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 D2.2: Workshop 2 proceedings

Abstract: This document includes the presentations and the related supporting documents provided by the speakers from the second EUNITY workshop held in Brussels, 24 January 2019. The proceedings also include a discussion section with the feedback, the discussion triggered by the presentations as well as the results from the questionnaires.

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

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

The *EUNITY* consortium consists of:

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

Contents

1 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's main goal was to develop and encourage 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 European 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 initially gathered relevant stakeholders at two workshops, one in each region (Europe and Japan), taking advantage of the co-location with other events as much as possible. Thanks to the expertise of its members, EUNITY has collected the appropriate existing research agendas, legislation and business practices in Europe and Japan.

We then analyzed the information collected to formulate recommendations, including business opportunities and a research agenda. A particular attention was brought to the similarities of the research and market strategies, as well as the differences that must be taken into account when addressing both markets. EUNITY operated in close relationship with the European Cyber Security Organization association, the cybersecurity cPPP signatory and the European Commission. EUNITY covered 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 ensured that the most relevant and recent information available was on one hand taken into account by the project and on the other hand was provided 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 first EUNITY workshop took place on October 11-12, 2017 in Tokyo, Japan and the proceedings are available in the deliverable D2.3: Workshop 1 proceedings of the EUNITY project.

The second EUNITY workshop was held in Brussels on January 24, 2019. The aim was to facilitate the exchange of good practices on cyber policy and investigate business opportunities in the context of the EU-Japan Trade agreement. The discussion helped identify where objectives or approaches of the European Union and Japan are close and where diverging if any. The workshop helped identify where cooperation could be strengthened beyond political aspects of cybersecurity, such as on aspects related to standards, certification, R&I, pilots for verticals.

Approximately, an amount of 63 people attended the workshop, including participants from academia, industry, SMEs. The workshop program consisted of three (3) sessions, in which apart from the introduction and setting the expectations of the workshop, covered the areas of European and Japanese Ecosystems, as well as working session on business solutions applied to selected vertical sectors.

The presentations triggered a discussion and feedback, which is included in Chapter 4. The feedback from the audience is also presented through answers to questionnaires, in which each participant provided her point of view on the topics discussed during the sessions of the workshop.

Brussels, 24th January 2019

The EUNITY Consortium

2 Workshop Program

2.1 Program Chairs

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

2.2 Program

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

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

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

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

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

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

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

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

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

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

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

12:30 - 13:30 Networking lunch

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

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

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

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

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

15:00 - 15:15 Networking coffee break

15:15 - 15:45 Training and awareness challenges

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

15:45 - 16:15 Information sharing challenges

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

16:15 - 17:00 Closing discussion on potential cooperation & next steps
Hervé Debar, Telecom SudParis/EUNITY

17:00 End of Meeting

3 Presentations

3.1 Session 1: Introduction

This section contains the presentations from the second EUNITY workshop which lasted one day.

3.1.1 Welcoming remarks from ECSO and EUNITY

3.1.2 Expectations of the workshop

The first session included the welcoming remarks from ECSO and EUNITY and the expectations of the workshop, presented in three presentations, by Hervé Debar (Telecom SudParis/EUNITY): “EUNITY project expectations”, Jakub Boratynski (DG CONNECT, European Commission): “DG CONNECT expectation” and the “Japanese delegation expectations”, by Reiko Kondo (Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC)).

3.2 Session 2: European and Japanese Ecosystems

3.2.1 Business approaches to cybersecurity

The next session was on the European and Japanese Ecosystems, moderated by Luigi Rebuffi from European Cyber Security Organisation (ECSO). The session included the “European view on the Cybersecurity Market” by Ulrich Seldeslachts, from LSEC and the “Japanese view on the Cybersecurity Market”, by Hiromichi Nakahara and Hiroo Inoue, from the Japan External Trade Organization (JETRO), presented below:

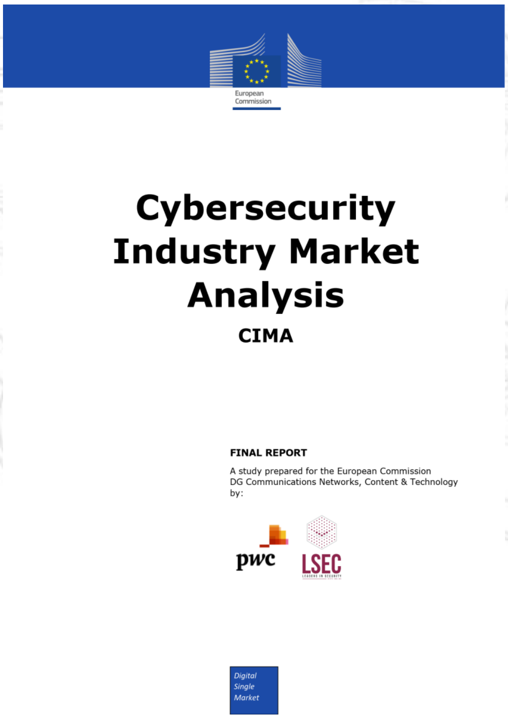
CIMA 2019

Cybersecurity Industry Market Analysis

ECSO EUNITY Workshop

Ulrich Seldeslachts, CEO LSEC, Chair ECSO WG2
Brussels, January 24th, 2019

CIMA : Cybersecurity Industry Market Analysis



European Commission

Cybersecurity Industry Market Analysis

CIMA

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

pwc LSEC

Digital Single Market

pwc LSEC

Cybersecurity Industry Market Analysis

CIMA

November 2018

4 © Anakyn bvba for LSEC – PWC - EC

Source: LSEC, 2018

Objective

Provide EU Commission independent and unbiased industrial cybersecurity strategy

- Survey cybersecurity markets and quantify the European industry and service sectors in this ICT product and service portfolio

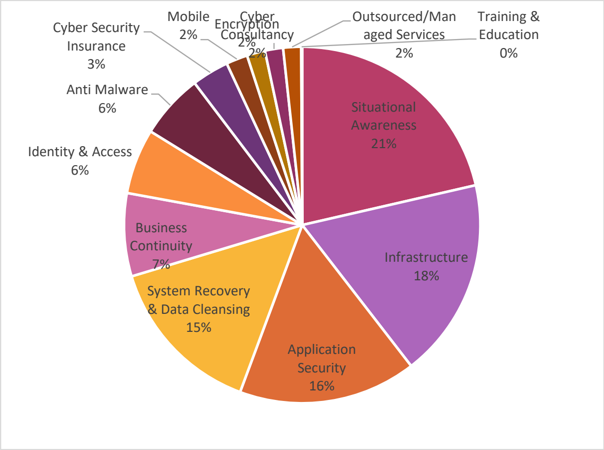
- Survey the import and export flows of cybersecurity products. Who are the large exporters and who are their clients?

- Survey the cross border trade flows in the European Union

Cybersecurity Spending likely exceeding Cybercrime

By 2017, the global Cyber Security market is expected to skyrocket to $120.1 billion from $63.7 billion in 2011.

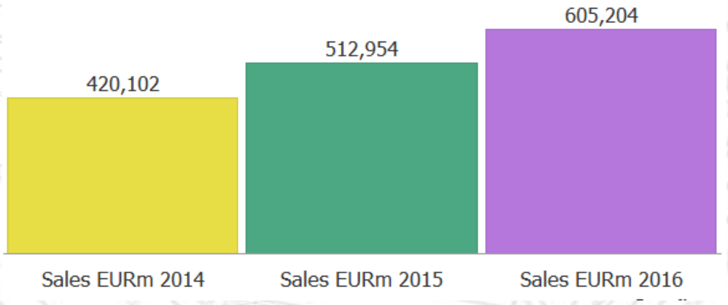
- Cybercrime costs the global economy $450 billion (Hiscox Insurance, 02/2017)
- Cost to the global economy of cybercrime has been estimated at $445 billion a year (World Economic Forum, 02/2017)

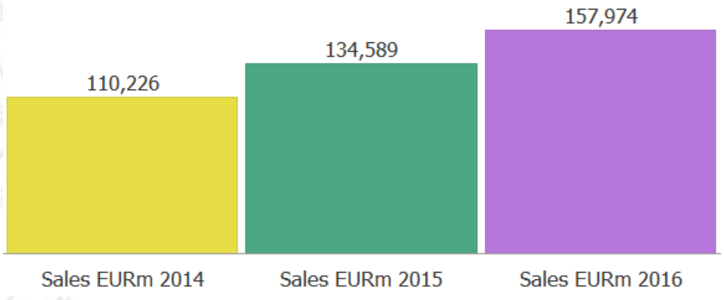


- Cybersecurity Economic Trade (Sales) amounted to €650 billion in 2016
- Biggest Spent is Situational Awareness and Intrusion Detection
- Only just over 500 mio € was spent on training and education

Source: LSEC, 2018

Global vs EU Cyber Market 2014 through 2016 - Spending



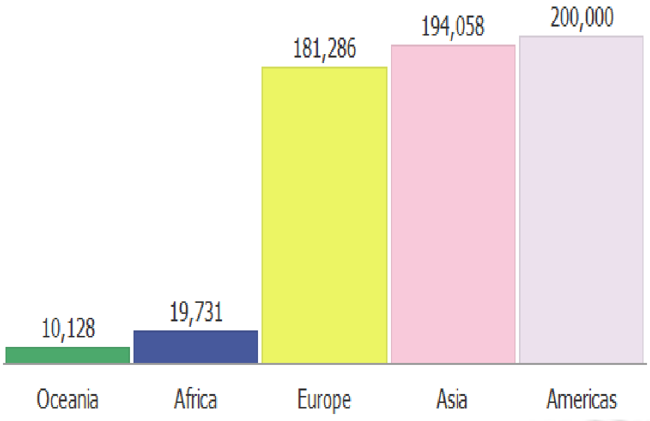


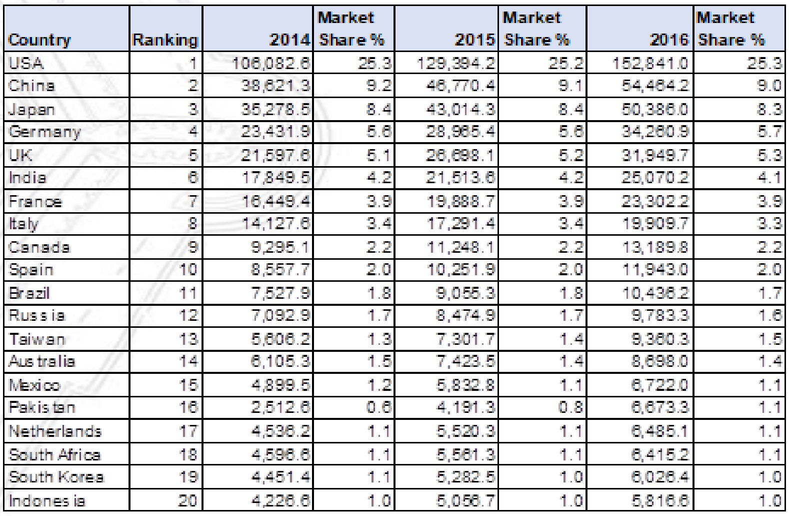
- Global market value of EUR 605bn in 2016
- 18% increase from 2015, compared with an increase of 22% between 2014 and 2015

- EU market value of EUR 158bn in 2016
- 17.4% increase from 2015, compared with an increase of 22% between 2014 and 2015
- EU accounts for 26.3% of global market

Source: LSEC, KMatrix 2017

Global Cyber Spending View – Europe vs RoW





Country	Ranking	2014	Market Share %	2015	Market Share %	2016	Market Share %
USA	1	106,082.6	25.3	129,394.2	25.2	152,841.0	25.3
China	2	38,621.3	9.2	46,770.4	9.1	54,464.2	9.0
Japan	3	35,278.5	8.4	43,014.3	8.4	50,386.0	8.3
Germany	4	23,431.9	5.6	28,965.4	5.6	34,260.9	5.7
UK	5	21,597.6	5.1	26,698.1	5.2	31,949.7	5.3
India	6	17,849.5	4.2	21,513.6	4.2	25,070.2	4.1
France	7	16,449.4	3.9	19,888.7	3.9	23,302.2	3.9
Italy	8	14,127.6	3.4	17,291.4	3.4	19,909.7	3.3
Canada	9	9,295.1	2.2	11,248.1	2.2	13,189.8	2.2
Spain	10	8,557.7	2.0	10,251.9	2.0	11,943.0	2.0
Brazil	11	7,527.9	1.8	9,055.3	1.8	10,436.2	1.7
Russia	12	7,092.9	1.7	8,474.9	1.7	9,783.3	1.6
Taiwan	13	5,606.2	1.3	7,301.7	1.4	9,360.3	1.5
Australia	14	6,105.3	1.5	7,423.5	1.4	8,698.0	1.4
Mexico	15	4,899.5	1.2	5,832.8	1.1	6,722.0	1.1
Pakistan	16	2,512.6	0.6	4,191.3	0.8	6,673.3	1.1
Netherlands	17	4,536.2	1.1	5,520.3	1.1	6,485.1	1.1
South Africa	18	4,596.6	1.1	5,561.3	1.1	6,415.2	1.1
South Korea	19	4,451.4	1.1	5,282.5	1.0	6,026.4	1.0
Indonesia	20	4,226.6	1.0	5,056.7	1.0	5,816.6	1.0

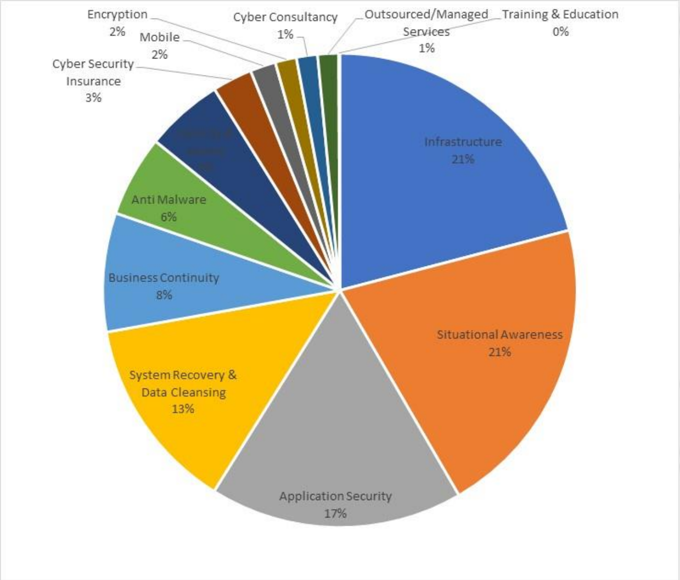
** Overall, the top 10 countries accounted for 69% of Cybersecurity sales in all three years and the top 20 countries accounted for 82%.*

Source: LSEC, KMatrix 2017

CyberSecurity Industry Market Analysis 2018 : Global

- Cybersecurity market is globally a EUR 600 billion market, that is expected to grow in the next five years on average by approximately 17% in terms of sales, number of companies and employment. The largest market is North America, followed by Asia and Europe.
- Looking at global sales figures the **USA is the dominant country** (25.3% of global sales) followed by China (9%), Japan (8.3%) and Germany (5.7%). In Sales terms the **EU (including the UK) represented 26% of the global market in 2016**, above the USA, making the **EU the single largest Cybersecurity market** in the world **when accounted for as a single market**.

European Spending in Products and Services Breakdown



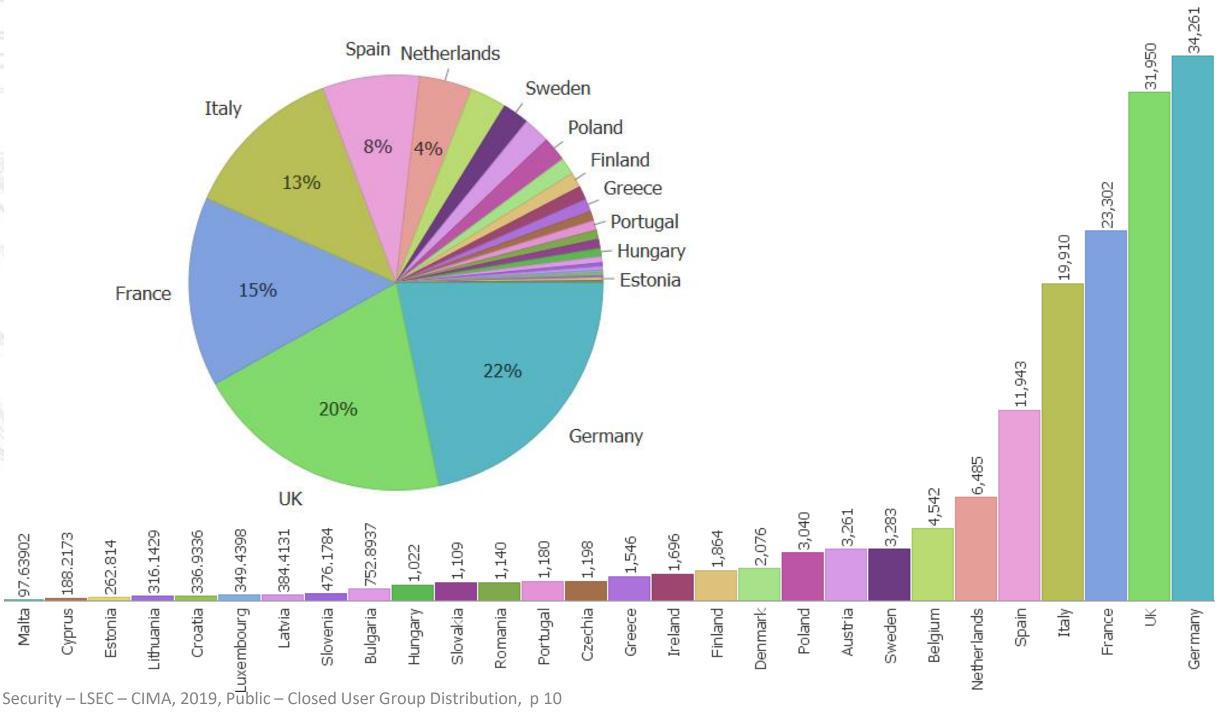
- Majority of the spending in **infrastructure** and **intelligence** (situational awareness)
- More **mature markets** spend more in **detection and prevention,** less mature markets spend more in incident management and recovery
- **Training and Education** only account for 500 m EUR
- Products and services **heavily fragmented** (over 1100 categories (level 5)
- **Continued growth** from **all product and services categories**, strongest growth still from top domains (Infrastructure, Application Security, Situational Awareness)

Source: LSEC, KMatrix 2017

CIMA 2018 Update

- From both a sales, company and employment perspective, **Situational Awareness** has been the **largest Cybersecurity market**, followed by Infrastructure and Application Security spending. The global Cybersecurity market has grown rapidly across all sub-sectors over the last 3 years, varying from 5% for Training and Education to 25% for Identity and Access and for Outsourced/ Managed Services in 2015/16, with the number of global companies and employment growing at similar rates. Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum out to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%.

Cyber Security Spending per EU Country



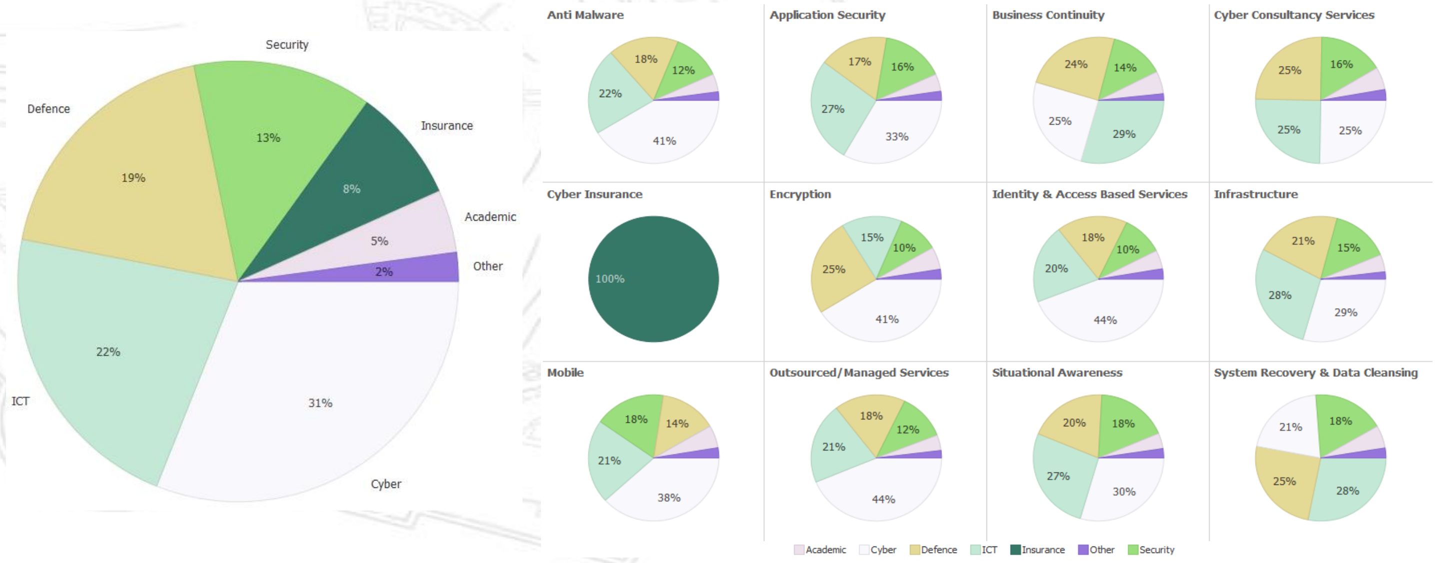
Cybersecurity Industry Market Analysis : Europe

- The EU Cybersecurity market has **grown** rapidly across all sub-sectors over the last 3 years, varying from **4% for Training and Education to 26% for Encryption in 2015/16,** with the number of EU companies and EU employment growing at similar rates. **Each Cybersecurity sub-sector is forecast to continue growing rapidly at a similar rate (above 10% per annum to 2021) apart from Training and Education which is forecast to grow at a rate of just above 5%.** Infrastructure (19%), Situational Awareness (17%) and Application Security (17%) are the largest EU sub-sectors in sales terms.

European Landscape continued

- **Europe is the location for the corporate headquarters of 14%** of the top 500 global Cybersecurity providers, compared to 75% for the Americas (North and South), 7% for Israel and 4% for Asia.
- **Cybersecurity activities and companies have not emerged solely from the ICT sector, but from across a range of market sectors**. Looking at the sectors involved in delivering Cybersecurity products and services for the EU in 2016, **31%** of the sales value originates from companies that are **solely** involved in the **Cybersecurity** sector, 22% originates from companies whose core business is ICT, 19% originates from companies whose core business is Defence/ Aerospace and 13% from companies whose core business is Security.

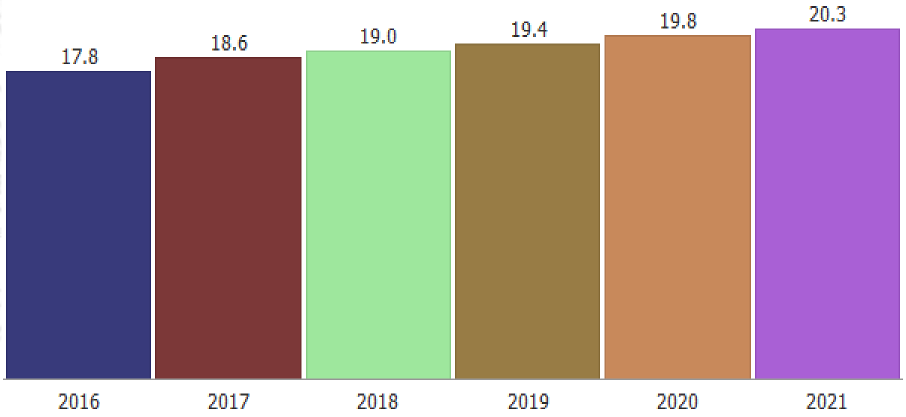
EU Cybersecurity Industry Market Breakdown*



*rely on some subjective assessments of company core activities and estimates of the proportion of revenues relating to Cybersecurity

Source: LSEC, KMatrix 2017

EU Market Growth Potential – 2016 – 2020 (CAGR in %)

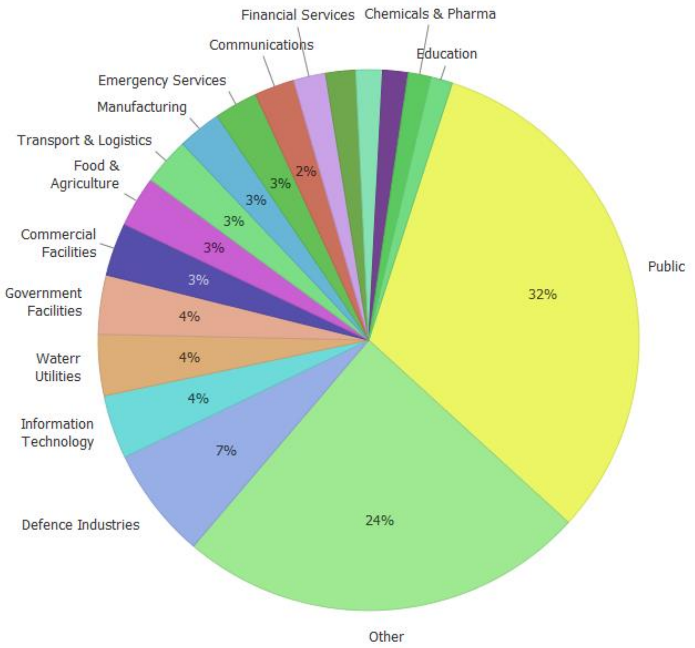


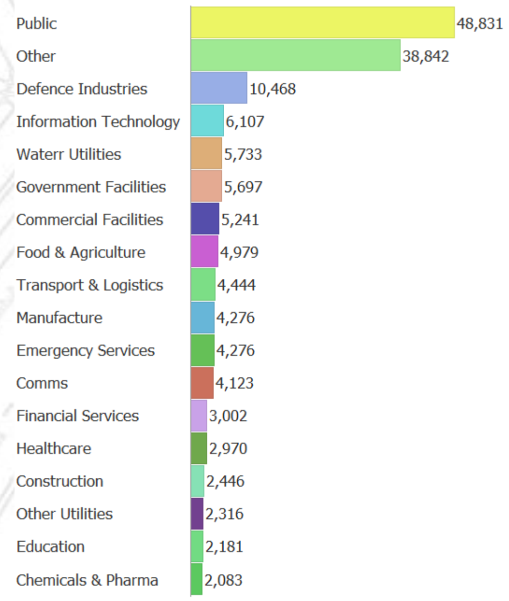
Source: LSEC, KMatrix 2017

CIMA 2018 Update : EU Exec Summ : Public – Private - Import

- 16 end user categories, based upon the Cybersecurity market flows. The EU End User markets in sales terms comprise **Private users (45% of sales), Public users (31%)** and "Other" users (25%). The "Other" category is large because it includes retail activities (10%) and un-attributable activities (10%). The Public Sector Cybersecurity market ranges between 24% (Germany) to 48% (UK.
- **The EU imports EUR 8.5 billion from outside the EU**, which is approximately **5.3% of the total EU Cybersecurity market in 2016**. The percentage of imports into each Member State from within the EU (as opposed to outside the EU) varies significantly by country, from 17% for the UK through to 53% for France (2016 figures). **Member States on average import 30% of products/ services from other EU countries and 70% from outside the EU**: their EU imports range from 20% for Encryption and Outsourced/ Managed Services through to 32% for Situational Awareness and System Recovery and Data Cleansing

European Perspective End User Breakdown

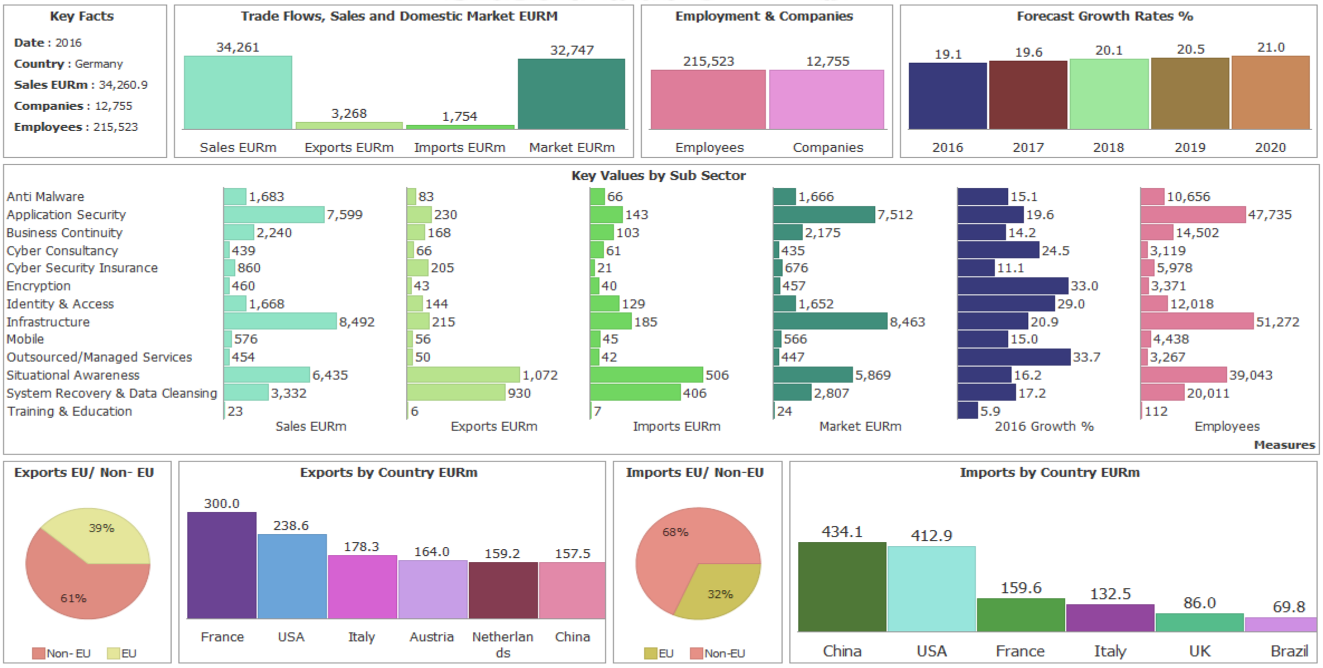




- 32% Public
- 68% Private, of which 24% is unattributed
- 44% relates to 16 industries
- Public % varies between 25-43% across the EU

Source: LSEC, KMatrix 2017

CIMA 2018 Update : Country Reports - Germany



Key Facts

Date : 2016

Country : Germany

Sales EURm : 34,260.9

Companies : 12,755

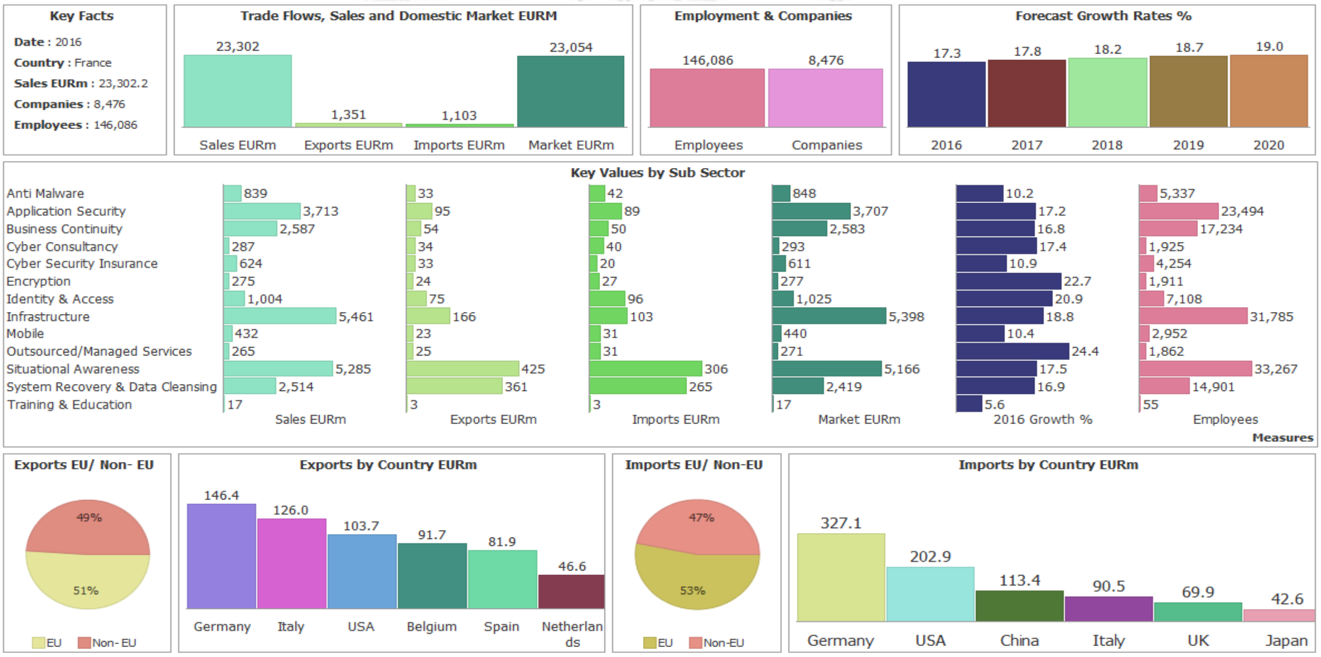
Employees : 215,523

Key Values by Sub Sector

	Sales EURm	Exports EURm	Imports EURm	Market EURm	2016 Growth %	Employees
Anti Malware	1,683	83	66	1,666	15.1	10,656
Application Security	7,599	230	143	7,512	19.6	47,735
Business Continuity	2,240	168	103	2,175	14.2	14,502
Cyber Consultancy	439	66	61	435	24.5	3,119
Cyber Security Insurance	860	205	21	676	11.1	5,978
Encryption	460	43	40	457	33.0	3,371
Identity & Access	1,668	144	129	1,652	29.0	12,018
Infrastructure	8,492	215	185	8,463	20.9	51,272
Mobile	576	56	45	566	15.0	4,438
Outsourced/Managed Services	454	50	42	447	33.7	3,267
Situational Awareness	6,435	1,072	506	5,869	16.2	39,043
System Recovery & Data Cleansing	3,332	930	406	2,807	17.2	20,011
Training & Education	23	6	7	24	5.9	112

Measures

CIMA 2018 Update : Country Reports - France



Key Facts

Date : 2016

Country : France

Sales EURm : 23,302.2

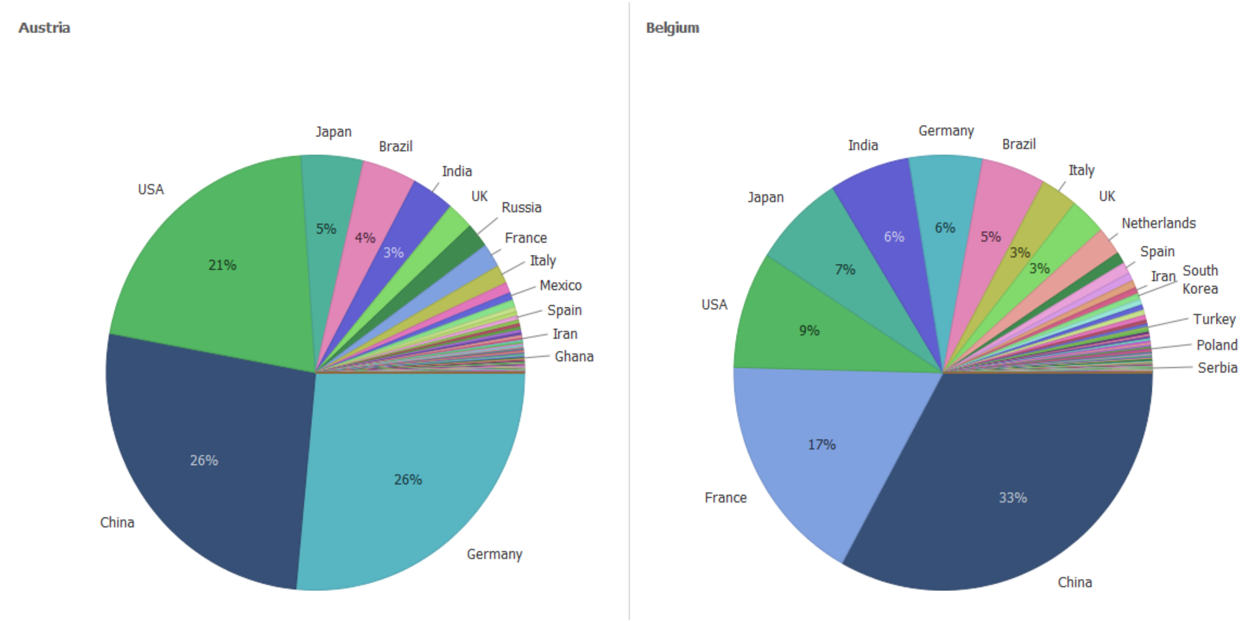
Companies : 8,476

Employees : 146,086

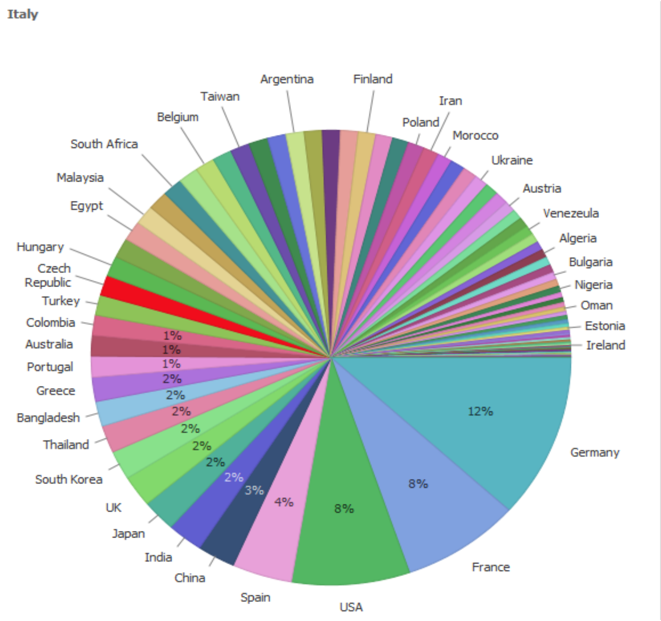
CIMA 2018 Update : EU Exec Summ – EU Competitveness

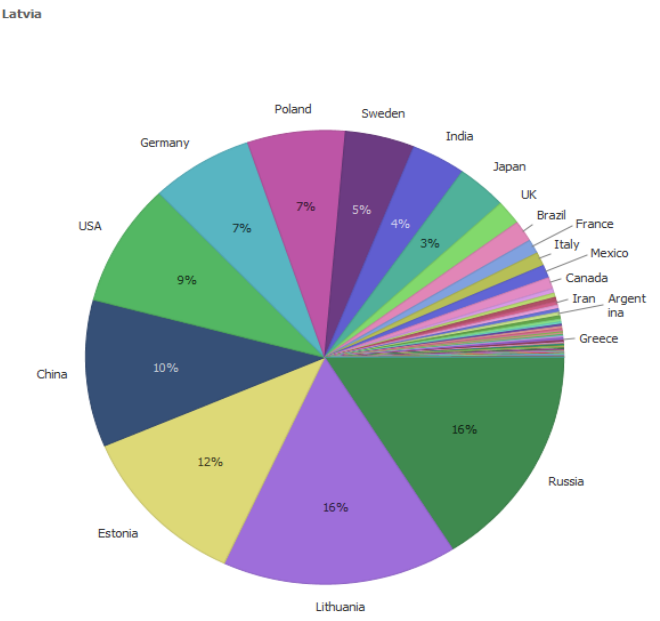
- Cybersecurity activities and companies have emerged from a range of market sectors where Europe is strong (ICT, defence/ aerospace and security) – this offers **future opportunities**.
- The **Digital Single Market** will promote Cybersecurity in the EU. The **NIS directive** will stimulate EU critical infrastructure sectors to address Cybersecurity and this will create an opportunity for EU Industry.
- Public users form a significant part of the EU End User market in sales terms (at least 31%) and so **public procurement** policies can significantly influence the Cybersecurity market.
- While the USA is the EU's main competitor in global markets (followed closely by China), China followed by the US is the main competitor to EU suppliers in EU markets and specifically in the smaller EU countries.

CIMA 2018 Update : Imports by Country of Origin per EU MS



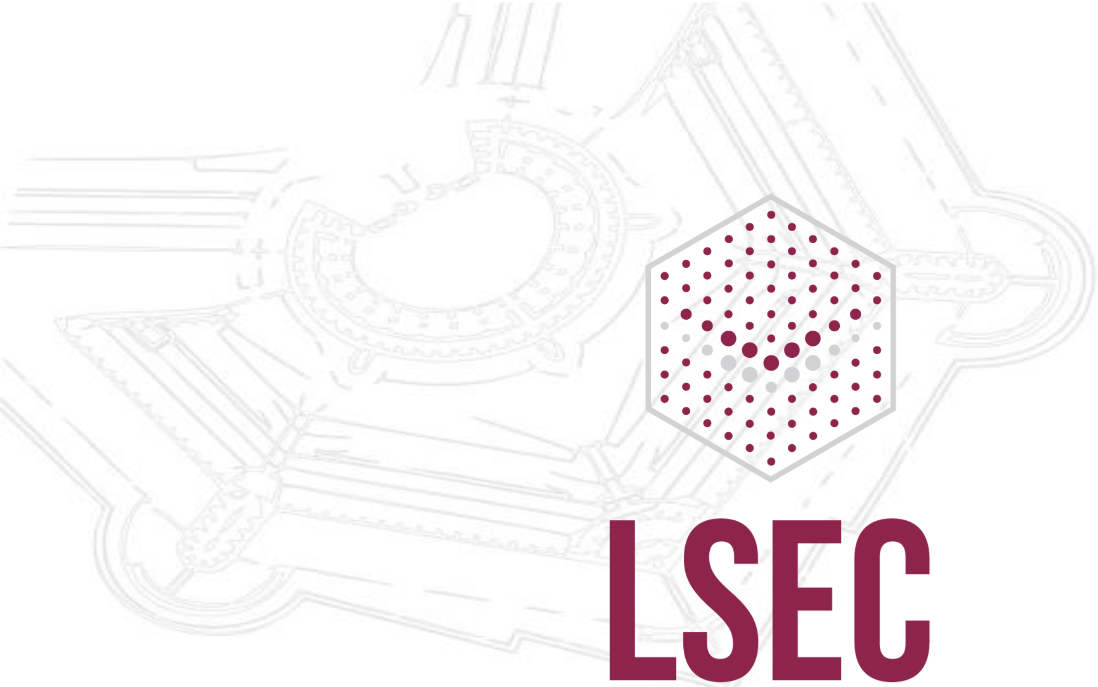
CIMA 2018 Update : Exports by Country of Origin per EU MS





2019 Update

- Current document to be published relying on 2016 market data
- While this is still relevant, published by the EC, it won't have a long lifetime
- LSEC, ECSO & partners could publish and update of the 2018 report focusing on relevant data, updating numbers and using the materials to support the further policy discussions
- Updated data could be published as an interactive market analysis, as a interactive tool allowing to browse per country and per category, linking it to the radar;
- This might be in collaboration with the EC & Japan EUNITY



LSEC

LEADERS IN SECURITY

www.lsec.eu

NOT THE END

More information, slides and follow-up

www.lsec.eu

www.3if.be - .eu

Q or C

Ulrich Seldeslachts
ulrich@lsec.eu
+32 475 71 3602

METI
Ministry of Economy, Trade and Industry

Cybersecurity Business Opportunities and Environment in Japan

Hiromichi Nakahara
Ministry of Economy, Trade and Industry, Japan

1. Market Trend (1)General Overview

■With coming in force of “The Basic Act on Cybersecurity”(Note1), Japanese government has instituted Cybersecurity Strategic Headquarters and Cabinet Secretariat National center of Incident readiness and Strategy for Cybersecurity(NISC) in January 2015 to strengthen the system.

■In recent times, cyber attacks have become quite smart and sophisticated and run the risk of inflicting serious damage. In order to minimize the damage by cyber attacks, importance of thorough security countermeasures and monitoring services is increasing.

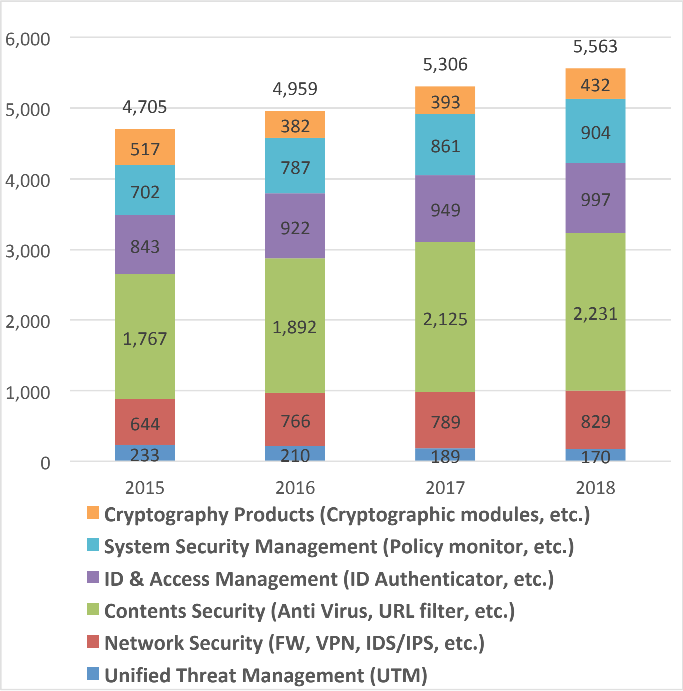
2016	948.2 billion yen
2017	996.5 billion yen
2018	**1045.5 billion yen** （**Over a trillion yen**）

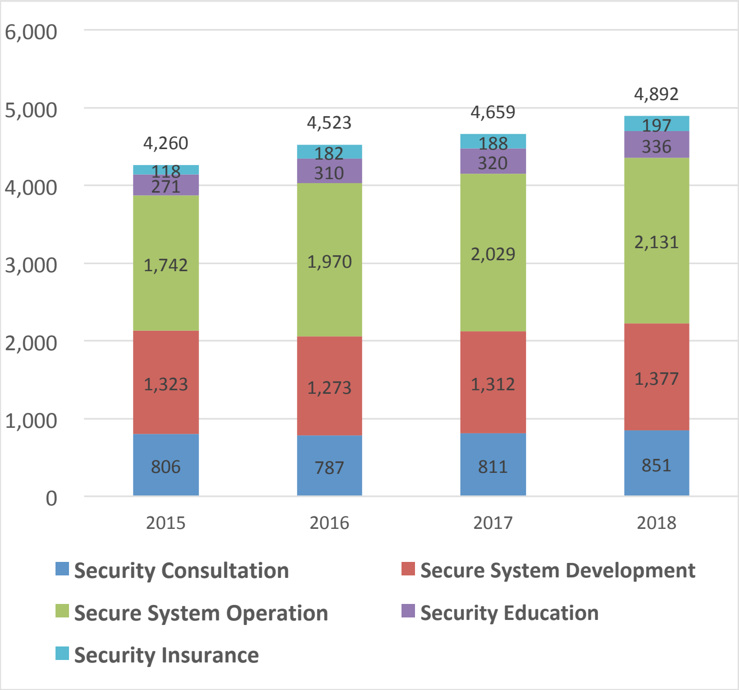
※Expectancy

[Source] Japan Network Security Association “Domestic Cyber Security Market2017’s investigation report(preliminary figures)”.

1. Market Trend (2) Products and Services

- Both Products and Services Market expand.
- The Growth of Services Market in 2018 is slightly higher than that of Products in 2018.





Changes of scale in the market of
Domestic Cyber Security Products

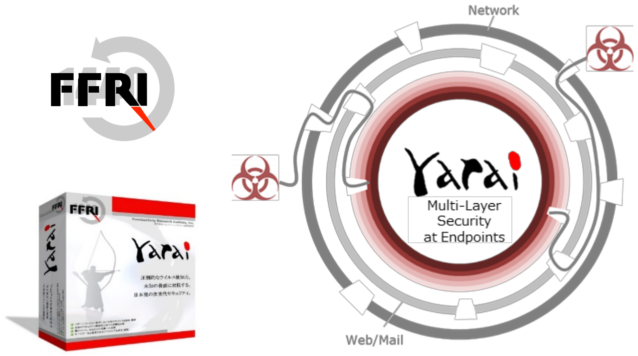
Changes of scale in the market of
Domestic Cyber Security Services

【Source】Japan Network Security Association "Domestic Cyber Security Market2017's investigation report(preliminary figures)".

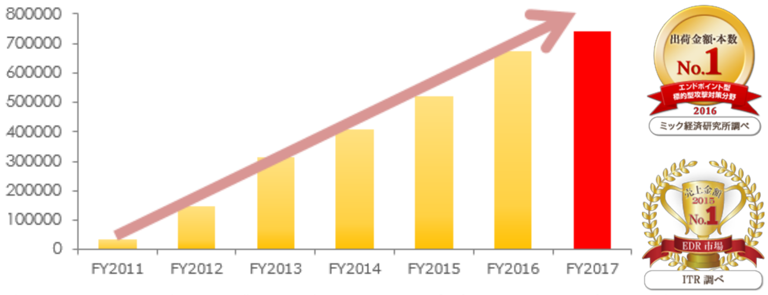
2. Japanese Major Players (1) Companies

■Japanese companies pursue development and expansion of services using advanced technology. (Examples)

Next Generation Endpoint Protection



FFRI In-house Study | Strong Trend in Installation Licenses



*Sources : MIC Research Institute, "Status and Future Prospects of Information Security Solutions Market 2016 [External Attack Protection Solutions Edition]"
: ITR, "ITR Market View: Information Leakage Countermeasure Market 2016"

Name of company	Core Business in this field	Net sales (M yen)	Note
NEC Corporation	• It will deploy services such as "Security-integrated management and response solutions" where devices like servers and PCs connected to internal network will be centralized control in real time and "Threat and vulnerability information management solutions" that instantly provides information on and method to deal with cyber attack. • In February 2017 it started Security Consulting service for corporates.	2,665,000 2,844,447	FY March, 2017, Consolidated FY March2018
Internet Initiative Japan Inc.	• It will implement technical validation that will dynamically change the monitoring level of security on cloud and control unauthorized communication. It expanded the scope of validation to office network and devices in October 2017 and started demonstration experiment. It plans to offer full-range security as network service solution by the latter half of 2018.	157.790 176,040	FY March, 2017, Consolidated FY March 2018
LAC Co., Ltd.	• As the leading Japanese company in the field of cyber security, it will expand the service offerings utilizing state-of-the art technologies in security domain against cyber attacks that will target global events like Tokyo Olympics and Paralympics 2020 by re-building "JSOC" security monitoring center, building CSITR and providing support for its operation, enhancement of specialists capable to carry out security diagnosis service etc. • Registered as METI Information Security Audit Company.	37,109 38,432	FY March, 2017, Consolidated FY March2018

[Source] JETRO "Market report: Business Opportunities related to the Olympics and the Paralympics" March 2018, Website of each companies, Press release materials.

2. Japanese Major Players (1) Companies

■Japanese companies pursue development and expansion of services using advanced technology. (Examples)

◆ In Industrial Control System, or “Ooperation Technology”, Infrastructure Industry also enters into Cyber security Market and promotes overseas business expansion.

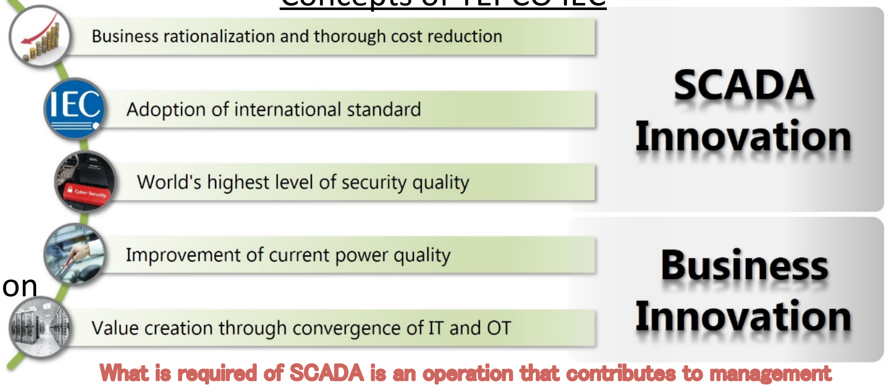
Ex) TEPCO IEC

-TEPCO IEC is a design and operation consulting company for power control systems, established in 2017.

-Putting emphasis on SCADA(Supervisory Control And Data Acquisition).

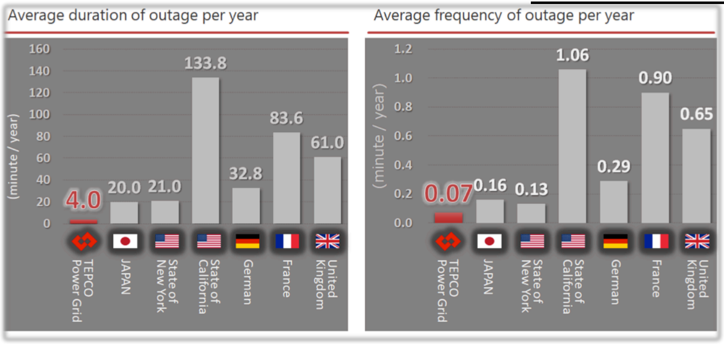
-Promoting overseas expansion in cooperation with McAfee, NTT Data and so on.

Concepts of TEPCO IEC

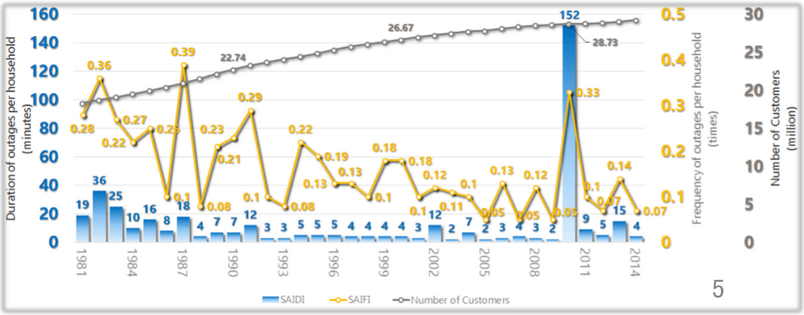

Business rationalization and thorough cost reduction
IEC
Adoption of international standard
Cyber Security
World's highest level of security quality
SCADA Innovation
Improvement of current power quality
Value creation through convergence of IT and OT
Business Innovation

What is required of SCADA is an operation that contributes to management

World-class high power quality



In the world



In the TEPCO

2. Japanese Major Players (2)International Collaboration

IPA CoE Global Training in Core Resource Development Program (France and UK)

Training in France

- September 17–18, 2018, 18 trainees from Japan visited universities and research laboratories in France to attend training to get better understanding of global standards and advanced level initiatives in cybersecurity and to have opportunities of networking with the local top level organizations and professionals.

Training at a French laboratory

Training in UK

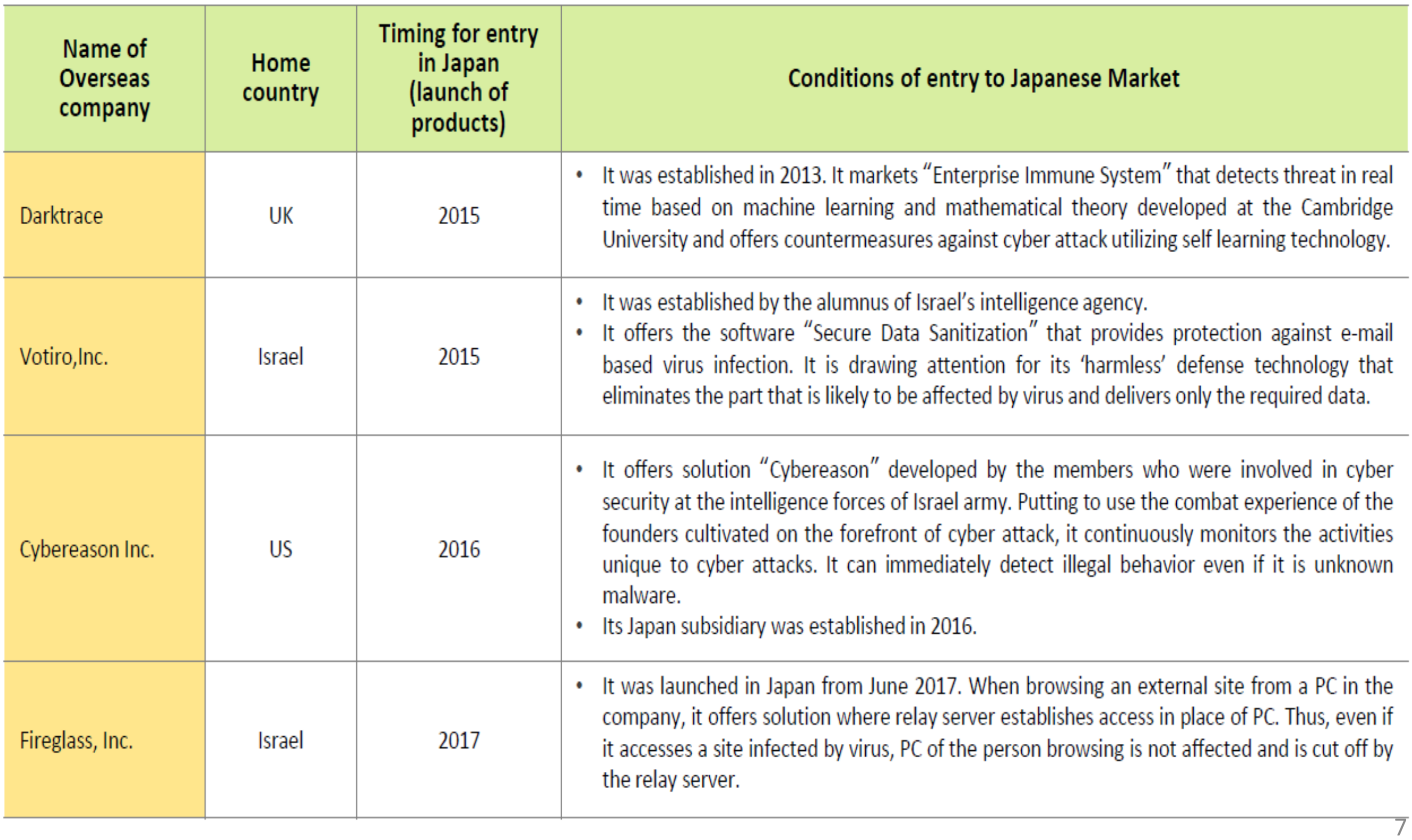
- December 3–4, 2018, 33 trainees from Japan visited UK to attend training by government organizations and representatives of auto and finance industries as well as start-up companies in cybersecurity.

Training by auto industry cybersecurity professionals (UK)

Note: Contents in this page were provided by IPA.

3. Situation of Major Overseas Companies Entering the Market

- Examples of entry of security related foreign companies in the Japanese market.
- In recent years, entry of companies that possess information security technologies using AI has increased to provide safe guard against cyberattacks. They include Israeli companies that are armed with advanced technical competence.



Name of Overseas company	Home country	Timing for entry in Japan (launch of products)	Conditions of entry to Japanese Market
Darktrace	UK	2015	• It was established in 2013. It markets "Enterprise Immune System" that detects threat in real time based on machine learning and mathematical theory developed at the Cambridge University and offers countermeasures against cyber attack utilizing self learning technology.
Votiro,Inc.	Israel	2015	• It was established by the alumnus of Israel's intelligence agency. • It offers the software "Secure Data Sanitization" that provides protection against e-mail based virus infection. It is drawing attention for its 'harmless' defense technology that eliminates the part that is likely to be affected by virus and delivers only the required data.
Cybereason Inc.	US	2016	• It offers solution "Cybereason" developed by the members who were involved in cyber security at the intelligence forces of Israel army. Putting to use the combat experience of the founders cultivated on the forefront of cyber attack, it continuously monitors the activities unique to cyber attacks. It can immediately detect illegal behavior even if it is unknown malware. • Its Japan subsidiary was established in 2016.
Fireglass, Inc.	Israel	2017	• It was launched in Japan from June 2017. When browsing an external site from a PC in the company, it offers solution where relay server establishes access in place of PC. Thus, even if it accesses a site infected by virus, PC of the person browsing is not affected and is cut off by the relay server.

[Source] JETRO "Market report: Business Opportunities related to the Olympics and the Paralympics" March 2018

4. Government Support for Market Expansion

(1) Tax system for encouraging IoT investment with security

- When a company invest for IoT systems (e.g., robots) for improving the productivity, they can earn the corporate tax reduction from around 30% up to around 25%.
- As a prerequisite for having this tax reduction, the corporation should implement certain security measures.

→ Encourage security investment

<Case>

If a company submit a business plan for investing to a smart factory with certain security measures which can improve productivity, the corporate tax will be reduced up to 5%.

Source: Mistubishi Electric HP

Corporate tax amount

About 30%

↓

Up to about 25%

4. Government Support for Market Expansion (2)Regulatory Sandbox

1. New Regulatory Sandbox framework in Japan

- The Government of Japan (GOJ) introduced this framework on June 6, 2018 as one of the mechanisms for regulatory reform to facilitate realization of innovative technologies and business models in Japan.

- The framework does not limit the area of regulations, but covers those on financial services, healthcare industry, mobility and transportation.

- Companies, including overseas companies, can
  - ➢ apply to conduct “demonstrations” under this new framework and
  - ➢ test the possibilities of using innovative technologies such as AI, IoT or block chains for future business,

  especially when they cannot start businesses due to existing Japanese regulations.

Overview of the process for regulatory reform

In cases where
- you would like to conduct business activities which utilize new technologies or new business models,
- but they conflict with existing Japanese regulations, because they do not assume such new technologies:

→ You can apply to conduct operations not as business activities but as "demonstrations" with limited time periods and participants.

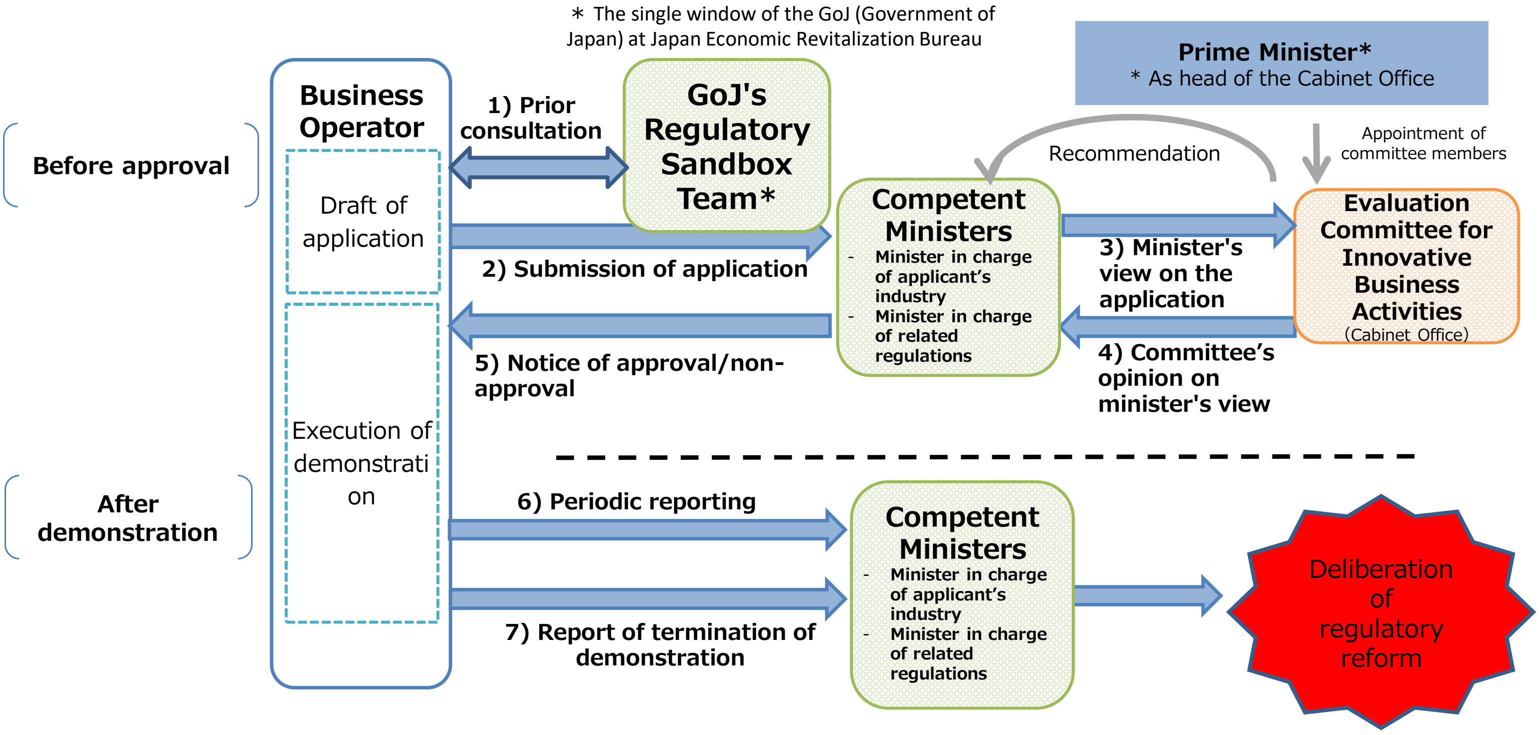
→ Data collected through the demonstrations will be utilized in deliberation for regulatory reform, which will facilitate the creation of such innovative business activities with new technologies and new business models.

Contact: GoJ’s Regulatory Sandbox Team at Japan Economic Revitalization Bureau, which works as the single window of the GoJ （Government of Japan)
http://www.kantei.go.jp/jp/singi/keizaisaisei/regulatorysandbox.html
E-mail: Shingijutsu_sb@cas.go.jp
Tel: +81 3－3581-0769

If you are of an overseas company or a foreign-affiliated company in Japan, you can consult the ‘’Invest Japan Hotline" of JETRO before consulting the GoJ's Regulatory Sandbox Team.
https://www.jetro.go.jp/en/invest/hotline.html
E-mail: Please send by “Inquiry Form”
Tel: +81 3-3582-4684

4. Government Support for Market Expansion (2)Regulatory Sandbox

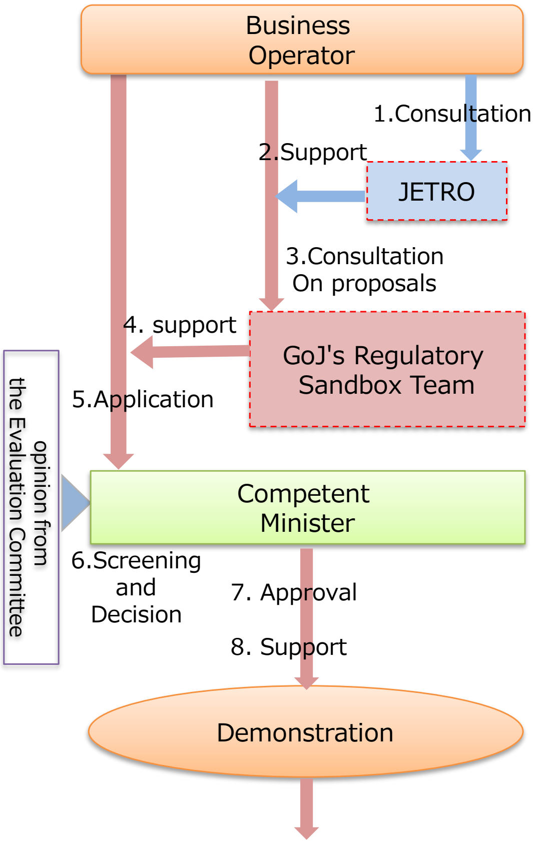
2. Process under Regulatory Sandbox (RS) framework



＊ The single window of the GoJ (Government of Japan) at Japan Economic Revitalization Bureau
Prime Minister*
＊ As head of the Cabinet Office
Before approval
Business Operator
Draft of application
Execution of demonstration
After demonstration
1) Prior consultation
GoJ's Regulatory Sandbox Team*
2) Submission of application
5) Notice of approval/non-approval
Recommendation
Appointment of committee members
Competent Ministers
- Minister in charge of applicant's industry
- Minister in charge of related regulations
3) Minister's view on the application
4) Committee's opinion on minister's view
Evaluation Committee for Innovative Business Activities
(Cabinet Office)
6) Periodic reporting
7) Report of termination of demonstration
Competent Ministers
- Minister in charge of applicant's industry
- Minister in charge of related regulations
Deliberation of regulatory reform

4. Government Support for Market Expansion (2)Regulatory Sandbox

3. Support when using “Regulatory Sandbox” framework



9. Review the regulations where necessary

1. If you are of an overseas company or a foreign-affiliated company in Japan, you can consult JETRO before consulting the GoJ's Regulatory Sandbox Team.

2. JETRO will support you to consult the GoJ’s Regulatory Sandbox Team.

3,4,5. GoJ‘s Regulatory Sandbox Team works as the single window of the GoJ(Government of Japan)
- to provide consultation for private businesses, and
- to exchange views with regulators, when appropriate,

on the proposals to be made under the Regulatory Sandbox framework.

6,7. Screening and decision making by the competent minister referring to the opinion from the evaluation committee.

8. After the approval, provide information and advice from the competent minister necessary for the smooth and secure implementation of the demonstration

9. Competent minister will review the regulations where necessary by using the demonstration data.

3.2.2 Introducing European cybersecurity ecosystem: from threats to industrial policy

The next session included the cybersecurity Public-Private Partnership (cPPP) and European Strategic Agenda on Research & Development, for 2016: "An overview of the ecosystem and cyber technologies", by Roberto Cascella, from ECSO Secretariat:

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity PPP & ECSO Strategic Research Innovation Agenda

Roberto G. Cascella
Senior Policy Manager (ECSO Secretariat)

ECSO – EUNITY Workshop
– 24 January *2019 – Brussels (Belgium)* –

About the European Cyber Security cPPP

The European Commission has signed on July 2016 a cPPP with the private sector represented by ECSO for the development of a common approach and market on cyber security.

AIM

1. Foster cooperation between public and private actors
2. Stimulate cyber security industry
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). Cyber security market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total up to €1800 mln.

UPDATE: EC will invest more than €500 mln. Private sector investments for the 1st year had a leverage factor 5

cPPP Monitoring at Glance – 1st Period

Investment on R&D

- Nearly 455 million € estimated in 2016 by the European Cyber Security community and 534 million € in 2017

- Nearly 68 million € invested by the EC in the PPP, 4 projects started so far under the frame of H2020 (DS-06-2017), other 13 projects of the 2017 call to be started soon.

➔ **Leverage factor for cPPP investments higher than 3 (target)**

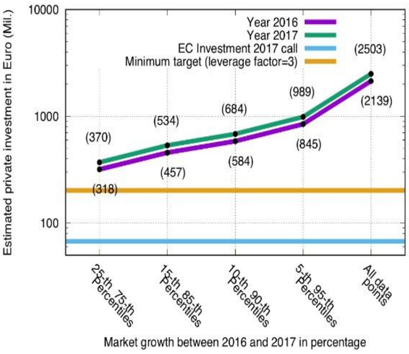


FIG 1 Estimated private investment for 2016 and 207

Cyber security employment

- Following our survey, employment has growth between 2016 to 2017 by 10% in large companies, 80% in SMEs and 45% in RTOs.

➔ **cPPP target job growth = at least 10%**

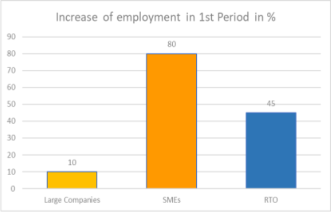
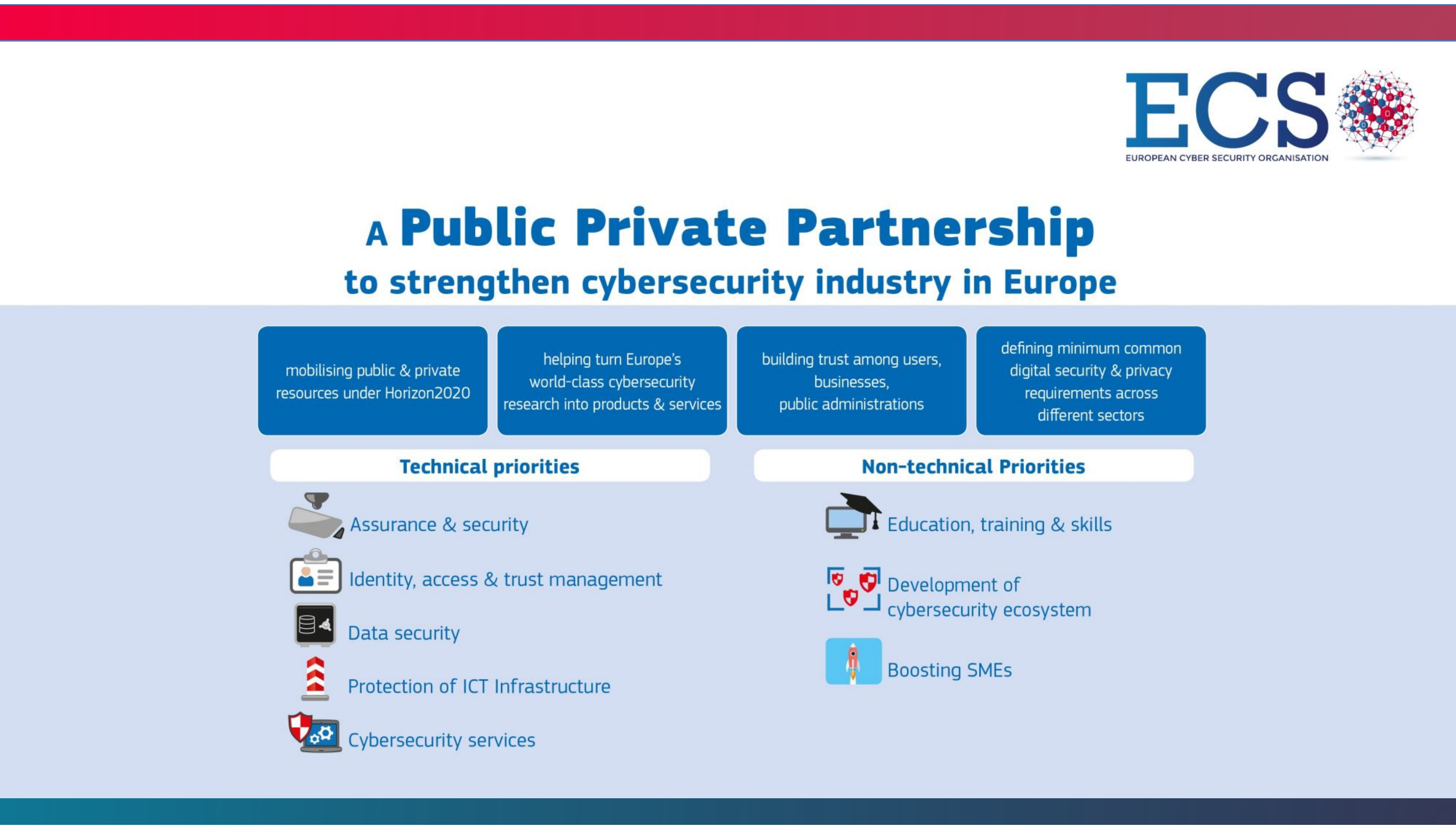


FIG 2 Employment in 1st Period

Survey for 2018 investment expected to be launched on 1st February



ECS
EUROPEAN CYBER SECURITY ORGANISATION

A Public Private Partnership
to strengthen cybersecurity industry in Europe

mobilising public & private resources under Horizon2020	helping turn Europe's world-class cybersecurity research into products & services	building trust among users, businesses, public administrations	defining minimum common digital security & privacy requirements across different sectors

Technical priorities

- Assurance & security
- Identity, access & trust management
- Data security
- Protection of ICT Infrastructure
- Cybersecurity services

Non-technical Priorities

- Education, training & skills
- Development of cybersecurity ecosystem
- Boosting SMEs

We are representative of all kinds of stakeholders (situation on 8 January 2019)

WG1
Standardisation, certification, labelling and supply chain management
152 members
28 countries
333 experts

WG2
Market deployment, investments and international collaboration
98 members
22 countries
200 experts

WG3
Sectoral applications
Industry 4.0; Energy; Transport; Finance; Public Admin/eGov; Health; Smart Cities; Telecom/Content/Media
139 members
29 countries
330 experts

233 Members 29 countries

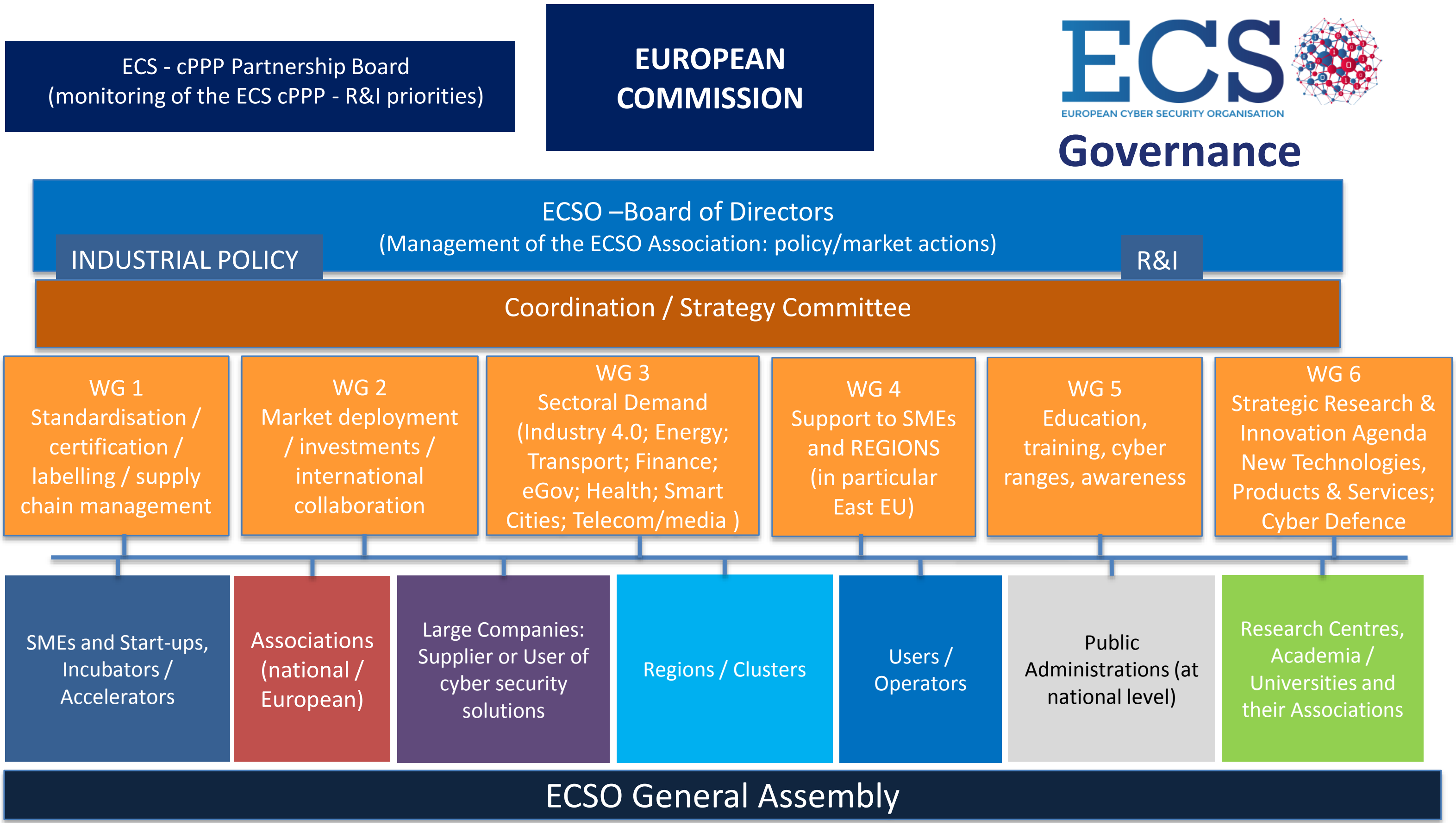
WG4
Support to SMEs and collaboration with Regions including East & Central Europe
101 members
26 countries
186 experts

WG5
Education, training, raising awareness and cyber ranges
132 members
29 countries
270 experts

WG6
Strategic research & innovation agenda (SRIA) and cyber technologies
178 members
29 countries
414 experts

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

WG 1
Standardisation / certification / labelling / supply chain management

WG 2
Market deployment / investments / international collaboration

WG 3
Sectoral Demand (Industry 4.0; Energy; Transport; Finance; eGov; Health; Smart Cities; Telecom/media)

WG 4
Support to SMEs and REGIONS (in particular East EU)

WG 5
Education, training, cyber ranges, awareness

WG 6
Strategic Research & Innovation Agenda New Technologies, Products & Services; Cyber Defence

SMEs and Start-ups, Incubators / Accelerators

Associations (national / European)

Large Companies: Supplier or User of cyber security solutions

Regions / Clusters

Users / Operators

Public Administrations (at national level)

Research Centres, Academia / Universities and their Associations

ECSO General Assembly

WG6: Strategic Research and Innovation Agenda

ECS

STRATEGIC RESEARCH AND INNOVATION AGENDA

WG6 I Strategic Research and Innovation Agenda

JUNE 2017

www.ecs-org.eu

ECSO SRIA to identify research priorities for 2018-2020

➔ A strategic vision is needed to demonstrate how industrial priorities contribute to the implementation of the strategy

➔ 7 thrusts organised in 4 different areas have been identified

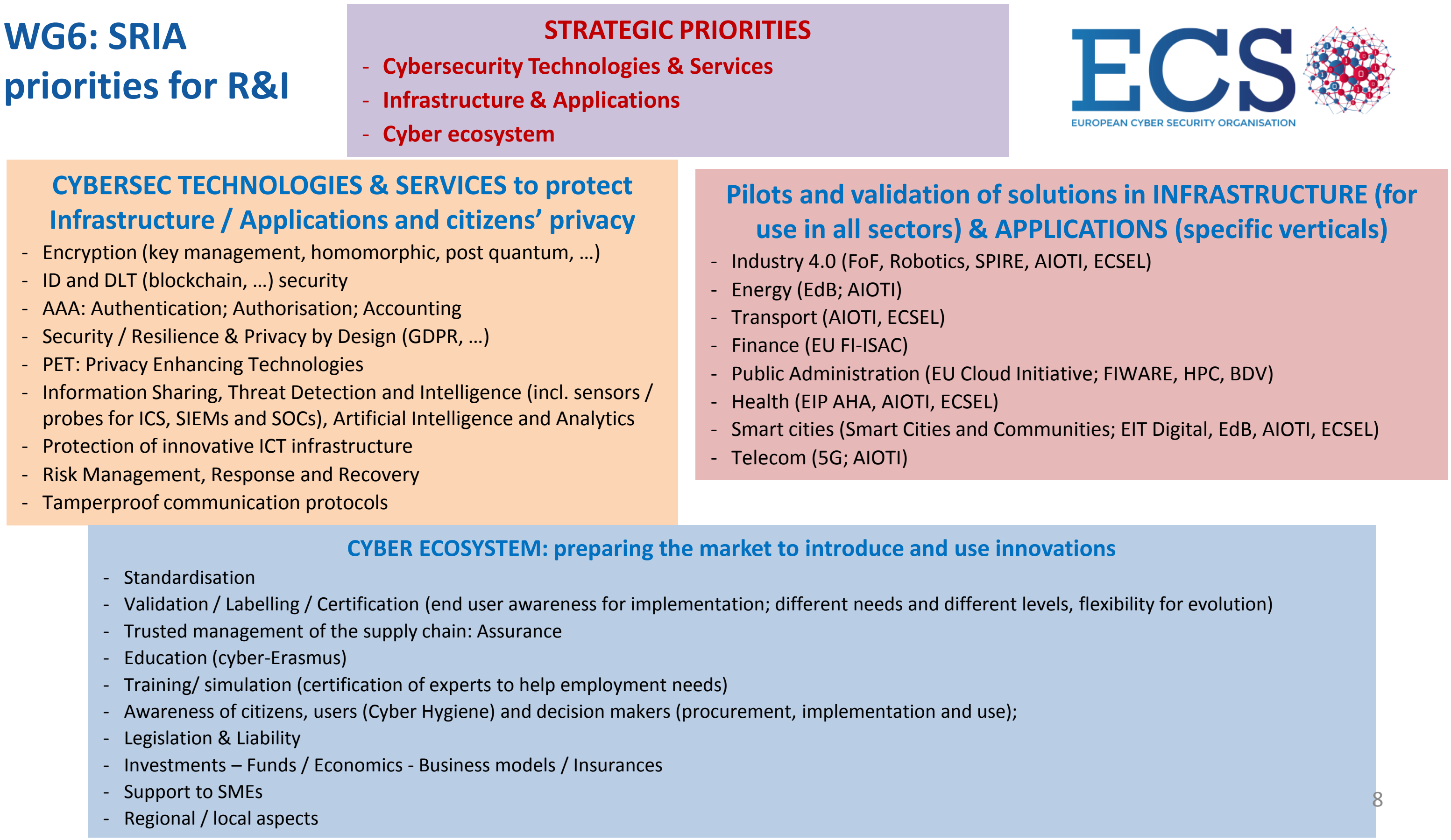
1 European ecosystem for cyber security
2 Demonstrations for the society, economy, industry and vital services
3 Collaborative intelligence to manage cyber threats and risks
4 Remove trust barriers for data-driven applications and services
5 Maintain a secure and trusted infrastructure in the long-term
6 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications
7 From security components to security services

Analysis of the Work Programme 2018-2020 and continuous advocacy of priorities

➔ good match and public & private priorities well aligned

Lesson learnt

- Coordination with cPPPs (on specific transversal technologies & verticals) is important to ensure the SRIA presenting coordinated cyber security strategy in EU
- Coordination with the EC Programme Committee and NAPAC R&I Group wrt internal deadlines is key to guarantee high quality delivered when expected
- Development of innovative cybersecurity technologies and validation of the solutions in key infrastructures and applications



WG6: SRIA priorities for R&I

STRATEGIC PRIORITIES

- Cybersecurity Technologies & Services
- Infrastructure & Applications
- Cyber ecosystem

ECS
EUROPEAN CYBER SECURITY ORGANISATION

CYBERSEC TECHNOLOGIES & SERVICES to protect Infrastructure / Applications and citizens' privacy

- Encryption (key management, homomorphic, post quantum, …)
- ID and DLT (blockchain, …) security
- AAA: Authentication; Authorisation; Accounting
- Security / Resilience & Privacy by Design (GDPR, …)
- PET: Privacy Enhancing Technologies
- Information Sharing, Threat Detection and Intelligence (incl. sensors / probes for ICS, SIEMs and SOCs), Artificial Intelligence and Analytics
- Protection of innovative ICT infrastructure
- Risk Management, Response and Recovery
- Tamperproof communication protocols

Pilots and validation of solutions in INFRASTRUCTURE (for use in all sectors) & APPLICATIONS (specific verticals)

- Industry 4.0 (FoF, Robotics, SPIRE, AIOTI, ECSEL)
- Energy (EdB; AIOTI)
- Transport (AIOTI, ECSEL)
- Finance (EU FI-ISAC)
- Public Administration (EU Cloud Initiative; FIWARE, HPC, BDV)
- Health (EIP AHA, AIOTI, ECSEL)
- Smart cities (Smart Cities and Communities; EIT Digital, EdB, AIOTI, ECSEL)
- Telecom (5G; AIOTI)

CYBER ECOSYSTEM: preparing the market to introduce and use innovations

- Standardisation
- Validation / Labelling / Certification (end user awareness for implementation; different needs and different levels, flexibility for evolution)
- Trusted management of the supply chain: Assurance
- Education (cyber-Erasmus)
- Training/ simulation (certification of experts to help employment needs)
- Awareness of citizens, users (Cyber Hygiene) and decision makers (procurement, implementation and use);
- Legislation & Liability
- Investments – Funds / Economics - Business models / Insurances
- Support to SMEs
- Regional / local aspects

Coordination of R&I cybersecurity activities in Europe

EUROPEAN CYBER SECURITY ORGANISATION

STRATEGIC RESEARCH AND INNOVATION AGENDA

WG6 | Strategic Research and Innovation Agenda

JUNE 2017

www.ecs-org.eu

Federating discussions on cybersecurity challenges with other PPPs under ECSO

BDVA: updated list of shared topics and areas of collaboration on AI

EFFRA: Analysis of requirements and cyber security challenges for digitisation of industry

5G IA: Common interest to work on cybersecurity aspects for 5G

EURobotics: cybersecurity for Digitisation of the Industry (e.g., eHealth)

Other initiatives (A.Spire, ShiftToRail, ECSEL) contacted. ...

Other external collaborations

- **EDA:** Understand EDA research priorities. EDA has joined the ECSO Strategic Technical Committee. ECSO SWG6.5 on cyber defence
- **ENISA:** Contribute to the research priorities identified (crystal ball) and recommendation report. Continuous interaction
- **JRC**: Work on the cybersecurity taxonomy
- **DG-ENER:** Contribute with specific cybersecurity challenges and priorities for the energy sector (with WG3)
- **IoTForum** and **AIOTI:** Focus on cybersecurity for IoT technology to update the research priorities and impact for vertical sectors

Continuous monitoring of the European cyber secure ecosystem, including technology and needs evolution to build, maintain, and provide innovative trustworthy solutions to protect European citizens and industry

ECSO SRIA: Where we are heading

Identification of global trends & key implications on strategy → 2027

R&I needs on specific verticals to address new disruptive technologies – Working papers on new technology drivers
Artificial Intelligence, Internet of Things and Blockchain (impact on different WG aspects to sustain the industrial policy)

- Technical cyber security challenges: relevance, current status and future directions (roadmap)
- The impact on vertical sectors and their needs (cross-sectorial challenges and specificities of each vertical sector)
- The relevant standardisation activities and the implications for cyber security certification and supply chain management.
- Relevant regulations and legislations and their implications

Initial priorities and challenges for HorizonEurope (2021)

- Society and Citizens (Social Good) → Bring trust into the technology and in the Machine Economy
- Data and Economy → Data as main ICT value and/or target and main driver for decision making
- Basic and Disruptive Technologies (e.g. Artificial Intelligence, Blockchain, Quantum-resistant crypto) → Ensure a sustainable and trustworthy ecosystem, including integrating M2M and M2H interaction and autonomous systems as technical, ethical, safety issues
- Digital Transformation in Verticals → Continuous evolving systems and integration of legacy systems with new technology, threat intelligence and information sharing, and ICT infrastructure protection

➢ Define **Strategic Research and Innovation Agenda (v2.0)**

Link with relevant cPPPs and new initiatives (DEP) to coordinate strategy for future EU cybersecurity R&I

BECOME MEMBER!
CONTACT US

European Cyber Security Organisation 10,
Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0)
27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Manager
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu

Next the "EU strategy & legal response for strengthening cybersecurity: An update on the European Commission 2017 Cyber Security Package and focus on 2018 initiative" was presented by Jakub Boratynski, from DG CNECT, European Commission:

EU Cybersecurity

24 January 2019
Brussels

Jakub Boratynski
Head of Unit
DG CONNECT – H2 Cybersecurity & Digital Privacy Policy
European Commission

NIS Directive
The First EU Cybersecurity Law

Boosting the overall cybersecurity in the EU

- Increased national cybersecurity capabilities
- EU level cooperation (NIS Cooperation Group)
- Security & Notification requirements
- National Cybersecurity Strategies
- National Computer Security Incident Response Teams (CSIRT Network)

State of play :

24 Member States notified full transposition.

2 Member states notified partial transposition.

Ongoing identification of Operators of Essential Services

Next? Monitoring of implementation process followed by in-depth checks.

Cybersecurity Act
EU Cybersecurity Agency (ENISA)

What's new?

- Permanent Status
- Adequate Resources
- Focused Mandate

Mandate & Objectives - Contribute to high Cybersecurity

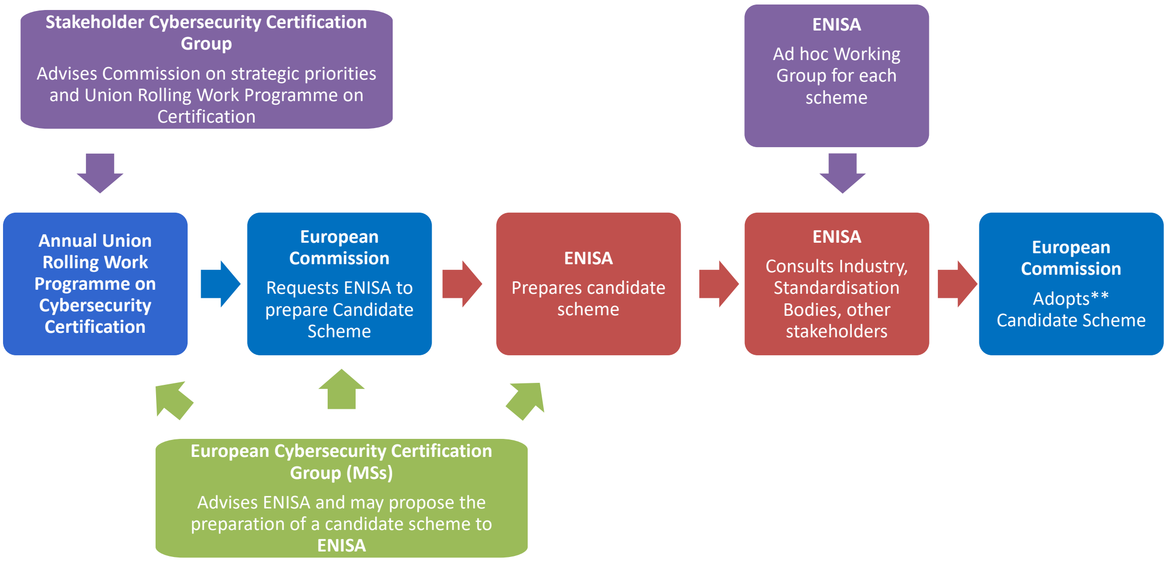
- Promote the use of certification & contribute to the cybersecurity certification framework
- Be an independent center of expertise
- Assist EU Institutions and MSs in policy Development & implementation
- Support capacity building & preparedness
- Promote high level of awareness of citizens & businesses
- Promote cooperation & coordination at Union level
- Increase cybersecurity capabilities at Union level to complement MSs action

Cybersecurity Act
EU Cybersecurity Certification Framework

Some key elements

- EU Cybersecurity Agency (ENISA)
- Member State involvement - European Cybersecurity Certification Group (ECCG)
- Stakeholders' involvement – Stakeholder Cybersecurity Certification Group (SCCG)
- Union rolling work programme for European Cybersecurity Certification
- Voluntary certification schemes throughout the EU.
- Independent assessment of the schemes.

How: Establishment of an EU Cybersecurity Certification Scheme*



Stakeholder Cybersecurity Certification Group

Advises Commission on strategic priorities and Union Rolling Work Programme on Certification

ENISA

Ad hoc Working Group for each scheme

Annual Union Rolling Work Programme on Cybersecurity Certification

European Commission

Requests ENISA to prepare Candidate Scheme

ENISA

Prepares candidate scheme

ENISA

Consults Industry, Standardisation Bodies, other stakeholders

European Commission

Adopts** Candidate Scheme

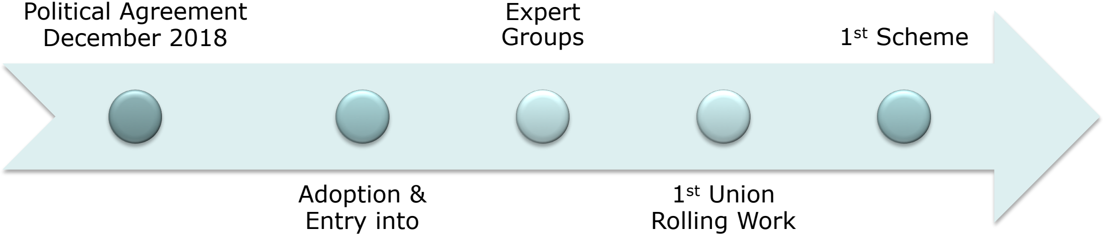
European Cybersecurity Certification Group (MSs)

Advises ENISA and may propose the preparation of a candidate scheme to **ENISA**

*   subject to final political agreement

** “better regulation” + Commitology

State of Play and Timeline



Political Agreement
December 2018

Adoption &
Entry into
force
April 2019

1st request;
Set up
Expert
Groups

1st Union
Rolling Work
Programme
April 2020

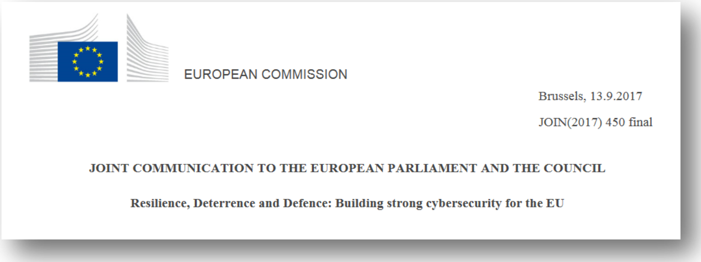
1st Scheme

European Commission

European Cybersecurity Industrial, Technology & Research Competence Centre
&
Network of National Coordination Centres

European Commission

Cybersecurity Package Commitment



EUROPEAN COMMISSION

Brussels, 13.9.2017
JOIN(2017) 450 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

The EU has added value to provide, given the sophistication of cybersecurity technology, the large-scale investment required, and the need for solutions that work across the EU.

Building on the work of Member States and the Public-Private Partnership reinforce EU cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart.

This network and its Centre would stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level.

The proposal in a nutshell

European Cybersecurity Technology & Innovation Ecosystem

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

European Commission

The Competence Centre – what will it do?

Facilitate and help coordinate the work of the Network

Implement cybersecurity parts of Digital Europe and Horizon Europe Programmes

Enhance cybersecurity capabilities, knowledge and infrastructures

Contribute to the wide deployment of state-of-the-art products and solutions; support SMEs

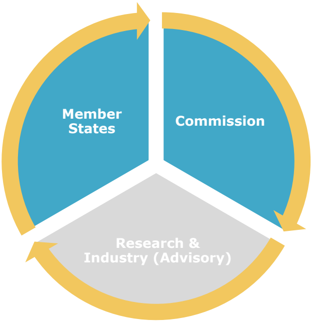
Contribute to reducing cybersecurity skills gaps

Support cybersecurity research and development

Enhance cooperation between the civilian and defence spheres with regard to dual use technologies

Enhance synergies in relation to the European Defence Fund

The Competence Centre – governance



Member States

Commission

Research & Industry (Advisory)

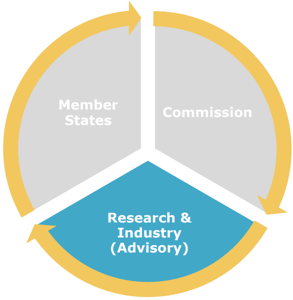
Governing Board:

- ➢ **1 representative of each Member State** (+alternate) with cybersecurity knowledge and managerial skills
- ➢ **5 representatives of the Commission**
- ➢ **Renewable term of 4 years**
- ➢ **Observers admitted** (ENISA as a permanent observer)
- ➢ **Executive Director** chosen for 4 years (renewable once)

Voting Rules:

- ➢ **Union** holds **50% of voting rights**
- ➢ **Every participating Member State = 1 vote**
- ➢ Decisions taken by a **majority of at least 75% of all votes,** representing **at least 75% of the total financial contributions** to the Competence Centre.
- ➢ **The Chairperson takes part in the voting**.

Industrial & Scientific Advisory Board



Member States

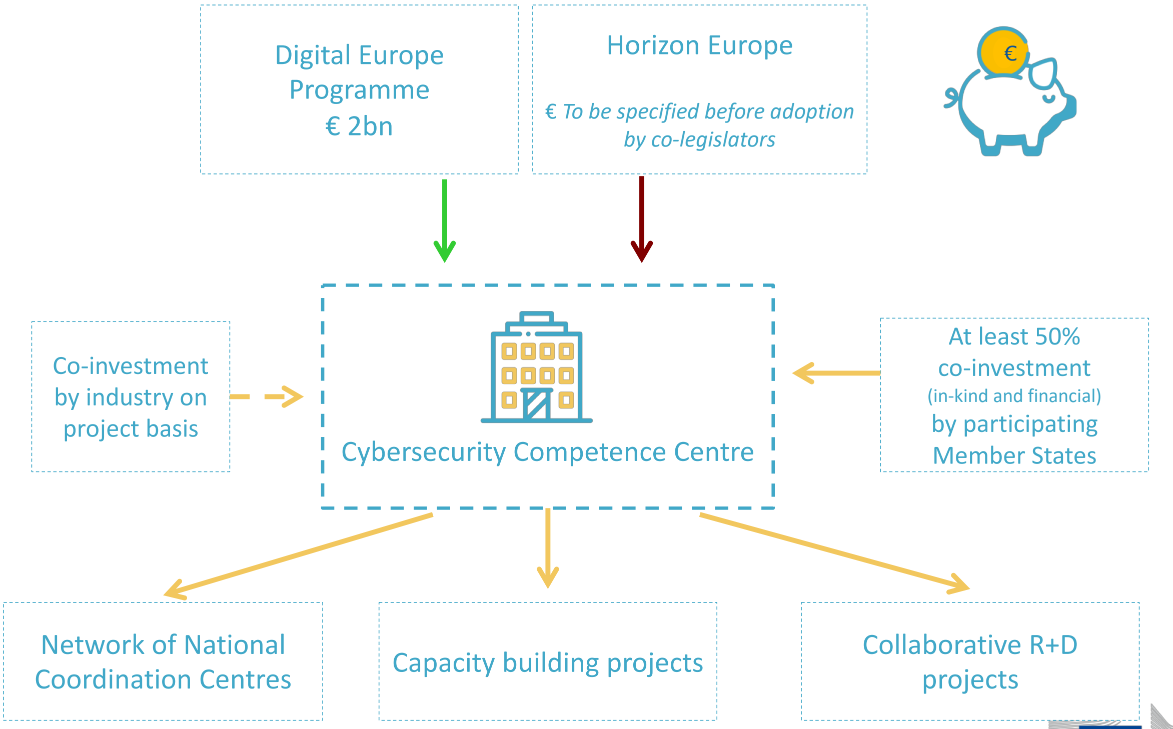
Commission

Research & Industry (Advisory)

- **16 members** appointed by the Governing Board from among the representatives of the entities of the Competence Community
- **Expertise** in cybersecurity research, industrial development, professional services or deployment
- **Investment of cPPP experience**
- **3 years' renewable** term
- **Commission** and **ENISA** participates in the works of the Advisory Board
- Meets at least 2 x year
- **Tasks:**
  - Advises on establishing working groups
  - Organises public consultations and provides input for drafting the work plan & multi-annual strategic plan
  - promotes and collects feedback on the work plan and multi-annual strategic plan of the Competence Centre.

Financing of the initiative

2021-2027 proposed EU cybersecurity funding sources



Digital Europe Programme
€ 2bn

Horizon Europe

€ To be specified before adoption by co-legislators

Co-investment by industry on project basis

Cybersecurity Competence Centre

At least 50% co-investment (in-kind and financial) by participating Member States

Network of National Coordination Centres

Capacity building projects

Collaborative R+D projects

Next Steps

By Q2/2019

Finalise negotiations

2019-2020

Preparatory Phase

2020

Prepare to launch 2021 actions

Thank you for your attention!

3.2.3 Introducing Japanese cybersecurity ecosystems: legal and policy framework

The next session included the presentations for “Cybersecurity Policy for Industry Sector in Japan”, by Hiromichi Nakahara and Hiroo Inoue, from the Japan External Trade Organization (JETRO):

METI
Ministry of Economy, Trade and Industry

Cybersecurity Policy for Industry Sector in Japan

Hiroo Inoue

Ministry of Economy, Trade and Industry

Japan External Trade Organization

1. The Cyber/Physical Security Framework

2. HR development for Industrial Control System (ICS) cybersecurity

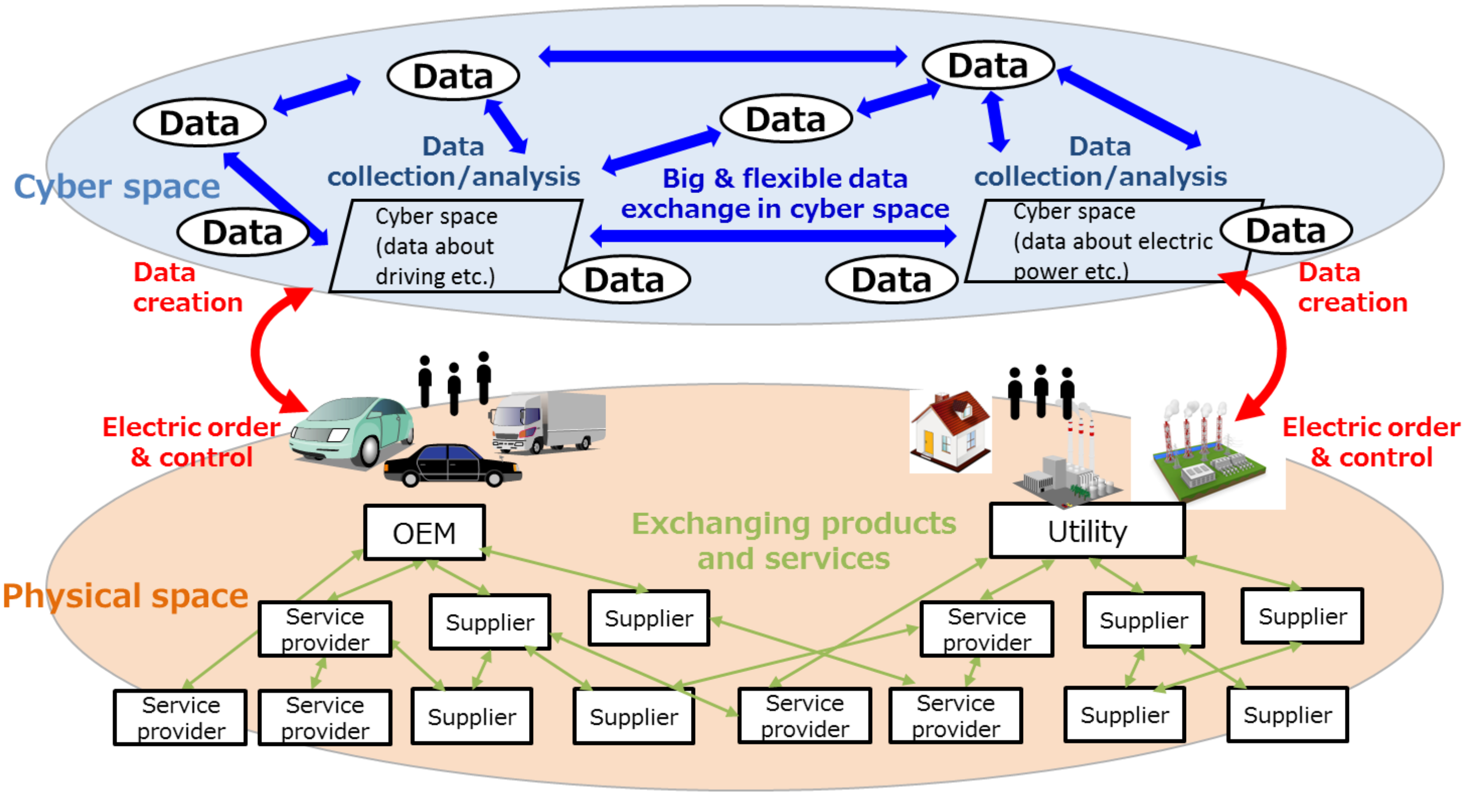
3. Capacity building for securing global supply chain

4. Cybersecurity supporters for SMEs

5. Collaboration Platform

Risks in Cyber/Physical Integrated Society (Society 5.0)

Cyber threats which give serious damages on products and their services are expanding in whole supply chains



The Cyber/Physical Security Framework
~for value creation process in Society5.0's supply chain ~

METI gives the second draft of the cyber/physical security framework to manage supply chain risks for secured products and services

Proposing "Three-Layer Approach" to articulate risks in supply chains and take appropriate measures, including labeling, in the new FW

The Third Layer
(Data circulation)

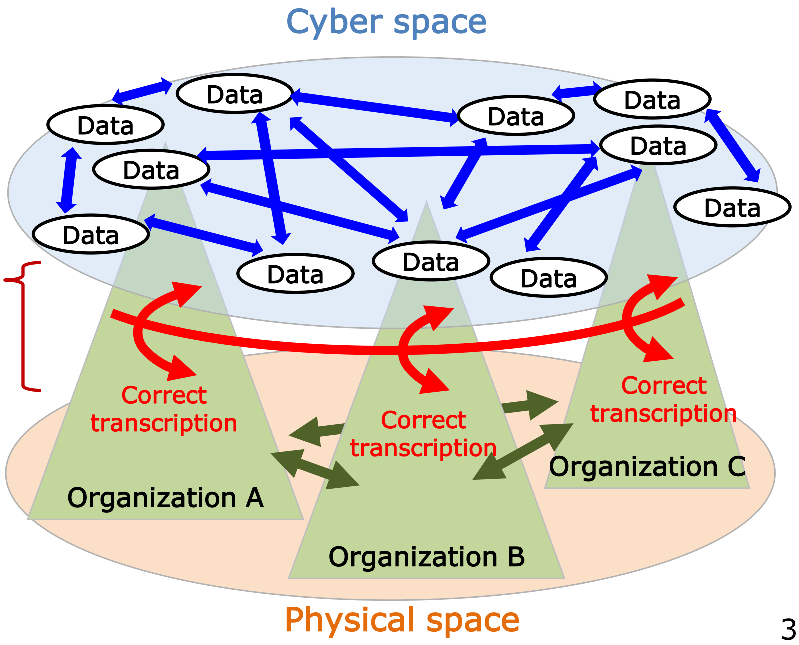
- **Trustworthiness of data** is a key for secured products and services

The Second Layer
(Cyber to physical/Physical to cyber)

- **Trustworthiness of function for "correct transcription"** between cyber/physical space, which is IoT system's essence, is a key

The First Layer
(Connection between Organizations)

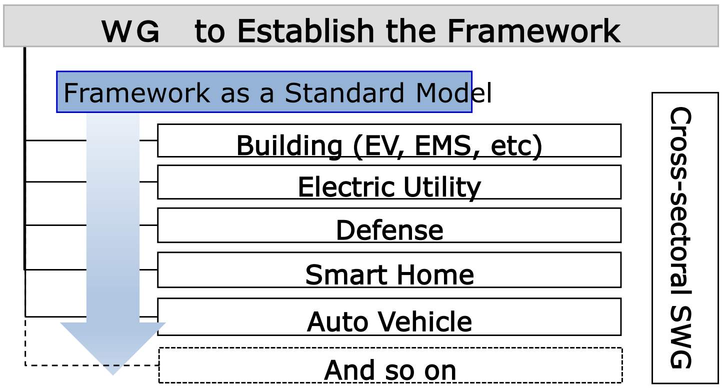
- **Trustworthiness of organization's management** is a key for secured products and services



Activities related to the CPS Framework

Sector by Sector Approach

- *Developing sector specific measures industry by industry with the framework as a Standard Model*
- *Building Sector Cyber/Physical Security Guideline β version has already publicized*



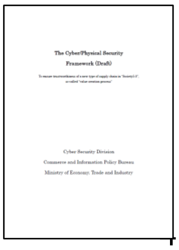
International Harmonization

- *Many debates, presentations, and feedbacks about the Framework*

Reference: US Chamber of Commerce HP

- *Correspondence tables to ISO/IEC 27001, NIST CSF and SP800-171*
- *Public comments of the draft is not only in Japanese but also in English*

Now on the 2nd public comment period! ***(Jan. 9 – Feb. 28)***
http://www.meti.go.jp/press/2018/01/20190109001/20190109001-3.pdf



The Cyber/Physical Security Framework (Draft)

To ensure trustworthiness of a new type of supply chain in "Society5.0", so-called "value creation process"

Cyber Security Division
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry

1. The Cyber/Physical Security Framework

2. HR development for Industrial Control System (ICS) cybersecurity

3. Capacity building for securing global supply chain

4. Cybersecurity supporters for SMEs

5. Collaboration Platform

Industrial Cyber Security Center of Excellence (ICSCoE)

ICSCoE was established in Apr. 2017

IPA

Industrial Cyber Security
Center of Excellence (ICSCoE)

- Center of Excellencece with expertise on IT and OT (Operation Technology) cybersecurity
- Education for both IT and OT security
- Assess the security and reliability of the Industrial Control Systems and plan measures by utilizing mock-up plants
- Investigate and analyze cyber attacks

Cultivate leaders of industrial cybersecurity

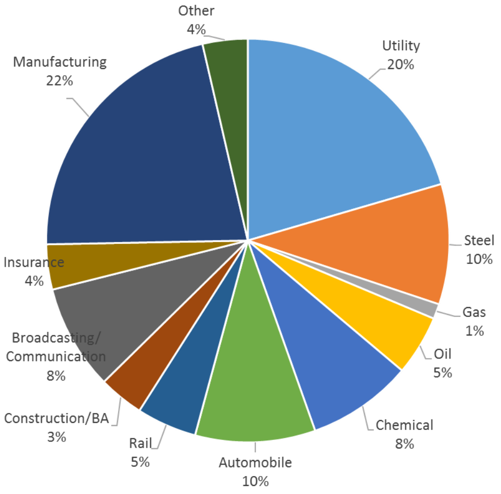
Mock-up plants

Manufacturing facility

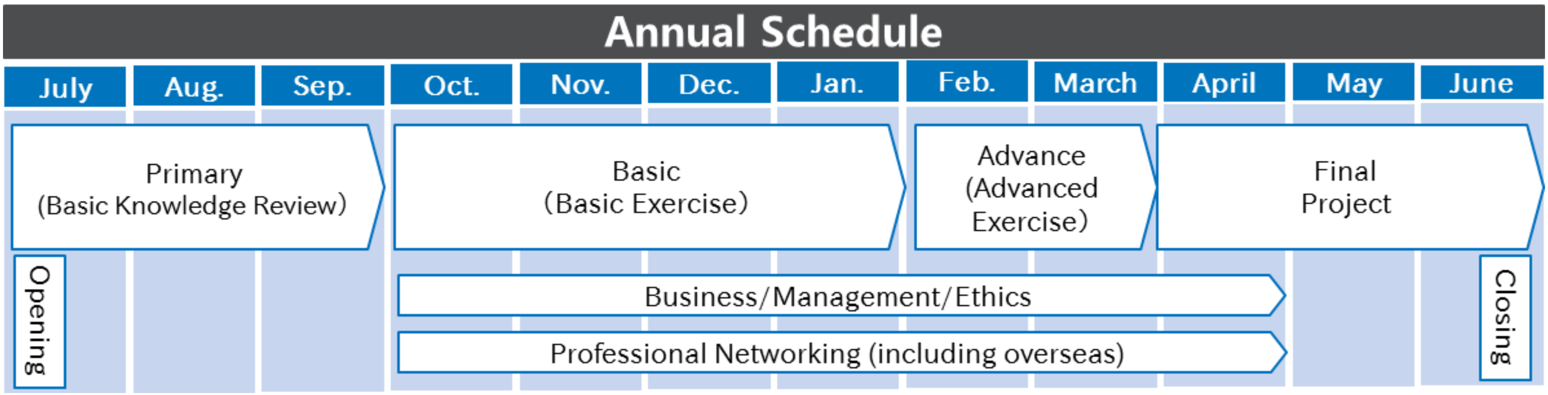
Utility facility

ICSCoE One-year Core HR Development Program

- 2nd year students' background companies (on the right)
- Students are funded by both the government and the companies
- Students will go back to the companies as a core HR for IT/OT cybersecurity



Industry	
Utility	17
Steel	8
Gas	1
Oil	4
Chemical	7
Automobile	4
Rail	8
Construction/BA	3
Broadcasting/ Communication	7
Insurance	3
Manufacturing	18
Other	3
Total	83



Annual Schedule
July
Aug.
Sep.
Oct.
Nov.
Dec.
Jan.
Feb.
March
April
May
June
Primary (Basic Knowledge Review)
Basic (Basic Exercise)
Advance (Advanced Exercise)
Final Project
Opening
Business/Management/Ethics
Professional Networking (including overseas)
Closing

1. The Cyber/Physical Security Framework

2. HR development for Industrial Control System (ICS) cybersecurity

3. Capacity building for securing global supply chain

4. Cybersecurity supporters for SMEs

5. Collaboration Platform

Japan & US Joint Training for ICS Cybersecurity

■**Date:** Sep. 10 – 14, 2018 (will be held annually)

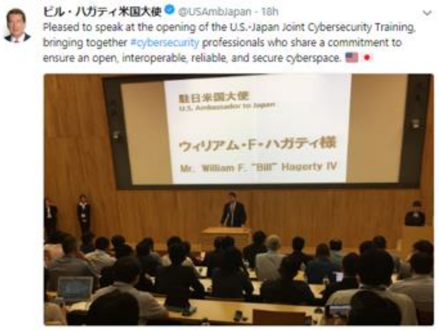
■**Location:** Tokyo

■**Contents:** 5 days training for ICS cybersecurity

■**Participants:**

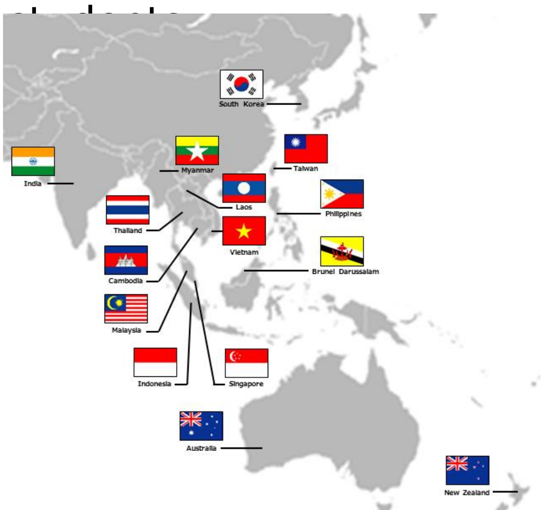
- ASEAN10 countries, Australia, India, NZ, South Korea, Taiwan 36 students
- IPA ICSCoE Core HR development program 83 students
- DHS/NCCIC 5 lecturers, and etc.

Speech of Yoji Muto, Former State Minister of METI (Fuji TV)


ビル・ハガティ米国大使 @USAmbJapan · 18h

Pleased to speak at the opening of the U.S.-Japan Joint Cybersecurity Training, bringing together #cybersecurity professionals who share a commitment to ensure an open, interoperable, reliable, and secure cyberspace. 🇺🇸 🇯🇵

Speech of U.S. Ambassador Hagerty (Twitter)



Participated Countries

Japan & US Joint Training for ICS Cybersecurity

■Sep. 10-11, 2018

Fundamentals of OT security
101, 201 Training (NCCIC)

■Sep. 12-14, 2018 (3 groups with 3 venues)

Hands-on training with ICS
J202 Training (ICSCoE)

Practice sharing, etc.
(DHS/METI/US & JP
Enterprises)

- ICSCoE and DHS/NCCIC-ICS conducted a joint training for Asian countries
- Japan & US provided lectures and hands-on training for 5 days.

Lecture with mock-up plants (ICSCoE)

1. The Cyber/Physical Security Framework

2. HR development for Industrial Control System (ICS) cybersecurity

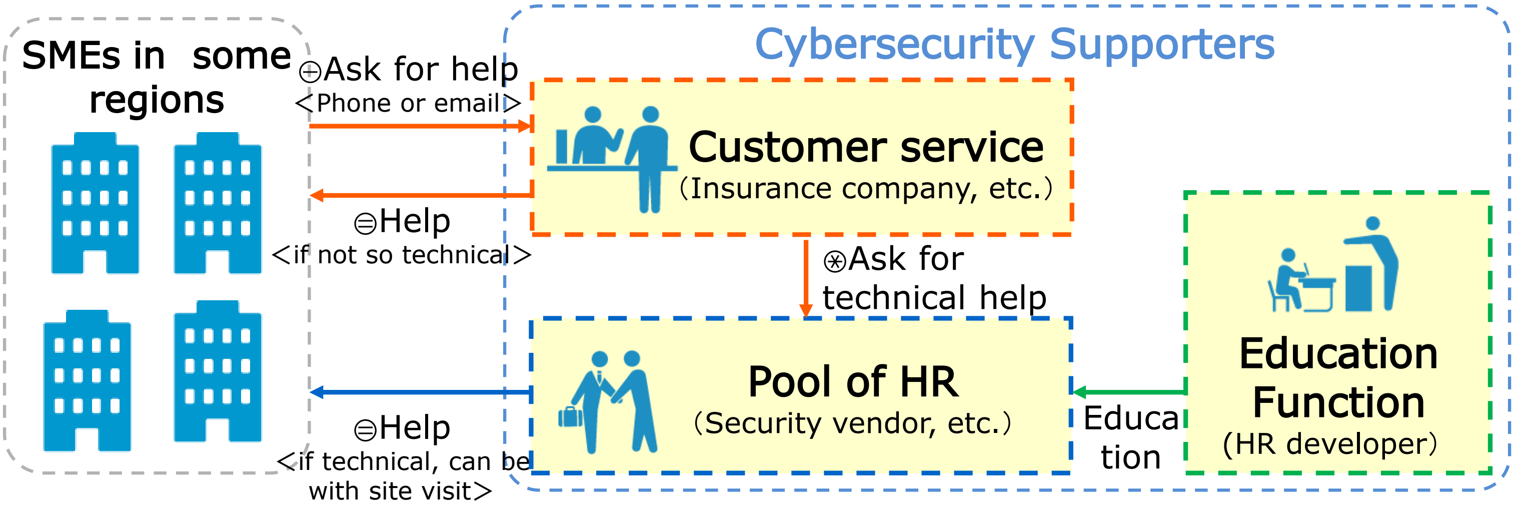
3. Capacity building for securing global supply chain

4. Cybersecurity supporters for SMEs

5. Collaboration Platform

Establish “Cybersecurity Supporters” for SMEs

Image of the Feasibility Study (FS) from Next Year



Through this FS, we will study:

1) the threat situation surrounding SMEs;

2) the required tools and skills for supporting SMEs; and

3) the ideal system for promptly and efficiently support SMEs.

1. The Cyber/Physical Security Framework

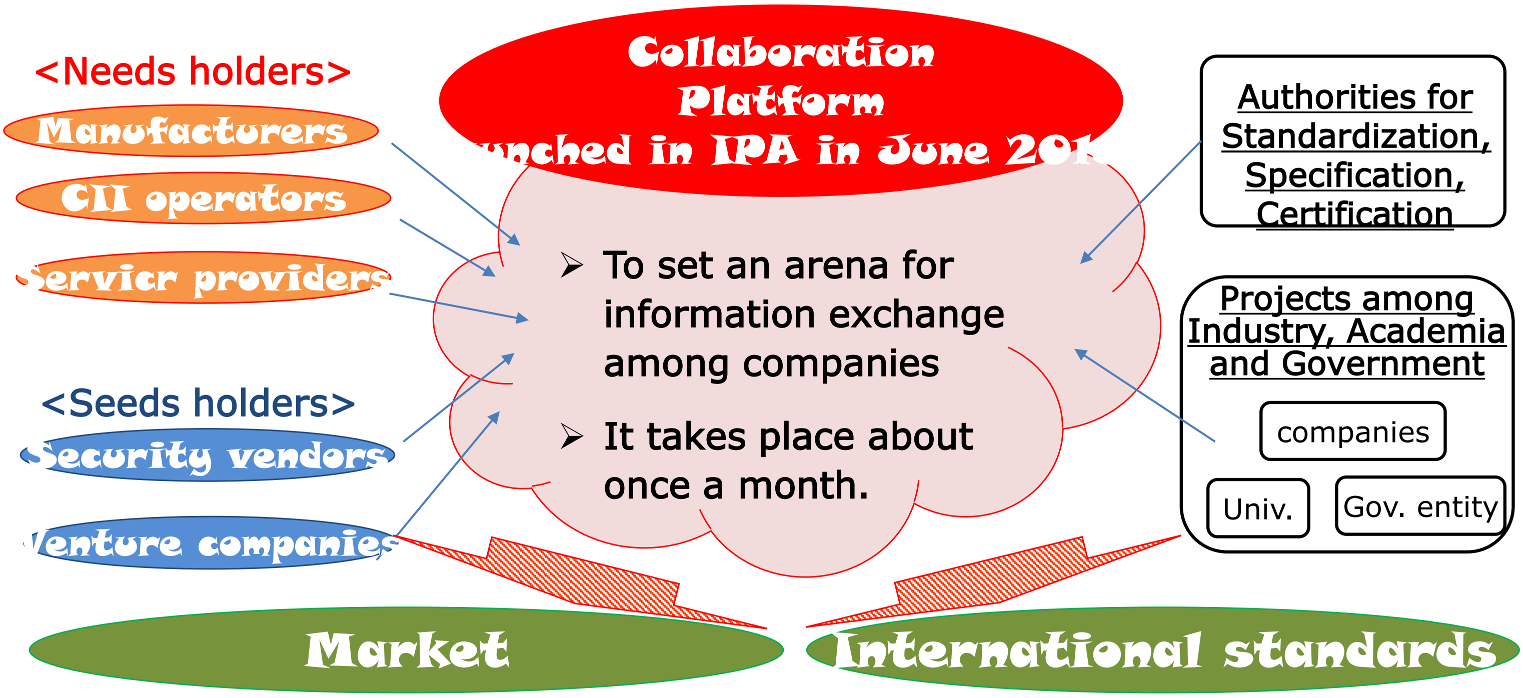
2. HR development for Industrial Control System (ICS) cybersecurity

3. Capacity building for securing global supply chain

4. Cybersecurity supporters for SMEs

5. Collaboration Platform

“Collaboration Platform” to match needs and seeds



Collaboration Platform
unched in IPA in June 201

<Needs holders>

Manufacturers

CII operators

Servicr providers

<Seeds holders>

Security vendors

Venture companies

- To set an arena for information exchange among companies
- It takes place about once a month.

Authorities for Standardization, Specification, Certification

Projects among Industry, Academia and Government

companies

Univ.

Gov. entity

Market

International standards

Presentation

Group Discussion

- Around once in a month
- Foreign entities can also join!

https://www.ipa.go.jp/security/announce/collapla_index.html

METI
Ministry of Economy, Trade and Industry

Thank You!

The last presentation of this session was the “IoT Security Measures in Japan” by Reiko Kondo, from the Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC):

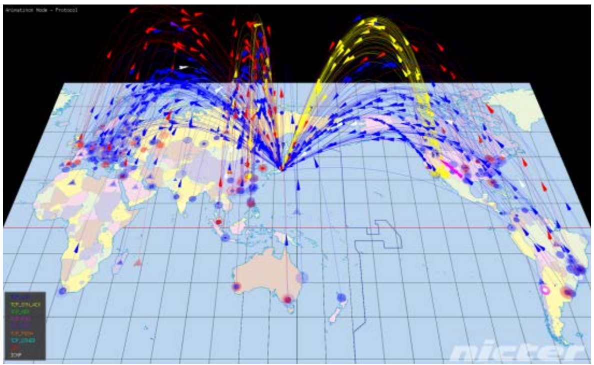
IoT Security Measures in Japan

January 24th, 2019

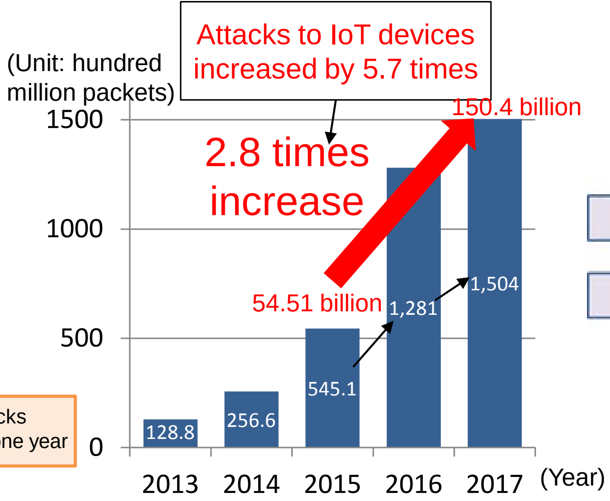
Reiko Kondo
Director
Office of the Director-General for Cybersecurity
Ministry of Internal Affairs and Communications (MIC)
JAPAN

Attacks on IoT Devices (Observed by NICTER)

NICT(National Institute of Information and Communications Technology) is observing cyber attacks globally by monitoring 300,000+ unused IP addresses (darknet).

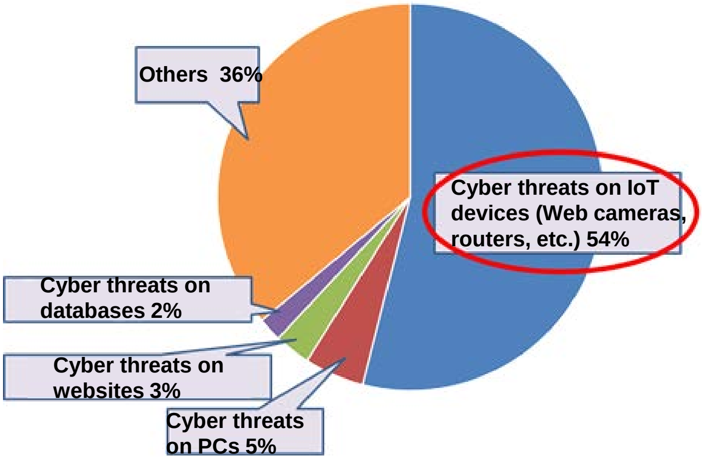


- 🟦 TCP SYN
- 🟨 TCP SYN/ACK
- 🟩 TCP ACK
- 🟪 TCP FIN
- 🟪 TCP RESET
- 🟧 TCP PUSH
- ⬜ TCP Other
- 🟥 UDP
- ⬜ ICMP



Number of cyberattacks observed by NITCER in one year

More than half were attacking on IoT devices!



Comprehensive Package of IoT Security Measures

The Cybersecurity Task Force administered by MIC published the comprehensive package of IoT security measures in October 2017. The progress made so far was reviewed this month. The progress report of this package has been published on 27th July 2018.

Measures on IoT devices vulnerabilities

- Necessary to implement measures on IoT devices vulnerabilities, covering the entire lifecycle (design, development, sale, installation, operation & maintenance and use)
- Necessary to organize the structure to conduct vulnerability assessment

Promotion of research & development

- Share security operation know-how and promote research and development in need

Acceleration of security measures in the private sector

- Accelerate cybersecurity investment in the private sector
- Encourage to share cyber attack/threat information to prevent damage or its spread

Strengthening of HR development

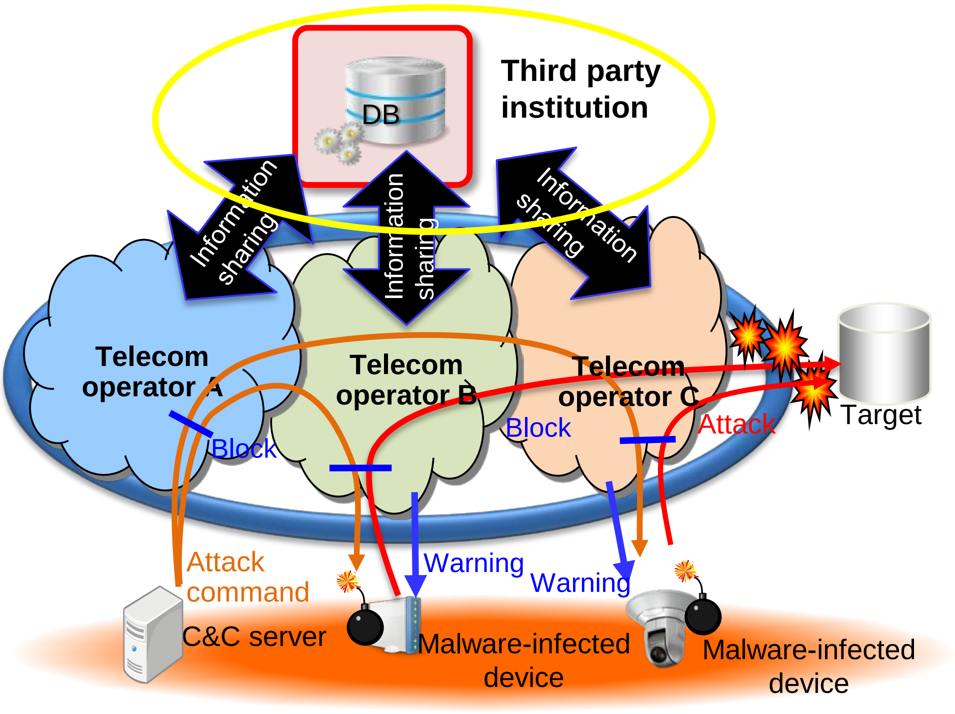
- Strengthen hands-on cyber defense exercise when predominantly lacking security experts

Promotion of international cooperation

- Promote information sharing, rulemaking, HR development and R&D bilaterally and multi-nationally

Information Gathering Hub with Firm Security Measures

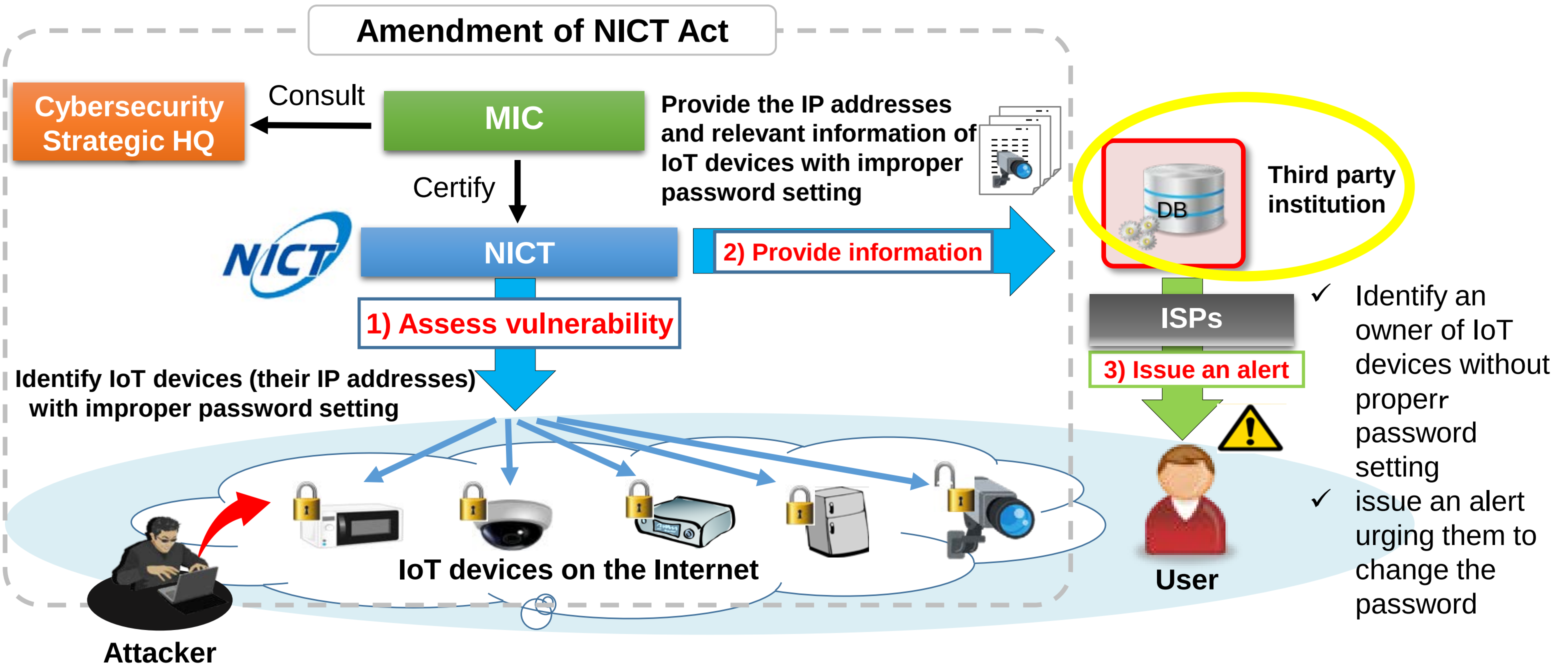
In May 2018, revised Telecommunications Business Act and NICT ACT were promulgated. By the revised Telecommunications Act, it is allowed to establish **the third party, working as an information gathering hub with firm security measures to manage sensitive information**.



- ✓ C&C server, through which the attacker gives instructions to infected terminals, is connected to the network of telecom operator A
- ✓ Infected terminals are connected to the networks of telecom operators B and C
- ✓ Telecom operators A, B, and C can share threats information such as IP addresses and time stamps through the third party institution without violating secrecy of information
- ✓ Telecom operator A blocks C&C server
- ✓ Telecom operators B and C can make alerts to their customers

Vulnerability Assessment of IoT Devices with Improper Password Settings

Revised ACT on National Institute of Information and Communications Technology (NICT) enables NICT to **actively scan** IoT devices over the Internet and **identify IoT devices with improper password settings**, of which actions had been prohibited by the Act on Prohibition of Unauthorized Computer Access.


Amendment of NICT Act
Cybersecurity Strategic HQ
Consult
MIC
Certify
Provide the IP addresses and relevant information of IoT devices with improper password setting
NICT
2) Provide information
1) Assess vulnerability
Identify IoT devices (their IP addresses) with improper password setting
DB
Third party institution
ISPs
3) Issue an alert
IoT devices on the Internet
Attacker
User

- ✓ Identify an owner of IoT devices without properr password setting
- ✓ issue an alert urging them to change the password

Amendment on the Technical Standard of Terminal Equipment for IoT Security Purpose（IoT Certification）

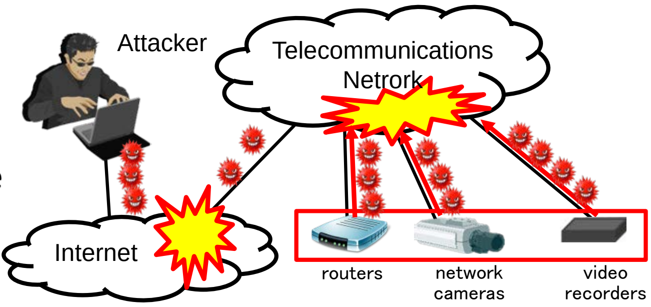
- In order to prevent massive malware infection on IoT devices, the Information and Communications Council in MIC discussed an addition of security measures to a technical standard of terminal equipment required by the Telecommunication Business Act and released a report on September 12, 2018 after public consultation.
- MIC is now preparing related ordinances, notifications, and guidelines for implementing the security measures, which will be enforced in April 2020.

Summary of the report

✓ Terminal equipment that has a remote control function to send/receive data through the internet is required to:

1) have access control on the remote control function,
2) have a mechanism to encourage its user to change the default IDs/passwords, if the access control uses IDs/passwords for the authentication and
3) have a feature to be able to update firmware,

or any equivalent/better security measures to/than above.



✓ The requirement does not apply to PCs or smartphones that are generally protected by other security measures such as anti-virus software.

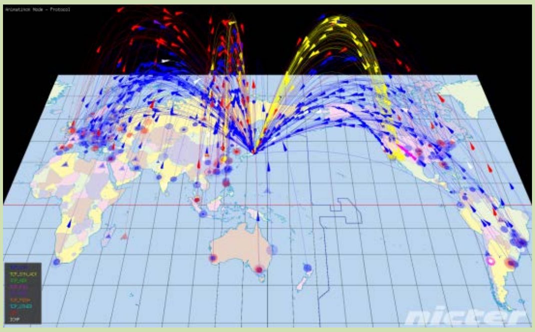
✓ These measures should be implemented after some period (one to two years) for allowing IoT device makers and certification bodies to prepare for adding new measures.

R&D Activities against Indiscriminate/Targeted Attacks

NICT (National Institute of Information and Communications Technology) has been conducting R&D activities against indiscriminate and targeted cyberattacks.

(1) **NICTER** [Countermeasures against Indiscriminate attack]

- **Visualize geographical information, amount, and type of cyberattacks in real time** by observing communication in the darknet (unused IP addresses) with sensors.
- The system based on this technology is introduced to **provide alerts to local governments infected with malware**.



Introduced to approx. 600 local governments (as of November 2017)

(2) **NIRVANA-Kai** [Countermeasures against targeted attacks]

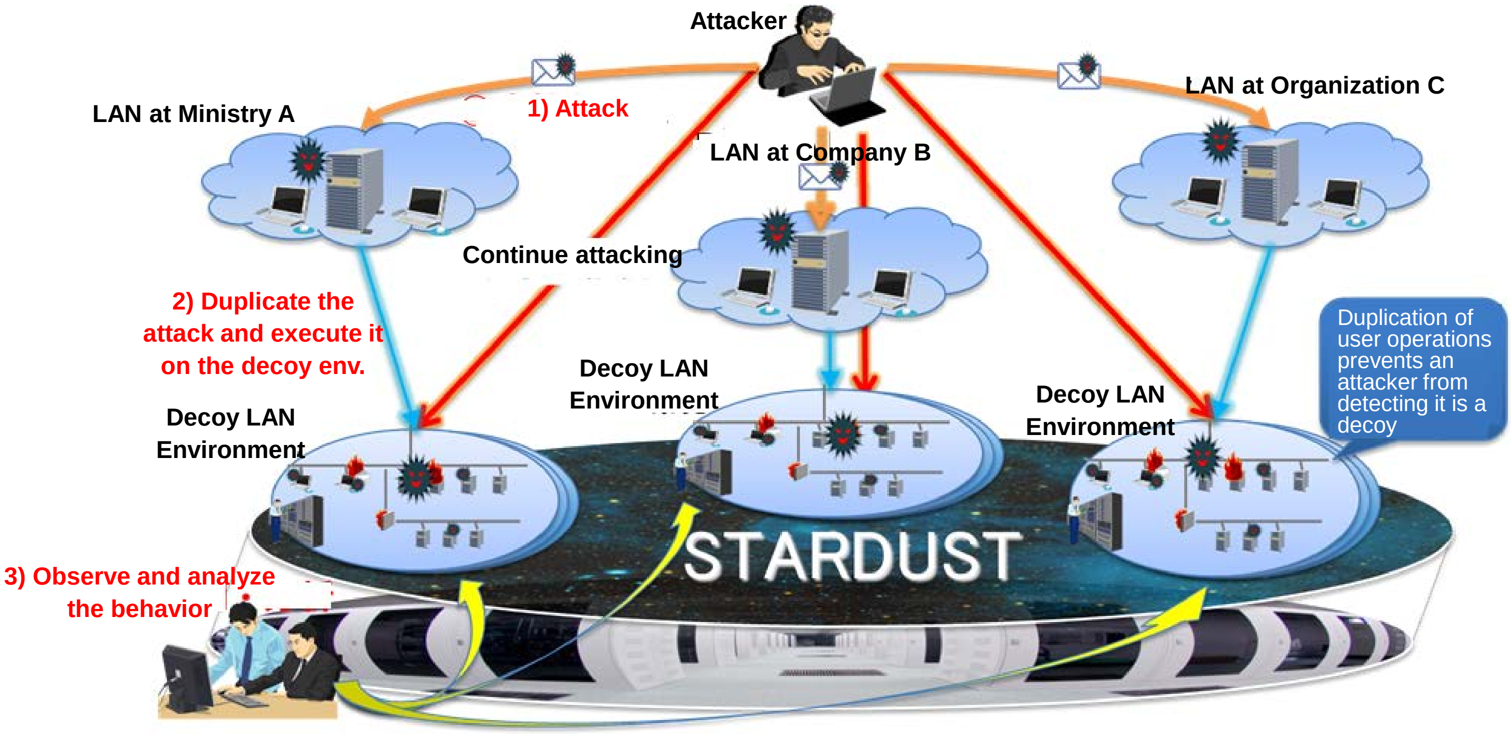
- **Visualize traffic occurred within the organization in real time** by installing the sensors in the environment.
- Further developments which enable **automatic block for abnormal communications once it is detected**

Started technology transfer (June 2015)

R&D Activities against Indiscriminate/Targeted Attacks

(3) STAR DUST (Honeynet)

STAR DUST is a honeynet to study targeted attacks in detail, lead by NICT. When an attacker sends malicious emails to a specific organization, the attached file is executed in “decoy environment implemented in advance" to observe and analyze the behavior.


Attacker
LAN at Ministry A
1) Attack
LAN at Organization C
LAN at Company B
Continue attacking
2) Duplicate the attack and execute it on the decoy env.
Decoy LAN Environment
Decoy LAN Environment
Decoy LAN Environment
Duplication of user operations prevents an attacker from detecting it is a decoy
STARDUST
3) Observe and analyze the behavior

Human Resource Development (National Cyber Training Center)

In order to develop cybersecurity human resource capable of practically handling sophisticated and complex cyberattacks, MIC has started the following hands-on training programs since April 2017 in the National Cyber Training Center, which has been established under the NICT.

(1) CYDER

A **CY**ber **D**efense **E**xercise with **R**ecurrence (**CYDER**) program for governmental administrations, local governments, independent administrative agencies, and critical infrastructure providers, etc.

(2) Cyber Colosseo

A cyber defense exercise for those who are in charge of cybersecurity in the organizations related to the Tokyo 2020 Olympic and Paralympic Games. (**Cyber Colosseo**)

(3) SecHack365

Training program for young cybersecurity innovators. (**SecHack365**)

CYber Defense Exercise with Recurrence (CYDER)

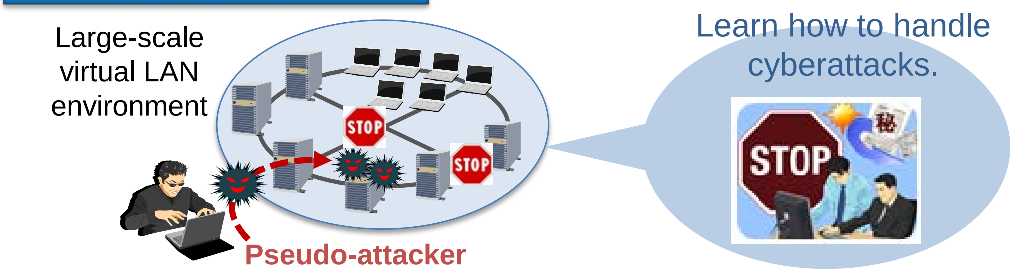
National Cyber Training Center

○ MIC provides **CYDER exercises**, which is conducted by NICT, **for those who are in charge of information systems in administrative organizations and critical infrastructure providers**.

○ **Participants can experience a series of incident handing** against cyberattacks, **by hands-on operation of real machines in the large-scale virtual LAN environment simulating the organizations network**.

○ In FY 2017, CYDER exercises were held **100 times** and a total of **3,009 trainees** were attended.

Image of CYDER



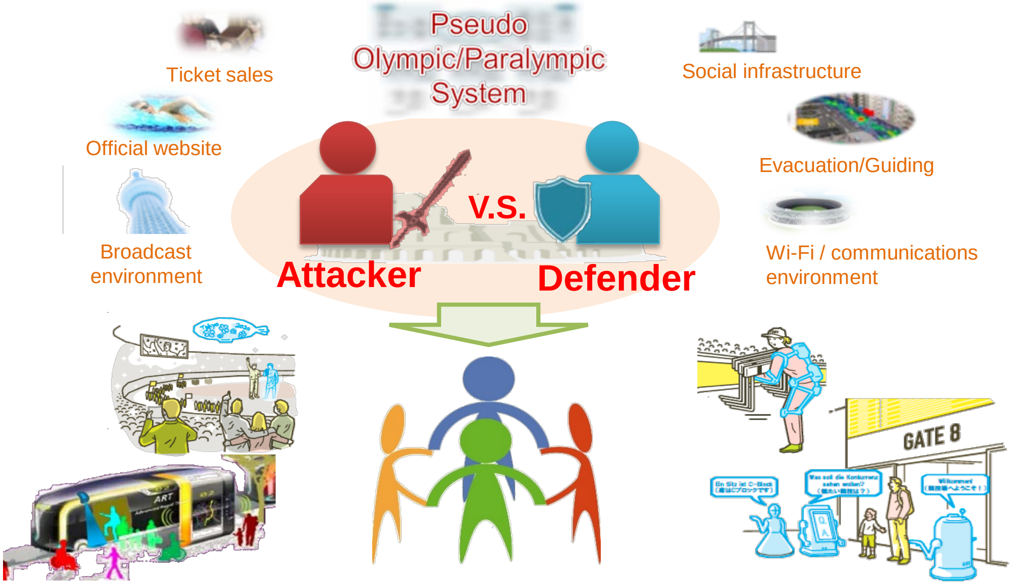
Exercise Plan for 2018

Course	Target organizations	Venue	Number of courses
Course A (Beginner)	(For all organizations)	47 prefectures	60 times
Course B-1 (Intermediate)	For local governments	11 regions	20 times
Course B-2 (Intermediate)	For governmental organizations	Tokyo	10 times
Course B-3 (Intermediate)	For critical infrastructure providers	Tokyo	10 times

Practical Cyber Exercise for the Tokyo 2020 (Cyber Colosseo)

National Cyber Training Center

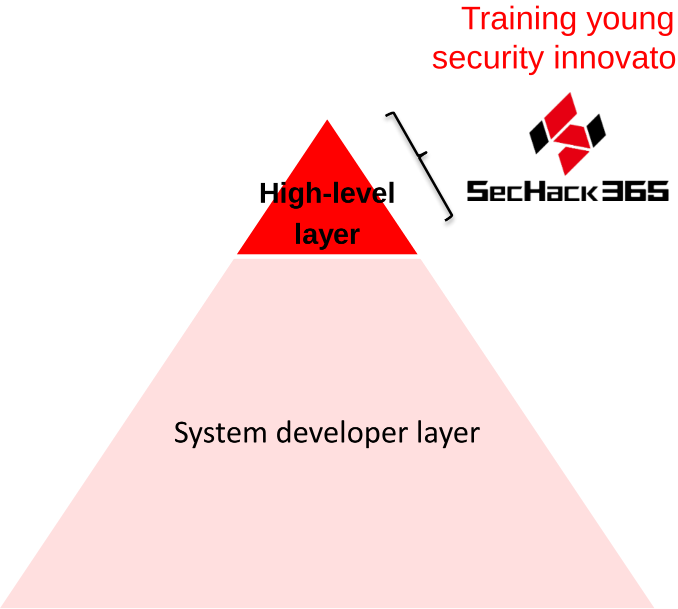
- **Cyber Colosseo** exercise started February 2018 to develop human resources capable of handling advanced cyberattacks, which is conducted for those who are in charge of cybersecurity in the organizations related to Tokyo 2020 Olympic and Paralympic Games.
- At the exercise venue of the Cyber Colosseo (NICT Innovation Center in Tokyo), battle-style (attacker v.s. defender) exercise is conducted in the virtual network environment using physical machines and software.

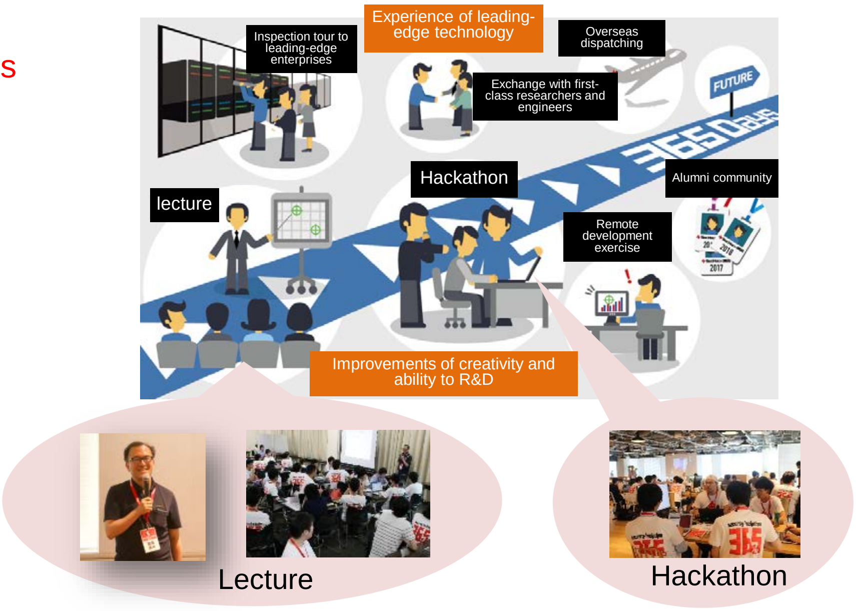


Training Young Security Innovators (SecHack365)

National Cyber Training Center

- In order to increase the number of advanced cybersecurity researchers and entrepreneurs in the future, NICT provides an one-year cybersecurity training program with hands-on training and remote software development training for young talents, utilizing its own cybersecurity research assets.
- Participants are ICT engineers who are 25 years old or younger, living in Japan (39 trainees have completed the one-year program in FY2017).

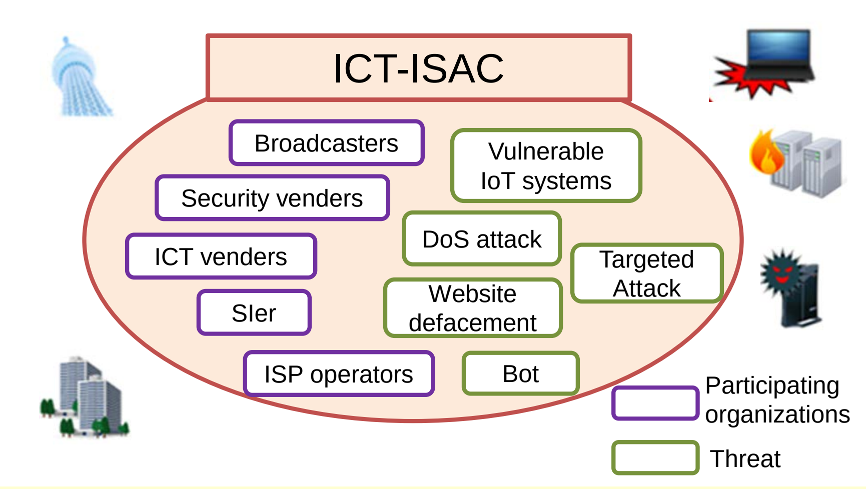



Inspection tour to leading-edge enterprises
Experience of leading-edge technology
Overseas dispatching
Exchange with first-class researchers and engineers
FUTURE
365Days
Hackathon
Alumni community
lecture
Remote development exercise
Improvements of creativity and ability to R&D
Lecture
Hackathon

Cooperation through ISAC

- **ISAC (Information Sharing and Analysis Center)** has been established for each industry for the purpose of collecting, analyzing, and sharing the incident information on cyberattacks.
- **Telecom-ISAC Japan was established in 2002, as the ISAC for telecom industry.**
- Financial ISAC was established in 2014. Electricity ISAC and J-AUTO-ISAC were established in 2017.
- Broadcasters, ICT vendors, and cybersecurity vendors have participated in Telecom-ISAC Japan, which has been renamed as **ICT-ISAC** Japan since March 2016, in order to reinforce information sharing function throughout the ICT field.
- International Cooperation has been promoted.

Overview of ICT-ISAC Japan



President:
Tadao Saito

Members:
39 companies, including telecommunications carriers, broadcasters, ICT vendors, security vendors, etc.

3.2.4 Discussion on common approaches and possible synergies

There were no materials presented in this session.

3.3 Session 3: Working Session on Business Solutions Applied to Selected Vertical Sectors

The next session on Business Solutions Applied to selected vertical sectors was moderated by Nina Olesen from European Cyber Security Organisation (ECSO).

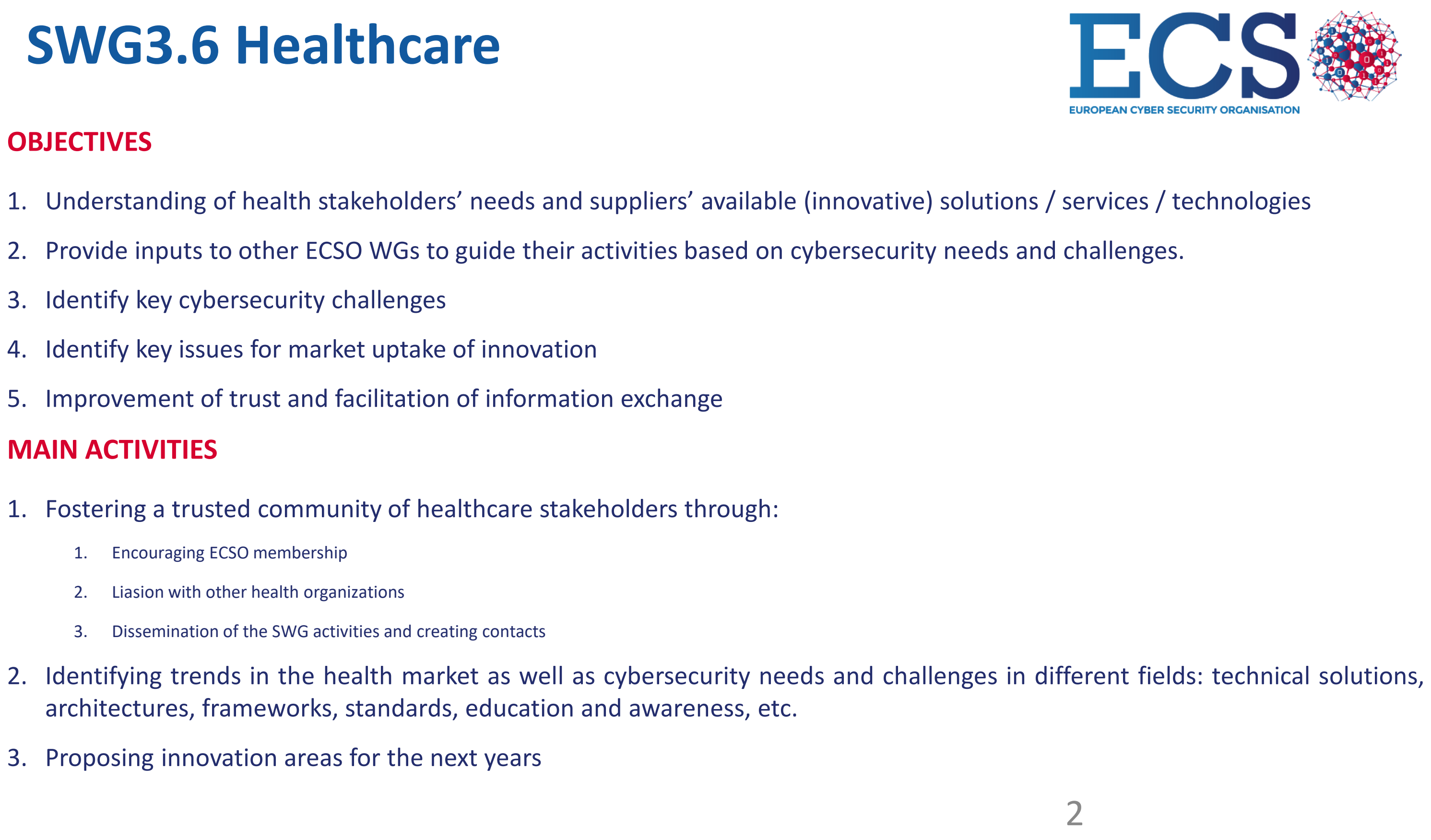
3.3.1 Challenges and capabilities needs from the selected verticals

The next sessions were about the challenges and capabilities needs from the selected verticals and included three presentations. The first was about the Health sector and was given by Julio Vivero, from GMV:

EUROPEAN CYBER SECURITY ORGANISATION

HEALTH: CHALLENGES AND NEEDS (European Cyber Security Organisation)

24 January 2019



SWG3.6 Healthcare

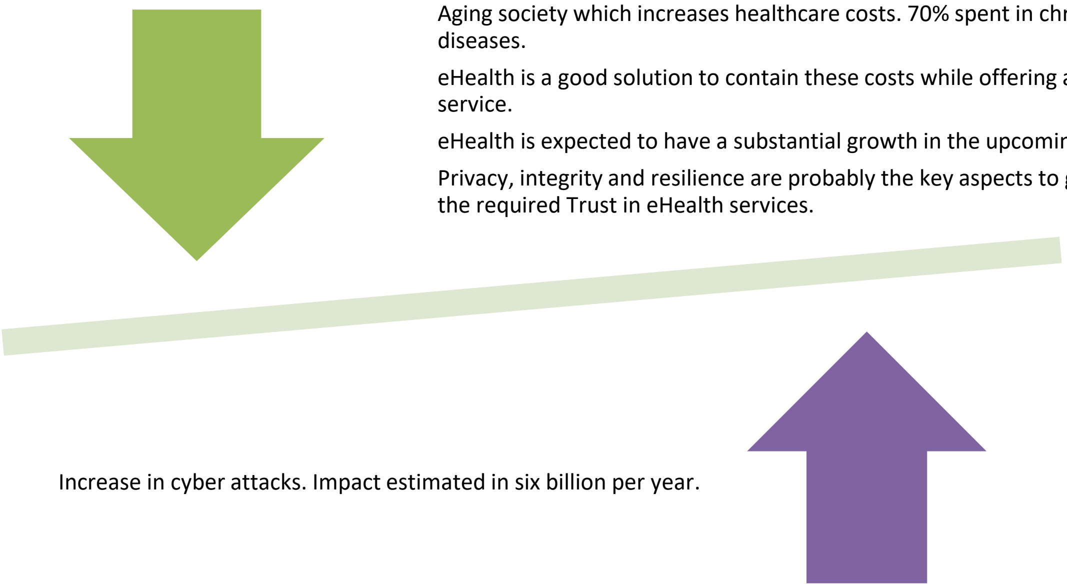
OBJECTIVES

1. Understanding of health stakeholders’ needs and suppliers’ available (innovative) solutions / services / technologies
2. Provide inputs to other ECSO WGs to guide their activities based on cybersecurity needs and challenges.
3. Identify key cybersecurity challenges
4. Identify key issues for market uptake of innovation
5. Improvement of trust and facilitation of information exchange

MAIN ACTIVITIES

1. Fostering a trusted community of healthcare stakeholders through:
    1. Encouraging ECSO membership
    2. Liasion with other health organizations
    3. Dissemination of the SWG activities and creating contacts
2. Identifying trends in the health market as well as cybersecurity needs and challenges in different fields: technical solutions, architectures, frameworks, standards, education and awareness, etc.
3. Proposing innovation areas for the next years

Health Cybersecurity: Context



Aging society which increases healthcare costs. 70% spent in chronic diseases.

eHealth is a good solution to contain these costs while offering a better service.

eHealth is expected to have a substantial growth in the upcoming years.

Privacy, integrity and resilience are probably the key aspects to generate the required Trust in eHealth services.

Increase in cyber attacks. Impact estimated in six billion per year.

Health Cybersecurity: Market

eHealth market is expected to reach over 280.000 million Euro by 2022 (http://www.grandviewresearch.com/industry-analysis/e-health-market)

Fields:

- Health Analytics and BigData in Health
- mHealth
- TeleHealth
- Integrated Electronic Health Records
- eLearning in eHealth
- Social Media in Health

Health Cybersecurity: Challenges

EUROPEAN CYBER SECURITY ORGANISATION

1. Increase in cyberattacks
2. Aging society favours eHealth services
3. Patient ecosystem: delocalized network of care services
4. Medical devices cybersecurity
5. Trust in eHealth shall be obtained through: privacy, integrity and resilience of services.
6. Trends towards exploitation of health BigData <-> privacy
7. An EU integrated Electronic Health Record <-> heterogeneous legislation within Europe

Health Cybersecurity: Needs

Key levers for the following years:

1. **My data, my decisions.** Patients and institutions share their data with flexible consent mechanisms.
2. **Liberate the data**. Health outcomes and performance data will be freely published with full transparency.
3. **Revolutionise health**. Technology and information management drives the pace of change.
4. **Connect up everything**. This will link the lifestyle data with health data by means of lots of new apps and tools.
5. **Include everyone**. In other words, the contribution and benefits from eHealth for all.

CONTACT US

European Cyber Security Organisation 10, Rue
Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770256

E-mail:
Dr. Julio Vivero
Healthcare SWG3.6 Chair
jvivero@gmv.com

Follow us
Twitter: @ecso_eu

The second was on Banking and Finance sector by Giorgio Cusmà Lorenzo, from Intesa Sanpaolo:

INTESA SANPAOLO

Cyber Security Strategy: Stakeholders Networking

Enhancing Cyber Resilience

Bruxelles, 24 January 2019

INDICE

A global perspective

Cyber Security and Digital Strategy

The Banking sector is facing a paradox: Financial Institutions need to reshape their business models investing heavily on innovative technologies and new skills, whilst coping with a structural contraction of revenues due to several contingency forces, such as the unprecedented interest rates reduction, the increasing competitive pressure, and the non performing loans challenge. Bearing this landscape in mind, the financial institutions have to create ***new digital business models*** *and to cope with cybersecurity issue.*

Digital Transformation:
Digital Banking in a EU Digital Single Market and beyond it, creates a paradigm shift on traditional Business Models

Regulation & Harmonisation:
To face the continuously evolving Regulatory Requirements, it is of utmost importance to foster the dialogue among institutions and private stakeholders

Cybersecurity Holistic Vision:
Borderless and interconnected economy leverages new opportunities arising from innovative technologies, whilst introduces cyber risks also related to processes, culture and awareness

Collaboration, Coordination, Communication:
To enhance the cyber-resilience cooperation and info-sharing are the cornerstones at sectorial and cross sectorial level, these are identified as pillars also within the EU Cyber Security Strategy

Six areas to enhance ISP cyber resilience

Collaboration among Financial Institutions

Among all the issues related to Cyber security ISP has identified the following areas of collaboration among Financial Institutions, to be tackled as priorities through the Stakeholders Network:

Infosharing

Enhancing information sharing among Financial Institutions and Member States is a prerequisite to foster cyber security at EU level. These could be adopted both within the specific Financial sector and across industries.

Incident Reporting

The EU framework for Incident reporting foresees the involvement of multiple authorities, applying different procedures and templates, creating possible overlaps and redundancy in reported information. Likely, a single incident might entail to fulfill multiple reporting requirements. It is clear the need for harmonisation and coordination among actors.

Crisis Management Procedures

There is a need for common procedures of cyber crisis management. The definition of such procedures might be done leveraging the progresses achieved in info sharing & incident reporting, and conducting simulation and war gaming exercises.

Secure Supply Chain Management

Supply chain is often the weakest cyber security link and in an integrated and interconnected eco-system this is an unbearable risk. Evaluating every single entity along the supply chain, in order to enhance the overall resilience, is of utmost importance.

Cyber Risk Measuring

The evolution of the measurement models and methodologies for Cyber risk assessment, represents the cornerstone to have an efficient management of Cyber Security within the institution, dynamic in intercepting emerging threat, and risk-based in identifying countermeasures.

Education & Training

Human factor is critical in Cyber Security, thus, to increase the resilience of the entire system, it is necessary to raise awareness and knowledge around cyber-risk. Training and awareness programs for customers and employees should be considered as very relevant.

Improving Cyber resilience

Collaboration among Financial Institutions

Intesa Sanpaolo believes that Cyber Security is a ***collective intangible asset*** and considers that ***improving Cyber Resilience is a common goal***, that ***requires a collaborative peer-to-peer approach*** and a joint effort to assess and address the underlying ***multidisciplinary challenge*** the financial institutions have to cope with. To achieve this common goal, ISP has launched a ***Stakeholders Networking*** initiative with the EU institutions a group of peers.

Improving Cyber resilience is a must

- It is a regulatory requirement
- It is a business survival need
- It is a business growth enabling factor
- It is often coming as a top down approach
- It is often foreseeing a (multi) Hub and spoke approach

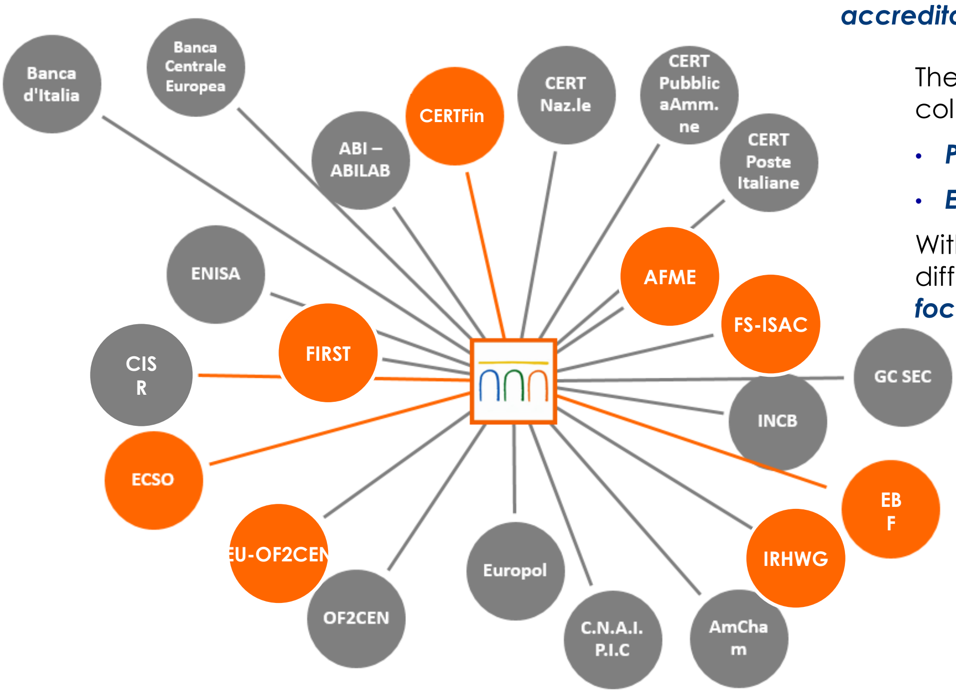
Intesa Sanpaolo ***is willing to combine a top down approach,*** arising from regulations and market trends, ***with a collaborative one*** putting forward the ***practitioners experience and their holistic views*** to share best practices and innovative ways to address the Cyber Risk.

While there is no need to create another institutional body, ***there is room for collaboration in harmonising tools and procedures and in getting ready for swift reaction to cyber attacks***

Collaboration among Financial Institutions

Ongoing cooperation in ISP Network

During the last years, several international collaboration activities have been set-up to foster and enhance Intesa Sanpaolo Group cyber security strategy aiming to: A) ***extend the leadership role*** within the Financial sector in the European Cybersecurity domain; B) ***become trustworthy partner*** for Institutions and peers; C) leverage the process of ***accreditation with international financial sector***.



The strategy has been declined in specific collaboration with selected ***partners*** for:

- ***Potential to influence***
- ***Effectiveness in execution of the objectives***

With the partners, have been developed different activities referable to ***three different focus area*** with the aim to:

1. ***Address cybersecurity strategy at European level;***
2. ***Implement solutions of common interest with peers;***
3. ***Support an effective spending of European funds***

See following page for details

INTESA SANPAOLO

Intesa Sanpaolo’s Strategy

Focus areas and Common Application Project

Main partner

1 Address cybersecurity strategy at European level

Support – through Institutional meetings, events organisation and partecipation, position paper drafting, proposition of amendments (direct or through trade associations) to the normative drafts of the European Commission – **Definition of EU strategies** consistent with the real needs of *Financial Institutions both in terms of cyber risk and the provision of critical services for the community.*

- ECSO
- EBF
- AFME
- CEPS

2 Implement solutions of common interest with peers

Enable - through relationships with peers, vendors and institutional actors - the development of specific projects (eg **Common Application Tool** *– for* **Mandatory Incident Reporting** *and* **Voluntary Info sharing)** *able to offer a practical solution to the needs of Financial Institutions. Participate proactively in dedicated working groups such as the Incident Reporting Harmonization Working Group (***IRHWG***),*

- ECSO
- EBF
- AFME
- ENISA
- BBVA
- JP MORGAN
- RABOBANK

3 Support an effective spending of European funds

Also through the European CyberSecurity Organisation (ECSO), advising the European Commission on the funding priorities within the European Horizon 2020 program. ISP with the involvement in managerial and operational roles in the ***public / private partnership*** *created in collaboration with the private sector (the c-PPP)* and by taking part to the funding opportunities of the European Commission *with EU peers*

- ECSO

ISP Cyber Security Initiatives

Stakeholders Networking: Institutional initiatives

Intesa Sanpaolo strategic approach is to **collaborate with external entities both at local and international level**, and is actively involved in the following initiatives:

1 CERTFin

The **Italian CERT for the Financial sector**, driven by the Italian Banking Association (ABI) and Bank of Italy, has the aim of setting up a coordination and information sharing group for the financial sector on Cyber Security issues, with the objective to enhance cyber resilience in the financial sector.

2 *Italian Cyber Security Framework*

The Italian Cyber Security Framework aims to provide **public and private organizations with a voluntary and homogeneous approach**. The framework purpose is to address cyber security, reduce Cyber Risk, increase the exchange of information cross-industries and foster cyber-resilience.

3 EBF

EBF works mainly on the regulatory side by analyzing the incoming regulations and by representing the European banking sector position. EBF recognizes that **cyber security is a key priority** and ranks it **high in its regulatory agenda**.

4 ECSO

ECSO works with the EC to foster cyber resilience and security. The cPPP between ECSO and EC defines the **investment priorities** and **ensures that funds allocated** are contributing to the achievement of a Cyber Secure EU Digital Single Market.

5 AFME

AFME is the voice of all Europe's ***wholesale financial markets***, providing expertise across a broad range of regulatory and capital markets issues.

6 *Glocal ventures*

Major Financial Service providers having a worldwide presence in order to manage cyber threats and to be fully compliant with requirements arising from the involvement in different national and international FMIs, need to adopt **borderless ICT & Cyber Security Governance Models** based on international standards and frameworks (i.e. NIST) **sharing information** with other critical infrastructure and law enforcement agencies.

ISP Cyber Security Initiatives

A Glocal Approach

Intesa Sanpaolo Group is a major ***European*** Financial Service provider active in Banking and Insurance Sectors. With its worldwide presence, the Intesa Sanpaolo Group, has adopted a ***Glocal approach***, thinking Global and acting Local, witnessed by its international attitude and active participation:

Incident Reporting Harmonisation WG for a Common Application

IRHWG

ISP Group is leading a private sector initiative, involving major banks at EU level, to be at the forefront of the IRH challenge. The purpose is to **define a common data-set to standardize Incident Reporting** and **Crisis Management procedures and to design/implement a Common Application** for bi-directional flows between Financial Institutions and Supervisory Authorities. As part of the Consortium CyberSec4Europe that was granted EU funds by the European Commission, ISP will be part of a **Pilot Project aiming at the development of a tool** addressing the common need to respond to incident reporting mandatory requirements.

Information Sharing

Carnagie endowment

This initiative is focused on the discussions among **the G20 regarding cybersecurity and financial stability**. Over the past two and a half years, the Carnegie Endowment for International Peace has been working on this issue including engaging several of the G20 members and other countries as well as experts in private industry.

Information Sharing

FS-ISAC

FS-ISAC Critical Infrastructure Notification System (CINS) is a service that allows to notify all the members about important information in the event of an urgent or crisis situation. The aim of the service is to **speed security alerts to multiple recipients** around the globe near-simultaneously while providing for user authentication and delivery confirmation.

Best practices

FSB – Cyber Lexicon

ISP Group is involved to develop a cyber lexicon for supporting the work of the FSB, standard-setting bodies, authorities and private sector participants, e.g. financial institutions and international standards organisations, to **address cyber security and cyber resilience in the financial sector**.

Best practices

FIRST

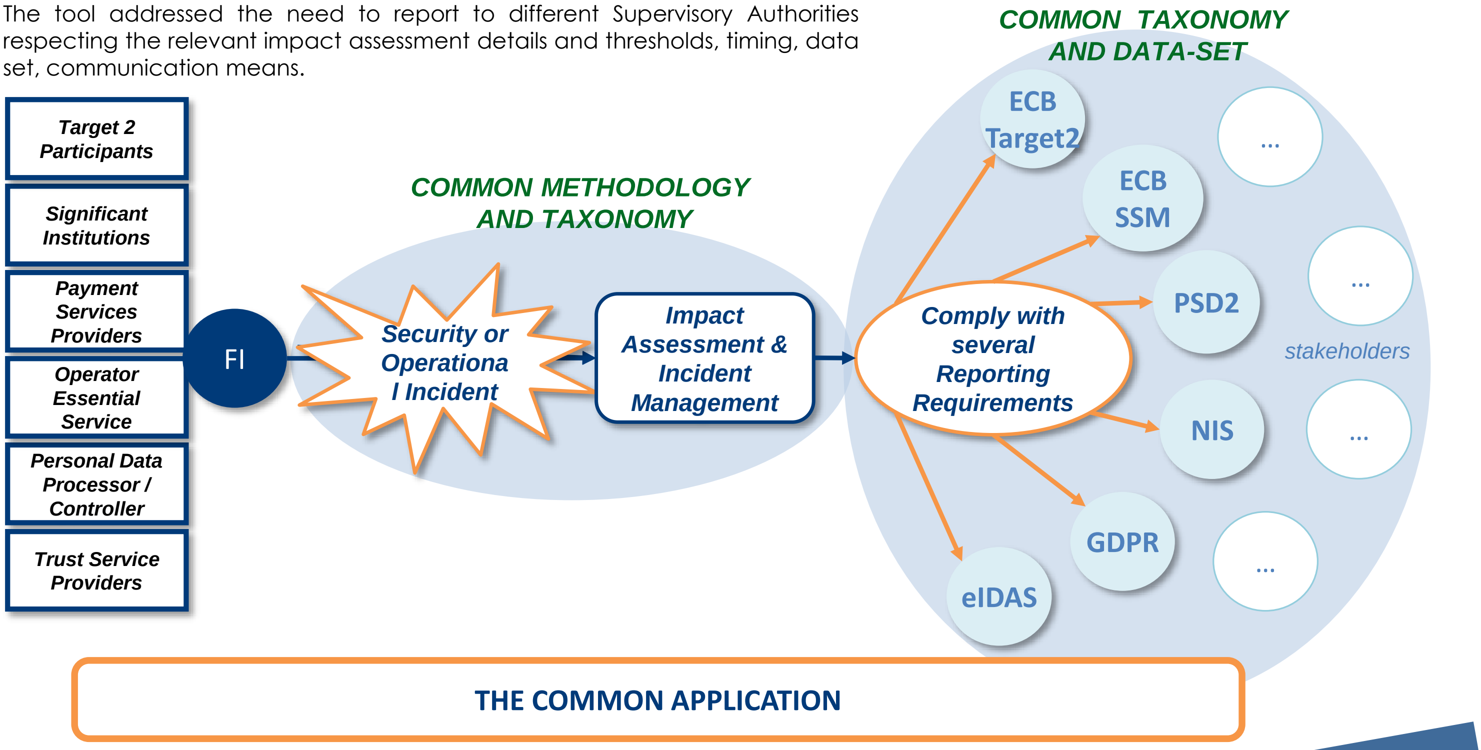
ISP-CERT becomes a ***FIRST full member*** entering in a trusted network of security practitioners and incident response teams which allows a quicker and closer collaboration with other organisations through trusted communication channels.

The Common Application

A project tackling the need for enhanced cooperation

The Project proposal to develop a Common Application to address the need of Mandatory Incident Reporting was granted funds by the European Commission in response to the European Call for Proposal SU-ICT03. BBVA,ATOS and ISP, as part of the CyberSec4Europe Consortium will benefit of Horizon2020 funding to for the development of the tool.

The tool addressed the need to report to different Supervisory Authorities respecting the relevant impact assessment details and thresholds, timing, data set, communication means.


COMMON TAXONOMY AND DATA-SET
Target 2 Participants
Significant Institutions
Payment Services Providers
Operator Essential Service
Personal Data Processor / Controller
Trust Service Providers
FI
COMMON METHODOLOGY AND TAXONOMY
Security or Operationa l Incident
Impact Assessment & Incident Management
Comply with several Reporting Requirements
ECB Target2
ECB SSM
PSD2
NIS
GDPR
eIDAS
…
…
stakeholders
…
…
THE COMMON APPLICATION

Achievements of the Stakeholders Networking

Goals reached

Proactively collaborating in many initiatives, the ***Intesa Sanpaolo Group*** has provided a significant contribution to different Working Groups, improving ISP **positioning among major EU players**. As of today the following goals have been achieved:

Goals

- Recognised **leading role** on Cybersecurity topics at European Level, not only by private institutions, but also by EU Bodies, Agencies and Authorities
- Creation of a selected **Network of Trusted Partners** whilst becoming a recognized trustworthy partner for peers across jurisdictions and across industries.
- Identify and design with other Stakeholders, cybersecurity related solutions, addressing common needs, starting with Mandatory **Incident Reporting Fragmentation** and **Information Sharing.**

The third presentation was on the Energy sector by Mario Jardim, from Schneider Electric:

Cyber security for energy sector

Challenges and needs

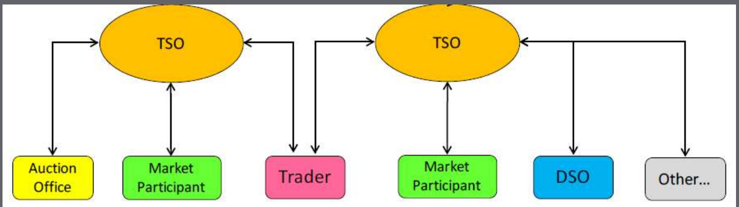
22/01/19

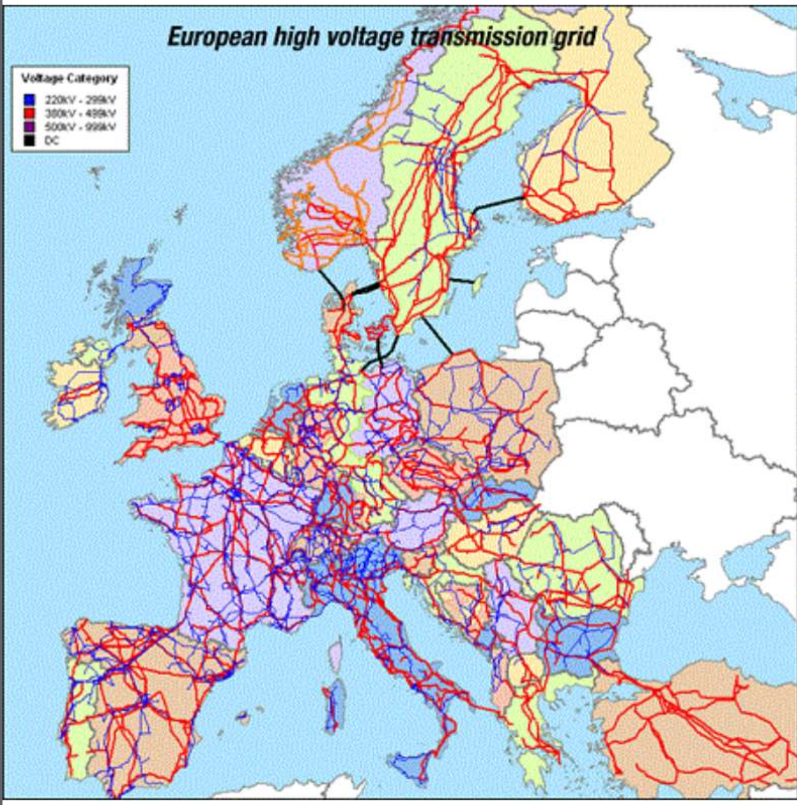
Mario Jardim

Energy sector challenges

Electrical Grid is Pan-European shared by different actors.

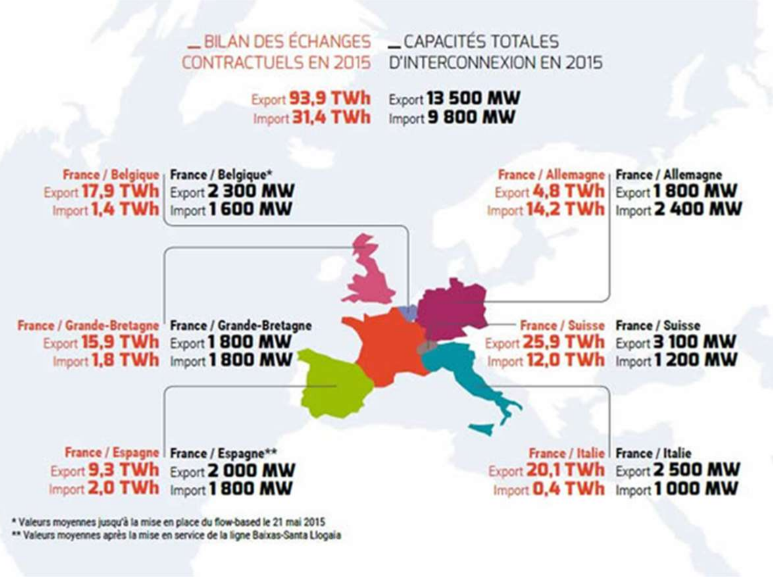
- Energy is at the center on modern world enabling society digitization
- Vital functions are energy dependent : water, health, food, transportation, banking …
- All critical infrastructures are impacted by the loss of energy





Domino effect

- Domino effect between countries and legal entities (ex. Kosovo frequency shift)
- Large installed base of distributed systems composed of solutions from different manufacturers mixing old and new technologies.
- End to end protection and data integrity are critical
- Objective is grid resilience, supporting the functioning of European society and economy in crisis situation

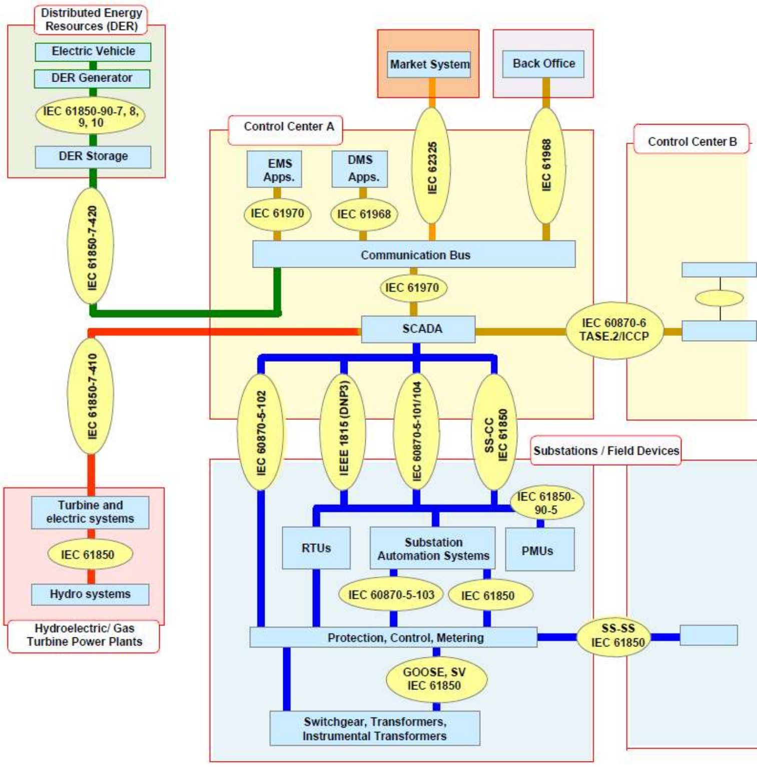


France example of power exchanges

Utilities challenges

Key points

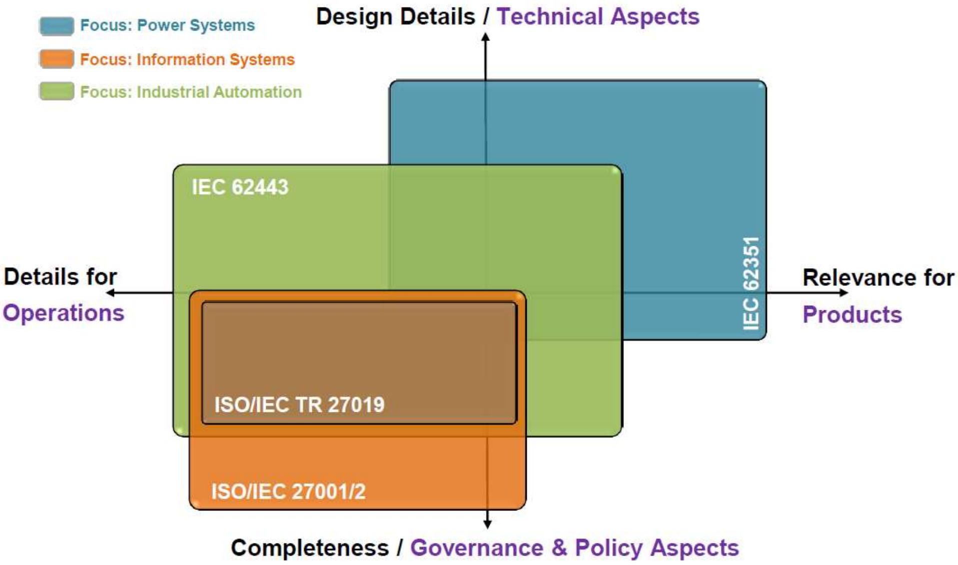
- A system approach based on risk analyses
- Cannot treat grid operating systems as conventional IT systems
- System life cycle, architectures and operational process are fundamental
- Are deploying security measures in aging infrastructure
- People training and education on security measures
- Supply chain adaptations
- Certification costs



Energy sector main standards

Approach from systems to products

- SCADA and trading systems are following ISO/IEC 27001/2/19 recommendations for people, processes and controls.
- Substation systems and related components are following IEC62443 recommendations including system integrators
- Communication protocols between and inside systems are following IEC62351.


Focus: Power Systems
Focus: Information Systems
Focus: Industrial Automation
Design Details / Technical Aspects
IEC 62443
IEC 62351
Details for Operations
Relevance for Products
ISO/IEC TR 27019
ISO/IEC 27001/2
Completeness / Governance & Policy Aspects

Key Take away

•Electrical grid infrastructure is interconnected across Europe and shared by many actors and countries

•Primary focus is grid resilience and service continuity

•International security standards like ISO/IEC 27001/2/19, IEC62443, IEC62351 are the basic support to a shared level of security among actors

Life Is On | Schneider Electric

3.3.2 The answers from technology and trusted supply chain perspective

The next session included two presentations on the “Cybersecurity for the Internet of Things” by Ana Ayerbe, from Tecnalia and “Challenges of cybersecurity certification and supply chain management”, by Roberto Cascella, from ECSO Secretariat:

WE CAN
DO SO
MUCH
TOGETHER

ECS
EUROPEAN CYBER SECURITY ORGANISATION

EUNITY

Cybersecurity in the Internet of Things (Building Trust in the Machine Economy)

Ana Ayerbe
ana.ayerbe@tecnalia.com
@anaayerbe

tecnalia Inspiring Business

TECNALIA
RESEARCH AND TECHNOLOGICAL DEVELOPMENT

SINCE 2011

TECNALIA is a benchmark Research and Technological Development Centre in Europe.

_MULTISECTORAL

_MULTI-TECHNOLOGY

tecnalia Inspiring Business

A model
ANTICIPATING THE FUTURE

A COMBINATION
OF TECHNOLOGY,
TENACITY,
EFFICIENCY, COURAGE
AND IMAGINATION

WE RESEARCH TO OVERCOME CHALLENGES FACED BY MANKIND

HEALTH AND AGEING
ADVANCED MANUFACTURING
URBAN HABITAT
DIGITAL AND HYPERCONNECTED WORLD
LOW-CARBON ENERGY
CLIMATE CHANGE AND LACK OF RESOURCES

A broad and transversal topic from basic technologies to the applications

Enabling Technologies

SMART Industry

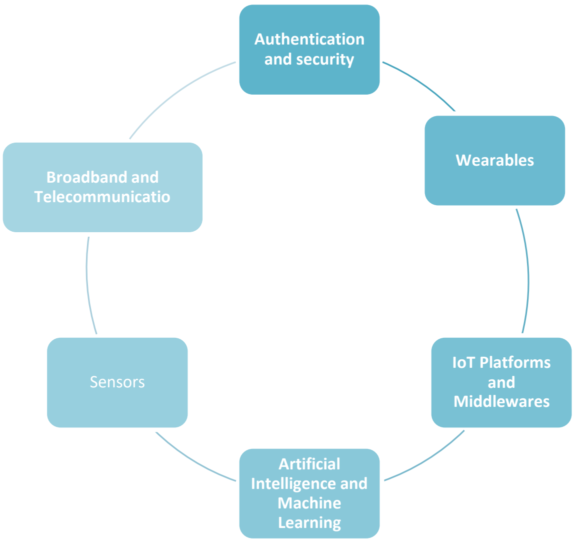
SMART Cities

SMART Environ ment

SMART Energy

SMART Living

Application Domains



Authentication and security

Wearables

IoT Platforms and Middlewares

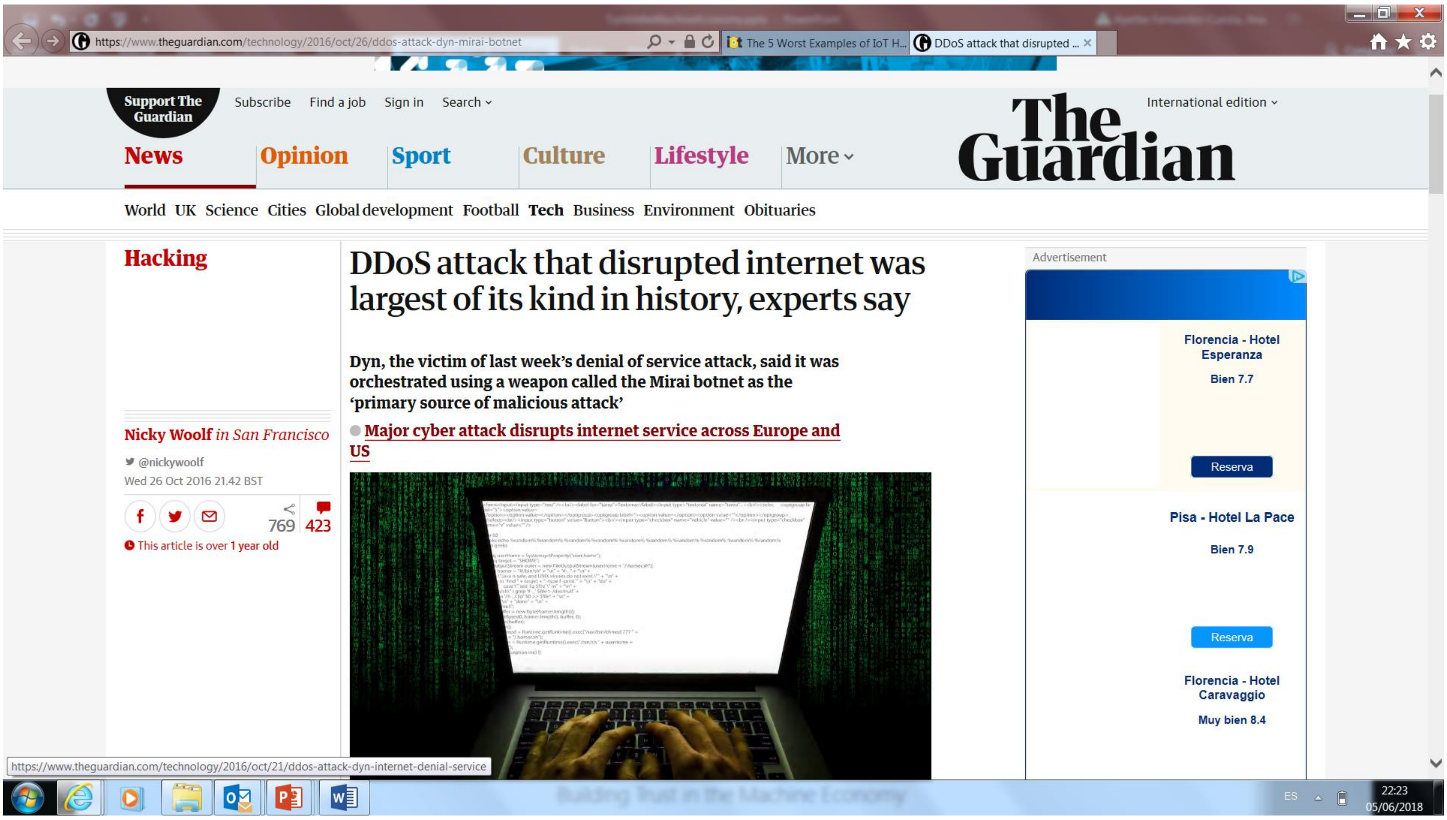
Artificial Intelligence and Machine Learning

Sensors

Broadband and Telecommunicatio

IoT Mass Market (B2C)

Things are massively produced and they are used by private users with little technical or security know-how



https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
The 5 Worst Examples of IoT H...
DDoS attack that disrupted ...
Support The Guardian
Subscribe
Find a job
Sign in
Search
International edition
The Guardian
News
Opinion
Sport
Culture
Lifestyle
More
World UK Science Cities Global development Football Tech Business Environment Obituaries
Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

● Major cyber attack disrupts internet service across Europe and US

Nicky Woolf *in San Francisco*

@nickywoolf

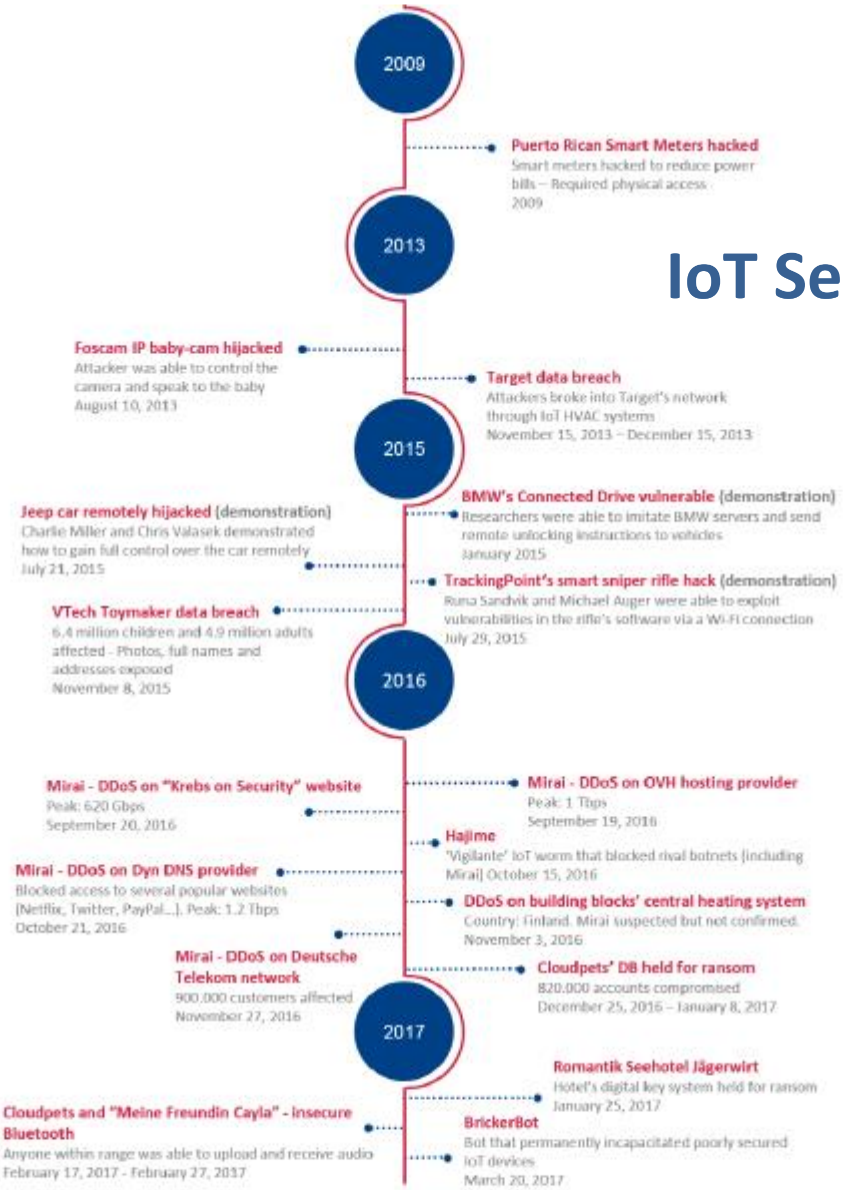
Wed 26 Oct 2016 21.42 BST

769 423

This article is over 1 year old

https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service
ES
22:23
05/06/2018

IoT Security Incidents



Puerto Rican Smart Meters hacked
Smart meters hacked to reduce power bills – Required physical access
2009

Foscam IP baby-cam hijacked
Attacker was able to control the camera and speak to the baby
August 10, 2013

Target data breach
Attackers broke into Target's network through IoT HVAC systems
November 15, 2013 – December 15, 2013

BMW's Connected Drive vulnerable (demonstration)
Researchers were able to imitate BMW servers and send remote unlocking instructions to vehicles
January 2015

Jeep car remotely hijacked (demonstration)
Charlie Miller and Chris Valasek demonstrated how to gain full control over the car remotely
July 21, 2015

TrackingPoint's smart sniper rifle hack (demonstration)
Runa Sandvik and Michael Auger were able to exploit vulnerabilities in the rifle's software via a Wi-Fi connection
July 29, 2015

VTech Toymaker data breach
6.4 million children and 4.9 million adults affected - Photos, full names and addresses exposed
November 8, 2015

Mirai - DDoS on OVH hosting provider
Peak: 1 Tbps
September 19, 2016

Mirai - DDoS on "Krebs on Security" website
Peak: 620 Gbps
September 20, 2016

Hajime
'Vigilante' IoT worm that blocked rival botnets (including Mirai) October 15, 2016

Mirai - DDoS on Dyn DNS provider
Blocked access to several popular websites (Netflix, Twitter, PayPal...). Peak: 1.2 Tbps
October 21, 2016

DDoS on building blocks' central heating system
Country: Finland. Mirai suspected but not confirmed.
November 3, 2016

Mirai - DDoS on Deutsche Telekom network
900.000 customers affected
November 27, 2016

Cloudpets' DB held for ransom
820.000 accounts compromised
December 25, 2016 – January 8, 2017

Romantik Seehotel Jägerwirt
Hotel's digital key system held for ransom
January 25, 2017

Cloudpets and "Meine Freundin Cayla" - insecure Bluetooth
Anyone within range was able to upload and receive audio
February 17, 2017 - February 27, 2017

BrickerBot
Bot that permanently incapacitated poorly secured IoT devices
March 20, 2017

enisa

Baseline Security Recommendations for IoT
in the context of Critical Information Infrastructures

Industrial Internet of Things (B2B)

Using IoT in sectors like Industry 4.0, Energy, Health or Agriculture among others.

People:

Cybersecurity Awareness

Cybersecurity by Design:

Cybersecurity in the whole Software Development Process

Cybersecurity along the Supply Chain.

Try not to use B2C devices in B2B applications

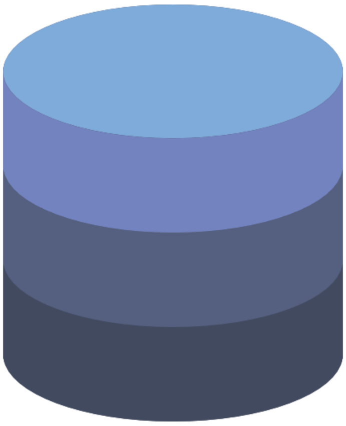
tecnalia Inspiring Business

Disruptive

adjective:
to shake things
up & make your
mark on
the world.

Blockchain is one of today's most disruptive technologies, it can change procedures and business models as we know them today.

Blockchain is a digital transactions and events log



Blockchain explained

Decentralized

Distributed P2P architecture

Blockchain explained

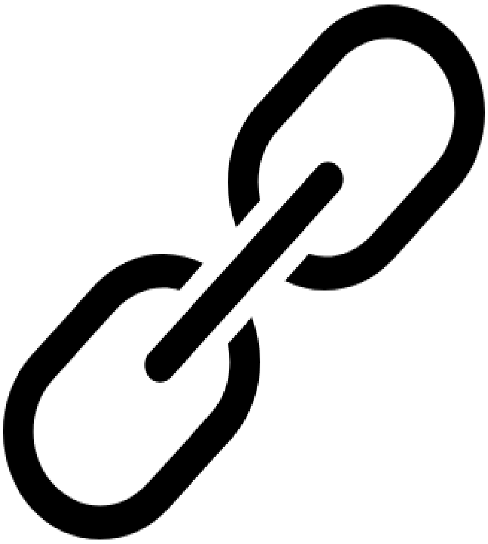
Whose information is approved by the

Consensus

of the majority of the network

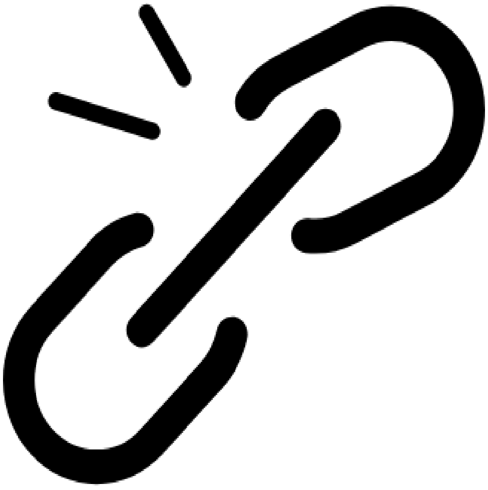
Blockchain explained

Cryptographycally linked to make it Unalterable



Blockchain explained

So the minimun change would break the (logical) chain

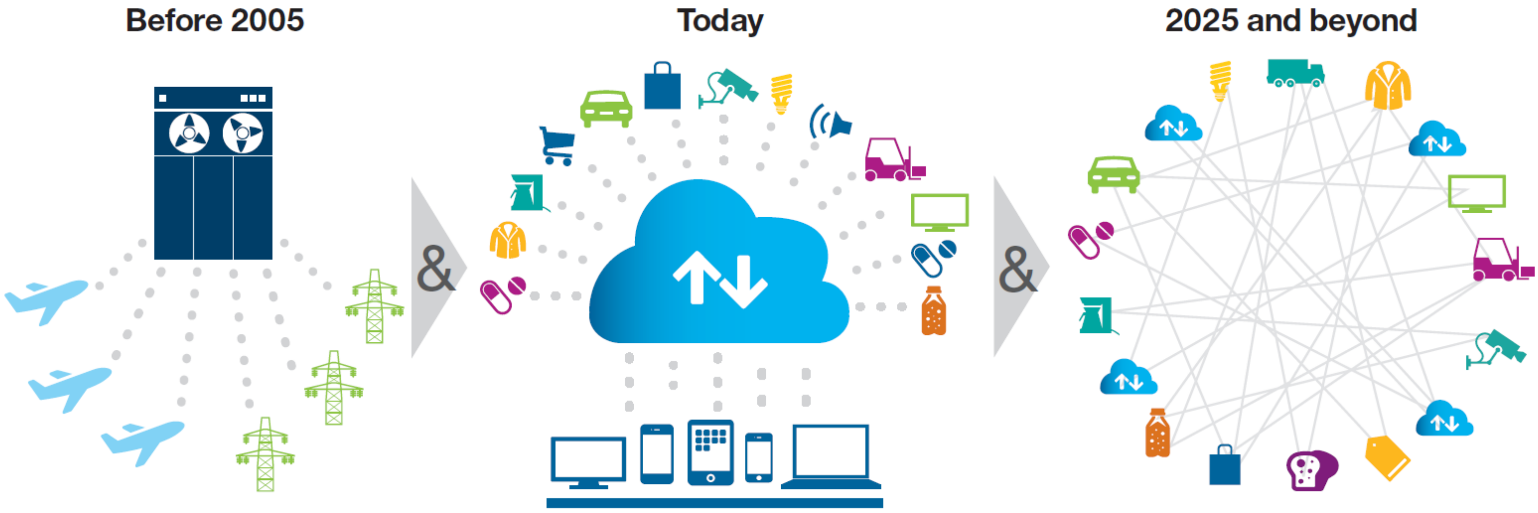


Advantages

- Disintermediation of processes and business models
- Integrated point of view of synchronized, agreeded and unalterable data
- Trustworthiness and non-repudiation of transactions
- Traceability and transparency of processes
- Machine economy: machines as active participants in the economy

Machine Economy

Architecture and escalability for IoT



Machine Economy

Machine Economy

Smart Contracts between machines

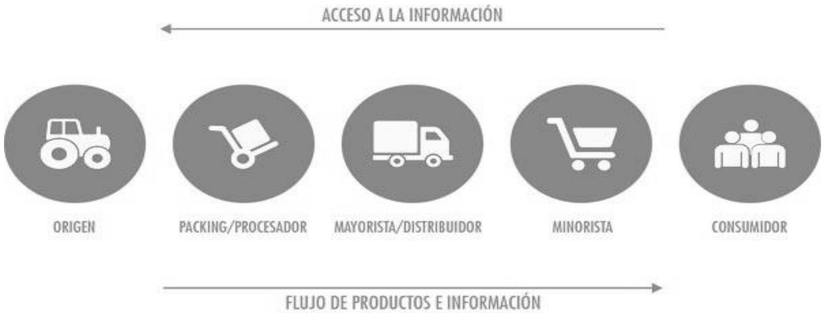
Raw materiales, parts, maintenance, energy, delegation/coordination of production, logistics…

M2M transactions & tokenized value exhange

Machine Economy

Traceability

of the whole supply chain. Incuding also the life cycle of the product.



Machine Economy

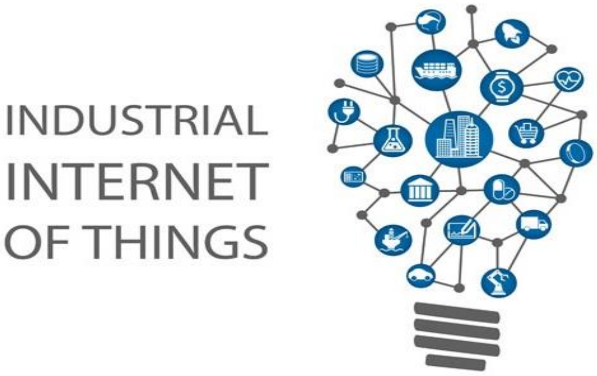
Authentication

Data Integrity

Decentralized registry

Reliable & Unalterable

Incident Forensics

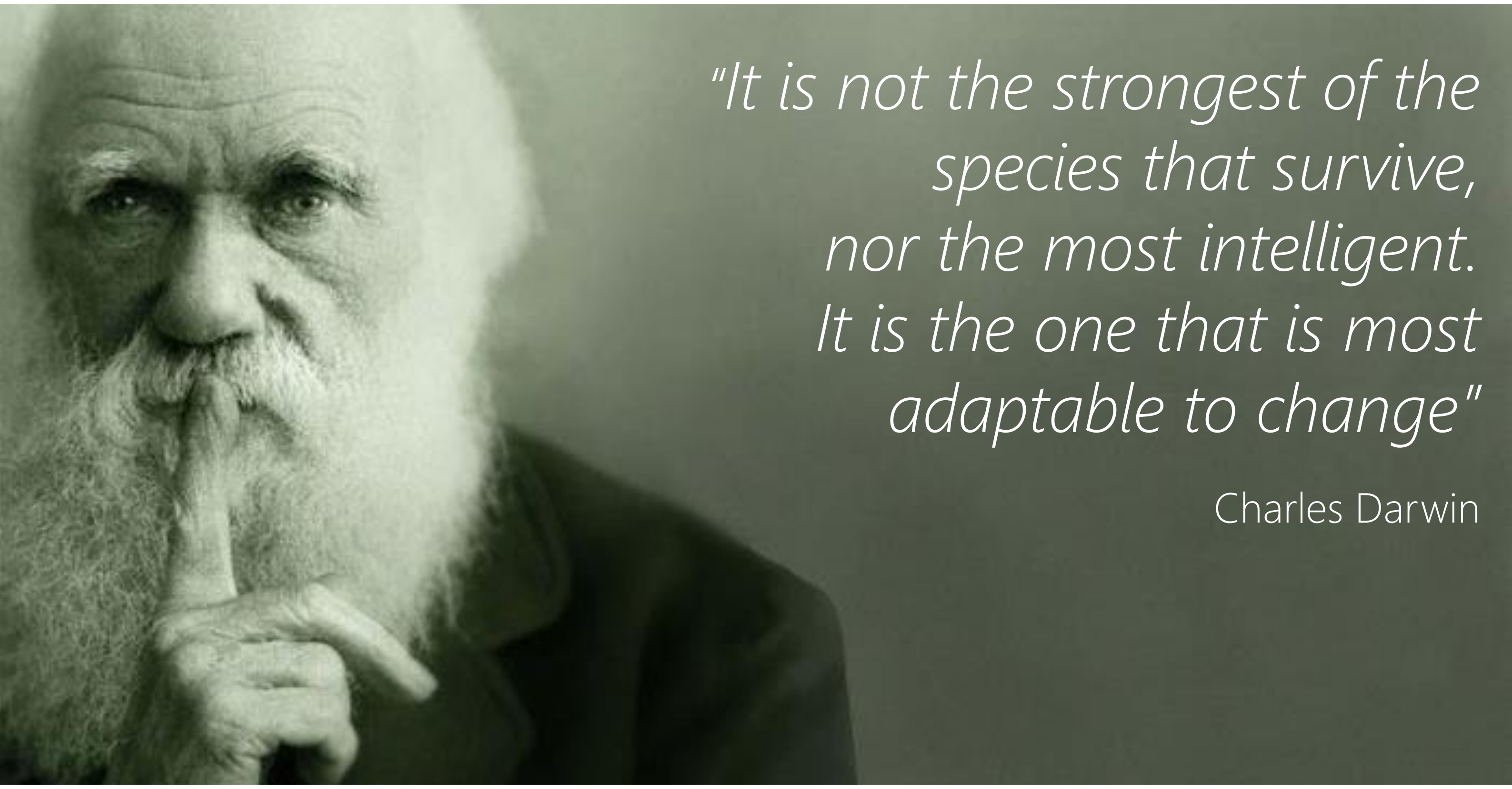


tecnalia Inspiring Business

1st Industrial Blockchain Laboratory in Europe

BLOCKCHAIN Lab
Inspiring Business. Enabling Trust

Blockchain is the next revolution



“It is not the strongest of the species that survive, nor the most intelligent. It is the one that is most adaptable to change”

Charles Darwin

Thanks for your attention!

www.cyberssbytecnalia.com

tecnalia Inspiring Business

Ana Ayerbe
ana.ayerbe@tecnalia.com
@AnaAyerbe

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

Challenges of cybersecurity certification and supply chain management

Roberto Cascella

Senior Policy Manager (ECSO Secretariat)

ECSO – EUNITY Workshop
– 24 January 2019 – Brussels

WG1 – Standardisation, certification, labelling & supply chain management

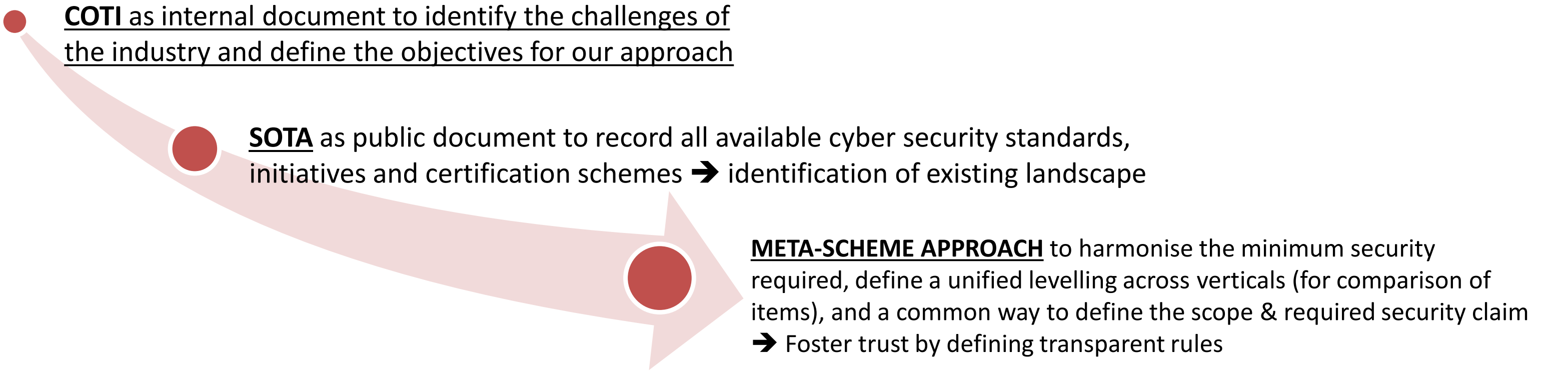
Current WG1 activities largely focus on **an updated version of the ECSO Meta-scheme approach -** how it works in practice.

Organisation of WG1

- ➢ SWG 1.1 “Self-assessment”
- ➢ SWG 1.2 “Third party assessment”
- ➢ SWG 1.3 “Base Layer”

http://www.ecs-org.eu/documents/uploads/updated-sota.pdf

http://www.ecs-org.eu/documents/uploads/european-cyber-security-certification-a-meta-scheme-approach.pdf



COTI as internal document to identify the challenges of the industry and define the objectives for our approach

SOTA as public document to record all available cyber security standards, initiatives and certification schemes ➔ identification of existing landscape

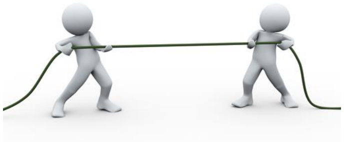
META-SCHEME APPROACH to harmonise the minimum security required, define a unified levelling across verticals (for comparison of items), and a common way to define the scope & required security claim ➔ Foster trust by defining transparent rules

What industry worries about (examples)

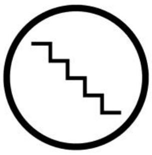
EUROPEAN CYBER SECURITY ORGANISATION

Too slow and too unpredictable

Not flexible enough


Lack of harmonization

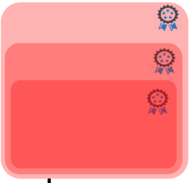
Too much formalisms


lack of agility

Undetected cheaters in the supply chain

Static certificates

Pure checklist evaluations


complex composite certifications

*Challenges of the Industry document of ECSO WG1

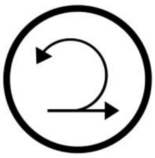
What industry expects (examples)

Fast and predictable

High level of flexibility

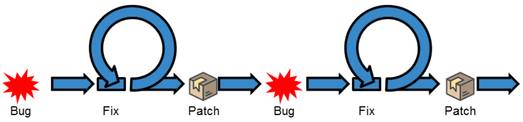
Full harmonization

Pragmatism



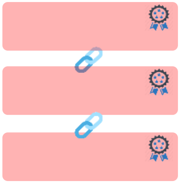
agility

Detecting cheaters in the supply chain



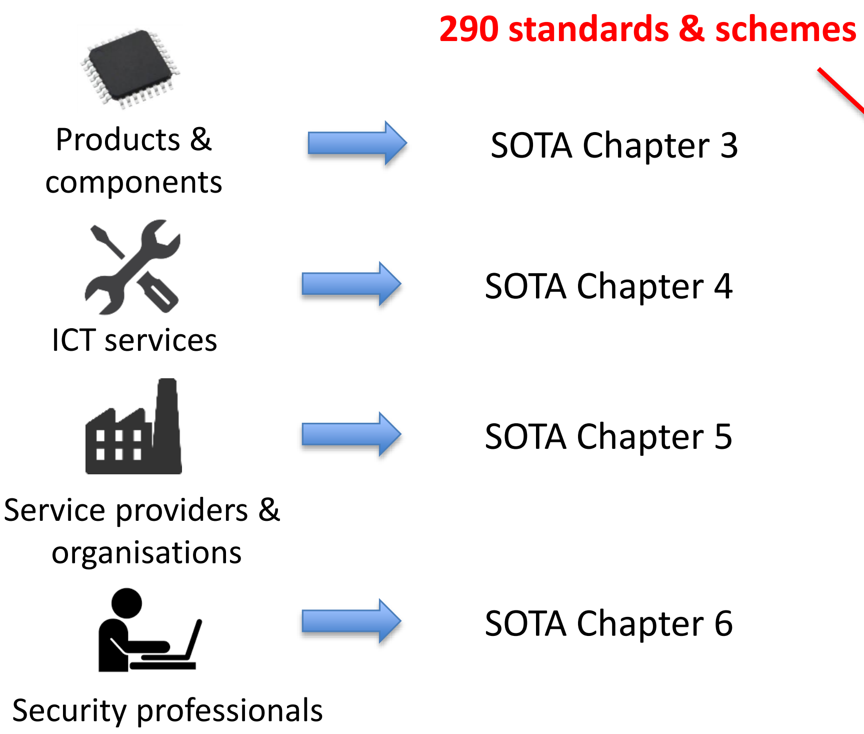
Patching and updates

Ethical hacking



Lean modular composite certifications

First of all: collection of what exists!



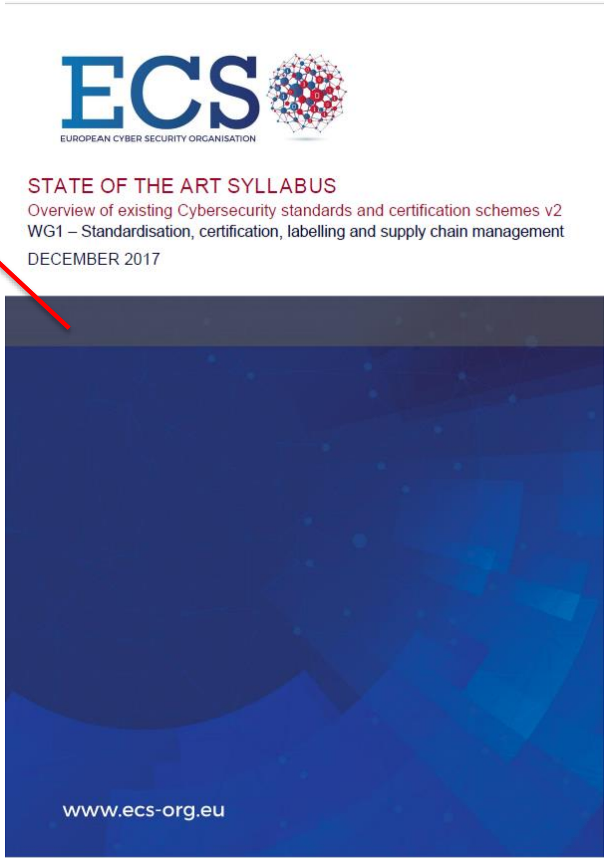
290 standards & schemes

Products & components → SOTA Chapter 3

ICT services → SOTA Chapter 4

Service providers & organisations → SOTA Chapter 5

Security professionals → SOTA Chapter 6



ECS

EUROPEAN CYBER SECURITY ORGANISATION

STATE OF THE ART SYLLABUS

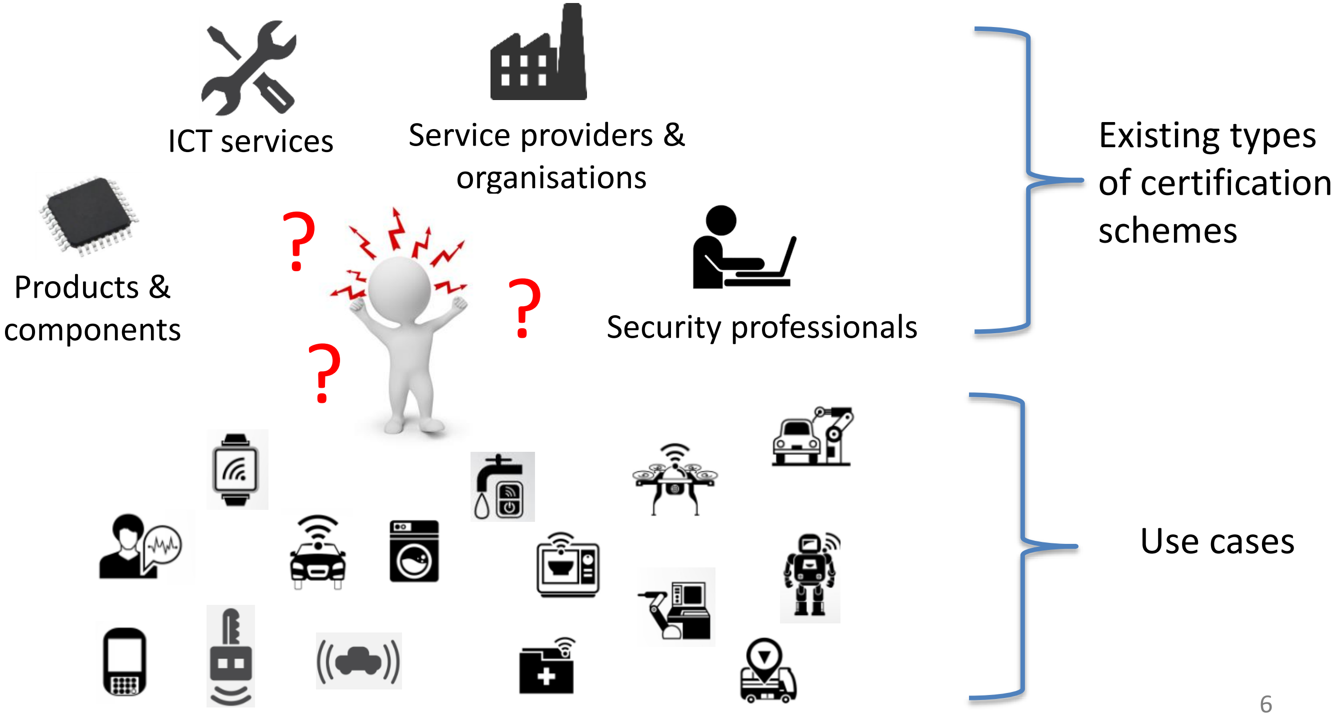
Overview of existing Cybersecurity standards and certification schemes v2

WG1 – Standardisation, certification, labelling and supply chain management

DECEMBER 2017

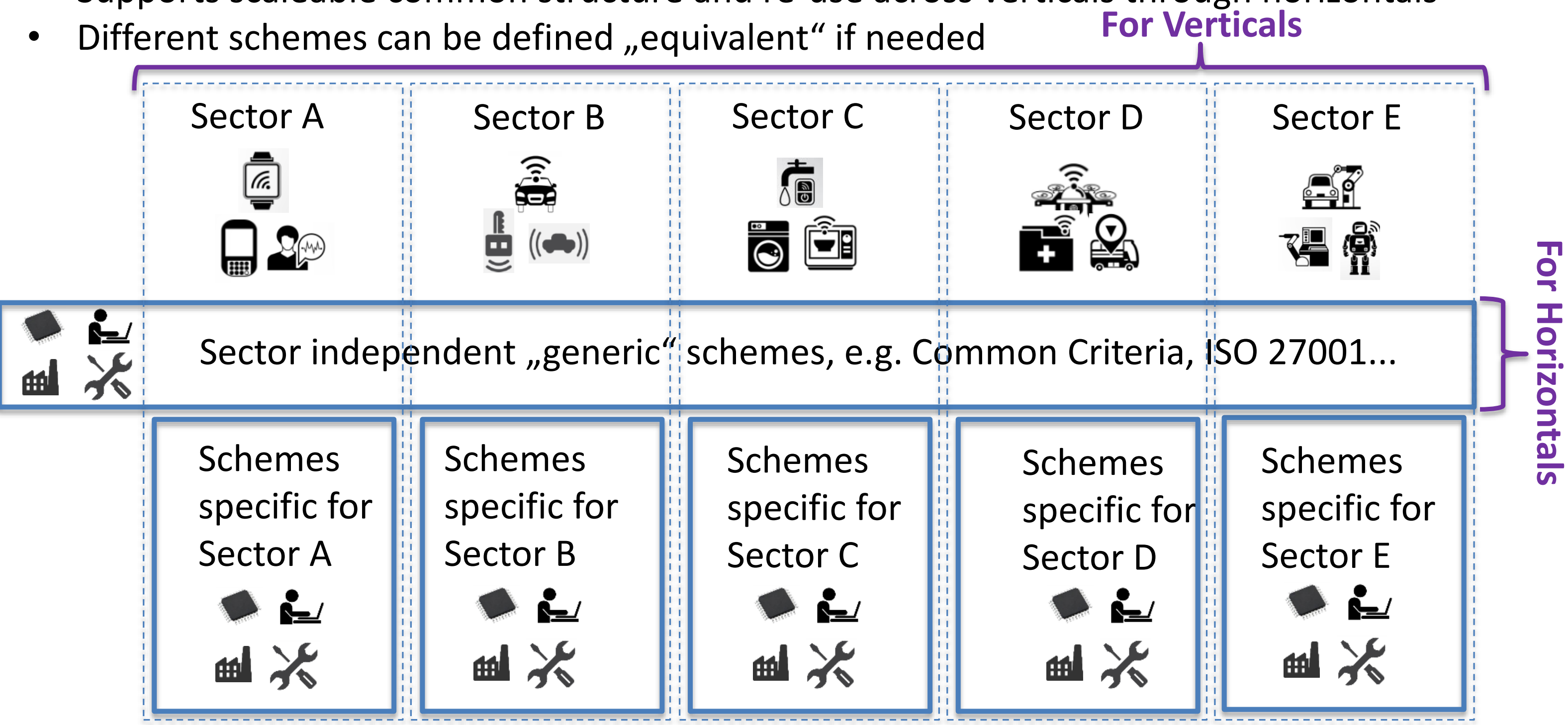
www.ecs-org.eu

What to do?
There is not a single scheme fitting all needs!


ICT services
Service providers & organisations
Products & components
?
?
?
Security professionals
Existing types of certification schemes
Use cases

Meta-Scheme Idea

- Allows composition across **different** schemes via a meta-language
- Supports scaleable common structure and re-use across verticals through horizontals
- Different schemes can be defined „equivalent“ if needed



For Verticals

Sector A

Sector B

Sector C

Sector D

Sector E

Sector independent „generic“ schemes, e.g. Common Criteria, ISO 27001...

For Horizontals

Schemes specific for Sector A

Schemes specific for Sector B

Schemes specific for Sector C

Schemes specific for Sector D

Schemes specific for Sector E

Levels of assurance and assessment types

	Symbol (Example)	Assessment Type	Assurance Level	Scope of Security Functionality Level = min	Scope of Security Functionality > min	Schemes allowed
Advanced	A	Accredited Third Party	High	Sector/Use Case dependent	Sector / Use Case dependent	<mapping from SOTA>
	B	Accredited Third Party	Moderate			<mapping from SOTA>
	C	Accredited Third Party	Enhanced Basic			<mapping from SOTA>
Base	D	Accredited Third Party	Basic	Sector/Use Case agnostic		<mapping from SOTA>
	E	Self	Entry			

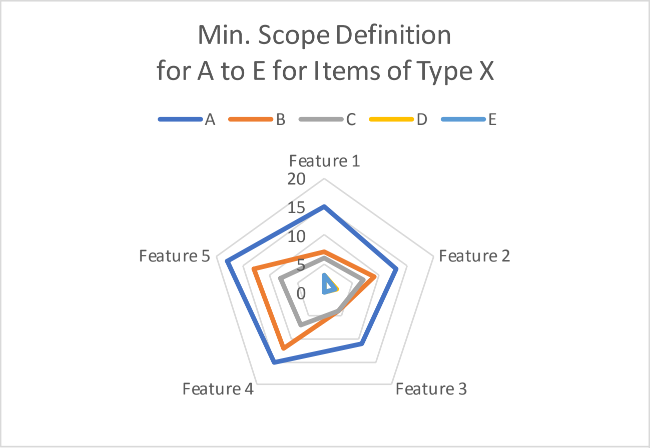
Disclaimer: should be seen as a default case/template for sectors. Depending on the sector this might be refined or overridden in exceptional cases where e.g. assessment by a company-internal independent organisation is done for the advanced levels. Notice, however that this can never replace the level of independence and trust which an external party can give. Moreover, for such cases a very strict shadowing process by an accredited third party is required, which tightly audits the internal organisation on a regular basis. This also has an impact on liability.

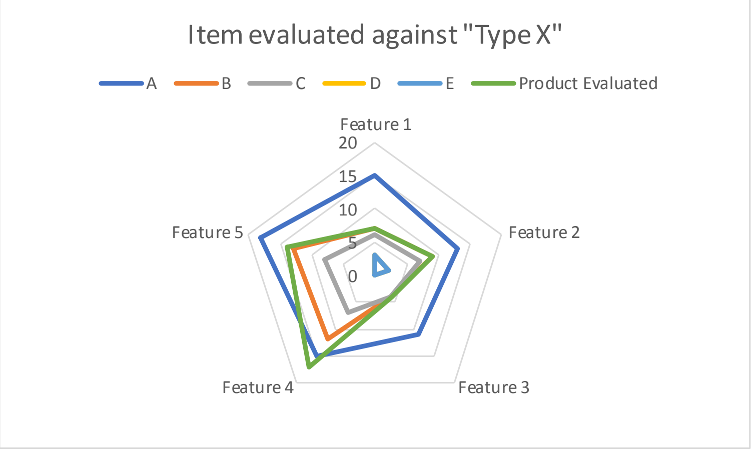
A sector can decide to not define certain levels → free to define if and which advanced levels to provide, whereas the basic levels D and E must be supported in any case

Example for a Radar-Diagram to visualize Scope of Security Functionality

Five features defined with their scope of security functionality assessed

The scope of security functionality of the Item evaluated cannot go below the respective claimed line (level A, B, C, D, E) in the radar diagram





This example shall give an understanding that visualization could help a lot to get a feeling on what an item covers.

The Role of Expert Groups

- Experts from Industry, labs, academia, national security agencies, ...
- Definition of **Protection Profiles** (threats/risks → security requirements)
- **Tailoring of evaluation methodologies** (what is „really“ important to look at)
- Maintaining **state-of-the art attack** methods

- Working on **checklists & compliance testing** ...

- ...but also incorporating **Ethical hacking especially for high security!**

Our contribution to the EU Cyber Security Framework

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Some conclusions that can be drawn from our work on the EU Cybersecurity Act

- **Experts from industry** part of decision process **for scheme selection and priority –** A roadmap of intended priorities is needed for the market → (The Union Rolling plan will be defined by the SCCG)
- **Minimum common baseline security** needs to be defined **across sectors.** → Threat analysis & risk assessment as source for security requirements
- The **scope of certification** should address the entire supply chain: what and how depends on the intended use
  - The level of assurance attained should consider the potential risk & related impact of potential attacks linked with the product/service usage
- **Ethical hacking shall be legally allowed and enforced for high security**; checklists are insufficient!
- Need for a common definition of the proposed assurance levels, i.e., **assessment methodologies (evaluation) associated**
- **Centrally steered harmonization** across CABs, NABs and National Certification Supervisory Authorities (NCSA) is crucial!

The **ECSO meta-scheme approach** can act as a methodological tool (e.g. for ENISA) to structure the landscape and "glue" existing schemes together and specify additional steps

Current focus

Support to the EU Cybersecurity Certification Framework and Trusted Supply Chain in Europe

- **SOTA, COTI reports update** →Better common understanding of situation and needs to prepare future priorities
- **ECSO Meta-scheme in practice** → Tool for qualitative market analysis to define focused initiatives and promote EU solutions as methodology for the European Certification Framework (identification of the characteristics under which certification schemes can be viewed and selected)
    - New version with general aspects of certification scheme composition, type of evaluations, continuous assessment and a mapping with the Cybersecurity Act
    - Document on Assessment, from self to third-party, looking into the available types of assessment and identifying some of the criteria to decide on the fit-for-purpose type of assessment
- **Analysis of security requirements, gaps in standardization and priorities for future EU certification schemes** → Identify common priorities for definition of certification schemes

Support to EU standardisation on cybersecurity

- **MoU with CEN/CENELEC (and ETSI to be signed).** Definition of priorities for developing EU standards. → Simplify tasks for ESOs to initiate standardisation, in particular linked to certification

BECOME MEMBER!
CONTACT US

📍 European Cyber Security Organisation 10,
Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0)
27770252

E-mail:
Dr. Roberto G. Cascella
Senior Policy Manager
roberto.cascella@ecs-org.eu

Follow us
Twitter: @ecso_eu

3.3.3 Training and awareness challenges

The session on training and awareness challenges included two presentations. The first was on “Update on Training & Cyber Range activities in Europe” by Nina Olesen, from ECSO Secretariat and the second on “Presentation on gap of cyber experts and skills in Japan Cybersecurity industries: Introducing Cyber Risk Intelligence Center, Cross Sectors Forum” by Miho Naganuma, from NEC Corporation. The presentations are listed below:

ECSO

EUROPEAN CYBER SECURITY ORGANISATION

Education, training, awareness, and cyber ranges

Roberto Cascella

Senior Policy Manager (ECSO Secretariat)

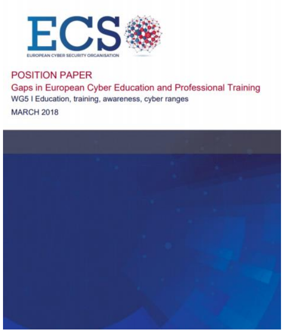
ECSO – EUNITY Workshop

24 January 2019 – Brussels

WG5 education, training, awareness

Education & Professional Training; Jobs & Skills

- Position Paper on **Gaps in Education & Professional Training**
- Participation in Digital Opportunity pilot scheme (EC) – focus on skills, traineeships for young people, etc.

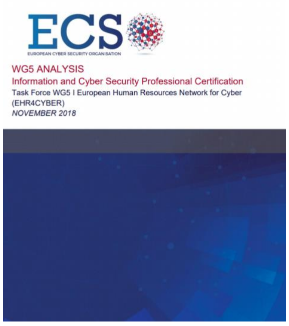


ECS
EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER
Gaps in European Cyber Education and Professional Training
WG5 I Education, training, awareness, cyber ranges
MARCH 2018

EHR4CYBER Network (Increase visibility and concrete actions for European human resources in cyber)

- Analysis Paper with best practices and recommendations / mapping for a European framework for education and competences (matching profiles and skill-sets) → **Cyber Security Professional certification**
- Envisaging the creation of an online jobs marketplace



ECS
EUROPEAN CYBER SECURITY ORGANISATION

WG5 ANALYSIS
Information and Cyber Security Professional Certification
Task Force WG5 I European Human Resources Network for Cyber
(EHR4CYBER)
NOVEMBER 2018

Awareness for decision makers: Increased dialogue with EU policy makers and CISO of operators

Awareness for citizens: Cooperation with Europol (No More Ransom campaign) and support to local/national initiatives and campaigns for cyber security education before University level

Creation of ECSO Women4Cyber initiative: gender issue on education & training to increase number of cyber experts

WOMEN
4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

WG5 cyber ranges

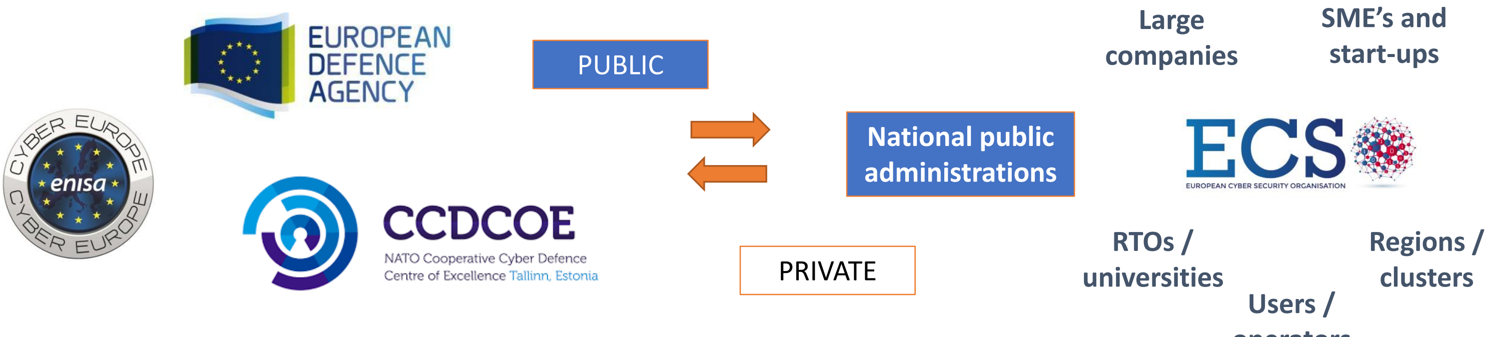
Cyber Ranges

ECSO internal survey conducted to assess cyber range capabilities and motivations → **cyber range workshop series initiated in collaboration with European Defence Agency (EDA)**

Workshop #1: **16-17 October 2018 in Brussels.** To align with EDA on cyber range approaches and agree on a baseline for continued collaboration, focusing on opportunities and motivations for federated approach. Established links between the private sector (industry and research) and EDA (Member States), with around 50 attendees (33 from ECSO members).

Workshop #2: **Spring 2019** in Tallinn (date tbd). To define federated cyber range approach, looking at an industry-wide framework or guidelines, governance, etc.

Workshop #3: **Autumn 2019** (location and date tbd). To test the federated cyber range approach with one or two use cases and conducting a small cyber drill.


EUROPEAN DEFENCE AGENCY
CYBER EUROPE
enisa
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
ECSO
EUROPEAN CYBER SECURITY ORGANISATION

PUBLIC

National public administrations

PRIVATE

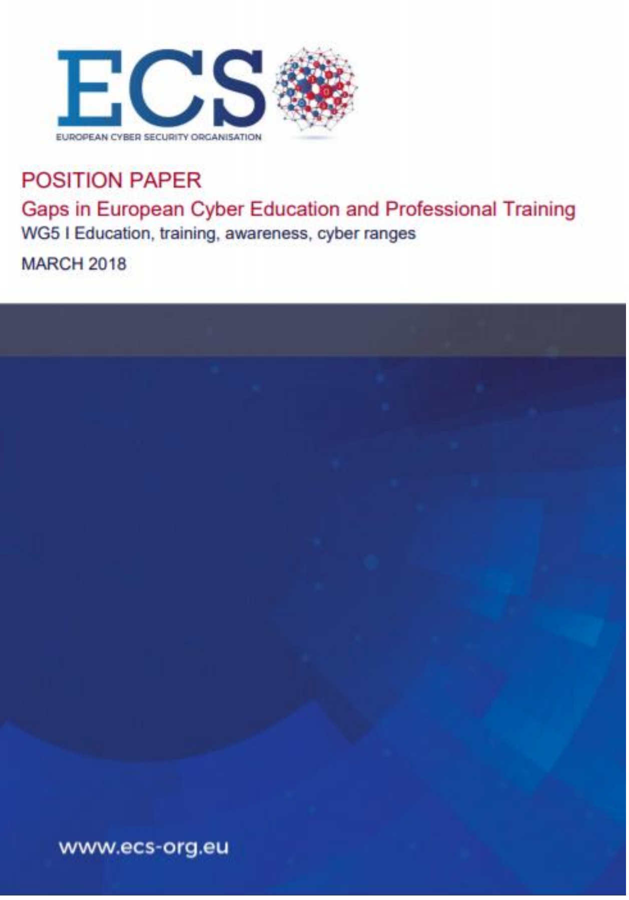
Large companies

SME's and start-ups

RTOs / universities

Regions / clusters

Users / operators



EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Gaps in European Cyber Education and Professional Training

WG5 I Education, training, awareness, cyber ranges

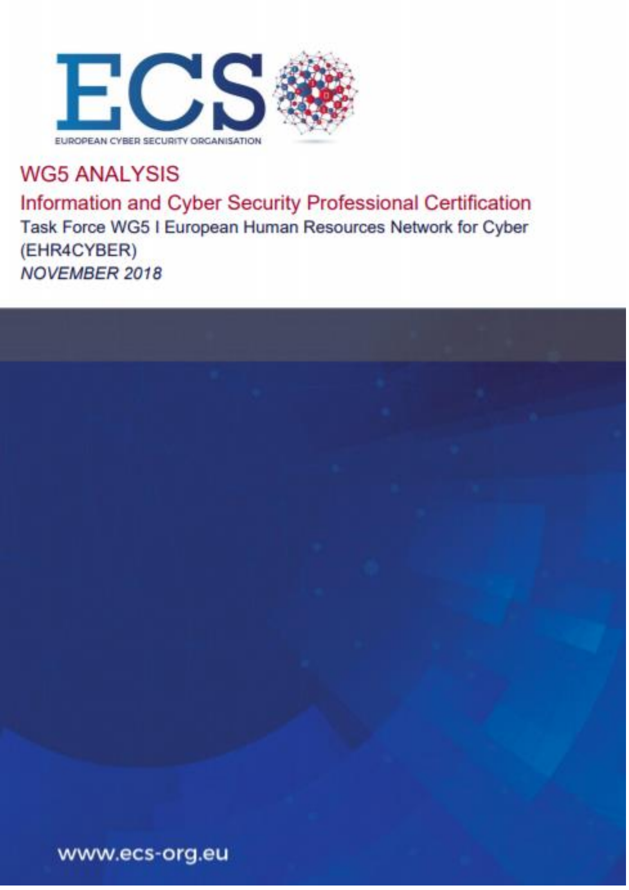
MARCH 2018

www.ecs-org.eu

Main conclusions

- Commercialisation of higher education, including the rising cost of education and growing number of students will soon lose students to affordable and widely accessible MOOCs → **online courses scale better and can sometimes offer the same level of knowledge at a cheaper price**
- We are **not producing enough skilled experts** that the industry is desperately looking for. To satisfy the growing demand for skilled cyber security professionals, we need to:
  - Expand educational opportunities at all levels
  - Increase the number of qualified educators
  - Create synergies between educational paths and training possibilities at the workplace
  - Reach the skilled unemployed and displaced workers (workers who are not happy with their current profession)
  - Create the fundamentals for lifelong learning in cyber security
- We also need to ensure **gender diversity and inclusiveness** of cyber security education and training, to inform and encourage girls and women to engage into cyber security careers.

➢ *To achieve this, a working cooperation is needed between academia and industry which utilises and combines their available resources to ultimately strengthen the cyber domain together*



ECS

EUROPEAN CYBER SECURITY ORGANISATION

WG5 ANALYSIS

Information and Cyber Security Professional Certification

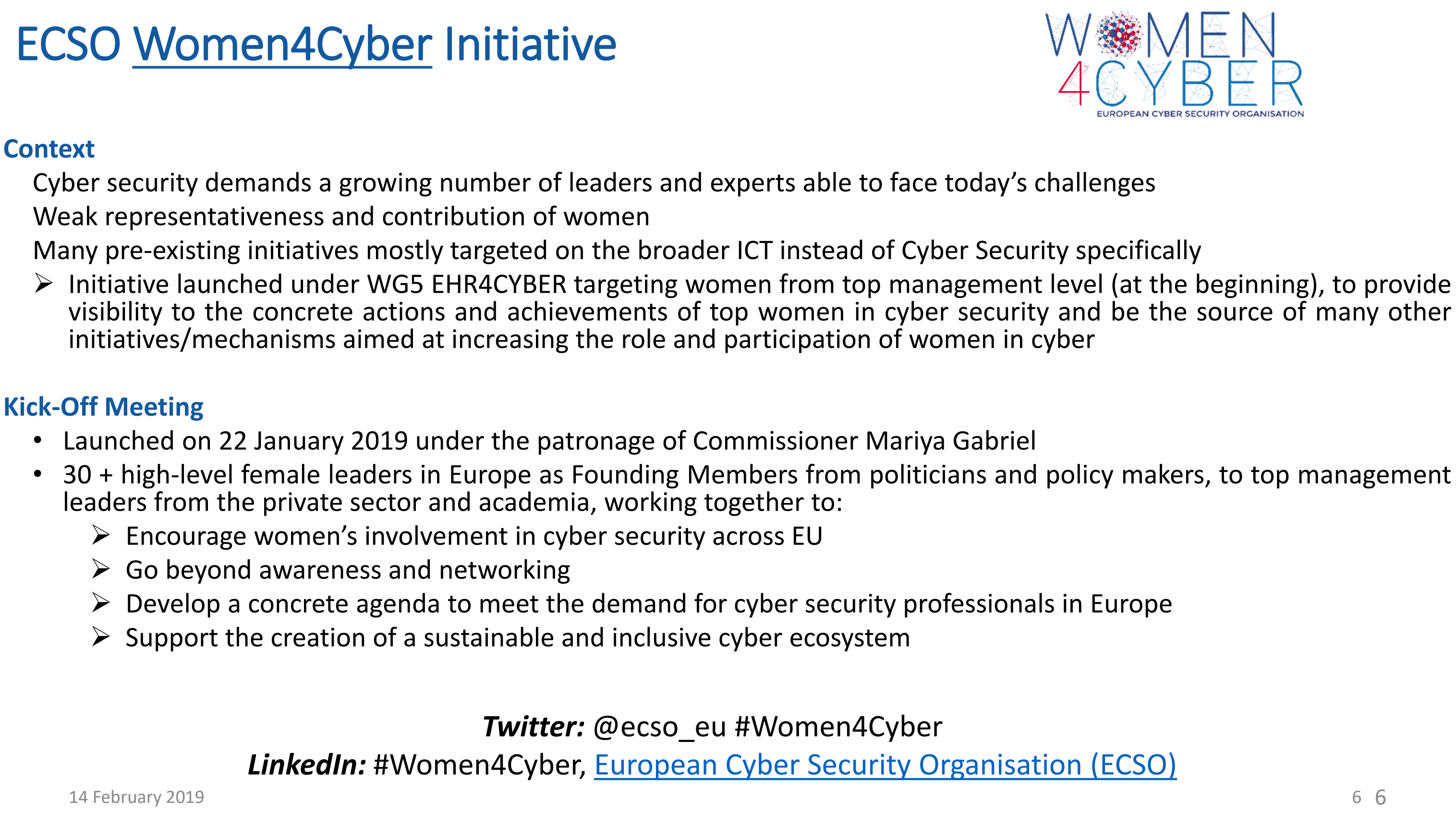
Task Force WG5 I European Human Resources Network for Cyber (EHR4CYBER)

NOVEMBER 2018

www.ecs-org.eu

Recommendations

- Comprehensive **market study** into the age structure and career history of information and cyber security professionals in the European market, training paths and industry demand should be conducted.
- ECSO should support ENISA and the European standardisation bodies in the development of one **European-wide certification scheme** and baseline requirements for certification schemes to be met under the purview of public procurement, cyber security and critical infrastructure regulation.
- ECSO should coordinate the development of one **European-wide education framework for cyber security** to support young professionals (via formal education), existing professionals, and professionals joining the cyber security field at a later stage (i.e. after completion of formal education).
- Representatives from existing initiatives at EU and national level should be involved to make this **a joint effort**.
- The education framework needs to be **internationally recognised** and accepted. Cooperation with other parties like NIST (US NICE framework) is recommended.



ECSO Women4Cyber Initiative

WOMEN 4CYBER EUROPEAN CYBER SECURITY ORGANISATION

Context

Cyber security demands a growing number of leaders and experts able to face today’s challenges

Weak representativeness and contribution of women

Many pre-existing initiatives mostly targeted on the broader ICT instead of Cyber Security specifically

- ➢ Initiative launched under WG5 EHR4CYBER targeting women from top management level (at the beginning), to provide visibility to the concrete actions and achievements of top women in cyber security and be the source of many other initiatives/mechanisms aimed at increasing the role and participation of women in cyber

Kick-Off Meeting

- Launched on 22 January 2019 under the patronage of Commissioner Mariya Gabriel
- 30 + high-level female leaders in Europe as Founding Members from politicians and policy makers, to top management leaders from the private sector and academia, working together to:
    - ➢ Encourage women’s involvement in cyber security across EU
    - ➢ Go beyond awareness and networking
    - ➢ Develop a concrete agenda to meet the demand for cyber security professionals in Europe
    - ➢ Support the creation of a sustainable and inclusive cyber ecosystem

Twitter: @ecso_eu #Women4Cyber

LinkedIn: #Women4Cyber, European Cyber Security Organisation (ECSO)

European Commission measures to boost key competences and digital skills, as well as the European dimension of education (January 2018)

1. A Council Recommendation on Key Competences for Lifelong Learning**:** Proposal aiming to improve the development of key competences of people of all ages throughout their lives and to provide guidance to Member States on how to achieve this objective. Particular focus is placed on promoting entrepreneurial drive and innovation-oriented mindsets in order to unlock personal potential, creativity and self-initiative. The EC is also recommending steps to foster competences in science, technology, engineering and mathematics (STEM) and motivate more young people to embark on a career in these fields.
2. A **Digital Education Action Plan** that outlines how the EU can help people, educational institutions and education systems better adapt to life and work in an age of rapid digital change by:
   - Making better use of digital technology for teaching and learning
   - Developing the digital competences and skills needed for living and working in an age of digital transformation
   - Improving education through better data analysis and foresight
   - Initiatives include supporting schools with high-speed broadband connections, scaling up a new self-assessment tool for schools on the use of technology for teaching and learning (SELFIE) and a public awareness campaign on online safety, media literacy and cyber hygiene.
3. A **Council Recommendation on common values, inclusive education and the European dimension of teaching:** This initiative proposes ways in which education can help young people understand the importance of and adhere to common values set out in Article 2 of the Treaty of the European Union. It aims at strengthening social cohesion and contributing to fight the rise of populism, xenophobia, divisive nationalism and the spreading of fake news.

European Commission proposal for Digital Europe Programme (June 2018)

1. Supercomputers
2. Artificial intelligence (AI)
3. **Cybersecurity and trust:** €2 billion will be invested into safeguarding the EU's digital economy, society and democracies through boosting cyber defence and the EU's cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure as well as **supporting the development of the necessary skills and knowledge**. The proposal builds on the wide range of cybersecurity measures presented in September 2017, and on the first EU-wide legislation on cybersecurity that came into force in May 2018.
4. **Digital skills: €700 million will ensure that the current and future workforce will have the opportunity to easily acquire advanced digital skills through long-and short-term training courses and on-the-job traineeships**, regardless of their Member State of residence. In the Digital Europe programme, the Digital Innovation Hubs will carry out targeted programmes to help small and medium-sized enterprises and public administrations to equip their personnel with the needed advanced skills to be able access the new opportunities offered by supercomputing, artificial intelligence and cybersecurity.
5. Ensuring a wide use of digital technologies across the economy and society

BECOME MEMBER!
CONTACT US

European Cyber Security Organisation 10, Rue
Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770251

E-mail:
Nina Olesen
Senior Policy Manager
nina.olesen@ecs-org.eu

Follow us
Twitter: @ecso_eu

Cybersecurity in industries
-- Introducing CRIC CSF --

24th January, 2019

Cyber Risk Intelligence Center,
Cross Sectors Forum

Miho Naganuma, NEC Corporation

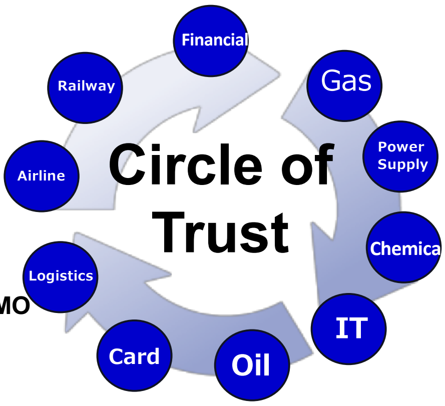
Agenda

1. CRIC Cross Sectors Forum
2. Shortage of Cybersecurity Talents
3. Activities and Results
4. Future work plan

1. CRIC Cross Sectors Forum

- URL: http://cyber-risk.or.jp/
- Launched in June 2015
- Trigger to Launched : Advisory Board of Cybersecurity in ”Keidanren”
- Our proposals adapted into "Cyber security strategy" of the Japanese government in July 2018
- More than 40 companies(44 Members as of Oct 2018) mainly from 14 Critical Infrastructure Industries (e.g. Finance, Airline, Railway, Power, Energy etc)

JX IT Solutions (Oil)
Sumitomo Chemical
Toyota
KDDI
All Nippon Airways
DNP (Printing)
TAKENAKA (Construction)
Nippon Express
Japan Post
Mitsubishi Electronics
NIPPON STEEL & SUMITOMO METAL
Yamato Holding (Transportation)



SONY
Panasonic
Nippon Life Insurance Company
Mizuho Financial Group
Mitsui E&S Holdings
NTT
NEC
Hitachi
Fujitsu
Toshiba
… and more

2. Shortage of Cybersecurity Talents

Situation in Japan

- Japan will be short of 193,000 cybersecurity professionals in 2020.
- Japanese Business Federation declared it is urgently crucial to increase such professionals.

  (http://www.keidanren.or.jp/en/policy/2015/017.html)

Key questions to ask

- What kind of Cybersecurity Talents do Japanese Critical Infrastructure companies need?
- HR Supply and Demand to match?
- Japanese business culture?

Uniqueness of Japanese Business

1. Life-time employment:

- Stay in a single company for entire lifetime
- Rotate every 2-3 years

● Implications

- Difficult for employees to accumulate cybersecurity expertise
- Mission Definition of teams and Documentation for new comers is crucial

2. More IT/Cybersecurity Outsourcing:

- Only 24.8% of IT professionals work in-house in Japan
- 71.5% in the U.S

● Implications

- End users rely on vendors for technical work such as Forensics, Malware Analysis

3. Multi-hat CISOs:

- Tend to lack IT/cybersecurity background

● Implications

- Crucial to assign experienced cybersecurity professionals to assist CISO team

3. Activities and Results

Activities

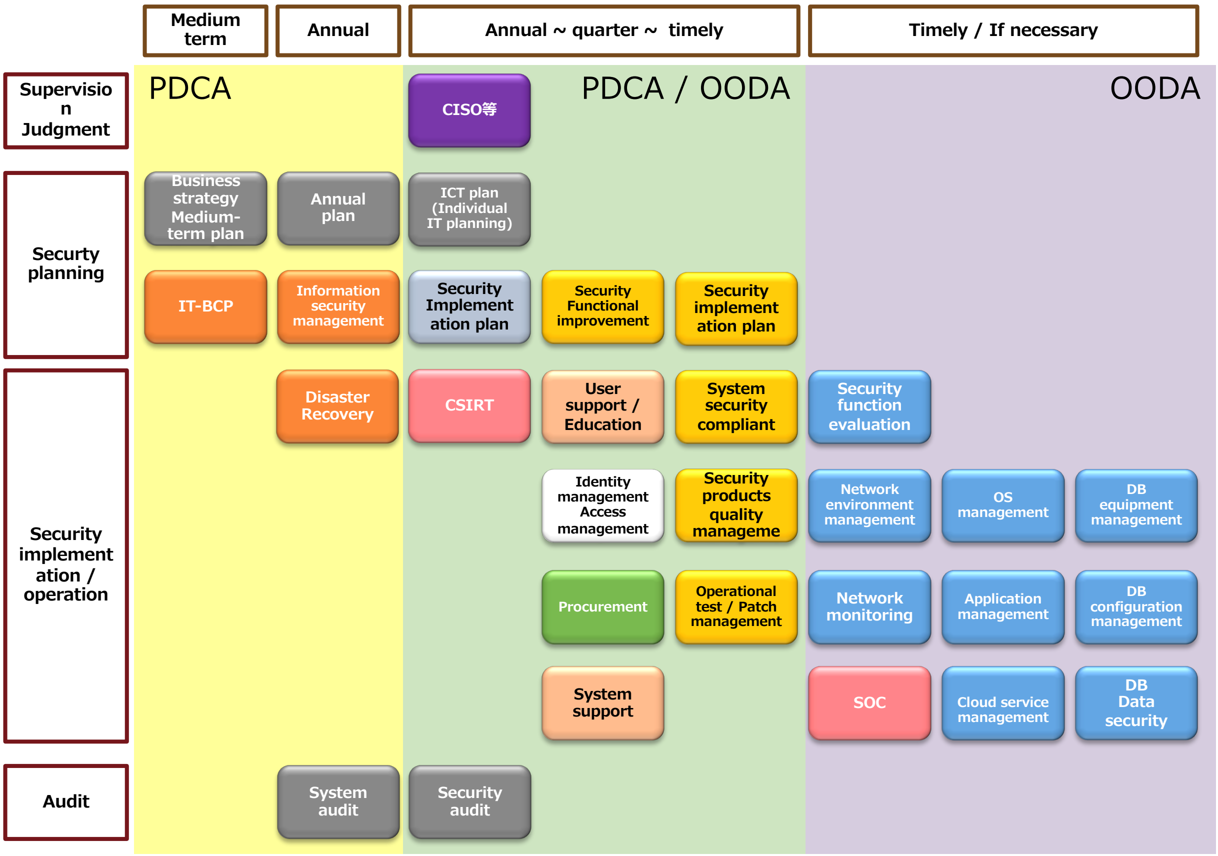
- Monthly Plenary Meeting
- 4 Monthly Working Group
  - Workforce Definition
  - Workforce Development
  - Information Sharing
  - Collaboration with Academia
- Annual Conference for C-Suites
- Participation to Cybersecurity Discussion at Government

3rd C-Suites Annual Conference

Outputs

- Activity Report
- Tools: Talent Definition, Outsourcing Guideline, CISO Calendar

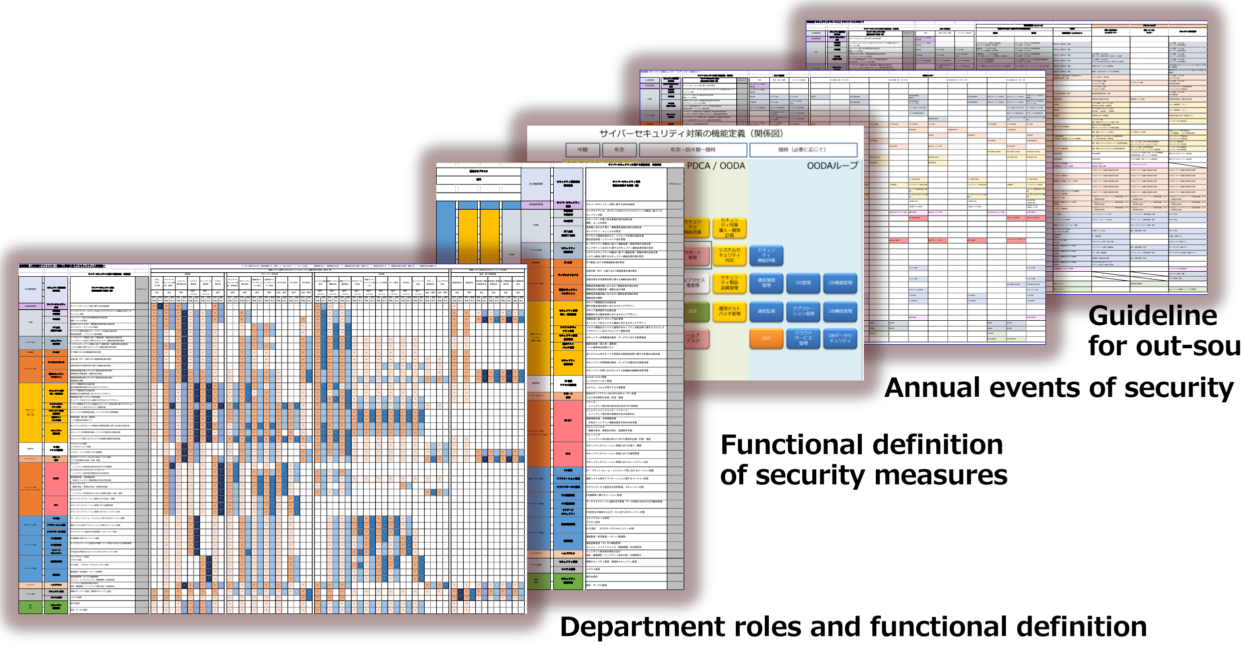
Function definition of cyber security measures



	Medium term	Annual	Annual ～ quarter ～ timely			Timely / If necessary		
Supervision Judgment			CISO等					
Securty planning	Business strategy Medium-term plan	Annual plan	ICT plan (Individual IT planning)					
	IT-BCP	Information security management	Security Implement ation plan	Security Functional improvement	Security implement ation plan			
Security implement ation / 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					

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

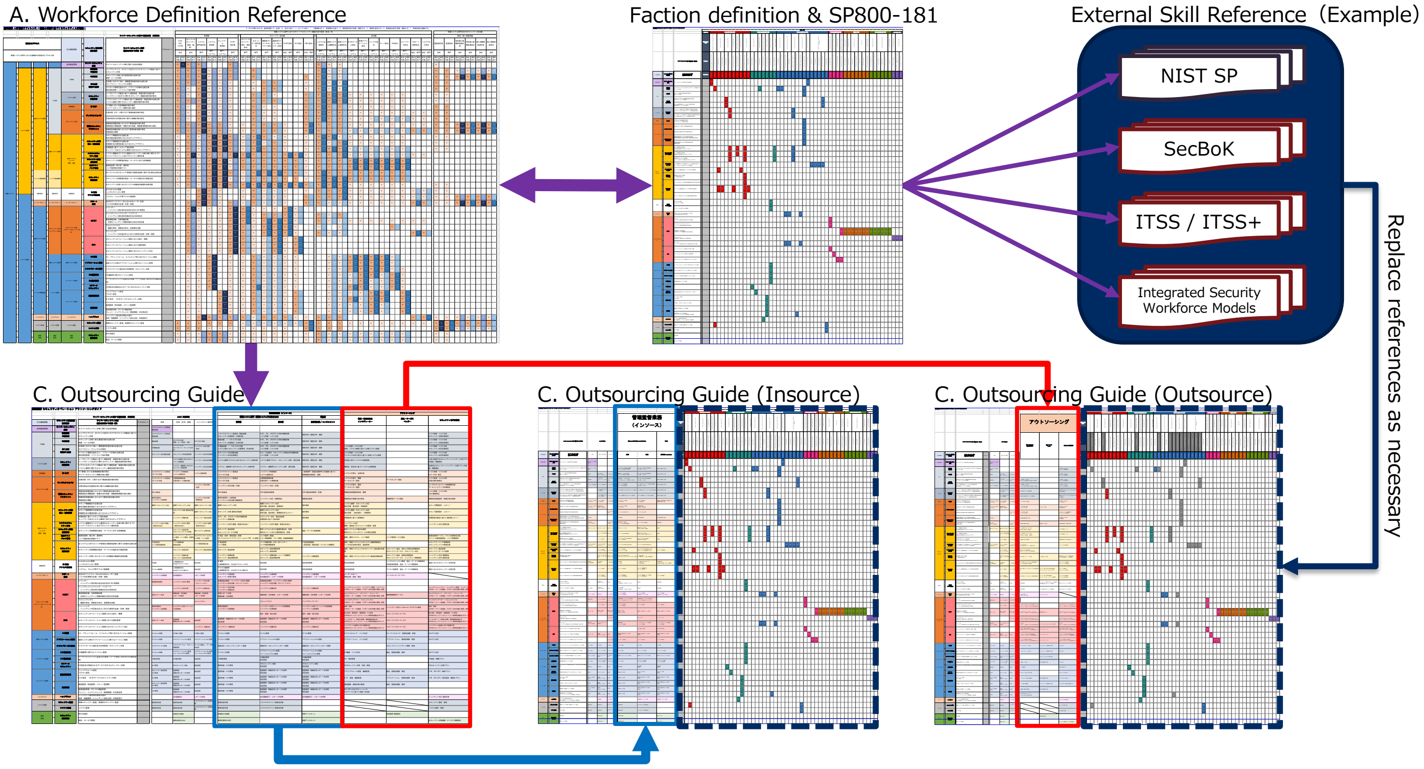
Functional definition
of security measures

Department roles and functional definition

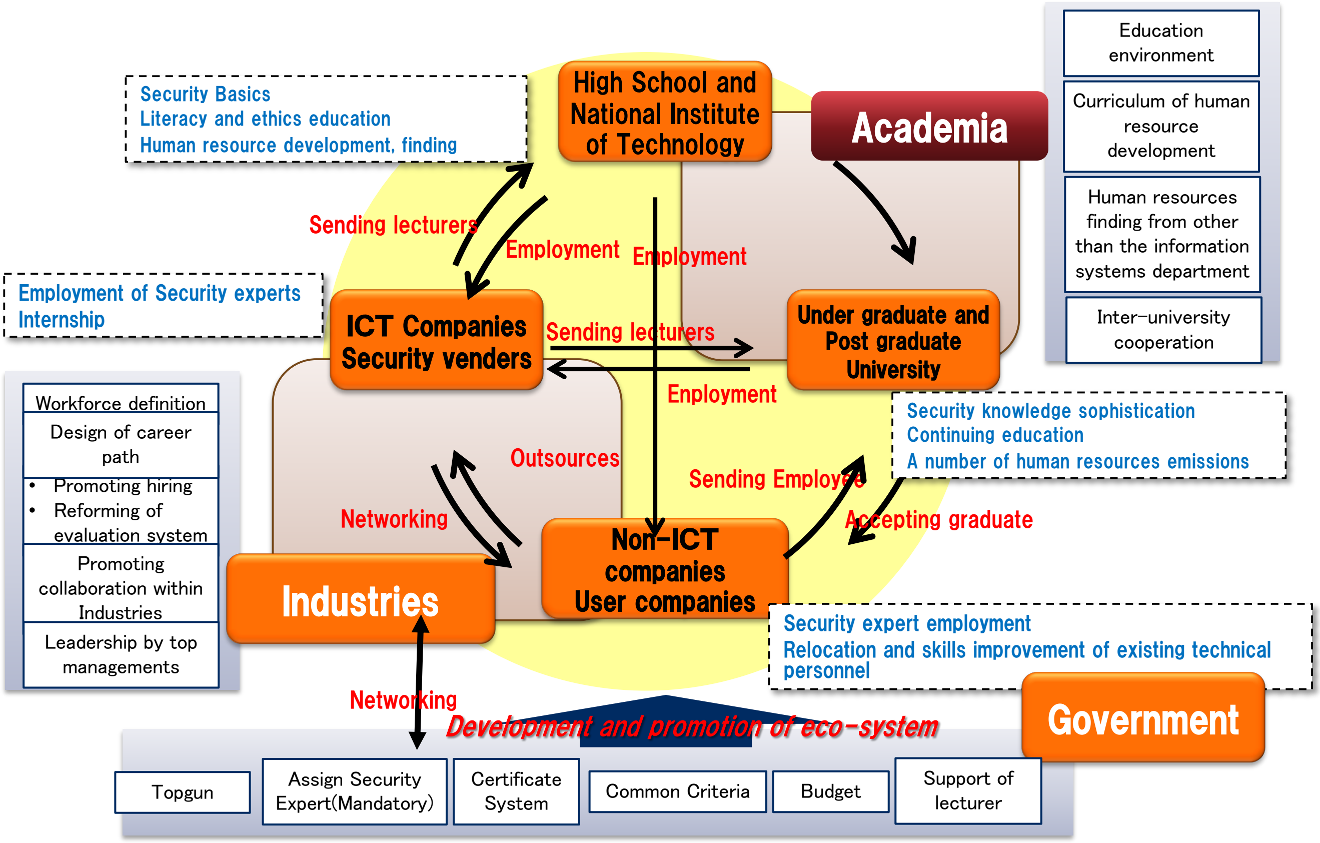
Workforce Definition Reference

Relationship between "Workforce definition reference" through external service personnel model through SP 800-181

The way of external skill reference cooperation based on workforce definition reference


A. Workforce Definition Reference
Faction definition & SP800-181
External Skill Reference（Example）
NIST SP
SecBoK
ITSS / ITSS+
Integrated Security Workforce Models
Replace references as necessary
C. Outsourcing Guide
C. Outsourcing Guide (Insource)
C. Outsourcing Guide (Outsource)

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 University

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

Government

Networking

Development and promotion of eco-system

Topgun

Assign Security Expert(Mandatory)

Certificate System

Common Criteria

Budget

Support of lecturer

4. Future work plan : The third phase (January 2019)

1. **Security Summit (tentative name)**
   - ●To further improve industrial awareness, it will be held just one year before the Tokyo Olympic Games and the Paralympic Games.
2. **Corporate Cybersecurity Case-collection/research TF**
   - ●Collect more concrete examples and conduct a practical case study on how security in enterprise management should be.
3. **WG activity** (continuation of the previous term)
   - ●Information linkage · Knowledge sharing WG
   - ●Cyber Security Corporate Strategy WG

Thank you

Info@cyber-risk.or.jp

3.3.4 Information sharing challenges

The next session was on information sharing challenges and included two presentations on the “Multiscale approach to information sharing activities: The use case of the Basque Cyber Security Centre” by Javier Dieguez, from the Basque Cybersecurity Centre:

BASQUE
CYBERSECURITY
CENTRE

Regional Approach to Build Cybersecurity Capacity

GRUPO
spri
TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO

EKONOMIAREN GARAPEN
ETA AZPIEGITURA SAILA

DEPARTAMENTO DE DESARROLLO
ECONÓMICO E INFRAESTRUCTURAS

Index

BASQUE CYBERSECURITY CENTRE

1. Scope

2. Economic Development

3. CSIRT

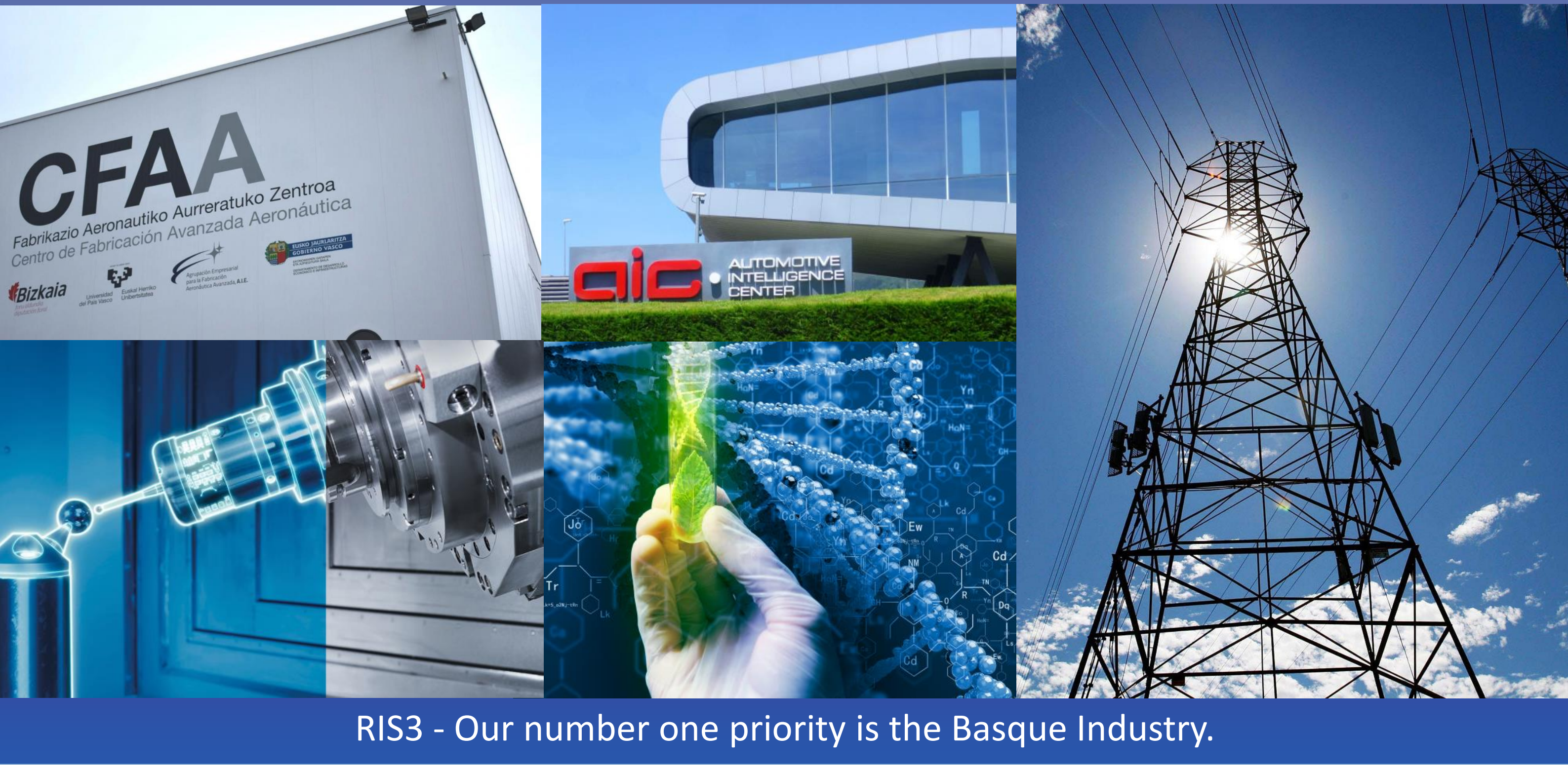
Scope: Functions

- Development
- Education
- Security / Police
- eGovernment
- Investment
- Research network
- Entrepreneurship

The Basque Cybersecurity Centre was created in Octuber 2017 within the Basque Agency for Business Development (SPRI)

Scope: Major Concerns

BASQUE CYBERSECURITY CENTRE


CFAA
Fabrikazio Aeronautiko Aurreratuko Zentroa
Centro de Fabricación Avanzada Aeronáutica
Bizkaia
aic
AUTOMOTIVE INTELLIGENCE CENTER

RIS3 - Our number one priority is the Basque Industry.

Scope: Functions

Economic Development

ECS
EUROPEAN CYBER SECURITY ORGANISATION

GLOBAL EPIC
Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity

CSIRT

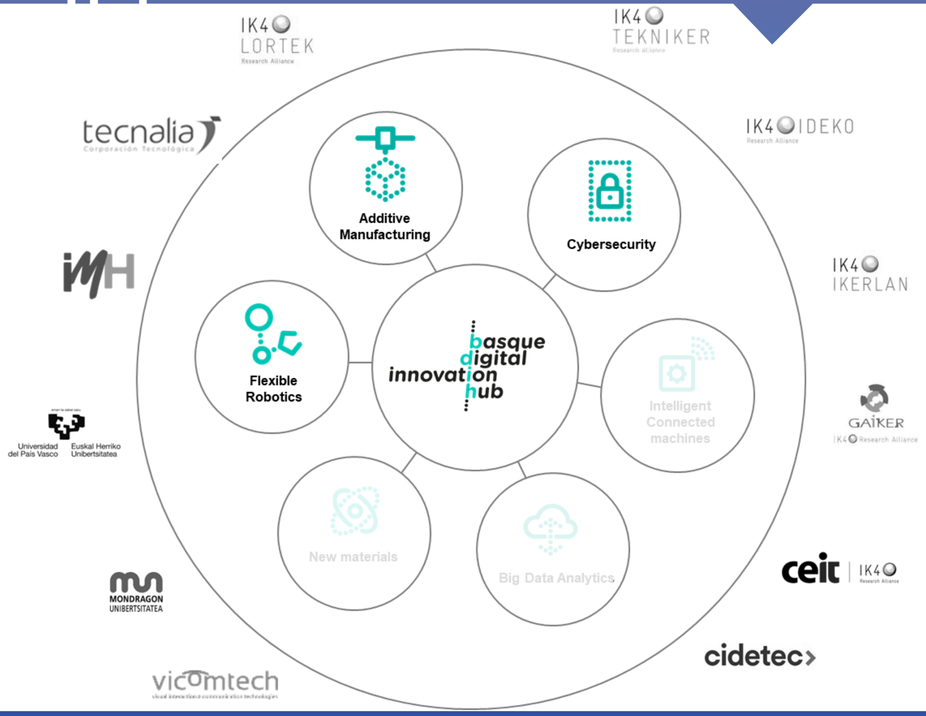
FIRST
Improving Security Together

TF-CSIRT
Trusted Introducer

CSIRT.es

Willing to cooperate and share.

Economic Development – Digital Innovation Hub


IK4 LORTEK Research Alliance
IK4 TEKNIKER Research Alliance
tecnalia Corporación Tecnológica
IK4 IDEKO Research Alliance
IK4 IKERLAN
IMH
Universidad del País Vasco
Euskal Herriko Unibertsitatea
GAIKER IK4 Research Alliance
MONDRAGON UNIBERTSITATEA
ceit IK4 Research Alliance
cidetec
vicomtech
Additive Manufacturing
Cybersecurity
Flexible Robotics
basque digital innovation hub
Intelligent Connected machines
New materials
Big Data Analytics

Basque Digital Innovation Hub

http://www.spri.eus/es/basque-industry/basque-digital-innovation-hub/

Part of the Digital Innovation Hubs Catalog created by the European Commission

http://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-catalogue

An opportunity to foster interregional collaborative projects and to create an European network of DIHs.

Infrastructure for Research and Innovation (Cybersecurity node under assessment)

Economic Development – Cyber Range

Education, Awareness and Training for Professionals

Economic Development – Education X.0

Dual vocational training programmes adapted to the specificities of the local industry.

Post-degree Cybersecurity Programme.

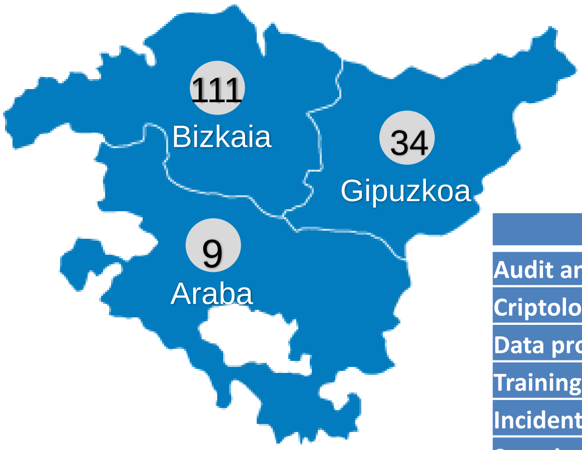
Recycling and reorienting

Awareness raising in the usage of digital devices.

Talent search and attraction.

Professionals of today and citizens of the future.

Economic Development – R&D&I



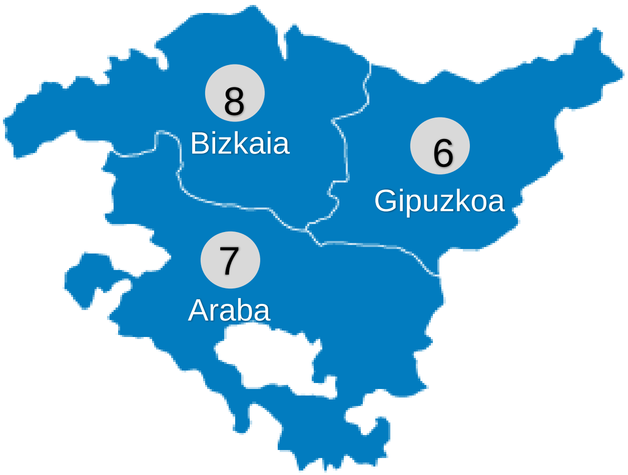
More than 150 researchers working in 125 R&D&I projects in Cybersecurity coordinated by the Basque Cybersecurity Centre.

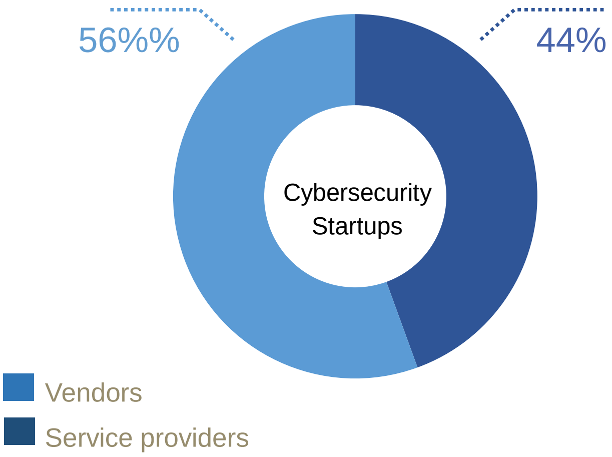
More than 200 publications in the last 5 years.

Areas of expertise	Publications
Audit and certification	13
Criptology	11
Data protection and privacy	28
Training and education	5
Incident management and digital forensics	5
Security governance and management	11
Distributed networks and systems	89
Software and hardware security engineering	40
Security measures	2
Technology and legal aspects	2
Security analysis and design theoretical foundations	3

Technological transference is the real challenge.

Economic Development – Entrepreneurs profile





Entrepreneurship is a key innovation driver.

Economic Development – Business friendly

BASQUE CYBERSECURITY CENTRE

The Basque Country has been recognized – among 171 Agencies worldwide – in the **Strategy Awards 2018 by the Financial Times** (also attached "fDi Strategy Awards 2018") in different categories:

- First-Prize winner in "Aftercare" category. This category is about the relationship of the Government with companies (foreign capital) established in the Region.
- First-Prize winner in "Start-ups and SME support" category. Because of the Acceleration Program **Bind 4.0**
- Second-prize Winner in "Incentives" category. Incentives to Research, Development and Innovation have been the most remarkable.
- Second-prize Winner in "Project of major interest by an Agency of Investment Attraction". **VIRALGEN project.**

We facilitate business relationships in the Basque Country, both local and foreign capital.

CSIRT – Present

- Collaborating with local agents to identify their real Internet perimeter and adjusting reputational rating with vendors.

- We have deployed basic infrastructure (MISP and MINEMELD) to share information and we expect to be ready to make the most of it by the end of 2019.

- Our focus is to work together with ISPs present locally to sensor and analyze sectoral threats to our core industry (advanced manufacturing, energy and biosciences), regional government and critical infraestructures.

- Local:
  - ❑ Connected to the MISP of CSIRT.ES.
  - ❑ Collaboration Agreement with PuntuEUS Foundation.

- International:
  - ❑ Connected to the MISP of FIRST.
  - ❑ Possibility of accessing to different Working Groups in FIRST and EUROPOL.
  - ❑ Sharing information with ShadowServer regarding the IP Space of the Basque Country.

We have just begun, progressing at a rapid pace.

CSIRT – Short-term

BASQUE CYBERSECURITY CENTRE

- Working with ShadowServer to join SISSDEN Project, a honeypot network, and to gain access to datasets that could be useful for our research community.

- In contact with some international CSIRTs to explore specific cooperation activities:
  - Team Cymru
  - CERT-EE
  - CIR-CL
  - CERT-IL

- Local collaboration agreements with INCIBE, AVPD and VOST are in progress.

- Developing a Project with local Cybersecurity service providers to begin monitorizaring information leaks related to the compromise of regional government's credentials.

We have just begun, progressing at a rapid pace.

CSIRT – NIS Directive

BASQUE CYBERSECURITY CENTRE

- In Spain, the competency to deal with critical infrastructures protection as well as internal incidents regarding public institutions has been assigned to National CSIRTs.

- Some ammendments have been proposed to the transposition of the NIS Directive, that does not attribute any role to the regions, in order to highlight the advantages of having presence in the last-mile:
  - ❑ Proximity.
  - ❑ Knowledge.
  - ❑ Trust.

- Working with National CSIRTs (CCN-CERT and INCIBE) to identify the role of regional CSIRTs.

- In the meantime:
  - ❑ Constructing strong relationships with local organizations.
  - ❑ Enabling locally established critical operators to elevate their level of protection.

Exploring opportunities to make the most of regional capacities.

Future

Technological dependancy reduction, local capacities development, inter-regional cooperation.

THANK YOU

www.basquecybersecurity.eus @basqueCScentre Linkedin YouTube

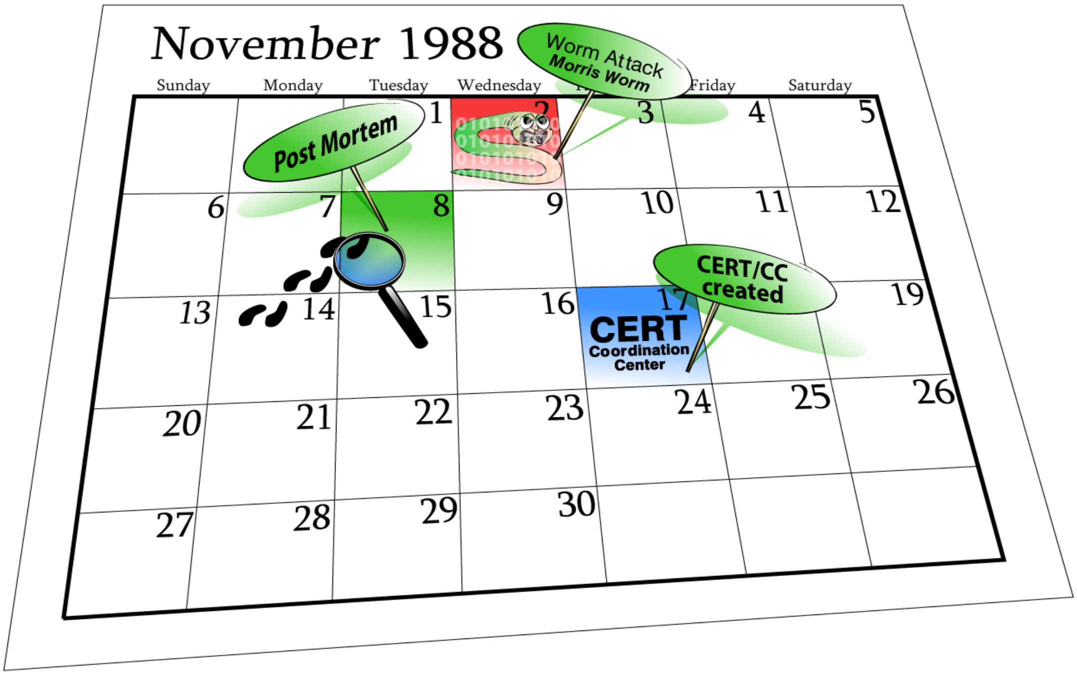
The second presentation of this session was on “Global Cooperation: Perspectives of Incident Response Practitioner” by Koichiro Komiyama, from the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC):

Perspectives of incident response practitioner

Koichiro Sparky Komiyama
Global Coordination Division
JPCERT/CC

Jan 24, 2019 ECSO-EUNITY Workshop, Brussels

Morris Worm and the first CSIRT was made



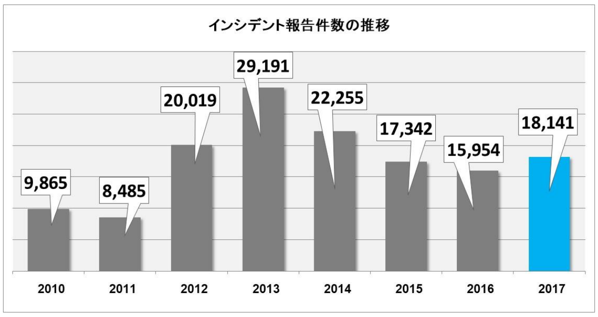
CSIRT’s mission

- Provides a single point of contact (POC)
  - info@jpcert.or.jp for reporting incident
  - office@jpcert.or.jp for general contact
- Assists the constituency and community in preventing and handling computer security incidents
- Share information and lesson learned with other CSIRT / response teams and appropriate organizations and sites.

No Accreditation or Certification body for CSIRT

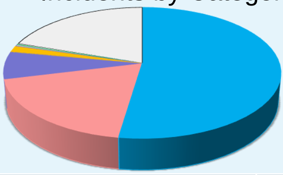
Incidents（Apr 2017 - Mar 2018）

- Reported Incidents
  - Incoming Report
    18,141
  - Incoming Incidents
    18,768
- Coordinated Incidents
  8,891



Source:
https://www.jpcert.or.jp/ir/report.html

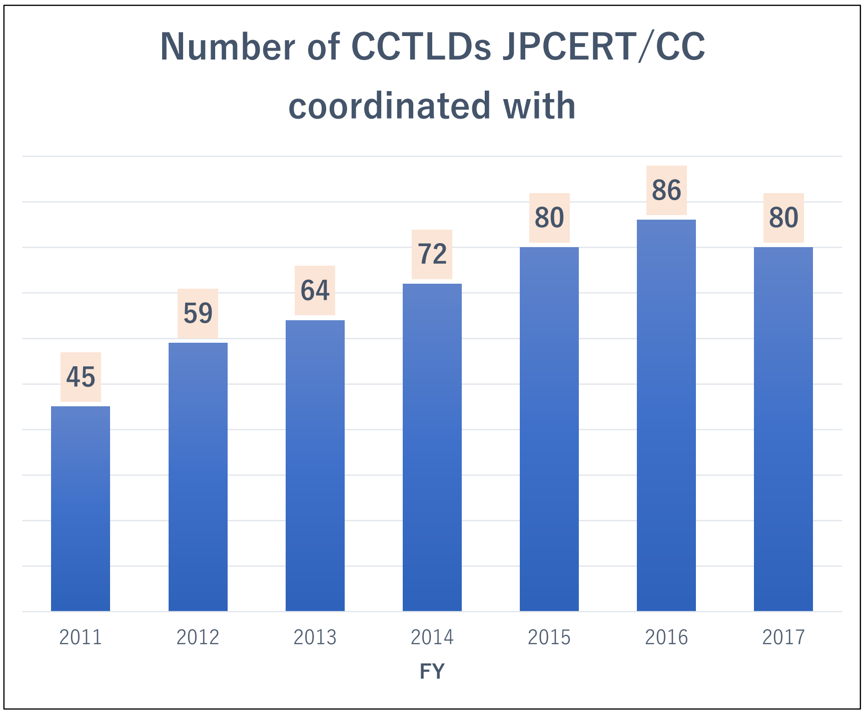
Incidents by Category



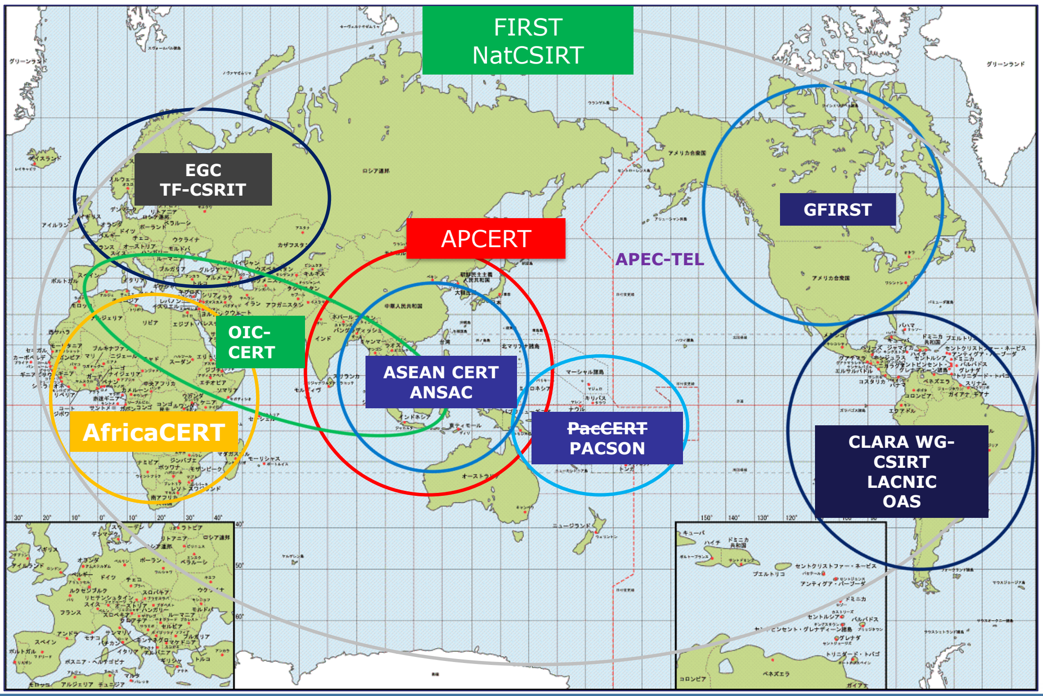
Category	Ratio
Scan	52.3%
Web Defacement	6.7%
Phishing	18.8%
Malware	1.6%
DoS / DDoS	0.1%
APT/Targeted Attack	0.2%
Control system	0.4%
Misc	19.8%

Wide range of cooperation (per CCTLD)

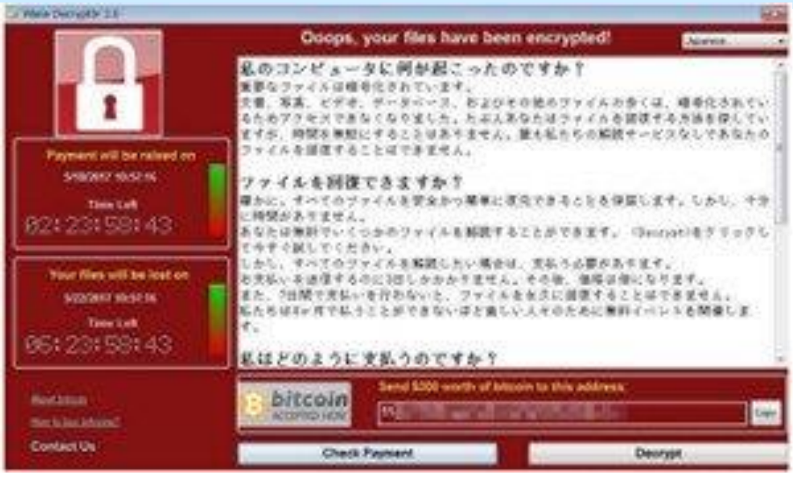
- Coordinated with 130 countries during last 7 years
- Composition?
  1. US
  2. China
  3. Hongkong
  4. Germany
  5. Taiwan
  6. Brazil
  7. Singapore
  8. France



International and Regional Collaborative Activities



Challenge 1: Role of Tech community for Attribution



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

私のコンピュータに何が起こったのですか？

重要なファイルは暗号化されています。

文書、写真、ビデオ、データベース、およびその他のファイルの多くは、暗号化されているためアクセスできなくなりました。たぶんあなたはファイルを回復する方法を探していますが、時間を無駄にすることはありません。誰も私たちの解読サービスなしであなたのファイルを回復することはできません。

ファイルを回復できますか？

確かに、すべてのファイルを安全かつ簡単に復元できることを保証します。しかし、十分に時間がありません。

あなたは無料でいくつかのファイルを解読することができます。<Decrypt>をクリックして今すぐ試してください。

しかし、すべてのファイルを解読したい場合は、支払う必要があります。

お支払いを送信するのに3日しかかかりません。その後、価格は倍になります。

また、7日間で支払いを行わないと、ファイルを永久に回復することはできません。

私たちは6ヶ月で払うことができないほど貧しい人々のために無料イベントを開催します。

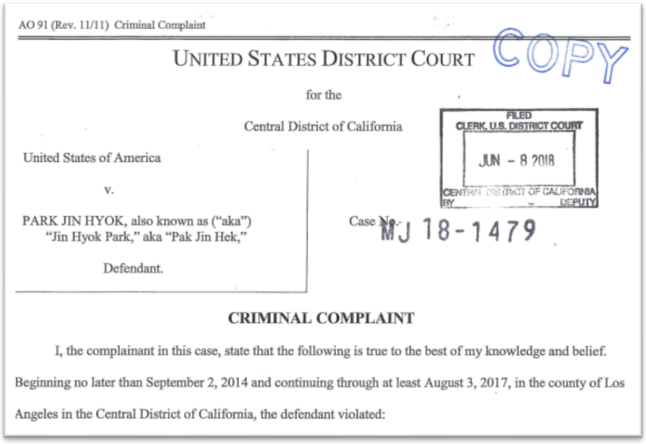
私はどのように支払うのですか？

Payment will be raised on
5/19/2017 10:52:16
Time Left
02:23:58:43

Your files will be lost on
5/22/2017 10:52:16
Time Left
06:23:58:43

Send $300 worth of bitcoin to this address:

bitcoin
ACCEPTED HERE
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt



AO 91 (Rev. 11/11) Criminal Complaint

COPY

UNITED STATES DISTRICT COURT
for the
Central District of California

FILED
CLERK, U.S. DISTRICT COURT
JUN - 8 2018
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

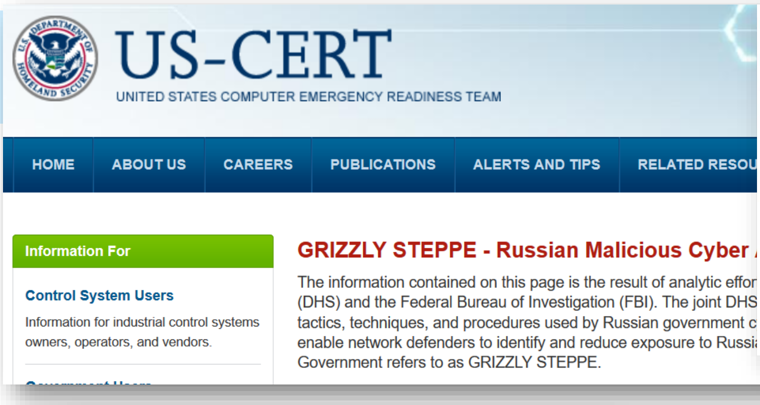
United States of America
v.
PARK JIN HYOK, also known as ("aka") "Jin Hyok Park," aka "Pak Jin Hek,"
Defendant.

Case No. MJ 18-1479

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning no later than September 2, 2014 and continuing through at least August 3, 2017, in the county of Los Angeles in the Central District of California, the defendant violated:

DOJ criminal complaint against an alleged spy for the North Korean goverment

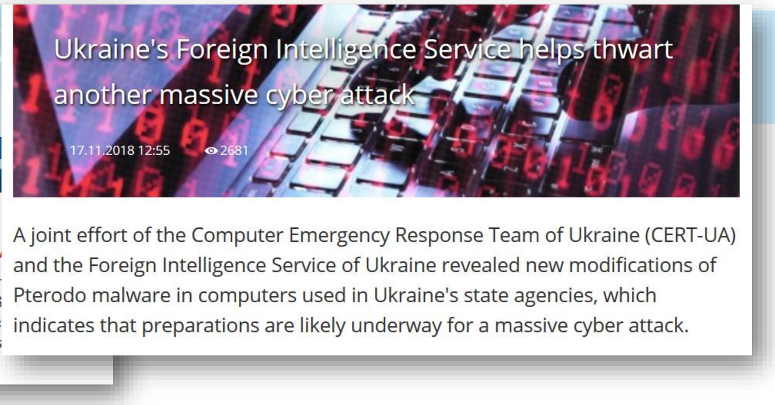


Control System Users

Information for industrial control systems owners, operators, and vendors.

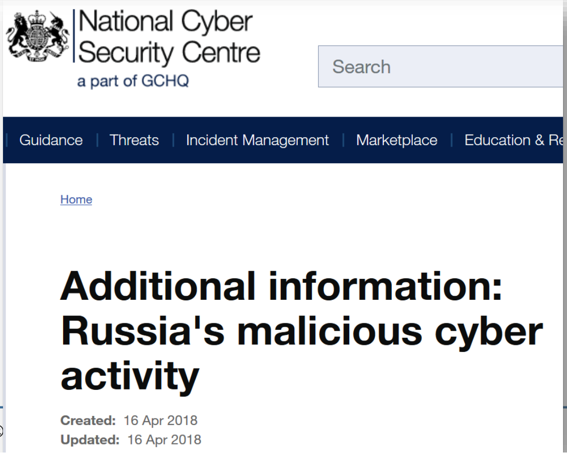
GRIZZLY STEPPE - Russian Malicious Cyber A

The information contained on this page is the result of analytic effor
(DHS) and the Federal Bureau of Investigation (FBI). The joint DHS
tactics, techniques, and procedures used by Russian government c
enable network defenders to identify and reduce exposure to Russi
Government refers to as GRIZZLY STEPPE.



Ukraine's Foreign Intelligence Service helps thwart another massive cyber attack

A joint effort of the Computer Emergency Response Team of Ukraine (CERT-UA) and the Foreign Intelligence Service of Ukraine revealed new modifications of Pterodo malware in computers used in Ukraine's state agencies, which indicates that preparations are likely underway for a massive cyber attack.



Additional information: Russia's malicious cyber activity

Created: 16 Apr 2018
Updated: 16 Apr 2018

- CSIRTs are accusing others

Challenge 2: Normative approach

OSCE
IGF Internet Governance Forum
November 11-13, 2018
PARIS PEACE FORUM
a global platform for governance projects
asean
GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE
G7 2018 CHARLEVOIX
G20 Japan 2019

Challenge 2: Normative approach

- 11 recommendation of UNGGE Report (July 2015)
  - (k) States should not conduct or knowingly support activity to harm the information systems CSIRTs of another State.
  - State should not use CSIRTs to engage in malicious international activity.

(Photo by Andrew Burton/Getty

Our Future

- Information sharing among CERTs/CSIRTs will become harder
- Shared value, individual trust is key to overcome

3.3.5 Closing discussion on potential cooperation & next steps

The last session of the workshop included the closing discussion on the potential cooperation and the next steps by Hervé Debar, from Telecom SudParis/EUNITY:

Conclusions and future steps

Hervé Debar

Institut Mines-Télécom

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

Objectives and expectations

- Prepare the policy recommendations that will be provided by the EUNITY project to the European Commission (D4.2)
  - Cybersecurity
  - Privacy
  - Business development
- Present and gather feedback on the challenges elicited during the last 18 months
  - Questionnaire
  - Cybersecurity and privacy priorities
  - Cybersecurity business development
- Stimulate awareness and reciprocal knowledge of requirements and activities between Europe and Japan
- Further feedback by email appreciated as well

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

Cybersecurity strategic directions

- Please indicate where you see hot topics
- Feel free to extend the list in the empty lines
- Please share more qualitative input by email

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

Legal and privacy aspects

- Legal and privacy frame our interactions
  - Information sharing
  - Cooperation
  - Regulation
  - Certification
- New regulations
  - Upcoming activities on certification in the EU
  - Network of competence centers
  - Revised Telecommunications Business Act in Japan
- Additional recommendations welcome

Research and Innovation

- ICT is a fast moving field and cybersecurity must follow
  - Research
  - Education
  - Information sharing on opportunities
- Investment in education seems limited with respect to needs
  - Support education programs
  - Leverage investment through collaboration
  - Define skills and competencies required
    - For cybersecurity
    - For professional education

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

Industry and standardization

- Supporting business development
  - Joint framework
  - SMEs
  - Common standards roadmap
    - Sector specific ?
- Arbitration between services and products
  - Economic tradeoff
    - Also related to skills shortage
  - Who should be the service offerers
    - E.g role of insurance companies

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

Future steps

- Deliverables and recommendations
  - Published on the project’s website
    - https://www.eunity-project.eu/
  - Communicated through social media
    - Twitter
    - LinkedIn
- EUNITY partners workshop in Japan
  - April-May timeframe
  - Communicate results and further feedback
  - Privacy seminar in Tokyo in April

EUNITY (GA No 740507) receives funding from the @EU_H2020 Research and Innovation Programme (H2020-DS-2016-2017/DS-05-2016). The information reflects only the views of the project owner.

info-eunity@eunity-project.eu

herve.debar@telecom-sudparis.eu

Additional feedback and suggestions are welcome

4 Discussion and Feedback

4.1 Session 1: Introduction

4.1.1 Welcoming remarks from ECSO and EUNITY

The first session included a welcome message by Hervé Debar and the general secretary of ECSO, as well as the presentation of the agenda. The Japanese representation in the workshop was impressive and although there is a significant distance between the two regions, there are many connecting points and common interests between Europe and Japan.

The remarks by the ECSO general secretary included an introduction on the ECSO, reporting that it is an association created in 2016, purposed to build a PPP partnership in research priorities. It was also added that there was a research focus in the beginning but later the focus was not only in research but also in certification, standards, international activities, education, training, health, energy, etc. The organization includes SMEs, industry, universities, research centres, as well as the public administration sector. EU include many countries with different approaches in cybersecurity, prompting ECSO to: (1) build a common approach in cybersecurity, (2) provide suggestions to the EC Parliament, (3) suggest and support the Members States at national level, as well. One point is to start a dialogue at the international level and the EUNITY project helps initiate this dialogue with Japan.

4.1.2 Expectations of the workshop

4.1.2.1 Hervé Debar, Telecom SudParis/EUNITY

Hervé Debar, partner of EUNITY project from Telecom SudParis, mentioned that by the end of EUNITY in May, we will have published information about European and Japanese landscapes, including suggestions that the European Commission could build on, regarding research, education and business. Within the context of EUNITY, we would like to formulate the output and provide policy recommendations to the EC.

4.1.2.2 DG CONNECT expectations - Jakub Boratynski, DG CNECT, European Commission

Jakub Boratynski mentioned that the importance in the area of cybersecurity is growing and that Europe and Japan can learn from each other. The intention is to be more competitive with a specific focus on cybersecurity, as we would like to see policy recommendations and practical indications for the future.

4.1.2.3 Japanese delegation expectations

Reiko Kondo from the Office of the Director-General for Cybersecurity, Japan Ministry of Internal Affairs and Communications (MIC) mentioned that in this workshop can facilitate the discussion for the cyber space in general, as it just followed a December meeting where an ICT Europe-Japan dialogue was established, although not focused only on cybersecurity but on other fields as well.

4.2 Session 2: European and Japanese Ecosystems

4.2.1 Business approaches to cybersecurity

The next session, on European and Japanese Ecosystems, was moderated by Luigi Rebuffi, from the European Cyber Security Organisation (ECSO).

4.2.1.1 European view on the Cybersecurity Market, Ulrich Seldeslachts, LSEC

The first subsection was on “Business approaches to cybersecurity”, starting with the “European view on the Cybersecurity Market” by Ulrich Seldeslachts, from LSEC. The presentation mentioned the LSEC’s (International IT & Information Security cluster)[1] results. Concerning the contents of CIMA (Cybersecurity Industry Market Analysis), some of the highlights of the analysis (in total 120 pages) include information from various countries on cybersecurity, as well as information on the cyber crime market cost estimation. It was also mentioned that only 500M euros were invested in education and that this area bears many more promises. Most of the funds were invested towards infrastructure. As a next step, a comparison between the global

[1] https://www.leadersinsecurity.org/

and European market value was provided, in various terms. The presentation also indicated how EU is standing in a global position and that Japan holds the third place, leading LSEC to conclude that we have a lot to learn from Japan.

Next, an extract of the executive summary was presented. The presentation stated that all EU countries combined represent a larger player in the area. Europe's spending in products and services breakdown showed a very small part invested in training and education. The situation awareness has been the largest for the cyber security market. 20% of growth is expected in the area for the EU. Considering the cybersecurity spending per EU country, it is noticed that the eastern countries spend the most in system recovery, while others spend in detection and prevention capabilities. Also, 14% of the top 500 cybersecurity providers are located in Europe, while ICT and traditional players, like identity management, are also present here. About the EU market growth potentials, 16 categories have been identified among the end users, while the public sector represents a 31% part (including military).

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

About the market trend in Japan, the presentation stated that the products and services are expanding, with the services in higher demand compared to products and the service market is expected to expand further. The major players are the NEC corporation[2], the Internet Initiative Japan inc. [3] and the LAC Co. Ltd. [4]. The Industrial Control Systems and the Operational Technology (OT) are also entering the cybersecurity market and promote overseas business expansion (e.g., TEPCO IEC[5]).

Concerning the Japanese major players for international cooperation, IPA ICS CoE, a Global Training in Core Resource Development Program, organized two training sessions in France and UK in 2018, with 18 and 33 trainees from Japan respectively. There are foreign companies from UK and Israel entering the Japanese market (Darktrace - UK, Votiro Inc. - Israel, Cybereason Inc. - US, Fireglass, Inc.- Israel).

Considering the governmental support for the market expansion through tax reduction system (encouraging security investment), the presentation stated that the corporate tax was reduced from 30% to 25%. With respect to the regulatory sandbox, a new regulation framework was introduced on the 6th of June 2018, which was initially introduced in the UK. Within this new framework, the companies can demonstrate their activities and capabilities,

[2] https://www.nec.com/

[3] https://www.iij.ad.jp/en/

[4] https://www.lac.co.jp/english/

[5] http://www.tepcoiec.com/en/

invite new technologies into the market and finally consider and adapt those systems. A whole process is in place to help such companies promote their business. It is much more friendly than the previous established system, specifically because support is provided when using this regulatory sandbox system.

4.2.2 Introducing European cybersecurity ecosystem: from threats to industrial policy

The next session included two presentations from Roberto Cascella, from the ECSO Secretariat and Jakub Boratynski from the DG-CONNECT of European Commission.

4.2.2.1 2016 cybersecurity Public-Private Partnership (cPPP) and European Strategic Agenda on Research & Development: overview of the ecosystem and cyber technologies - Roberto Cascella, ECSO Secretariat

The presentation initially stated the three main goals of ECSO: foster the cooperation between public and private actors; stimulate the cyber security industry; and coordinate the digital security industrial resources in Europe. Additionally, it is important to push education and training, as mentioned earlier by Mr. Seldeslachts. Considering the "WG6 - Strategic Research & Innovation Agenda on New Technologies Products, services and cyber defence", the ECSO SRIA is to identify research priorities for 2018-2020. The published document identified 7 different large pillars:

- European ecosystem for cyber security.
- Demonstrations for the society, economy, industry and vital services.
- Collaborative intelligence to manage cyber threats and risks.
- Remove trust barriers for data-driven applications and services.
- Maintain a secure and trusted infrastructure, in the long-term.
- Intelligent approaches to eliminate security vulnerabilities in systems, services and applications.
- From security components to security services.

There is a good alignment between the private and the public priorities. The strategic priorities include the cybersecurity technologies and services to protect the infrastructure, the applications and the citizens' privacy (encryption, ID and DTL, AAA, security resilience and privacy by design, etc.); the infrastructure and applications (Industry 4.0, Energy, Transport, Finance, etc.); and the cyber ecosystem (standardization, validation/labeling, trusted management of the supply chain, assurance, education, etc.). Some important points that were mentioned were: the technologies map with industry verticals and the awareness initiatives towards the citizens. There are various PPPs in Europe like the BDVA, the EFFRA, the 5G IA, and EURobotics. ECSO SRIA's next main goals include the identification of the global trends, such as AI, IoT and Blockchain that can be in use for the regulatory sandbox, in which EU has also an interest, considering how these technologies could be important in the future. Of course, there are technical cybersecurity challenges like the relevance, the current status and the future directions. The initial priorities and challenges for Horizon Europe (2021) include the Society and Citizens (Social Good), the Data and Economy, the Basic and Disruptive technologies and finally the Digital transformation of verticals.

4.2.2.2 EU strategy & legal response for strengthening cybersecurity: update on the European Commission 2017 Cyber Security Package and focus on 2018 initiatives - Jakub Boratynski, DG CNECT, European CommissionNIS directive. The First EU cybersecurity law.

Jakub Boratynski, from DG CONNECT, initially, presented the NIS Directive, the first EU Cybersecurity Law. Directive means that this should be applied by the Member States. Considering the EU Cybersecurity Agency (ENISA), there was a renewal of the ENISA mandate, which is expected to grow thanks to a doubled budget, as well as an increase in personnel by 50%. There are two specific tasks demonstrating the new cybersecurity agency: operational cooperation and a key role in the development of cybersecurity certification. Also, the new European cybersecurity certification scheme was presented, which will be a collective work with stakeholders and industry, coordinated by ENISA. The timeline of Union rolling WP was presented, including a 1st scheme for 2020.

Considering the cybersecurity competence centers, the budget for 2021-2027 is being prepared at the time of the workshop. There are discussions ongoing discussions not only on the objectives but also on the instruments as well. About the European Competence Center, the central node could manage all the funds for cybersecurity and the goal is to implement the programme. The European Competence Centre manages the funds foreseen for cybersecurity, under Digital Europe and Horizon Europe 2021-2027; it facilitates and helps coordinate the Network and Community, in order to drive the cybersecurity technology agenda; and finally it supports joint investments by the EU, Member States and industry and supports the deployment of products and solutions.

The initiative will be financed by the two programmes, Digital Europe and Horizon Europe. The next steps include the finalization of the negotiations by Q2 of 2019, the preparatory phase in 2019-2020 and the preparation to launch 2021 actions in 2020. It was also mentioned that 50% of the partners are ECSO partners in those projects.

4.2.3 Introducing Japanese cybersecurity ecosystems: legal and policy framework

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

The next presentation was given by Hiromichi Nakahara and Hiroo Inoue from Japan External Trade Organization (JETRO).

Considering the cyber/physical security framework, Japan proposes the initiative for Society 5.0 including AI, IoT and Blockchain. It seems also that there is a necessity of a new form of supply chain. The new form should mitigate the vulnerabilities imposed by the vertical expansion of the security surface.

There are notably three layers of trust anchors:

- The first layer includes the connections between the organizations. The trustworthiness of an organisation's management is the key for secure products and services.
- The second layer is about the cyber to physical and to cyber again, including the trustworthiness of the function for "correct transcription" between cyber/physical space (IoT).
- The third layer includes the data circulation. The trustworthiness of data is the key for secure products and services.

The activities related to the CPS framework, in a sector by sector approach includes the development of sector specific measurements, industry by industry with the framework, as a standard model. The guidelines for building the sector of cyber/physical security have already been publicized. Considering the Industrial Cyber Security Center of Excellence (ICSCoE), the HR development programme includes a one year course. The students are funded by the government and the companies. The students will go back to the companies as a core HR for IT/OT cybersecurity. About capacity building, Japan and US will join hands in training for cybersecurity and this training session will be held annually, including 5 days training for cybersecurity. The participants of the last session were:

- 36 students from ASEAN countries, Australia, India, NZ, South Korea and Taiwan,

- 83 students from IPA ICSCoE Core HR development program,
- and 5 lecturers from DHS/NCCIC.

Considering the establishments of "Cybersecurity Supporters" for SMEs, the Feasibility Study (FS) for the next year will include:

- The threat situation surrounding SMEs,
- The required tools and skills for supporting SMEs and
- The ideal system for promptly and efficiently support SMEs.

About the collaboration platform in Japan, it was launched by IPA, in June 2018 and will set the arena for information exchange among companies, including the "needs holders": manufacturers, CII operators and the service providers, while the "seeds holders" are the security vendors and the venture companies. The collaboration platform will feed the market, as well as the international standards.

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

NICTER is observing the attacks on IoT devices using NICT data, including cyber attacks globally monitored through 300.000 unused IP addresses (darknet). They observe that more than half of the attacks are on IoT devices and attacks on IoT have increased by 5.7 times from 2015 to 2017.

The attacks are divided as follows:

- 2% cyber threats on databases,
- 3% cyber threats on websites,
- 5% cyber threats on PCs,
- 54% cyber threats on IoT devices (web cameras, routers, etc.).

The comprehensive package of IoT security measures, administered by MIC, was published in October 2017. The progress made so far was reviewed on January 2019 and the progress report has been published on 27th July 2018.

It seems a necessity to implement measures on IoT devices vulnerabilities, covering their entire lifecycle (design, development, sale, installation, operation, maintenance and use), as well as to organize the structure to conduct vulnerability assessment.

In May 2018 the revised Telecommunication Business Act and NICT Act were promulgated. By the revised Telecommunication act, it is allowed to establish a third party as an information gathering hub with firm security measures to manage sensitive information. Examples of the attack were provided with the use of a C&C server and its operations. The revised Act on NICT enabled an active scan on IoT devices over the internet and identified IoT devices with improper password settings, out of which actions had been prohibited by the Act on Prohibition of Unauthorized Computer Access.

Concerning the Amendement on the Technical standards of terminal equipment for IoT security purposes (IoT certification), in order to prevent massive malware infection on IoT devices, the information and communication council in MIC discussed an addition of security measures to a standard of technical equipment. MIC is now preparing related ordinances, notification and guidelines for implementing the security measures, which will be enforced in April 2020.

The R&D activities against Indiscriminate/Targeted attacks include the usage of the following tools:

- The NICTER countermeasures against indiscriminate attacks include the visualization of geographical information, the amount and type of attacks in real time by observation of the darknet (IP addresses) and the alerts to local governments of infected malware.

- The NIRVANA-Kai countermeasures against targeted attacks include real time visualization of traffic and automatic blockages of abnormal communication, after its detection.

- The StarDust (Honeynet) is a honeynet to study targeted attacks in detail learned by NICT. It also sends emails to organizations, with an attached file that is executed in a decoy environment, implemented in advance to observe and analyze the behavior.

Considering the Human Resource Development, NICT has initialized the hands-on training programs from April 2017, including the following programmes:

- CYDER is a program for local governments, government administrations, independent administrative agencies, critical infrastructure providers, etc.

- Cyber Colosseo is a cyber defence exercise for those who are in charge of cybersecurity in organizations, related to Tokyo Olympics 2020.

- SecHack365 is a training program for young cybersecurity innovators, in order to increase the number of advanced cybersecurity researchers and entrepreneurs in the future. One year cybersecurity training program with hands on training and remote software development.

ISAC has been established for each industry, in order to collect, analyze and share incident information on cyberattacks. The Telecom-ISAC Japan has been established in 2002. The ICT-ISAC participating organizations include broadcasters, security vendors, ICT vendors, Sler, ISP operators against the following threats: vulnerable IoT systems, targeted attacks, DoS attacks, website defacement and bots.

4.2.4 Discussion on common approaches and possible synergies

The first issue that was discussed in this session was the cyber security certification process, the specific schemes and whether these could be tailored for each sector. The DG CONNECT representative replied to the Japanese ministry that there is a limit on what can be said at this point: priorities were set and a whole system was set up in order to find out how it should be done. In particular, certification must be affordable for consumers and end user devices. The other main direction concerns the ICT components, used in the context of critical infrastructures. There is one existing scheme in place, which is used for the certification of smart cards but the sectoral approach is not so obvious right now. ECSO also replied that there are needs for further discussion, in order to choose and develop a specific scheme. Specific bodies will usually develop such schemes. Once developed, schemes can be reviewed in light with the Japanese certification. ECSO itself is providing suggestions on creating such schemes. DG CONNECT also added that there is a possibility that the legal part of the EU scheme may take into consideration the international cooperation.

Someone from the audience also added that there are many points of joint interests. He also asked both European and Japanese representatives whether there will be specific programmes to dig into these common interests. The Japanese representatives replied that they had a European - Japanese ICT dialogue in December, not only for cyber security matters but with several programmes to discuss, where the IoT ICS national security was mentioned. A representative from the EU added that FP7 supported the collaboration with Japan, as also H2020 (e.g the EUNITY project, along with many other collaborations). She mentioned that they have learned a lot, via conferences, exchange programmes for trainees. Horizon Europe 2021-2017 (the next programme) is expected to continue the collaboration between the regions on cyber security. Finally, the upcoming cybersecurity competence center will be the regional collaboration hub on cyber security. At this point, an ECSO representative added that the process with the dialogues is useful, but when they speak about industry, they want to go beyond this dialogue and speak about concrete results and objectives. There are different ways to accomplish international cooperation, e.g. supporting SMEs and sharing best practices. There are various ways to accomplish strong cooperation between the two regions.

A CERT JP representative asked, regarding the NIS mandate, whether there has been seen any tangible outcome from the application of the NIS directive. DG CONNECT replied that it needs time before they see concrete results, and it was still early at the time of the workshop. The first reporting period is between May and August. DG CONNECT does not expect to have details of incidents but aggregate information which is still valuable. They may have some quite meaningful results within one year. An ECSO representative added that this could be considered also as an area of cooperation in the future, considering the ISACs in Japan and the ISACs which are developing in Europe. There could be an exchange of information on this.

Hervé Debar from EUNITY project added that one thing that we should also mention is education. EUNITY has taken a real interest in the process of exchanging students. The model is very interesting, although it is small in scale. Supporting education is mostly done through training programmes. A Japanese representative mentioned that the training between JP and UK is also a fact. Apart from the training for expertise in cyber security, they also get the opportunity to know each other and agreed that is a good opportunity for both of them. An ECSO representative asked if the training is too much dependent on the language, and Hervé Debar replied that most of the material is in English, but is not really certain if the language is an issue. The issue is that a platform is needed, as well as real use cases, scenarios and instructors. ECSO added that they are going beyond training to cyber ranges, while Hervé Debar added that cyber ranges are one example, there is a need for technologies, machines, use cases, scenarios and trainees.

DG CONNECT added that this seems to belong to the concept of competence centre/network. Models of training can be replicated. There is space for an international outreach. The audience also added that we can have some exercises for managers, while international exercises can be one way of collaboration. The infrastructures in Japan are independent, while in EU they are inter-dependent, so the case is somehow different. It would be nice though to think about how collaboration could take place.

A representative from the EU asked whether Honeynet is for various attacks or only for governmental bodies. A Japanese representative replied that StarDust is a sophisticated environment for cyberattacks. It is a platform to check the behaviour of cyberattacks. Someone from the audience also added that they run a number of training sessions for managers and technical people. They try to run joint exercises, war gaming type exercises with specific scenarios (for CIs, telcos, energy and banks). The conclusion is that technical people find these exercises not too technical and the managers too technical. The assumptions made by either technical people or managers can be somewhat difficult to capture. A Japanese representative added that these are common issues in Japan as well. There is a department to provide instructions on how to run these exercises. They have a cybersecurity framework, so that people have a common understanding of cybersecurity language.

ECSO for closing, added that they have similar points of view on what could be common interests. They have seen that there is a need for increased digital autonomy. For now, there is heavy trust placed in systems provided by other countries. Along with Japanese colleagues (in another meeting) they had a similar observation, prompting them to push ways of thinking towards strategic solutions. On one hand, they have to invest in regional/local solutions and on the other hand, they still have to trust partners.

A Japanese representative agreed that it is a very important point. They also need to further develop trust and co-operations and further develop the domestic legislation. Currently, there are intensive discussions regarding the procurement. Japan would like to extend the cooperation with the EU side and build trust in this new era of data.

4.3 Session 3: Working Session on Business Solutions Applied to selected vertical sectors

The last session of the workshop was moderated by Nina Olesen, from the European Cyber Security Organisation (ECSO).

4.3.1 Challenges and capabilities needs from the selected verticals

The first session, on “challenges and capability needs” from the selected verticals, included three presentations.

4.3.1.1 Health sector, Julio Vivero from GMV

The first subsection of the last section was on health sector, presented by Julio Vivero from GMV. The main objectives of the health care sector were presented, as well as the main activities and challenges, the needs and a description of the SWG3.6 (Healthcare) of ECSO. The market of health cybersecurity is expected to reach over 280.000 million euros, by 2020, in the fields of Health Analytics and Big Data in Health, mHealth, TeleHealth, Integrated Electronic Health Records, eLearning in eHealth and Social Media in Health. The list of health cybersecurity challenges include the increase in cyberattacks, the patient ecosystem (delocalization of the network of care services), the medical devices cybersecurity, the trust in e-Health through privacy, the integrity and resilience of services, the trends towards exploitation of health Big Data – privacy and the EU integrated Electronic Health

Record – heterogeneous legislation within Europe. The key levels for the needs in health cybersecurity include:

- Personalization of the consent mechanism for each patient's data.
- Free publication of the data.
- Revolution of health through technology and information management.
- Connectivity of data apps and tools.
- The involvement of everyone in the eHealth process.

The audience asked two questions. The first was about the data from wearable computing, and aimed at questionning if we could know who is affecting the body and have access to it, in the case of implant usage. The second point was whether data centers are strategical points or not. It is interesting to know who is defending these data centers, whose is responsible, if there is protection there. Julio Vivero agreed with the question and added that the amount of data is growing. With the wearable devices, the generated data are located in many companies that provide those services, e.g., Google fitbit.

4.3.1.2 Banking and Finance sector, Giorgio Cusmà Lorenzo from Intesa Sanpaolo

The next presentation on was given by Giorgio Cusmà Lorenzo, from Intesa Sanpaolo. The presentation stated that the banking sector is facing a paradox: the financial institutions need to reshape their business models investing heavily on innovative technologies and new skills, whilst coping with a structural contraction of revenues, due to several contingency forces, such as the unprecedented interest rates reduction, the increasing competitive pressure and the non performing loans challenge. Bearing this landscape in mind, the financial institutions have to create new digital business models and cope with cybersecurity issues. There are six areas to enhance ISP cyber resilience: infosharing, incident reporting, crisis management procedures, secure supply chain management, cyber risk measuring and education & training.

The main reasons for improving cyber resilience are the following:

- It is a regulatory requirement,
- It is a business survival need,
- It is a business growth enabling factor,
- It is often foreseeing a (multi) hub and spoke approach,

- It is often coming as a top down approach.

There is an ongoing cooperation in the ISP network, which has three main goals: extend their leadership role within the financial sector in the European cybersecurity domain, become a trustworthy partner for institutions and peers, and leverage the process of accreditation with international financial sector.

Sanpaolo's Strategy focuses on three main points: address cybersecurity strategy at EU level, implement the solutions of common interest with peers, and support an effective spending of EU funds. The main partners for the first focus area are: ECSO, EBF, AFME, CEPS. The main partners for the second focus area are: ECSO, EBF, AFME, ENISA, SSVA, JP MORGAN and Rabobank, while the main partner for the third focus area is ECSO.

Intesa Sanpaolo strategic approach is to collaborate with external entities both at local and international level and is actively involved in the following initiatives: CERTFin, the Italian Cyber Security Framework, EBF, ECSO, AFME and *glocal* ventures (i.e. thinking global and acting local).

Proactively collaborating in many initiatives, the Intesa Sanpaolo Group has provided a significant contribution to different working groups, improving ISP positioning among major EU players. As of today, the following goals have been achieved:

- Recognized leading role on cybersecurity topics at European Level, not only by private institutions, but also by EU bodies, agencies and authorities.

- Creation of a selected network of trusted partners, whilst becoming a recognized trustworthy partner for peers across jurisdictions and across industries.

- Identification and design with other stakeholders, cybersecurity related solutions, addressing common needs, starting with mandatory incident reporting

- Fragmentation and information sharing.

4.3.1.3 Energy sector - Mario Jardim, Schneider Electric

The first issue presented in this presentation was the energy sector challenges. The electrical grid is a pan-European network shared by different actors. Energy is at the center on modern world enabling society digitilization, where vital functions are energy dependent: water, health, food, transportation, banking etc. But all critical infrastructures are impacted by the loss of energy.

The domino effect is between countries and legal entities (e.g., the Kosovo frequency shift), where large installed bases of distributed systems composed of solutions from different manufacturers are mixing old and new technologies. The end to end protection and data integrity are critical and the objective here is the grid resilience, i.e., the support of a functioning European society and economy in a crisis situation.

The key points for the utilities challenges are the following:

- A system approach based on risk analyses,
- Cannot treat grid operating systems as conventional IT systems,
- System life cycle, architectures and operational process are fundamental,
- Whether we can deploy security measures in aging infrastructure,
- People training and education on security measures,
- Supply chain adaptations,
- Certification costs.

The take away message is the following: the electrical grid infrastructure is interconnected across Europe and shared by many actors and countries, the primary focus is the grid resilience, the service continuity and finally the international security standards like ISO/IEC 27001/2/19, IEC62443, IEC62351, which are the basic support for a shared level of security among actors.

4.3.2 The answers from technology and trusted supply chain perspective

4.3.2.1 Cybersecurity for the Internet of Things - Ana Ayerbe, Tecnalia

The presentation from Ana Ayerbe started with the issue of IoT mass market. Things are massively produced and they are used by private users with little technical or security know-how. The ENISA report lists these IoT security incidents. IoT is used in sectors as varied as Industry 4.0, Energy, Health, Agriculture, etc. Cybersecurity by design, in the whole software and development process, along the supply chain is a prerequisite. Considering blockchain, it is one of today's most disruptive technologies; it can change procedures and business models as we know them today. The main advantages are listed here:

- Disintermediation of processes and business models,
- Integrated point of view of synchronized, agreed and unalterable data,

- Trustworthiness and non-repudiation of transactions,
- Traceability and transparency of processes,
- Machine economy: machines as active participants in the economy.

4.3.2.2 Challenges of cybersecurity certification and supply chain management - Roberto Cascella, ECSO Secretariat

The next presentation by Roberto Cascella started with the standardization certification and supply chain management support. The current WG1 activities largely focus on an updated version of the ECSO Meta-scheme approach and how it works in practice. The Organisation of WG1 is: SWG 1.1: Self-assessment, SWG 1.2: Third party assessment and SWG 1.3: Base Layer. COTI is an internal document to identify the challenges of the industry and define the objectives for our approach. SOTA is a public document to record all available cyber security standards, initiatives and certification schemes and therefore the identification of the existing landscape. The meta-scheme approach is determined to harmonise the minimum security required, define a unified leveling across verticals (for comparison of items) and a common way to define the scope & required security claim, in order to foster the trust by defining transparent rules.

Industry worries about the lack of agility, complex and composite certifications, the load of much formalism, slow processes and their unpredictability, the lack of flexibility, undetected cheaters in the supply chain, the lack of harmonization, static certificates and pure checklist evaluations. On the other hand, industry expects speed and predictability, high level of flexibility, full harmonization, pragmatism, agility, detecting cheaters in the supply chain, patching and updates, ethical hacking and lean on modular composite certifications. Currently, there are 290 standards & schemes in SOTA Chapters 3,4,5, and 6 about products and components, ICT services, service providers and organizations and security professionals. Since there is not a single scheme to fit all the needs, we need existing certification schemes and use cases. The meta scheme idea includes the allowance of the composition across different schemes via a meta-language, the support of scalable common structure, the re-usage across verticals through horizontals and finally different schemes that can be defined as “equivalent”, if needed.

The experts are coming from industry, labs, academia and national security agencies. The role of the expert groups are:

- Definition of protection profiles (threats/risks, therefore security requirements)
- Tailoring of evaluation methodologies (what is “really” important to look at)

- Maintaining state-of-the art attack methods
- Working on checklists & compliance testing
- Incorporating ethical hacking especially for high security.

Considering the contribution to the EU Cyber Security Framework, experts from industry are part of the decision process for scheme selection and priority. There is a minimum common baseline security that needs to be defined across sectors. Threat analysis and risk assessment can be a source for security requirements. The scope of certification should address the entire supply chain, the content and the methodology depend on the intended use. Ethical hacking shall be legally allowed and enforced for high security, while checklists are insufficient. There is a need for a common definition of the proposed assurance levels, i.e., assessment methodologies (evaluation) associated. Finally, centrally steered harmonization across CABs, NABs and National Certification Supervisory Authorities (NCSA) is crucial.

The current focus in order to support the EU Cybersecurity Certification Framework and Trusted Supply Chain in Europe is on:

- SOTA, COTI reports update: towards a better common understanding of the situation and the needs to prepare future priorities.
- ECSO Meta-scheme in practice, including tools for qualitative market analysis to define focused initiatives and promote EU solutions, as a methodology for the European Certification Framework (identification of the characteristics under which certification schemes can be viewed and selected)
- New version with general aspects of certification scheme composition, type of evaluations, continuous assessment and a mapping with the Cybersecurity Act
- Document on Assessment, from self to third-party, looking into the available types of assessment and identification of the criteria to decide on the fit-for-purpose type of assessment
- Analysis of security requirements, gaps in standardization and priorities for future EU certification schemes, in order to identify common priorities for definition of certification schemes
- Support of EU standardisation on cybersecurity
- MoU with CEN/CENELEC (and ETSI to be signed). Definition of priorities for developing EU standards, in order to simplify tasks for ESOs to initiate standardisation, in particular linked to certification.

The audience expressed the concern of how the certification process will be done: “The ECSO work on certification is very important. Because there are different schemes and there will be a diversification of the certification programme. Who is going to certify? Is each sectyor going to have its own certification body?” ECSO replied that Europe wants to create the schemes and the implementation of the schemes will be done by the companies themselves. There are many companies involved in certification activities. Some of them are focused on hardware. The aim is to certify the processes of those certification companies. Also ECSO is going to provide the tools to be used and they will create the certification schemes. They are not going to develop new standards. This is done by other organizations. Regarding the cybersecurity, the certification is voluntary at the moment. After some years, some sector could be regulated, e.g., health is a highly regulated sector, but there is no third-party certification that has self-assessment.

A Japanese representative also asked about third parties, whether there are any examples of third party certifiers involved.

An ECSO representative replied that some members of ECSO are certifiers. They indicate the benefits of using third-parties for certification in the document that is going to be issued. They have also some national level certification.

4.3.3 Training and awareness challenges

4.3.3.1 Update on Training & Cyber Range activities in Europe Nina Olesen, ECSO Secretariat (Roberto on behalf of Nina Oleson (WG5, Education Training)

Regarding ECSO WG5 education, training and awareness, there is a position paper on gaps in education & professional training. There is also the participation in Digital Opportunity pilot scheme (EC) that focuses on skills, traineeships for young people, etc. The EHR4CYBER network increases the visibility and the concrete actions for the European human resources in cybersecurity. The analysis paper contains the best practices and recommendations, as well as the mapping for a European framework for education and competences (matching profiles and skill-sets) that will lead to the Cyber Security Professional certification. Additionally, the EHR4CYBER network is envisaging the creation of an online jobs marketplace.

The ECSO WG5 on cyber ranges is an ECSO internal survey conducted to assess cyber range capabilities and motivations and therefore a series of cyber range workshops were initiated in collaboration with the European Defence Agency (EDA). They organized the following workshops :

- 16-17 October 2018 in Brussels, in order to align with EDA on cyber range approaches and agree on a baseline for continued collaboration, focusing on opportunities and motivations for a federated approach.

Established links between the private sector (industry and research) and EDA (Member States), with around 50 attendees (33 from ECSO members).

- Spring 2019 in Tallinn (date to be determined), in order to define federated cyber range approach, looking at an industry-wide framework or guidelines, governance, etc.
- Autumn 2019 (location and date to be determined), in order to test the federated cyber range approach with one or two use cases and conduct a small cyber drill.

The main conclusions from the position paper on gaps in European Cyber Education and professional training are listed here:

- The Commercialization of higher education, including the rising cost of education and growing number of students will soon lose students to affordable and widely accessible MOOCs. Online courses scale better and can sometimes offer the same level of knowledge at a cheaper price.
- We are not producing enough skilled experts that the industry is desperately looking for. To satisfy the growing demand for skilled cyber security professionals, we need to:
  - Expand educational opportunities at all levels
  - Increase the number of qualified educators
  - Create synergies between educational paths and training possibilities at the workplace
  - Reach the skilled unemployed and displaced workers (workers who are not happy with their current profession)
  - Create the fundamentals for lifelong learning in cyber security
- We also need to ensure gender diversity and inclusiveness of cyber security education and training, to inform and encourage girls and women to engage into cyber security careers.

To achieve this, a working cooperation is needed between academia and industry which utilizes and combines their available resources to ultimately strengthen the cyber domain together.

Concerning the ECSO Women4Cyber Initiative, it was launched on 22 January 2019, under the patronage of Commissioner Mariya Gabriel. 30+ high-level female leaders in Europe as Founding Members from politicians and policy makers, to top management leaders from the private sector and academia, working together to: encourage women's involvement in cyber security across EU; go beyond awareness and networking; develop a concrete agenda to meet the demand for cyber security professionals in Europe; support the creation of a sustainable and inclusive cyber ecosystem.

The European Commission proposal for Digital Europe Programme (June 2018) includes: Supercomputers, Artificial intelligence (AI), Cybersecurity and Trust (2-billion-euro investement), Digital Skills (700 million euros), wide usage of digital technologies across the economy and society.

4.3.3.2 Presentation on gap of cyber experts and skills in Japan Cybersecurity industries: Introducing Cyber Risk Intelligence Center, Cross Sectors Forum Miho Naganuma, NEC Corporation

The next presentation by Miho Naganuma initially presented the CRIC Cross Sector Forum, initially launched in 2015, with more than 40 companies mainly from 14 critical Infrastructure Industries (finance, airline, railway, power, energy, etc.).

The current situation is that Japan will be short of 193,000 cybersecurity professionals in 2020 and the Japanese Business Federation declared that it is urgently crucial to increase the number of such professionals. The uniqueness of Japanese Business is because of the following factors: lifetime employment, more IT/SC outsourcing and multi-hat CISOs.

The activities that have been accomplished are a monthly plenary meeting, a 4-monthly working group defining and developing the workforce, sharing information and collaborating with the academia, an annual conference for CISOs and a participation in cybersecurity discussion with the government. The output is an activity report and the tools of talent definition, the outsourcing guideline and the CISO calendar. The future plan includes a security summit to further improve the industrial awareness, a corporate cybersecurity case collection/research, in order to collect more concrete examples and conduct a practical case study and finally a WG activity that will help in the information linkage, the knowledge sharing and the cybersecurity corporate strategy WG.

4.3.4 Information sharing challenges

4.3.4.1 Multiscale approach to information sharing activities: The use case of the Basque Cyber Security Centre

The next presentation by Javier Dieguez from the Basque Cybersecurity Centre started with the scope of the Centre, which was created in October 2017 within the Basque Agency for Business Development (SPRI). Its main scope function includes: development, education, security/police, eGovernment, investment, research network and entrepreneurship, with the number one priority being the Basque Industry. Within the economic development scope, they are cooperating and sharing with ECSO, GlobalEPIC, CSIRT, FIRST [6], TF-CSIRT and CSIRT.es.

The Basque Digital Innovation Hub [7] is part of the Digital Innovation Hubs Catalog, created by the European Commission [8] and gives the opportunity to foster interregional collaborative projects and create a European network of DIHs. Additionally, they aim to develop cyber exercises for cyber management with dual vocational training programmes, adapted to the specificities of the local industry, a post-degree Cybersecurity Programme, recycling and reorienting, awareness raising in the usage of digital devices and finally talent search and attraction.

The Basque Country has been recognized among 171 Agencies worldwide in the Strategy Awards 2018 by the Financial Times (also attached "fDi Strategy Awards 2018"), in different categories:

- First-Prize winner in "Aftercare" category. This category is about the relationship of the Government with companies (foreign capital) established in the Region.
- First-Prize winner in "Start-ups and SME support" category, because of the Acceleration Program Bind 4.0.
- Second-prize Winner in "Incentives" category. Incentives to Research, Development and Innovation have been the most remarkable.
- Second-prize Winner in "Project of major interest by an Agency of Investment Attraction".

The present agenda of CSIRTs includes the collaboration with local agents to identify their real internet perimeter and adjusting reputational rating with vendors, to join hands with ISPs present locally to sensor and analyze sectoral threats to core industry (advanced manufacturing, energy and biosciences), regional government and critical infrastructures. This includes locally: the connection with the MISP of CSIRT.es; the collaboration Agreement with PuntuEUS Foundation and internationally the connection with the MISP of FIRST; the possibility of accessing different working groups in FIRST and EUROPOL; and finally sharing information with ShadowServer, regarding the IP Space of the Basque Country.

4.3.4.2 Global Cooperation: Perspectives of Incident Response Practitioner

The last presentation of the workshop on "Global Cooperation: Perspectives of Incident Response Practitioner" by Koichiro Komiyama, from Japan

[6] https://www.first.org/

[7] http://www.spri.eus/es/basqueindustry/basque-digital-innovation-hub/

[8] http://s3platform.jrc.ec.europa.eu/digitalinnovation-hubs-catalogue

Computer Emergency Response Team Coordination Center (JPCERT/CC) referred to the history of Morris worm on the 2nd of November 1988, where 60K PCs were connected to the Internet and 65% were infected. After this incident, the CERT/CC was created on the 17th of November 1988.

There are currently 1500 CSIRTs, with 300 in Japan. The CSIRTs mission is to provide a single point of contact (POC), assist the constituency and community in preventing and handling computer security incidents, share information and lesson learned with other CSIRT/response teams and appropriate organizations and sites. The Reported Incidents for the period of April 2017 till March 2018, included 18,141 incoming reports, 18,768 incoming incidents and 8,891 coordinated incidents.

There is a wide range of cooperation (per CCTLD) with 130 coordinated countries, during the last 7 years, including US, China, Hong-kong, Germany, Taiwan, Brazil, Singapore and France.

Koichiro Komiyama also presented the Normative approach, which states that countries should not conduct or knowingly support activity to harm the information systems of CSIRTs in other States and that States should not use CSIRTs to engage in malicious international activities.

The future shows that information sharing among CERTs/CSIRTs will become harder and the key to overcome this challenge is the shared value and the individual trust.

4.3.5 Closing discussion on potential cooperation & next steps

The last subsection of the workshop included the closing discussion points, regarding cooperation and future steps. Initially, Hervé Debar from EUNITY project, provided information about EUNITY, the questionnaires and the possibility of a workshop in Japan (in April - May). He also required, regarding the questionnaire, to provide additional information and important feedback and views, e.g., which areas would be more useful to develop. It was also mentioned that there is a lack of experts. He also set the question of how MOOCs should be used in the future and not compromise the quality of the education. Someone from the audience replied that instead of focusing on too many books, someone could just go for a MOOC. It can be thought of a complement. It is also good to have webinars and these should be on top of the existing schemes. It is something that could exist as complementary of what we already have.

Hervé Debar added that it can be used to solve some practical problems, but it does not magically solve the main problem.

A representative from EC added that this is an opportunity for JP participants to contact EU members. The European Commission would like to see specific actions and recommendations in the last deliverable of the EUNITY project. There are some common interests but they need specific recommendations that should come from the project. There are examples that we are working on e.g., ISACs, certification, but there is a need for input. A Japanese representative added that it is a great experience working with all the members of the project. Common values were shared between Europe and Japan and having an exchange programme is really beneficial. The CSIRT network is well connected but this connection is sometimes missing in other industries, cybersecurity businesses and the general industries. The world is connected, but most industries are working in isolation, although connected to the Internet. This is a general concern to ECS0, EU and Japan: how to support this network of trust at an international level?

Hervé Debar added that within ECSO (WG6), they are also looking at other PPPs (factory of the future or energy). Basically, anything can be controlled by digital technologies, so if the business/sectoral impact is increasing, then it is important to take those recommendations since ICT is driving things fast.

A Japanese representative referred that this is a historical meeting because ECSO members met Japanese federation. He invited other associations to come and join. This is an open invitation from the EUNITY project to private associations to think broad and join.

Someone from the audience added that research collaboration has been easier than the past years. It has become possible to discuss cybersecurity and the cross-border issues, e.g., ECSO has dedicated WGs that look at different strategies in Japan, US (AEGIS project), the PICASA project and also discuss with people from Brazil about IoT and what is important to do in such systems. Collaboration is now active in the research area, and there is also another group of collaboration about standards (market/business oriented) which holds bilateral discussions between companies. It is agreed that it is important to facilitate the initiation of the flow of information and put all communities together.

Finally Hervé Debar added the closing remarks for the second EUNITY workshop.

4.4 Questionnaire results

A questionnaire was issued to the participants of this second workshop. By the end of the workshop, 29 responses were obtained. A large majority (19) of the respondents are from Europe, with only 6 from Japan, and 4 working for a Japanese organization in Europe. Moreover, among the 21 respondents who indicated their affiliation, 13 come from industry, while only 1 is working for the government.

Regarding the cybersecurity directions that are considered the most relevant at the respondents' institution, a few topics appear to stand out: Cybersecurity in IoT was cited as most relevant by 21 respondents, Cybersecurity in Critical Infrastructures by 20, operational cybersecurity by 19, CTI and threat analysis by 18, AI and cybersecurity by 17, Education, awareness and training by 16, and cybersecurity in Cloud Computing by 15. The three topics that appear to be the least relevant according to the respondents were social networks, cited as not relevant by 13 respondents, Network and routing security and hardware security, both cited by 7 as not relevant. Finally, one respondent from Japan suggested two other relevant topics: supply chain security and cybersecurity from SMEs.

On the legal and policy aspects, the respondents unanimously agreed that a common policy and legal framework would help in information exchange and joint work in industry, 24 of them even were considering it very useful. Moreover, no respondent indicated that legal and policy constraints would bring major issues in the cooperation between the police from Europe and Japan, while 7 of them were confident enough to state that perfect cooperation could be established. Regarding the need for further regulation, most respondents (18) thought that it is only partially adequate, whether at the national or the international level, while respectively 7 and 6 respondents were convinced that it is adequate. About current information sharing mechanisms, 19 respondents thought they are partially adequate at the national level, and 16 at the international level. However, respectively 7 and 12 respondents were convinced that they are not adequate. Several recommendations on international collaboration were provided by the respondents. Many suggestions were related to dialogue improvement, the standardization of common exchange formats, the need for more workshops for discussions about collaborations with possibly a larger audience spectrum, or the definition of quick response procedures and automation. One reply also pointed out the need for a high-level entity to centralize needs and seeds of Europe for interacting with Japan, one raised the idea of a common grant for collaboration and one suggested to work on the network of trust (e.g. building from the national CERTs).

Regarding certification, all but one respondents were convinced that a common scheme for certification and patents between Europe and Japan would be useful for improving cooperation. Likewise, 25 of the respondents indicated that IoT devices require such certification scheme. Several recommendations were also provided. The main suggestions were related to the idea of establishing a first and easy to reach certification level, the need to build common schemes or at least mutually recognized schemes, and the need to take specific measures for IoT devices like fast certification, or schemes similar to safety certification. The need to prevent excessive costs was also pointed out, as well as making sure that the schemes are applied. Finally, only 2 respondents stated that a common privacy framework to facilitate personal data exchange would be useless, whereas 26 of them were convinced it would be useful, among which 17 deem it to be very useful.

On research and innovation aspects, all respondents agreed that current opportunities for fostering collaboration do not cover all areas of cybersecurity. All respondents also agreed that joint education programmes would be beneficial to collaborations between Europe and Japan, among which 21 even indicated that it would be very beneficial. The vast majority of respondents were clearly in favor of the creation of a joint portal for sharing information about research and innovation, 15 of them stating that it would be very useful, 12 of them saying that it would improve collaboration, and only one respondent indicated that it is not necessary. Lastly, 22 of the respondents thought that the cybersecurity training in universities from Europe and Japan is insufficient, while 6 of them thought it is average.

Regarding industry and standardization aspects, 16 respondents thought that the industry market in Europe and Japan would benefit from a common cybersecurity framework, while 11 indicated it could be useful, and only one respondent thought it is not necessary. To the question whether SMEs have access to current cybersecurity tools in Europe and in Japan, 13 respondents thought they have access to only some of the tools, while the remaining 15 respondents felt there are difficulties to access these tools. Finally, all the respondents agreed on the fact that a common roadmap in Europe and Japan for ongoing international standardization would be useful, 18 of them were convinced that it would even be very beneficial.

A

Appendix: Questionnaires

Below is the empty form of the questionnaire.

2nd EUNITY Workshop – Questionnaire

The objective of the questionnaire is to gather your feedback on potential policy recommendations that the EUNITY project could formulate to the European Commission in may 2019. These leads have been drawn from EUNITY deliverables D3.1 and D4.1. Feedback is acknowledged and welcome. Feel free to provide any further feedback to herve.debar@telecom-sudparis.eu and/or info@eunity-project.eu.

You are :

□ In Europe □ In Japan □ In Europe for a Japanese organization

□ Government official □ Enterprise or representative of industry □ other

1. Which of the strategic cybersecurity directions at your institution are considered the most relevant (feel free to add your items)?

strategic cybersecurity directions	**most relevant**	**relevant**	**not relevant**
Cyber Threat Intelligence and threat analysis			
Data analytics for cybersecurity (including big data, high performance computing, visualization)			
Operational cybersecurity (incl. info sharing and tools for CSIRTs)			
Cybersecurity education, awareness and training (incl. Cyber Ranges)			
Data processing, privacy and identity management (incl. authentication/authorization)			
Artificial Intelligence and cybersecurity			
Network and routing security			
Cybersecurity in IoT			
Cybersecurity in Cloud Computing			
Cybersecurity in critical infrastructures			
Legal/policy aspects of privacy, cybersecurity and cybercrime			
Hardware security			
Social networks			

Cybersecurity legal and policy

2. Do you think a common policy and legal framework for EU and Japan would help in improving information exchange and joint work in industry?

□ Very useful □ Useful □ Not useful

3. Do you think EU and Japanese police and law enforcement would be able to cooperate at high level due to legal and policy constraints?

□ Perfect cooperation □ Some issues for cooperation □ Major issues for cooperating

4. Do you consider that further regulation is needed:

At your national level: □ Adequate □ Partially adequate □ Not adequate

At the international level: □ Adequate □ Partially adequate □ Not adequate

5. Do you consider that current information sharing mechanisms are,

At your national level: □ Adequate □ Partially adequate □ Not adequate

At the international level: □ Adequate □ Partially adequate □ Not adequate

6. What are your recommendations on international collaboration ?

____

____

7. Do you think a regulatory common scheme for certification and patents between EU and Japan would be useful for improving work and cooperation?

□ Very useful □ Useful □ Not useful

8. What are your recommendations on certification ?

____

____

9. Do you think that that IoT (Internet of Things) devices require such certification scheme? □ Yes □ No

10. Do you think a common privacy framework between Europe and Japan that could facilitate personal data exchange would be...

□ Very useful □ Useful □ Not useful

Research and innovation (R&I)

11. Do you think the current research and innovation opportunities are enough for fostering collaboration between EU and Japan in the different areas of cybersecurity?

□ Good support in all areas □ Some areas are not covered □ Difficulty to find opportunities

12. Do you think joint education programmes (exchange of students, training, etc.) would be beneficial for improving collaboration of work between EU-Japan?

□ Very beneficial □ It could be useful □ Not necessary

13. Would you support the creation of a joint portal for sharing information about R&I?

□ Very useful □ It could improve collaboration □ Not necessary (already enough support)

14. Do you think universities in EU and/or Japan provide enough cybersecurity training?

□ Provide many courses and training □ Cybersecurity training is normal □ Not enough training

Industry and standardization

15. Do you think the industry market in EU and Japan would benefit from a common cybersecurity framework?

□ Very beneficial □ It could be useful □ Not necessary

16. Do you think SMEs have access to current and necessary cybersecurity tools in EU and/or Japan?

□ They have many possibilities □ They can access some solutions or markets

□ Difficult to access solutions and markets □ They need to work in their own solutions or adapt

17. Do you think developing a common roadmap in EU and Japan for ongoing international standardization...

□ Very beneficial □ It could be useful □ Not necessary

B

Glossary

Name	Explanation
AoI	Area of Interest

Name	Explanation
CIMA	Cybesecurity Industry Market Analysis
CYDER	CYber Defence Exercise with Recurrence
ISAC	Information Sharing and Analysis center
LSEC	International IT & Information Security cluster, Leuven
MIC	Ministry of Internal Affairs and Communications
NICT	National Institute of Information and Communications Technology
NICTER	National Institute of Information and Communications Technology
ECSO,	EBF, AFME, CEPS ECSO, EBF, AFME, ENISA, SSVA, JP MORGAN and Rabobank,