and collaboration actions/projects
- Research problems and EU agenda on cybersecurity and privacy
- Mechanisms for realization
- Education

Education

- Promote cybersecurity training via:
  - University courses
  - Exchanges of students and personnel
    - Marie Curie actions (RISE)
    - INEA/CEF (exchanges in CERTs)
    - Other projects that support exchanges
  - Organization of workshops, conferences, panels, BoF sessions

Thank you for your attention

Questions ?

The next presentation was about ECSO and the Strategic Research and Innovation Agenda by Hervé Debar, as well as a short talk on the forthcoming EU-Japan joint collaborative call, given by Daisuke Inoue (NICT).

Below, we add the presentation of “ECSO WG6 Strategic Research and Innovation Agenda” by Dr. Hervé Debar.

ECSO WG6
Strategic Research and Innovation Agenda

Hervé Debar

Télécom SudParis

EUNITY Coordinator

What is EUNITY

- H2020 CSA Project
  - H2020: current European Framework Program for research and innovation
  - CSA: Coordination and Support Action
  - Objective: supporting European research and innovation Policy Development
- EUNITY Focus: support cyber-security dialogue between Europe and Japan
- Our goals:
  - Raise awareness of European views and activities on cybersecurity in Japan
  - Understand similar activities in Japan to complete European research roadmaps, e.g. with joint activities

What is ECSO

- Association established in Brussels
  - “Industry Proposal”
- Contractual Public-Private Partnership (cPPP)
  - Joint effort between the European Commission and the private sector
  - Leverage public research funding to develop business activity.
- Signed July 2016
  - Other cPPPs exist: DVA (big data); 5G (mobile 5G); EFFRA (smart industry), …
  - cPPP could evolve into a more ambitious structure (Joint Undertaking- like) following the recent EU cybersecurity strategy (Sept 2017)

ECSO Intro/L.Rebuffi

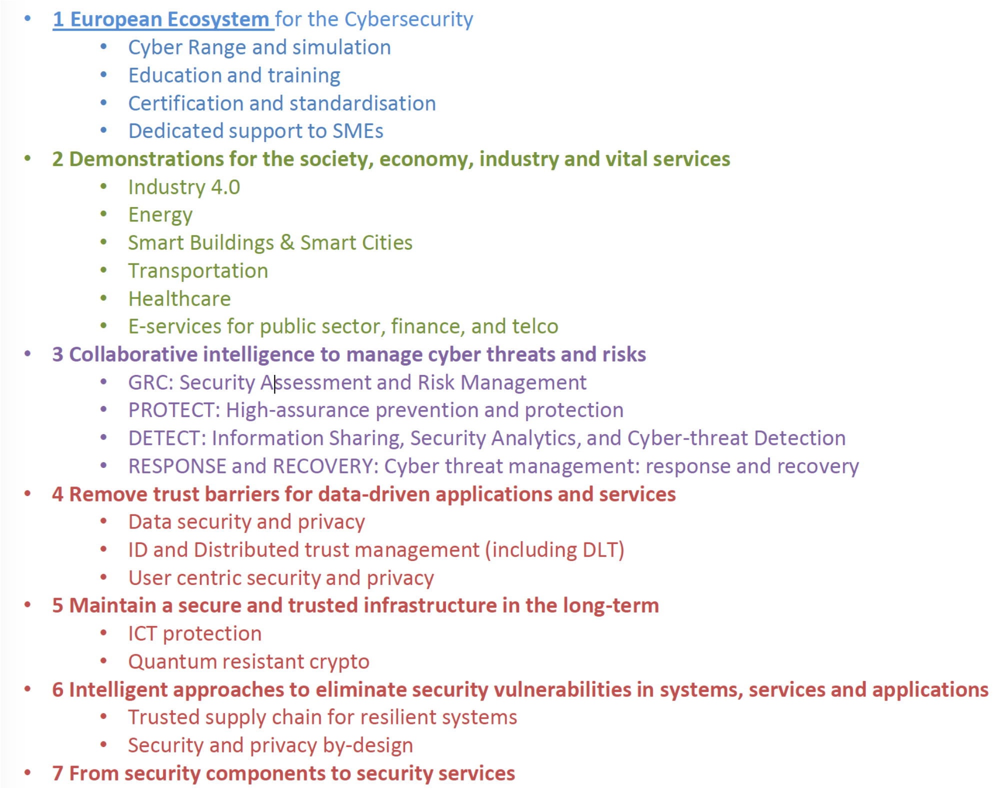
6 working groups

- WG1 (standards / certification / label / trusted supply chain)
- WG2 (market / funds / international cooperation / cPPP monitoring)
- WG3 (verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities)
- WG4 (SMEs, Regions, East EU)
- WG5 (education, training, awareness, cyber ranges…)
- *WG6 (SRIA)*

WG6 Subgroups

- SWG 6.1: Ecosystem
  - 6.1.1 Link across R&I projects
  - 6.1.2 Link with other cPPP / EC initiatives (5G, Cloud, IoT, Big Data, EIT etc.)
- SWG 6.2: Vertical application domains
  - 6.2.1 Energy, including smart grids
  - 6.2.2 Transport
  - 6.2.3 Finance
  - 6.2.4 Healthcare
  - 6.2.5 Smart & Secure Cities
  - 6.2.6 Public Services / eGovernment
  - 6.2.7 Industrial Critical Systems / Industry 4.0
- SWG 6.3: Trustworthy transversal infrastructures
  - 6.3.1 Digital citizenships (including identity management)
  - 6.3.2 Risk management for managing SOC, increasing cyber risk preparedness plans for NIS etc.
  - 6.3.3 Information sharing and analytics for CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)
  - 6.3.4 Secure Networks and ICT (Secure and trusted Routers, Secure and Trusted Network IDS, Secure Integration, Open source OS).
- SWG 6.4: Technical priority areas
  - 6.4.1 Assurance / risk management and security / privacy by design
  - 6.4.2 Identity, access and trust management (including Identity and Access Management, Trust Management)
  - 6.4.3 Data security
  - 6.4.4 Protecting the ICT Infrastructure (including Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
  - 6.4.5 Security services

Detailed structure: 7 main thematic priority areas



6.1

- 1 European Ecosystem for the Cybersecurity
  - Cyber Range and simulation
  - Education and training
  - Certification and standardisation
  - Dedicated support to SMEs

6.2

- **2 Demonstrations for the society, economy, industry and vital services**
  - Industry 4.0
  - Energy
  - Smart Buildings & Smart Cities
  - Transportation
  - Healthcare
  - E-services for public sector, finance, and telco

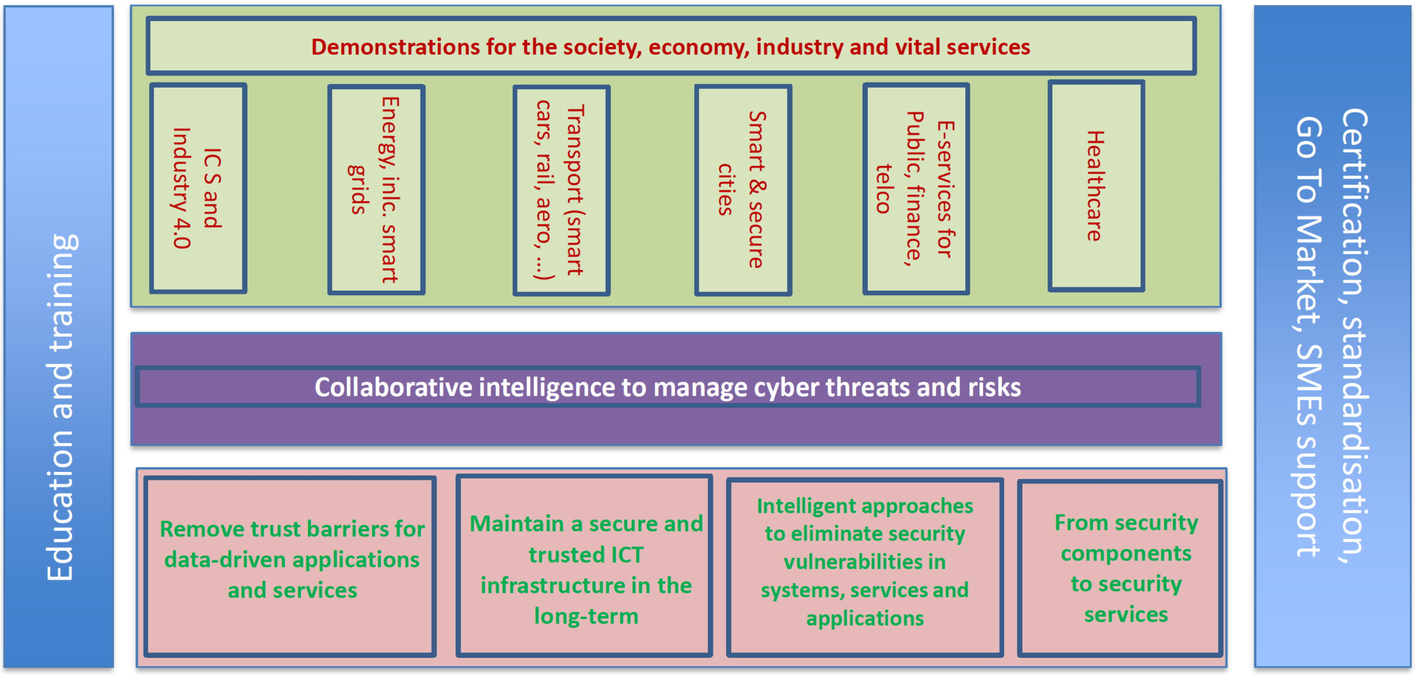
6.3

- **3 Collaborative intelligence to manage cyber threats and risks**
  - GRC: Security Assessment and Risk Management
  - PROTECT: High-assurance prevention and protection
  - DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection
  - RESPONSE and RECOVERY: Cyber threat management: response and recovery

6.4

- **4 Remove trust barriers for data-driven applications and services**
  - Data security and privacy
  - ID and Distributed trust management (including DLT)
  - User centric security and privacy
- **5 Maintain a secure and trusted infrastructure in the long-term**
  - ICT protection
  - Quantum resistant crypto
- **6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain for resilient systems
  - Security and privacy by-design
- **7 From security components to security services**

From basic R&I building blocks to products



Education and training
Demonstrations for the society, economy, industry and vital services
IC S and Industry 4.0
Energy, inlc. smart grids
Transport (smart cars, rail, aero, …)
Smart & secure cities
E-services for Public, finance, telco
Healthcare
Collaborative intelligence to manage cyber threats and risks
Remove trust barriers for data-driven applications and services
Maintain a secure and trusted ICT infrastructure in the long-term
Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
From security components to security services
Certification, standardisation, Go To Market, SMEs support

WG6 Initial Activities

- Informal suggestions delivered to the European Commission for the 2018 – 2020 H2020 Work Programme:
  - organisation of the priority topics identified by ECSO in the SRIA (good acceptance of suggested priorities).
- Contacts with other PPPs and similar EU activities to coordinate objectives.

ICT WP2018-2020

Indirect contribution to cyber-security

- ICT-08-2019: Security and resilience for collaborative manufacturing environments (Joint with FoF)
  - Practical solutions for securing digital collaboration between manufacturing environments
- ICT-10-2019-2020: Robotics Core Technology
  - Security by design for standardized robotics environments.
- ICT-11-2018-2019: HPC and Big Data enabled Large-scale Test-beds and Applications
  - Secure access and provisionning
- ICT-15-2019-2020: Cloud Computing
  - Address stringent security and data protection requirements
- ICT-27-2018-2020: Internet of Things
  - End-user trust in security and privacy of the IoT
- ICT-28-2018: Future Hyper-connected Sociality
  - Trustful and Secure Data Ecosystem for Social Media and Media
    - Content verification
- Calls schedule january 2018, april 2018, november 2018, january 2019, march 2019

Digital Europe 2018-2020

Indirect contribution to cyber-security

- DT-ICT-01-2019: Smart Anything Everywhere
  - Man-machine collaboration
  - Security and privacy
- DT-ICT-02-2018: Robotics - Digital Innovation Hubs (DIH)
  - DIHs should address ethical, data privacy and protection issues, and consider cyber-security issues (including security by design).
- DT-ICT-06-2018: Coordination and Support Activities for Digital Innovation Hub network
  - Secure and safe implementation of pilots
- DT-ICT-08-2019: Agricultural digital integration platforms
- Calls opening end of October, deadline April 2018

Cybersecurity (*H2020-SU-ICT-2018-2020*)

Directly contributing to cybersecurity cPPP

- SU-ICT-01-2018: Dynamic countering of cyber-attacks
  - Cyber-attacks management - advanced assurance and protection
    - Recognition of malicious blocks
    - Secure execution environments
    - Feedback to users
  - Cyber-attacks management – advanced response and recovery
    - Support human operators
    - Include theat intelligence and information sharing
    - Explore forensics, penetration testing, investigation and attack attribution services
    - Handling of encrypted network traffic
- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems
  - Cybersecurity/privacy audit, certification and standardisation
  - Trusted supply chains of ICT systems
  - Designing and developing privacy-friendly and secure software and hardware
- SU-ICT-04-2019: Quantum Key Distribution testbed

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (1)

- Cybersecurity/privacy audit, certification and standardisation
  - (i) design and develop automated security validation and testing, exploiting the knowledge of architecture, code, and development environments (e.g. white box)
  - (ii) design and develop automated security verification at code level, focusing on scalable taint analysis, information-flow analysis, control-flow integrity, security policy, and considering the relation to secure development lifecycles,
  - (iii) develop mechanisms, key performance indicators and measures that ease the process of certification at the level of services and
  - (iv) develop mechanisms to better audit and analyse open source and/or open license software, and ICT systems with respect to cybersecurity and digital privacy.
- Trusted supply chains of ICT systems
- Designing and developing privacy-friendly and secure software and hardware

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (2)

- Cybersecurity/privacy audit, certification and standardisation
- Trusted supply chains of ICT systems
  - (i) develop advanced, evidence based, dynamic methods and tools for better forecasting, detecting and preventing propagated vulnerabilities,
  - (ii) estimate both dynamically and accurately supply chain cyber security and privacy risks,
  - (iii) design and develop security, privacy and accountability measures and mitigation strategies for all entities involved in the supply chain,
  - (iv) design and develop techniques, methods and tools to better audit complex algorithms (e.g. search engines), interconnected ICT components/systems
  - (v) devise methods to develop resilient systems out of potentially insecure components
  - (vi) devise security assurance methodologies and metrics to define security claims for composed systems and certification methods, allowing harmonisation and mutual recognition based on evidence and not only on trust.
- Designing and developing privacy-friendly and secure software and hardware

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (3)

- Cybersecurity/privacy audit, certification and standardisation
- Trusted supply chains of ICT systems
- Designing and developing privacy-friendly and secure software and hardware
  - (i) security and privacy requirements engineering (including dynamic threat modelling/ attack trees, attack ontologies, dynamic taxonomies and dynamic, evidence based risk analysis),
  - (ii) embedded algorithmic accountability (in order to monitor the security, privacy and transparency of the algorithms/software/systems/services),
  - (iii) system-wide consistency including connection between models, security/privacy/accountability objectives, policies, and functional implementations,
  - (iv) metrics to assess a secure, reliable and privacy-friendly development,
  - (v) secure, privacy-friendly and accountability-enabled programming languages (including machine languages), hardware design languages, development frameworks, as well as secure compilation and execution,
  - (vi) novel, secure and privacy-friendly IoT architectures

Joint topics with 5G

- ICT-18-2018: 5G for cooperative, connected and automated mobility (CCAM)
  - Security for automotive V2x
- ICT-19-2019: Advanced 5G validation trials across multiple vertical industries
  - Consistent deployment of cyber-security
- ICT-20-2019-2020: 5G Long Term Evolution
  - Trusted workload deployment
  - Secure provisioning and deployment
  - Trusted multi-tenancy

Joint topics with BDVA

- The areas of interest for collaboration between BDVA and ECSO can be summarised as follows:
  - Cyber security to make big data analytics resilient and robust: trustworthy data;
  - Big data analytics for cyber security to prevent, infer and detect potential attack;
  - Leverage big data techniques, artificial intelligence and cyber security for application areas and verticals: joint approach.
- ICT-12-2018-2020: Big Data technologies and extreme-scale analytics
  - Secure federated systems
- ICT-13-2018-2019: Supporting the emergence of data markets and the data economy
  - Trusted and secure platforms
  - Privacy-aware analytics
  - Personnal and Industrial data platforms
- ICT-26-2018-2020: Artificial Intelligence
  - SRIA for AI including cyber-security

Thank you for your attention

Questions ?

4 Discussion & Feedback

This section summarizes the most informative feedback, provided by the audience, during the workshop sessions, as well as feedback from the questionnaires that were shared among the participants[1]. There are separate questionnaires for each workshop session, including: Industry, CSIRTs, ECSO, Legal & Privacy, and Research & Innovation.

4.1 Session 1

Chair: Hervé Debar, IMT and Youki Kadobayashi, NAIST

4.1.1 TF-CSIRT: CSIRT collaboration in Europe

The presentation, for the first session, was given by Baiba Kaskina (CERT.LV), the chair of TF-CSIRT. TF-CSIRT was established in 2000 and is the oldest forum for CSIRTs in Europe (focus is on the RIPE NCC service area but some of the members come from other regions). FIRST is the oldest one at global scale. Their main tasks focuses on exchanging experience and knowledge, improving the cooperation and coordination between members. It is hosted by the GEANT network and is involved in WGs on standards and procedures as well as in joint initiatives. It has been the liaison with FIRST, as a regional partner and is in cooperation with ENISA.

It includes a community of 315 teams, who are meeting 3 times a year (with 130-200 participants), hosted by a different CSIRT each time. New members can be introduced through the Trusted Introducer service.

[1] The empty forms of the questionnaires are included as Appendix A.

4.1.2 JPCERT capability building

The next presentation was by Takayuki Uchiyama from JPCERT/CC, concerning the JPCERT capability building. JPCERT/CC was founded in 1996 and is an independent, non-profit organization mainly targeted for enterprises.

The capacity building is in short-term on-site, mainly for training and workshops in Asian-Pacific and African regions. It is in collaboration with partners in Japan and overseas, and provides many courses covering secure coding, malware analysis, etc.

JPCERT/CC is committed to help out countries (particularly in Africa) that do not have CSIRTs or PoC yet. It offers many trainings in ASEAN, APAC, Africa regions. Many trainings have been performed during the Africa Internet Summit, this initiative lasted for 7 years.

4.2 Session 2 & 3: CERT / CSIRT community

Chair: Paweł Pawliński, CERT Polska

The next two sessions on the first day were focused on CSIRTs and included an hour-long open discussion and an invited presentation.

4.2.1 Structure of the session

The CSIRT session started with a discussion that was guided by the questionnaire (see Appendix A for the list of questions). After introducing the topics, discussions themselves were held in smaller groups, each led by a facilitator from one of the Japanese organizations. Such approach proved to be effective in stimulating conversations about the situation from both and Japanese and European perspectives.

The overall theme of the discussion was cybersecurity operations and international cooperation, which was divided into five topics:

- Incident coordination
- Information exchange
- Joint initiatives
- Exercises
- Future plans

A brief summary of the discussion was presented by Paweł Pawliński (NASK / CERT Polska) at the beginning of Session 3 (after a break). It was followed by the presentation from by Afonso Ferreira ("Task Force Software Vulnerability Disclosure in Europe").

Overall, there were many similarities in conclusions from each of the groups, which suggests that the collected feedback might be representative for CSIRTs and related communities. The following sections contain main conclusions from the discussions.

4.2.2 Incident coordination

For many participants, incident coordination across organizational boundaries is difficult. The main challenge is finding the right contacts in other entities. It can be addressed by face-to-face meeting in order to know the people that are key to collaboration. The issue of trust as a prerequisite for collaboration was raised by multiple participants.

Additionally, legal obligations or uncertainty was also cited by some as one of the barriers for effective coordination. More information on legal aspects are included in next sections as there was a dedicated session for that in the workshop on the second day.

One of the entities with most experience in international incident coordination is JPCERT/CC. They primarily collaborate with countries in Asia-Pacific (through APCERT) and interactions with US and EU are more limited and usually go through larger forums like FIRST.

4.2.3 Information exchange

Some of the challenges identified during the discussion of incident coordination were repeated for the topic of information exchange. In particular, the issue of finding trusted partners to enable useful information exchange channels. This challenge can be addressed by establishing contacts with key people in other organizations (especially in face-to-face meetings).

MoUs were also mentioned as a more formal approach to achieve smooth collaboration and ensure that when the information is shared, the threat/incident will be properly taken care of, by the involved partners.

Again, legal issues can be a blocker for sharing information. This is especially true for international collaboration due to differences in legal frameworks. Nevertheless, so far JPCERT has not experienced any legal problems (like a lawsuit for example) related to information sharing.

Overall, participants felt that data exchange work well for academics (research) but not for operational purposes. It may suggest that any attempts at improving this area of collaboration should focus on the operational use of information and involvement of the industry.

Practical advantages of information sharing is defeating sources of an attack in cases when it originates from outside the country. Additionally, comparison of reports from different countries was also identified as beneficial in understanding a particular threat.

On the technical level, there are existing solutions that can be used for information exchange. STIX is the best known standardized data format and JPCERT has been testing it for 2 years. STIX is also promoted by the US. On the other hand, MISP (information sharing system capable of export in multiple formats) is a de facto standard in Europe. Despite the availability of the technical solutions, some participants felt that they are underutilized and more training is needed to make the best use of them.

Finally, one of the postulates from the group was standardization of the analysis methods and taxonomies. Currently, analysis methods, as well as the interpretations of data differ across organizations and even team members. Standardization of some task, like malware analysis or vulnerability description could be beneficial for collaboration. Such efforts should be accompanied by appropriate training programmes.

4.2.4 Joint initiatives

Participants were not aware of any current significant joint EU-Japan projects. Within the region, CSIRTs collaborate on some long-term projects through APCERT.

Lack of funding was identified as the primary reason for this situation. Usual funding timeframe is 3 years, however it takes more time to achieve good effects and establish capabilities.

4.2.5 Exercises

Exercises (cyber drills) are considered very useful in developing capabilities and fostering collaboration. They allow to roll out procedures and assess the ability to respond to incidents, including performing some technical analysis. Examples of successful exercises included the annual APCERT exercise (Asia-Pacific), Cyber Europe (EU) and an annual exercise in Japan for critical infrastructure.

It was noticed that often approaches and expectations are different. Exercises organized by APCERT are more technically focused and organized within a shorter timeframe. In contrast, Cyber Europe puts relatively more importance on communications and the preparations take much longer (over a year).

In case of participation in a joint training, both sides need to be aware of these differences, otherwise there has been already a case when an EU CSIRT participating in the APCERT exercise was surprised by the type of contents.

The main challenge regarding exercises was the effort required to prepare them. Developing realistic scenarios is very time-consuming, so there is a trade-off between realism and the amount of work that needs to be put by the organizers.

4.2.6 Future plans and proposals

The last part of the discussion focused on the future plans, including suggestions of approaches that would address previously identified challenges.

The most commonly postulated activity is trust-building, since having connections to the competent people in other organizations and countries is the key prerequisite for collaboration. Participants agreed that face-to-face meetings are the most effective way of building trust.

On the policy level, availability of stable long-term funding mechanisms was emphasized as the main challenge to address. Joint EU-Japan project calls can be a good way to start an initiative, however long-term funding should be possible to secure as well, since duration of typical projects is often too short to achieve and sustain meaningful effects.

Joint EU-Japan exercises are one of the natural ways to improve collaboration between the regions. The first step for joint exercises should be to include European CSIRTs in existing Japanese exercises and vice-versa, especially in tasks related to communications and information sharing.

Given the shared interest in the protection of critical infrastructure, a joint initiative was proposed to develop a testbed focusing on systems typically used in these sectors.

Another area with a potential for joint initiatives is awareness. There is already a cybersecurity awareness month in October in EU and in February in Japan. In Europe, the activities are supported by ENISA, however they are organized by national CSIRTs and differ from country to country. For example, 5000 people attended an opening conference in Spain for family audience on cybersecurity awareness, sponsored by ENISA. In Japan, the annual awareness month involves mostly posters and communication campaigns for broad audience.

Capacity building in other countries (e.g., in African countries) was also identified as an activity that could benefit from a joint EU-Japan contribution. This may be easy to accomplish, since both Japan and EU (ENISA and individual CSIRTs) have programmes to support the development of CSIRTs.

Finally, standardizing some common methods of technical analysis and information exchange methods could be very helpful for enabling effective collaboration, especially across different sectors and countries. Standardization can also be applied to overcome potential legal obstacles by preparing common templates of agreements for information sharing and collaboration, both domestically and internationally.

4.2.7 CSIRTs questionnaire results

While most of the feedback has been collected interactively during the discussion in Session 2, some participants provided responses in writing via questionnaires.

In total, we collected 11 replies. Seven respondents were from academia, 3 from industry, none from government and one did not disclosed her affiliation. Three of them were not performing any operational security work, four of them occasionally and three of them daily. The respondents cooperation included JPCERT/CC, European partner companies, and EU-funded cybersecurity project partners (for the policy side). Four of the respondents shared incident information with international partners. The main challenges in information exchange, that they pointed out, were the lack of a platform to securely exchange data, the lack in sharing standards, and the lack of training. Concerning the future plans and whether they see a potential to improve Japan-EU cooperation, two answers were provided that included the development of information and data exchange best practices and process standards, as well as the exchange of operators in the industry.

4.3 Session 4 & 5: Industry: discussion

Chair: Pedro Soria, ATOS

This session included a number of invited talks, including an introduction of CRIC Cross Sectors Forum by Hiroshi Takeshi (NEC), and an introduction to another CSA project, the Cyberwatching.eu, by its coordinator, Nicholas Ferguson (Trust-IT Services). Pedro Soria and Alicia Garcia also made a presentation on Market Situations and ECIL Recommendations in Europe.

Mr Hiroshi Takechi in his presentation indicated that the Cyber Risk Intelligence Center Cross Sectors Forum (CRIC CSF) was launched in June 2015, in order to tackle cybersecurity issues in the industry, and in particular, the cybersecurity workforce shortage.

Their main motivations included: information sharing, security workforce development, workforce sharing, and training new promising talents.

The presentation highlighted some specificites of Japanese companies. For example, people without cybersecurity expertise may become CISO, due to the nature of the employment system, where senior people can be promoted to senior positions.

Another issue is the ambiguity between a business role and a security role. For example, a security role may not be clearly stipulated in a job description, while it is expected to be as such. Therefore, there is no clear definition of what a security role should include, that makes it distinguishable from a business role. Indeed, the workforce definition does not originate from the skill set, but from the functions. So the positions and job titles may vary from company to company, and so do the roles that have been defined for these specific positions. Defining the functions is a result from an investigation done among CSF participants.

Among others, the results of the CSF include: the workforce definition reference, including 30 roles based on functions and job types; the activities calendar, which is like a cheat sheet for novice CISOs; and the security operation outsourcing guide.

The planned activity for the 2nd period (October 2017-September 2018) includes the transition to a consortium with a corporate status, in April under the CRIC (the CSF used to be a voluntary organization). The future activities of the CSF include: building mutual support among the industries; establishing autonomous activities in each company; establishing an ecosystem through coordination of government, academia and industry; and monitoring Tokyo 2020 Olympics.

4.3.1 Industry questionnaire results

Among the 40 respondents, 17 were from industry, 14 from academia and 7 from government. The 2 respondents that were not classified, actually claimed to be from CSIRT, and from a private organization funded by the government, respectively.

20 respondents offered cybersecurity services or products, while 14 did not. Even more respondents (26) carried out research in cybersecurity. 31 respondents consumed cybersecurity as services or products and 34 of the respondents carried out cybersecurity research.

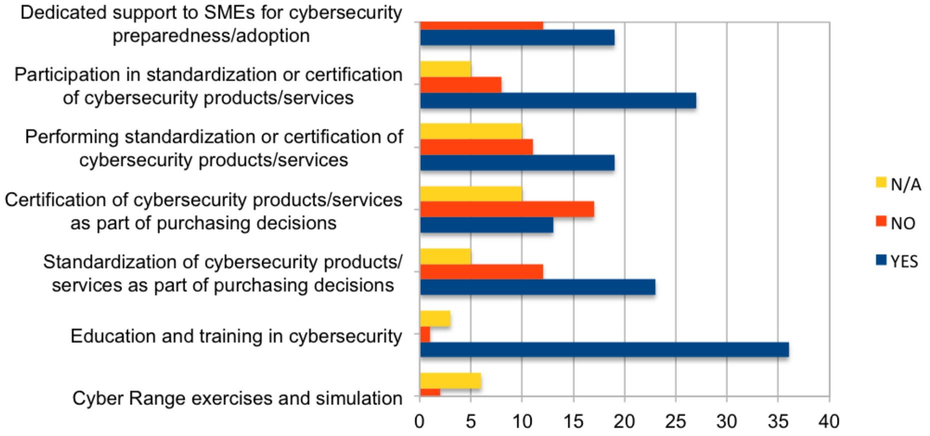


Figure 4.1: In this figure we notice the replies of the respondents to the question: “Do you consider these topics important for your organization?”. The replies show that “Education and training in cybersecurity” was considered as the most important topic.

34 of the respondents were from Japan and 5 from Europe. 1 respondent’s home market was neither Japan nor Europe, but Southeast Asia and Oceania. Among the 26 respondents whose home market was Japan, only

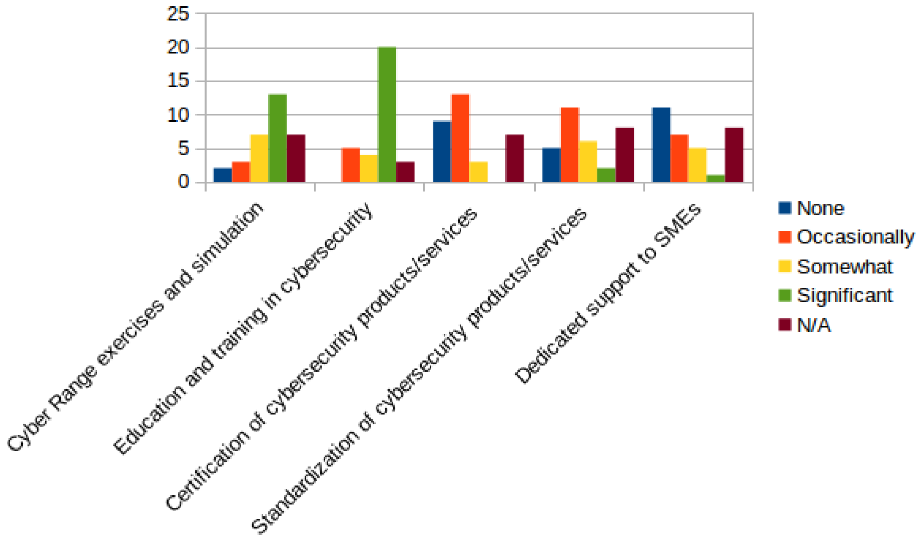


Figure 4.2: To the question on Industry: "What is your organization's involvement in these activities?", most respondents (23) picked "Education and training in cybersecurity", followed by "Cyber Range exercises and simulation" (14), as the most significant.

15 of them did sell security products or service to this market. 10 respondents did not reply to the question. Only 7 respondents were selling security products and services to the European countries, while 21 of the respondents did not sell to the European market. About the main international issues, 4 respondents stated that there is a lack of Japanese awareness of EU and US regulatory development budget, a human resources shortage, a lack of communication, cultural issues, a lack of adaptation of training with respects to technological maturity and 1 respondent suggested a joint budget to be distributed in accordance to blocking points.

4.3.2 ECSO questionnaire results

The chair of this session was Hervé Debar (IMT). The session included a featured number of talks on ECSO strategic agenda and standards. In total, we collected 11 replies to the questionnaires. 6 respondents were from academia, 4 from industry, 1 from CSIRT. 9 respondents did practice cybersecurity, and 2 of them did not. 10 of the respondents carried out cybersecurity research and 1 did not. Concerning the areas of interest of the respondents, we got only one answer that was entrepreneurship in cybersecurity.

On collaborative intelligence to manage "Cyber threats and risks", to the question "Do you consider the topics relevant ?", 8 of the respondents picked

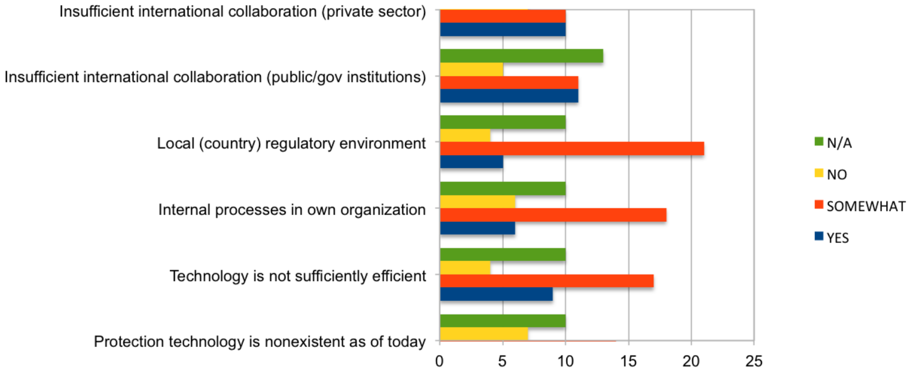


Figure 4.3: In the industry session, to the question "Are there research challenges affecting your business that need addressing by the cybersecurity research community?" the "Local (country) regulatory environment" was picked 21 times as somewhat, and "Internal processes in own organization" 18 times as somewhat.

"PROTECT: high-assurance prevention and Protection", 8 of the respondents picked "DETECT: information sharing, security Analytics, and cyber-threat detection" and 7 picked "GRC: security assessment and risk Management".

Most respondents were interested in exchanging information about the relevant topics, except for the topic of dedicated support to SMEs. Most respondents were working on the topics of industry 4.0, energy or smart building and smart cities. Transportation seemed to be a less-traveled topic.

To the question whether they would be interested in exchanging information and/or building joint projects, the respondents were mostly interested in exchanging information on all relevant topics, with data security and privacy being the least interesting topic. The respondents that answered NO are actually interested but not ready yet.

Concerning intelligent approaches to eliminate vulnerabilities in systems, services and applications; the respondents are not currently working on a trusted supply chain for resilient systems, but they are more involved in security and privacy by design.

4.4 Session 6: Landscapes: discussion

Chair: Hervé Debar, IMT

4.4.1 Restitution of 1st day: discussion

This presentation mainly referred briefly to the discussions and the presentations of the first day, which is already analyzed above.

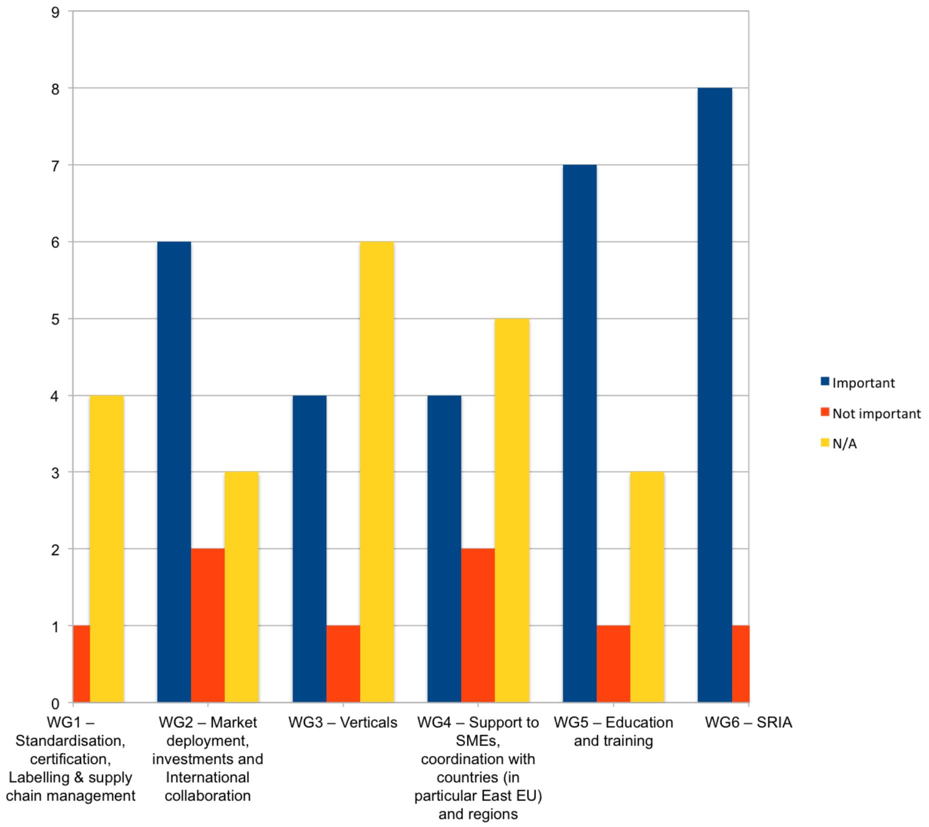


Figure 4.4: To the question of the importance of ECSO working groups, 8 of the respondents picked WG6 (SRIA), 7 picked WG5 (education and training), 6 picked WG1 (standardisation, certification, labelling & supply chain management), and 6 picked WG2 (market deployment, investments and international collaboration).

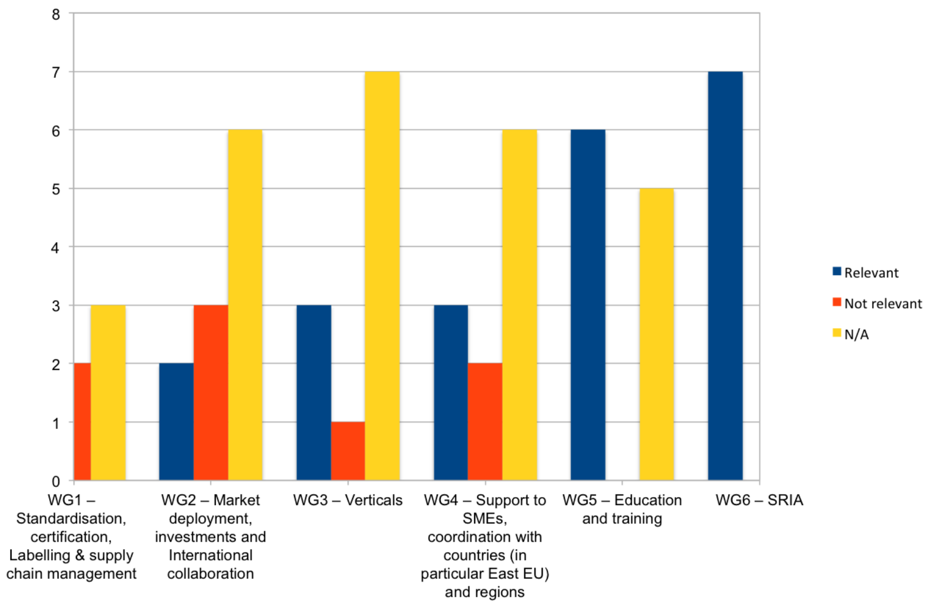


Figure 4.5: As for the relevance of ECSO WGs, 7 of the respondents picked WG6, 6 picked WG5 and 6 picked WG1.

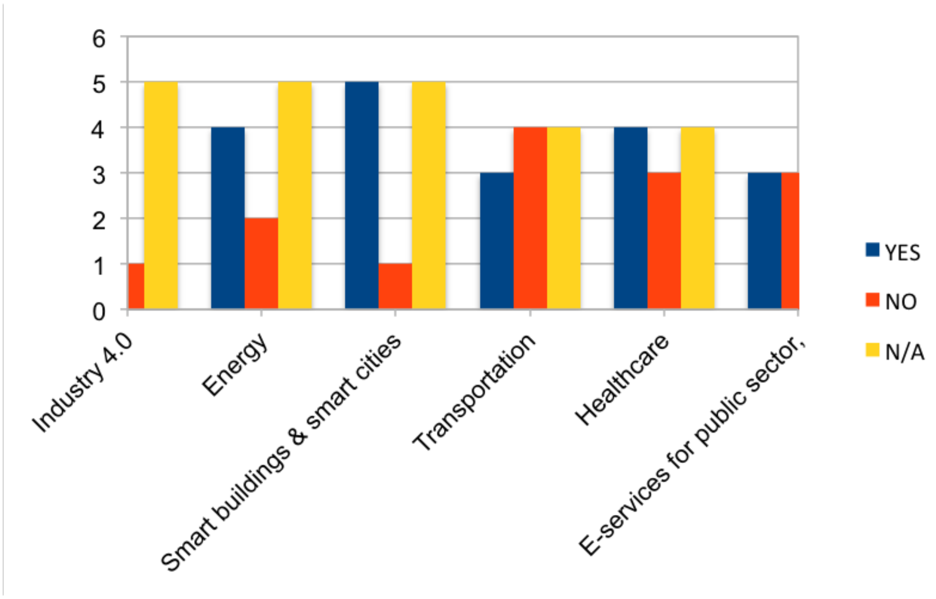


Figure 4.6: With regard to ECSO, to the question “‘Do you work on similar topics ?” 5 of the respondents answered Industry 4.0, 5 of the respondents answered Smart buildings & smart cities, 4 of the respondents answered Healthcare and 4 of the respondents answered Energy.

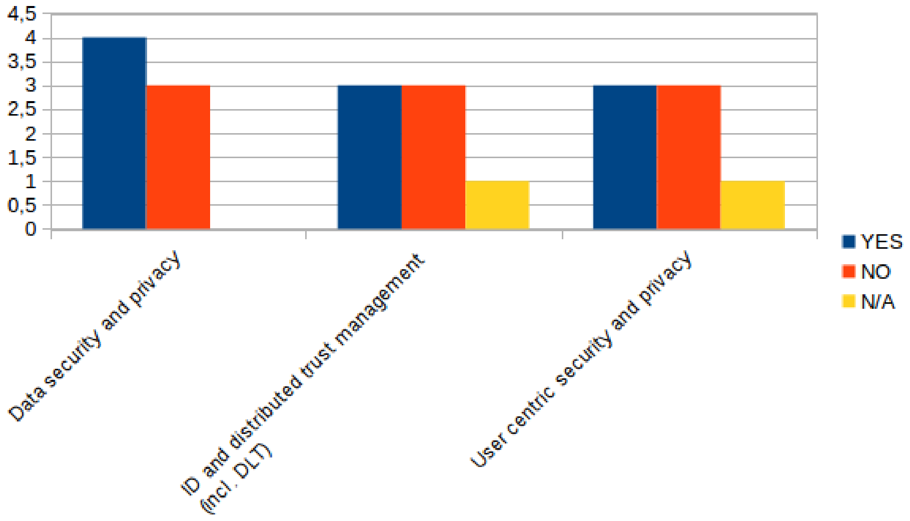


Figure 4.7: With respect to the ECSO session, in relation to the topic "User centric security and privacy", to the question "Do you work on similar topics?", "Data security and privacy" was picked by 4 respondents, "ID and distributed trust management (incl. DLT)" was picked by 3 respondents, and "User centric security and privacy" was picked by 3 respondents.

4.4.2 The Cybersecurity Policy Landscape in Europe: Legislation and Research (Afonso Ferreira, IRIT)(EC/MIC Project Officers): discussion

The Cybersecurity Policy Landscape in Europe is presented in two acts.
The Cybersecurity Strategy in 2013, Act 1 is aiming to:

- Achieve cyber-resilience.
- Reduce cybercrime.
- Develop cyber-defence policy.
- Develop industrial and technological resources.
- Establish international cyberspace policy.

It took two and a half years for NIS directive to reach an agreement. It was proposed in February 2013 and should be in place in April 2018. The priorities included:

- Development of capabilities: national NIS authority, national CSIRT and NIS national strategy

- Strengthen EU-level cooperation: cooperation group for strategic cooperation through MSs, EC, ENISA; and CSIRT network for operational cooperation through national CSIRTs, CERT-EU, ENISA
- Security and notification requirements: operators of essential service and digital service providers (DSPs)

Concerning the WG3 on Secure ICT R&I at ENISA, in order to develop the research policy, the strategic research agenda should synthesize the areas of interest (AoI). The methodology of the Strategic Agenda has 3 different perspectives: the individual person, the institutions and the private companies and infrastructures.

The WG3 SRA cornerstone of ECSO Act 2:

On September 2017 the cybersecurity strategy was renewed to combat cyber-attacks through:

- Building EU resilience by building up on the success of ENISA, pan-European cybersecurity exercises, ISACs and EU-wide certification framework.
- Stepping the EU's cybersecurity capacity through research and competence center, blueprint for response, cybersecurity emergency response fund, stronger cyberdefence capabilities and enhanced international cooperation.
- Creating an effective criminal law response against cyber-criminals by detection (but no attribution so far), traceability (forensics) and prosecution.

4.5 Session 7 & 8: Legal and Policy: discussion

Chair: Stefano Fantin, KU Leuven

This session focused on the European privacy landscape, including as well some background and context, the definition of GDPR, international transfers and NIS Conclusions, and the Japanese Landscape.

4.5.1 European privacy landscape: GDPR and others (Stefano Fantin, KU Leuven): discussion

During the workshop in Tokyo, session 7 was dedicated to the presentation of an overview of both European and Japanese legal, policy and regulatory landscapes with regard to cybersecurity and privacy. Attention was paid at the end of the presentations to active interactions with the audience, which triggered a number of points that had been touched more in depth by ways of Q&A session right after the talks by Stefano Fantin and Prof. Hiroshi Miyashita.

A first point was concerned with the gap between EU cybersecurity and EU privacy laws. The fact that these two fields are regulated by a regulation and a directive respectively supports the argument that, in the policy and legal mindset of the European legislator, cybersecurity still needs to grow its maturity at the national levels. Full harmonization is nevertheless envisaged, but will likely be an objective for the long run.

With regard to the GDPR, a number of clarifications were asked. Firstly, with regard to the sanctions cap, which will raise fines up to 20M Euros or up to 4% of the global annual turnover of the company. Furthermore, partners and audience showed extreme interest on the extra-territorial scope of the GDPR itself (it applies also to non-EU companies under certain conditions), as well as the age limits for children's consent. On the latter point, it was made clear that this is an area left to the domestic legislation. It is thus a prerogative of the Member State to define such age limit. It was argued that such decisions will likely be shaped and influenced by states' cultures and traditions.

On another note, the audience asked how will the new regulatory governance will work. Specifically, it was explained the functioning of the newly established EDPB (European Data Protection Board), as well as the new tasks of both national Data Protection Authorities and of the European Data Protection Supervisor.

Whilst EU is developing a jurisprudential line that tends to consider IP addresses as personal information (thus, applying privacy regulations to such identifiers), Japanese law does not consider them as personal data. A final update on the current negotiations between EU and Japan with regard to trade, commerce and privacy was made, from a policy and political point of view.

Concerning GDPR, we should also take into consideration the following:

- To be technology-agnostic: previous directive was not able to cope with technological advances
- Consider a risk-based approach rather than legal requirements for organizations
- Significant increase in fines: force companies to be compliant
- About the regulation it should be directly applicable to MSs (contrary to directive which needs to be implemented in national laws)

The application should be eligible by May 2018, and not only for personal data processed in Europe, but also for personal data of European citizens processed outside Europe. A non-EU company processing EU citizens' data falls under the scope of the GDPR. From a citizen perspective, GDPR empowers the user to access her personal data, as well as, other rights (already present in the previous directive) including some novelties, like the right to be forgotten (right of erasure) and the right to data portability. Also we should consider:

- More re-activity is required: obligation to report a security breach in 72 hours and inform data subject if there is personal data infringement
- More accountability and transparency requirements for data controllers: obligation to keep all record activities in a document, appointment of a data protection officer (DPO), stricter rules on consent, obligation to data protection by design/by default.
- Shift the mentality of companies away from compliance mindset, with the obligation to document, that privacy has been taken into account from the first steps of solution development
- More security: encryption, pseudonymization, with required documentations and certifications
- Consent of children: the age limit has been raised to 16 years old

Key regulatory bodies in May 2018:

- EDPS (EU data protection supervisor): no impact on EU firms
- EDPB (EU data protection board): composed of EDPS and national data protection authorities
- Discussions for data protection matters at European level but no enforcement powers
- National data protection authorities enforce laws

In the international level front we should mention that Japan and South Korea are in ongoing negotiations with EC for the exchange of personal data.

4.5.2 Japanese Landscape on Data Protection: discussion

Hiroshi Miyashita from Chuo University among presented the Joint declaration regarding the free flow of information between Europe and Japan that took place on July 2017 and provided comparison information between the GDPR and the Japanese Act.

Three different cases were presented, towards the mutual process for enhancing data flow between Europe and Japan:

- IC card systems (43M distributed across JP). JR East sold customers data to Hitachi for data analytics but after anonymization. There is a risk of re-identification.
- Facial recognition and CCTV in Osaka station. NICT sets up CCTVs but canceled in 2014/03 due to strong opposition from customers. There question ”Should the faces be protected” was raised.
- Educational companies sold 35M personal information to data broker. After investigation by METI, the company paid compensations but class action may ensue.

An interesting slide regarding the **Comparison of GDPR/Japanese Act** was presented during that session. A major difference between the two region is the amount of the penatly declared by its Regulation. While in the EU it is 4% of the total budget of the company, the penalty is just 4200 euros or 1 year prison for Japan. We should also note that there has not been a single company prosecuted so far.

The presentation also provided an **Overview of legal system**.

- The act on the protection of personal information (PPI: Protection of Personal Information) covers only private sector, but three additional laws cover the public sector.
- Concerning the reform of laws, there are 2 acts: the Act on the PPI and My Number Act.

The definition of personal information includes: the names, the birthdate and other descriptions easily matched (meaning that some other information are out of the scope such as IP address, customer ID and mobile numbers).

It was also discussed that the anonymous processing of data is not able to identify the individual and it is not possible to restore the data, but according to technical experts there is no generic way to process data in anonymous way. We should also mention that there is also the obligation to keep record on where data comes from.

About the global harmonisation, personal data cannot be transferred by Japan to Europe, unless a third party company or country ensures equivalent protection of data. The law is applicable to European member states, if the EU company offers services to Japanese citizens. There is an opt-out regime including an obligation to notify the PPI commission (vs consent in EU).

The session continued with examples of data breaches in the private and public sector. The graphs present a reduction of incidents in the private sector while it presents an increase in the public sector. There were many data breaches (approximately 1600 in public sector in 2013 according to MIC).

Last but not least a **Cyber Attack Case** and the recommendations report after the analysis of the incident was presented.
The Japanese pension system was hacked and 1.25M items of PI were stolen but the service was not halted. The improvements below are proposed, according to the report:

- Lack of preparation of human and organization measures (There was no DPO appointed and there was no specialized expertise on data protection because of rotation of personnel)
- Lack of information security system (no responsibility due to lack of records)
- Lack of sense of personal information protection (no password or other security mechanisms for shared folders)
- Inadequate policy

4.5.3 Legal and Policy questionnaire results

The chair included a questionnaire session as well. We collected 12 replies from the questionnaires. 11 respondents stated that data protection and privacy are part of the Japanese Digital Strategy, although one also mentioned that the related measures are not clearly publicized. 8 of the respondents were directly involved in the Japanese Digital Strategy implementation. 8 respondents felt that private businesses deal with cybersecurity and data protection separately, while 2 thought the contrary to be true.

DPOs or personnel that holds a similar position were usually IT people according to 4 respondents, while 7 of the respondents could not answer. Among the former 4 respondents, the DPO was considered to have the following background: IT, CSIRT and sales CISO (2), general manager. This low response rate is either due to the lack of knowledge from the respondent, the absence of such equivalent position in the respondent's company or a misunderstanding of the question.

To the question, whether Japan is a member of any inter-regional industrial or governmental federation in the area of cybersecurity and/or privacy, 3 of the respondents answered yes and 4 of them answered no. However, the positive respondents also stated Japanese federations, which demonstrate that the question was not fully understood. Other positive respondents were also not able to name any such federations. To the question of "How do the Japanese legal and regulatory regimes ensure interoperability of the systems and portability of (personal) data? Are you affected by such obligations?" the answers of the respondents were mixed. Regulations seem to still be a tricky topic, as one third was reluctant to answer. Someone mentioned that the mobile number portability (MNP) is an exception to

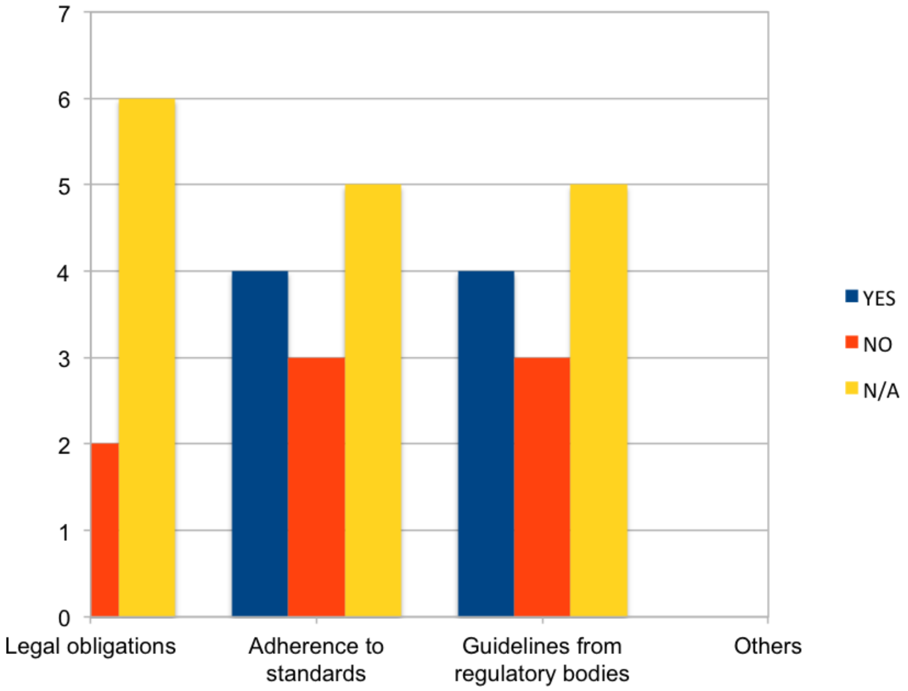


Figure 4.8: In the privacy session, to the question “How do the Japanese legal and regulatory. Regimes ensure interoperability of the Systems and portability of (personal) data ? Are you affected by such obligations ?”: Four picked YES to Legal obligations (2 answered NO), 4 picked YES to Adherence to standards (3 picked NO) and 4 picked YES to Guidelines from regulatory bodies (3 picked NO).

the Japanese legal and regulatory regimes, since one can move to another cellphone company while keeping the same number.

Concerning GDPR, only 1 respondent feels that his organization is GDPR-ready. 3 respondents stated the following obstacles: the appointment of a DPO, the implementation of data protection by design and the deployment of appropriate data security measures (encryption, anonymization, etc.).

4.6 Session 9: Research & innovation: discussions

Chair: Sotiris Ioannidis, FORTH.

The chair of this session was Sotiris Ioannidis (FORTH). The session included an ECSO presentation on the Strategic Research and Innovation Agenda by Hervé, a short talk on the forthcoming EU-Japan joint collaborative call given by Daisuke Inoue (NICT) and a presentation of the research roadmaps of various EU funded projects, as well as, cybersecurity and privacy topics in the EU research agenda (2018/2019 calls) by Sotiris Ioannidis. Next, the methodology for compiling such research roadmaps was presented which among other includes: (i) the organization of structured workshops like the EUNITY Tokyo workshop; (ii) analysis of both regions calls for projects for comparison (later possibly merging topics under a common umbrella) and (iii) concerning education, the cybersecurity training promoted through university courses, exchanges of students and personnel, workshops, conferences and panels.

4.6.1 Research & innovation questionnaire results

Like in the previous sessions, we also shared and received feedback through the questionnaires. We collected 22 replies. 6 respondents were from industry, 12 from academia, 3 form government and 1 respondent from CSIRT.

16 respondents answered that they practice cybersecurity as their job, 19 respondents carried out research on cybersecurity. 14 respondents identified themselves as being Japanese, 4 as being European, and 4 others did not disclose their origin.

To the question whether they are familiar with any national / international / sectorial research strategy, roadmaps and strategic agendas focused on cybersecurity or privacy in Japan, 12 of the respondents were familiar with these strategic agendas and 10 were not.

The latter seem to be mostly coming from industry. Among the positive respondents to the previous question, the following roadmaps and agendas were mentioned: cybersecurity R&D strategy by cybersecurity strategy office, H2020 (2), research roadmaps from CSA projects, ECSO, NISC cybersecurity R&D strategy, CREST, AIP, ICS-COE, Privacy in JP, information sharing between institutes and global coordination. Some of these are rather

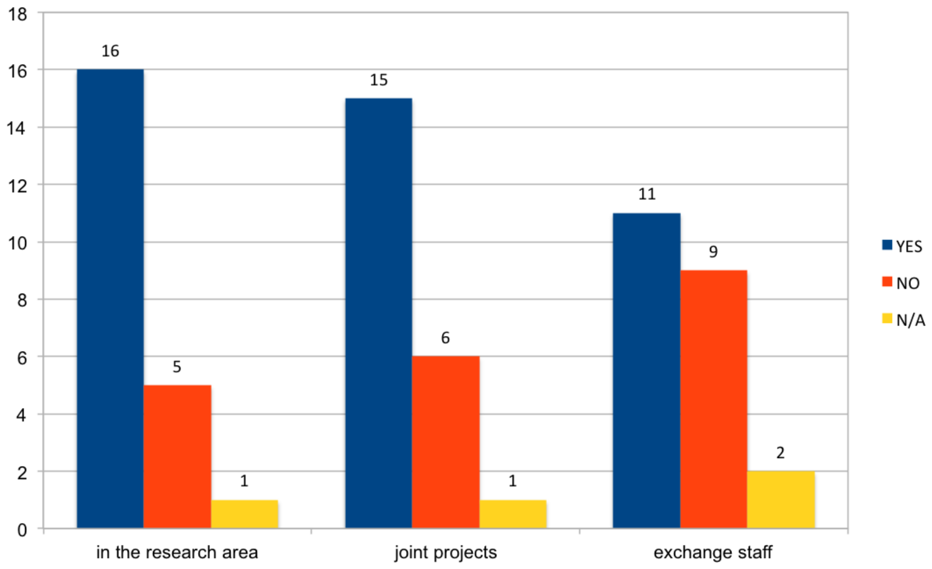


Figure 4.9: Research & Innovation: European cooperation

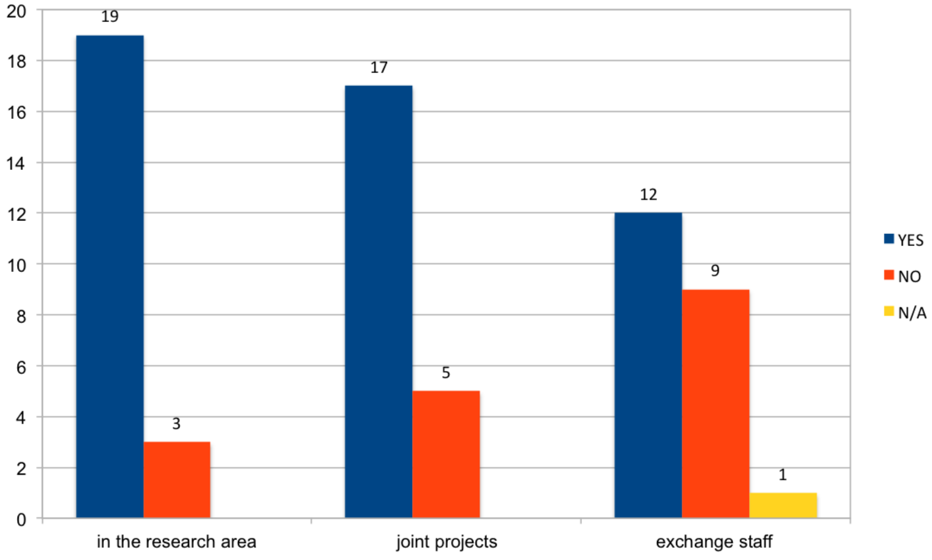


Figure 4.10: Research & Innovation: Non European cooperation

initiatives and projects than strategic agendas. Some respondents did not list any items and pointed us to the presentations made during the session.

13 respondents considered the roadmaps and agendas to be aligned with the industry needs. However, 7 respondents were not able to answer this question. To the question "On transforming outcomes of research into technologies and products is often a challenge: From your experience, what are the main obstacles in the field of cybersecurity?", the respondents were quite prolific and cited many reasons including the opposition between research and industry mechanisms (5 respondents), including monetizing, business chain, support and responsibility; the difficulty to keep up with a fast-paced market; budget and funding (3); regulations (3); privacy and confidentiality issues; deployment; and evaluation (in particular scalability).

17 respondents were aware of cybersecurity research funding mechanisms. The examples that they gave were: MIC(2), MEXT, NICT, METI (including IPA) (3 respondents), EU and H2020 (4), Government and National calls (3), Regional calls, CEF, EiT digital, Industrial partnerships, Research chairs and Private companies.

On the question whether industry finances cybersecurity research, the respondents are quite opposed on that question with 12 respondents answering YES and 9 answering NO. Interestingly, one respondent from government answered NO. Regarding the collaboration & investment question, most respondents declared that they maintain cooperation with at least a partner within the EU.

To the question "whether your company has any foreign cooperation with someone other than EU", most respondents maintained cooperation with a partner outside the EU. These partners were likely to be Japanese.

Concerning the top 3 threats that would be the most relevant in the upcoming years, irrespective of the order, the respondents cited a wealth of threats including: AI; IoT security (3); Privacy; Drones (2); 3D printers; Bluetooth threats (blueborne, BT-enabled critical systems); Advanced malware (incl. sophisticated IoT malware); APT (3); Cyber terrorism (incl. online radicalization) and state-sponsored hacking activities (3); Identity theft/fraud (2); Botnets and DDoS (5); Ransomware (4); BGP hijacking; Vulnerable radio communication systems; Industrial sabotage and safety-related attacks (3); Lack of integration/cooperation between CERTs; Spearphishing; Automotive cybersecurity and Quantum cryptanalysis.

Someone, from the Japanese government, stipulated a trio of different threats and mentioned: 1. the lack of trained personnel in Japan 2. the lower competition due to the lack of strategic data set accumulation 3. and the disappearance of Japan-made security products.

The respondents were asked to suggest 3 ways to promote cybersecurity and privacy. Irrespective of the order, the respondents cited a wealth of means including: Awareness raising, incl. cyber-hygiene campaigns and in the mass media (7); Accessible cyber (and privacy) range; Education and training, incl. specialized staff and hands-on (8); Cybersecurity regulations to improve cybersecurity level, incl. breach notification requirements (2); Research personnel support (incl. better wages, better workplace, permanent jobs); Politicians awareness; Competitions (2); Successful companies recognition; User-friendly, non-intrusive, seamless security mechanisms; and discussion forums.

A
Appendix: Questionnaires

Below are the empty forms of the questionnaires that were provided to the audience.

A.1 CSIRTs

EUNITY Feedback Questionnaire: CSIRTs

Workshop session: CSIRTs (11/10/2017 morning)

Dear workshop participant, we are interested in gathering your feedback on international cooperation in cyber security operations.

It is not necessary to disclose your identity or name of your organization. We may quote your opinions in the workshop proceedings but they will not be attributed without your explicit permission.

If you have any questions or additional comments, please reach out to one of the EUNITY representatives.

Profile

To which category does your organization belong?

Industry	
Academia	
Government	

In your current role, do you perform any operational cybersecurity work, for example incident handling or intelligence gathering?

NO / OCCASIONALLY / DAILY

Incident coordination

Working with international partners to coordinate incident response, perform incident analysis or work on remediation together.

Do you coordinate incidents with international partners?

YES / NO

What are the types of such incidents?

Who do you cooperate with (countries or regions)? In particular, do you work with EU partners?

What are your experiences with remediation when cross-border cooperation was involved (for example infection cleanup, takedowns)?

How would you rate current benefits from cross-border incident coordination?
minimal / occasionally beneficial / significant

What are the main challenges in incident coordination and remediation when international cooperation is involved?

What could be improved? (for example better contacts in other organizations, more trust)

Information exchange

Exchange of any type of information, including everything from the large-volume machine generated data from sensors, intelligence on threat actors, vulnerabilities and best practices.

Do you share information with international partners?
YES / NO

Who do you cooperate with (countries or regions)? In particular, do you work with EU partners?

What type of information is exchanged?

How would you rate current benefits from international information exchange?
minimal / occasionally beneficial / significant

What are the main challenges in information exchange?

What could be improved? (for example sharing mechanisms, having more contact points)

Joint initiatives

Projects that involve cooperation with international partners on a regular basis. For example, shared threat monitoring infrastructure.

Are you involved in any cross border projects with an operational focus?
YES / NO

Who do you cooperate with (countries or regions)? In particular, do you work with EU partners?

What are the topic areas of these projects?

How would you rate current benefits from joint international projects?
minimal / occasionally beneficial / significant

What are the main challenges in such initiatives?

What could be improved? (for example new areas of interest, more international partners)

Exercises

Are you participating in exercises that include international partners?
YES / NO

What are the main goals of such exercises?

Is it a regular effort or organized on an ad hoc basis?

Who do you cooperate with (countries or regions)? In particular, do you work with EU partners?

How would you rate current benefits from international exercises?

minimal / occasionally beneficial / significant

What are the main challenges in exercises?

What could be improved?

Future plans

From your perspective, do you see a potential to improve Japan-EU cooperation in any of the areas above?

A.2 Industry

EUNITY Feedback Questionnaire

Workshop session: Industry

October 11th, 2017

Dear workshop participant, we are interested in gathering your feedback on research activities that are carried out in Europe. Your answers will be anonymous, and we are only interested in the classification of the organization that you are working in.

If you have any questions or doubts, please look at the glossary and/or ask a EUNITY representative. We are available to answer any question you may have.

Glossary

- SME: Small and Medium Enterprise. It is defined by the European Commission according to headcount and balance sheet turnover (smaller than 250 persons and less than 50 millions euros turnover)
- ISAC: Information Sharing and Analysis Center

Organization information

To which category does your organization belong ?

Industry	
Academia	
Government	

Do you offer cyber-security services/products ? YES NO

Do you consume cyber-security services/products ? YES NO

Do you carry out cyber-security research? YES NO

Cybersecurity considerations

Do you consider these topics important for your organization?

	YES	*NO*
Cyber Range exercises and simulation		
Education and training in cyber security		
Standardization of cyber security products/services as part of purchasing decisions		
Certification of cyber security products/services as part of purchasing decisions		
Performing standardization or certification of cybersecurity products/services		
Participation in standardization or certification of cybersecurity products/services		
Dedicated support to SMEs for cybersecurity preparedness/adoption		

If your organization performs activities in these areas, please briefly comment on the level of involvement of your organization:

	None	*Occasionally*	*Somewhat*	*Significant*
Cyber Range exercises and simulation				
Education and training in cyber security				
Certification of cyber security products/services				
Standardization of products/services				
Dedicated support to SMEs				

Market aspects of cybersecurity

What is your home market?

JAPAN EU Other (specify);

If you are a producer of cybersecurity product/services:

- Do you sell cybersec products/services to the Japanese market? YES / NO
- Do you sell cybersec products/services to the European market? YES / NO

Do you encounter issues in harmonization of legal frameworks in EU and Japan for cross-market selling of your cybersec products/services?
(please list issues, if any)

Are there cross-border aspects of cybersecurity protection measures affecting your organization that need addressing between EU and Japan?
(please list)

Are there cross-border aspects of cybersecurity protection measures affecting your organization that need addressing involving other countries as well?
(please list issues and involved countries)

What are the main issues in international this regard?

Cybersecurity challenges

What are the main cybersecurity challenges to your business?
(please list)

Are the following aspects a factor in the cybersecurity challenge being unsolved?

Considerations:	*YES*	*SOMEWHAT*	*NO*
Protection technology is nonexistent as of today			
Technology is not sufficiently efficient			
Internal processes in own organization			
Local (country) regulatory environment			
Insufficient international collaboration (public/gov institutions)			
Insufficient international collaboration (private sector)			

Are there research challenges affecting your business that would need addressing by the cybersecurity research community?
(please list)

Collaboration & regulation

Have you been involved in EU-Japan collaboration in cybersecurity of some sort until now?
(please describe, if any)

In what international fora (industry / standardization / other types) does your organization participate?
(please list)

Do you see value for your organization and industry in general in the establishment of regulatory sandboxing mechanisms (like those promoted in Singapore or the United Kingdom), to support innovation in cybersecurity?

Is your company active in sectorial ISACs? In what country(ies)?
(please list)

Questionnaire follow-up

Would you be willing to collaborate with the EUNITY study by answering potential follow-up questions we may have?

YES NO

If yes, we would appreciate to receive your contact information:

Name:

Organization:

e-mail address:

A.3 ECSO

EUNITY Feedback Questionnaire

Workshop session: ECSO (11/10/2017 afternoon)

Dear workshop participant, we are interested in gathering your feedback on research activities that are carried out in Europe. Your answers will be anonymous, and we are only interested in the classification of the organization that you are working in.

To which category does your organization belong ?

Industry	
Academia	
Government	

Do you practice cyber-security ? YES NO

Do you carry out cyber-security research ? YES NO

Glossary

GRC: Governance, Risk Management, and Compliance.
SME: Small and Medium Enterprise. It is defined by the European Commission according to headcount and balance sheet turnover (smaller than 250 persons and less than 50 millions euros turnover)
DLT: Distributed Ledger Technology. The best known DLT is blockchain.

If you have any questions or doubts, please look at the glossary and/or ask a EUNITY representative. We are available to answer any question you may have.

Overall ECSO structure and organization

Out of the 6 working groups that are currently constituting the ECSO activities, which ones do you consider important

Working group	Important	NOT important
WG1 – Standardisation, certification, labelling & supply chain management		
WG2 - Market deployment, investments and international collaboration		
WG3 – Verticals		
WG4 – Support to SME's, coordination with countries (in particular East EU) and regions		
WG5 – Education and training		
WG6 – Strategic research and innovation agenda		

Would you add an area of interest that you consider important ?

Do you see the outcome of the documents produced by each of the working group as relevant?

	Relevant	NOT relevant.
WG1 – Standardisation, certification, labelling & supply chain management		
WG2 - Market deployment, investments and international collaboration		
WG3 – Verticals		
WG4 – Support to SME's, coordination with countries (in particular East EU) and regions		
WG5 – Education and training		
WG6 – Strategic research and innovation agenda		

The next parts of the questionnaire are with respect to the thematic areas.

European Ecosystem for Cybersecurity

This covers both links between projects inside the cyber-security domain, and links with other EU structural initiatives in application domains (Energy, Big Data, Health, …)

Do you consider the topics relevant ?

	YES	NO
Cyber Range and simulation		
Education and training		
Certification and standardisation		
Dedicated support to SMEs		

Do you work on similar topics ?

	YES	NO
Cyber Range and simulation		
Education and training		
Certification and standardisation		
Dedicated support to SMEs		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
Cyber Range and simulation		
Education and training		
Certification and standardisation		
Dedicated support to SMEs		

Do you see other areas in this domain ? If yes, please list or comment.

Demonstrations for the society, economy, industry and vital services

This topic is related to the development and use of cyber-security products and services into application areas. The listed areas are considered high priority for the European digital society.

Do you consider the topics relevant ?

	YES	NO
Industry 4.0		
Energy		
Smart Buildings & Smart Cities		
Transportation		
Healthcare		
E-services for public sector, finance, and telco		

Do you work on similar topics ?

	YES	NO
Industry 4.0		
Energy		
Smart Buildings & Smart Cities		
Transportation		
Healthcare		
E-services for public sector, finance, and telco		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
Industry 4.0		
Energy		
Smart Buildings & Smart Cities		
Transportation		
Healthcare		
E-services for public sector, finance, and telco		

Do you see other areas in this domain ? If yes, please list or comment.

Collaborative intelligence to manage cyber threats and risks

Cyber-threats are considered cross-border, and with multiple forms. Research and innovation activities in the EU must address all the aspects of cyber-threat management.

Do you consider the topics relevant ?

	YES	NO
GRC: Security Assessment and Risk Management		
PROTECT: High-assurance prevention and protection		
DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection		
RESPONSE and RECOVERY: Cyber threat management: response and recovery		

Do you work on similar topics ?

	YES	NO
GRC: Security Assessment and Risk Management		
PROTECT: High-assurance prevention and protection		
DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection		
RESPONSE and RECOVERY: Cyber threat management: response and recovery		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
GRC: Security Assessment and Risk Management		
PROTECT: High-assurance prevention and protection		
DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection		
RESPONSE and RECOVERY: Cyber threat management: response and recovery		

Do you see other topics in this domain ? If yes, please list or comment.

Remove trust barriers for data-driven applications and services

The development of the digital society will imply the development of new applications and services, driven by data collected from their use. However, the pervasiveness of data collection and abuse in data usage might discourage users, thus limiting the benefits of IT technology for society.

Do you consider the topics relevant ?

	YES	NO
Data security and privacy		
ID and Distributed trust management (including DLT)		
User centric security and privacy		

Do you work on similar topics ?

	YES	NO
Data security and privacy		
ID and Distributed trust management (including DLT)		
User centric security and privacy		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
Data security and privacy		
ID and Distributed trust management (including DLT)		
User centric security and privacy		

Do you see other areas in this domain ? If yes, please list or comment.

Maintain a secure and trusted infrastructure in the long-term

The topics mentioned in the previous pages will contribute to improving cyber-security for the digital society, but cyber-security must be ensured in the long term. These topics are thus highlighted to complement the previous topics already mentioned earlier in the questionnaire.

Do you consider the topics relevant ?

	YES	NO
ICT protection		
Quantum resistant crypto		

Do you work on similar topics ?

	YES	NO
ICT protection		
Quantum resistant crypto		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
ICT protection		
Quantum resistant crypto		

Do you see other areas in this domain ? If yes, please list or comment.

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

In addition to the previous topics, one of the key objectives of Europe is to have a more secure digital infrastructure, limiting the need for patch deployment.

Do you consider the topics relevant ?

	YES	NO
Trusted supply chain for resilient systems		
Security and privacy by-design		

Do you work on similar topics ?

	YES	NO
Trusted supply chain for resilient systems		
Security and privacy by-design		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
Trusted supply chain for resilient systems		
Security and privacy by-design		

Do you see other areas in this domain ? If yes, please list or comment.

From security components to security services

Europe is considering the development of the cyber-security industry but has not decided on the focus, either secure products, or secure services).

Do you consider these topics relevant ?

	YES	NO
Security components		
Integration of cyber-security in systems		
Cyber-security services		

Do you work on similar topics ?

	YES	NO
Security components		
Integration of cyber-security in systems		
Cyber-security services		

Would you be interested in exchanging information and/or building joint projects ?

	YES	NO
Security components		
Integration of cyber-security in systems		
Cyber-security services		

Do you see other areas in this domain (particularly, which cyber-security components are you interested in) ? If yes, please list or comment.

A.4 Privacy

Privacy Questionnaire

EUNITY Policy Workshop **Tokyo, 11/12 October 2017**

1) Are measures concerning data protection and privacy part of the Japanese Digital Strategy?

YES NO

2) Are you/your firm/your business directly involved in its implementation?

YES NO

3) Are cybersecurity and data protection treated separately by the Japanese private business?

YES NO

4) The Data Protection Officer. If your company has established a similar role to the one required by the GDPR, what is his/her background (Law, IT, other)?

………

………

………

………

5) Is Japan a member of any interregional industrial or governmental federation in the area of cyber security and/or privacy?

YES(name)…………………………………….. NO

6) Do you foresee that Japanese laws and regulations on privacy and/or cyber security are going to be up to date and applicable in ten years' time, considering technological advancements?

YES NO

7) How do the Japanese legal and regulatory regimes ensure interoperability of the systems and portability of (personal) data? *Are you affected by such obligations?*

Legal obligations	YES	NO
Adherence to standards	YES	NO
Guidelines from regulatory bodies	YES	NO
Others …………………………………………………………………………………….. ………………………………………………………………………………………		

8) Is your organization assessing its readiness to GDPR? If so, what is the main challenge you are encountering

- Appointment of a data protection officer

- Deploying data security measures (encryption, anonymization, others)

- Implementing data protection by design

9) List the three major cyber-attacks Japan suffered over the last 5 years and if you have been affected or targeted by one of those.

1……

2……

3……

A.5 Research and Innovation

EUNITY Feedback Questionnaire

Workshop session: Research & Innovation (12/10/2017 afternoon)

Dear workshop participant, we are interested in gathering your feedback on research activities that are carried out in Europe. Your answers will be anonymous, and we are only interested in the classification of the organization that you are working in.

To which category does your organization belong ?

Industry	
Academia	
Government	

If you have any questions or doubts, please ask a EUNITY representative. We are available to answer any question you may have.

Do you practice cyber-security ? YES NO

Do you carry out cyber-security research ? YES NO

Are you familiar with any national/international/sectorial research strategy, roadmaps and strategic agendas focused on cybersecurity or privacy in Japan?

YES NO

If yes, please list ones that you consider most relevant:

Do you consider them aligned with the needs of the industry? YES NO

Transforming outcomes of research into technologies and products is often a challenge. From your experience, what are the main obstacles in the field of cybersecurity?

Do you know the main strategic research directions in your institution?

YES NO

If yes, please list ones that you consider most relevant:

Do you know mechanisms to finance cybersecurity research available to your institution?
YES NO

If yes, please give some examples:

Does the industry finance cybersecurity research? YES NO

What kind of cybersecurity research does industry finance?

Does your company have any foreign cooperation with EU?

- in the research area	YES	NO
- joint projects	YES	NO
- exchange staff	YES	NO

Does your company have any foreign cooperation with someone other than the EU ?

- in the research area	YES	NO
- joint projects	YES	NO
- exchange staff	YES	NO

In your opinion, what are the top 3 threats that will be most relevant in the upcoming years?

1.

2.

3.

…

Suggest 3 ways to promote Cyber Security and Privacy?

1.

2.

3.

…

What percentage of your organization budget is invented in Cyber Security and Privacy? Do you think this is sufficient?

YES NO

Percentage invested (%):

Where would you invest? Core network, end point, infrastructure, training, etc.

Does your investment in Cyber Security have sufficient traction/is it a good investment? If not what should we do?
Is it a good investment?

YES NO

What should we do?

Is there a sufficient global collaboration on countering Cyber Security threats? If no, what are the steps to make it sufficient?

YES NO

What are the steps to make it sufficient?

Is the existing Legal Framework suitable and sufficient to address the changing nature of the Cyber Security and Privacy landscape

YES NO

Other than Cyber Security and Privacy what other ICT areas should EU-JP collaborate on?

1.

2.

3.

…

Would you be so kind and leave us your contact details so we can send you a more detailed questionnaire?

YES NO

If YES

Name:
Organization:
e-mail address :

Or contact Anna Felkner (anna.felkner@nask.pl) and/or Christos Papachristos (cpapachr@ics.forth.gr)

B

Glossary

Name	Explanation
AoI	Area of Interest
APAC	Asia Pacific
ASEAN	Association of Southeast Asian Nations
CCTV	Closed circuit television
CEPS	Center for European Policy Studies
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CRIC-CSF	Cyber Risk Intelligence Center Cross Sectors Forum
CSF	Cross Sectors Forum
CSIRT	Computer Security Incident Response Team
DPA	Data Protection Authorities
DPO	Data Protection Officer
DSM	Digital Single Market
EC	European Commission
ECSO	European Cyber Security Organisation
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
GEANT	pan -European data network for the research and education community
ICT	Information and Communications Technology
IoC	Indicator of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center

Name	Explanation
IT	Information Technology
JR East	Japan Railway East
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
METI	Ministry of Economy, Trade and Industry
MIC	Ministry of Internal Affairs and Communications
MISP	Malware Information Sharing Platform
MS	Member States
NICT	National Institute of Information and Communications Technology
NIS directive	Directive on security of network and information systems
OT	Operational Technology
PI	Personal Information
PoC	Point of Contact
PPI	Protection of Personal Information
R&I	Research and Innovation
RIPE NCC	”Réseaux” IP ”Européens” Network Coordination Centre
SRA	Strategic Research Agenda
STIX	Structured Threat Information Expression
TF/SVD	Task Force on Software Vulnerability Disclosure
TF&CSIRT	Task Force on Computer Security Incident Response Team
WG	Working Group