Cybersecurity and privacy dialogue between Europe and Japan

Cybersecurity Research Analysis Report for the two regions

Marek Janiszewski (NASK)

Objectives

- Establishing a clear picture on the cybersecurity and privacy domain in both regions by analysing existing regulations, standards, projects, programs, roadmaps, etc.
- Analysing the cybersecurity priorities in both the EU and Japan

in order to produce a **background document** on the status and **priorities** of cybersecurity and privacy **research and innovation** activities in Europe and Japan

The scope

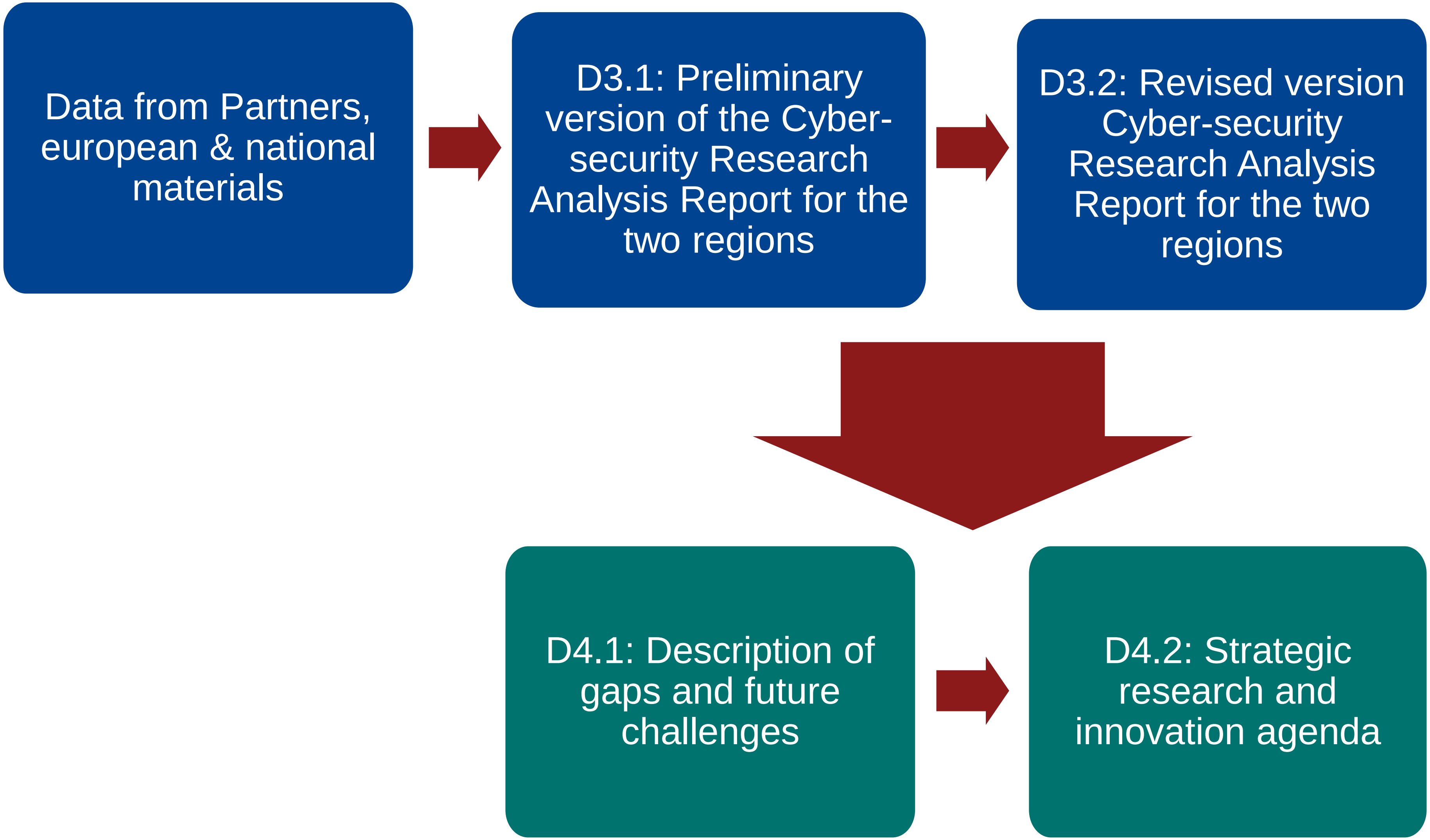
- Identification and description of the mechanisms used to finance research and innovation
- An overview of the main research directions in the field, identification of the strong and weak points in the both regions to indicate:
  - topics of common interest, where cooperation opportunity is clear
  - topics where some aspects are covered asymmetrically, allowing greater synergy
- Analysis of the current role and activity of different units (SMEs, research institutions, CSIRTs, etc.) in research and innovation in Europe and Japan to find:
  - possible asymmetries increasing the value of possible cooperation
- Analysis of long-term research programs at the national and international level
  - to find thematic parallels between the EU and Japan which may create opportunities for either co-financing of joint EU-Japan projects or at least synchronization of efforts enabling cooperation

Remarks

- The document is mainly a set of data, whereas a detailed analysis and drawing conclusions is implemented in other documents of the project
- The purpose of the analysis is only to indicate the most visible similarities and differences

- The document **3.2 - Revised version of Cybersecurity Research Analysis Report for the two regions** is updated and upgraded on the basis of the document **3.1 – Preliminary version of Cybersecurity Research Analysis Report for the two regions**

Data flow



Data from Partners, european & national materials

D3.1: Preliminary version of the Cyber-security Research Analysis Report for the two regions

D3.2: Revised version Cyber-security Research Analysis Report for the two regions

D4.1: Description of gaps and future challenges

D4.2: Strategic research and innovation agenda

Cybersecurity Research Analysis Report

1. Introduction

2. Legal and Policy Aspects

3. Research and Innovation Aspects

4. Industry and Standardization Aspects

Legal and Policy Aspects

Legal and Policy Aspects

2.1 Executive summary

2.2 The European landscape

- Privacy and data protection
- Cybersecurity

2.3 The Japanese landscape

- Privacy and data protection
- Cybersecurity
- Japan and the European Union: comparative aspects on privacy and data protection

2.4 Conclusions

- Summary of challenges and gaps
- Policy blockers

Legal and Policy - conclusions

Fundamental regulation acts in the area

	EU	Japan
Privacy	GDPR	Japanese Privacy Law
Cybersecurity	NIS	Japanese Basic Act on Cybersecurity

Similiarities and differences

- Privacy: the two frameworks are not perfectly matching
  - the concepts of sensitive personal data and some practical implications might become a critical point for both Japanese and European businesses and organizations wanting to enter each other's digital markets
- Cybersecurity:
  - **differences** might be spotted in the laws of the two
  - **similarities**: there is room left by both policy and legal frameworks allowing EU, Member States and Japanese Government to engage in international cooperation

Research and Innovation Aspects

Research and Innovation Aspects

3.1 Mechanisms to finance cybersecurity research

3.2 The main research directions in the field

3.3 The strong and weak points

3.4 Common interests between the EU and Japan

Mechanisms to finance cybersecurity research

3.1.1 In the European Union

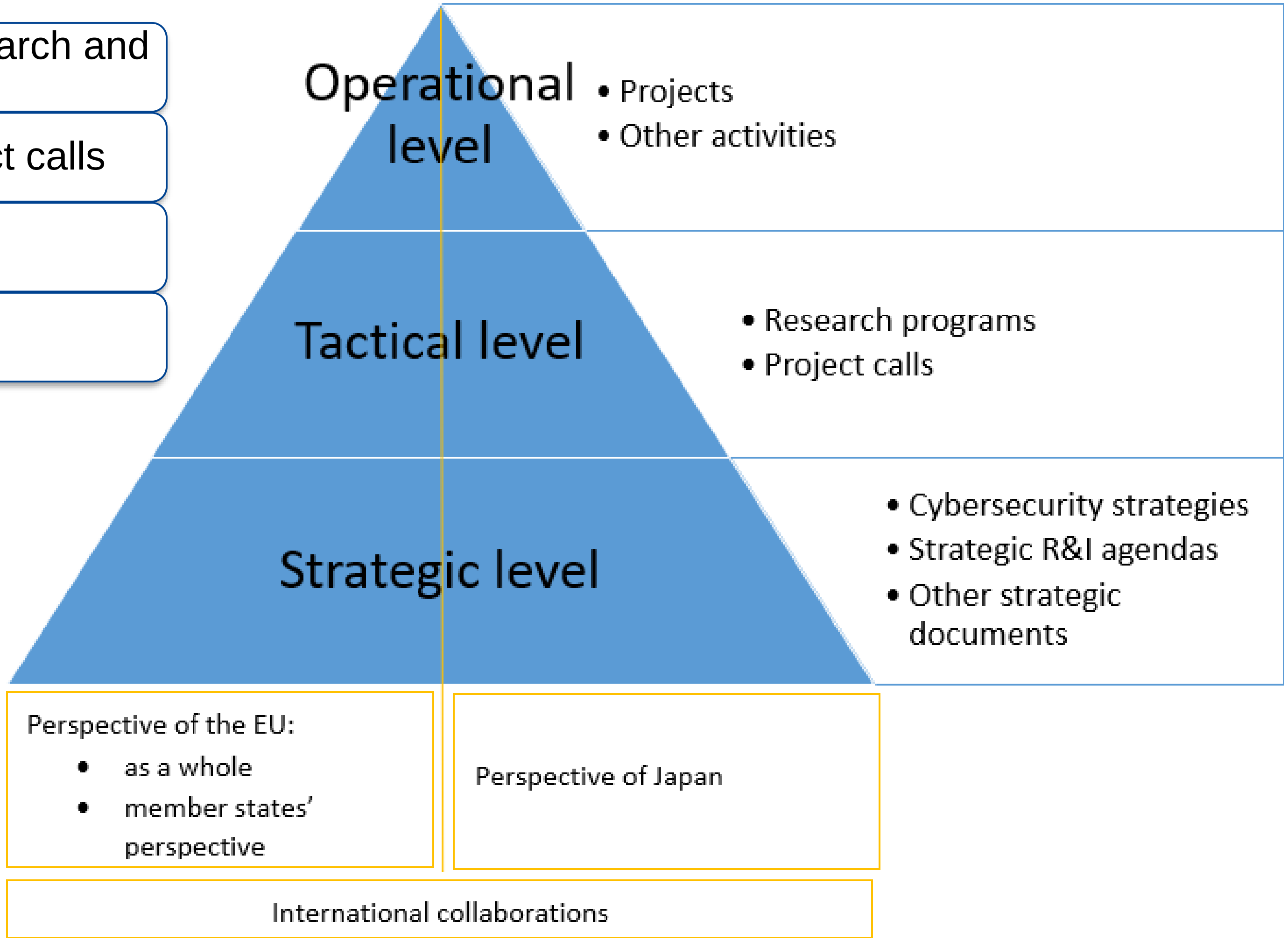
- European Programmes (e.g. H2020, CEF, etc.)
- National financing mechanisms - analysis using project partner's countries (France, Greece, Spain, Poland, Belgium) as a sample
  - National programmes
  - Mixed (national and international funds)
  - Own commercial activities (patents, services)

3.1.2 In Japan

- Various funds provided by the government

The main research directions in the field

- Strategies and Research and Innovation Agendas
- Programs and project calls
- Projects
- Other activities



Operational level

- Projects
- Other activities

Tactical level

- Research programs
- Project calls

Strategic level

- Cybersecurity strategies
- Strategic R&I agendas
- Other strategic documents

Perspective of the EU:

- as a whole
- member states' perspective

Perspective of Japan

International collaborations

Strategies and Research and Innovation Agendas

European top-level strategic documents

- Digital Single Market (DSM) Strategy
- Cybersecurity strategy of the EU

Strategic Research and Innovation Agenda

National cybersecurity strategies in the EU Member States

National strategy in Japan

Programs and projects

- project calls
  - Horizon 2020
  - national project calls
- projects
  - national and international roadmapping projects
  - selected projects in the area of cybersecurity
  - pilot projects: CONCORDIA, ECHO, SPARTA, CyberSec4Europe
- other activities

The strong and weak points

Strengths	Weaknesses
Establishment of the cybersecurity strategy • Review of the strategies **Declared focus on cybersecurity and privacy** • Review of the strategies • Questionnaires • Own observations	**Opposition between industry and research** • Questionnaires • Own observations **High-level cybersecurity's personel shortage** • Questionnaires • Own observations **Lack of coordination of research actions on various levels** • Questionnaires • Review of projects and programs • Review of financing mechanisms • Own observations **Lack of strong global cybersecurity enterprises and solutions originating in the EU and Japan** • Questionnaires • Own observations

Common interests between the EU and Japan

Main strategic directions in institutions	• Questionnaires
R&I cybersecurity priorities and current directions	• Review of strategies • Own observations
Identification of threats	• Questionnaires • Own observations
Examples of current collaborations	• Questionnaires • Review of projects and programs • Own observations
ICT areas which need collaboration between EU and Japan	• Questionnaires • Review of strategies, projects, programs • Review of financing mechanisms • Own observations
Areas which need the most collaboration	• Questionnaires • Own observations

Main strategic directions in institutions 1/3

cyber threat intelligence

- high performance data analytics for cybersecurity
- operational security including tools for CSIRTs
- information sharing
- cyber attack visualization
- threat analysis

education, awareness and cyber range

- cybersecurity education and training
- security awareness training
- security testbed (cyber range)

data processing and privacy

- privacy and identity
- big data

Main strategic directions in institutions 2/3

methods to enhance cybersecurity

- Artificial Intelligence for cybersecurity
- High Performance Computing for cybersecurity

security services

- authentication/authorization
- digital certificate-based authentication infrastructure

network security

- routing security
- file sharing methods

Main strategic directions in institutions 3/3

cybersecurity in various domains

- IoT and cybersecurity in IoT
- Cloud Computing and cybersecurity in the cloud,
- cybersecurity in critical infrastructures
- legal/policy on IT, IP, privacy, cybersecurity and cybercrime
- hardware security
- cloud computing
- social networks

other

- cybersecurity technologies usable for the 2020 Tokyo Olympics

R&I cybersecurity priorities and current directions

- risk management and critical infrastructure protection
- cybersecurity in various technologies
- threat detection and threat intelligence
- cryptology design, techniques and protocols
- network security
- hardware and systems security
- cybersecurity measures at the Tokyo Olympic Games in 2020

Identification of threats

- malware
- APT
- cyber terrorism
- network threats
- lack of integration/cooperation between CERTs,
- poor cyber literacy,
- cyber attacks for critical infrastructure,
- quantum cryptanalysis
- specific threats against various technologies
- data theft
- social engineering

Areas which need the most collaboration

education and awareness

- education on various levels
- enhancing security awareness
- development of human resources
- promoting the exchange of personnel

standards and regulations

- harmonization on standards and regulations among government and industrial associations
- guidelines by industry sector
- sharing best practices regarding cybersecurity

information sharing

- sharing environments to monitor attacks
- sharing security intelligence among security vendors/organizations
- continuous information feeds on web sites, e.g., blogs or whitepapers
- continuous exposure in conferences/exhibitions
- continuous workforce activities

Industry and Standardization Aspects

Industry and Standardization Aspects

4.1 Industry activity around research

- Methodology
- Associations and clusters at EU level
- Associations and clusters in Japan
- Associations and initiatives at member states level

4.2 Common topics of interest

Industry landscape

- Study based on:
  - EU-wide industry associations

Area	EU	Japan
Industrial policy	ECSO, EOS, others	Keidanren
Big Data	BDVA	VLED
Communications	5GPPP	5GMF
Network	NESSI, ECSO	JNSA

  - Stated priorities/interests
    - long term trusted ICT infrastructure
    - computer intelligence in security management
    - privacy in big data
    - cybersecurity in safety
    - Security as a Service

Summary of common industry aspects

- Two key areas of industry-led research around cybersecurity in EU & Japan
  - Big Data
  - 5G

- Common industrial research interests:
  - privacy of big data
  - availability and reliability of open data
  - security of 5G communication networks and protocols

EUNITY

Thank you for your attention

marek.janiszewski@nask.pl