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

## D4.1 Description of gaps and future challenges: †

**Abstract**: The EUNITY project addresses scope 2 (international dialogue with Japan) of objective DS-05-2016 of the H2020 work programme. This two years project aims at developing and encouraging the dialogue between Europe and Japan on cybersecurity and privacy topics. This deliverable, using D3.1 as basis, analyses existing and potential challenges in cybersecurity where relevant opportunities and strategies can be shared between Europe and Japan. It formulates a preliminary set of topics in which EUNITY can engage the community further, and align these topics with the work of the scope of the European research activities.

| | |
|---|---|
| Contractual Date of Delivery | 31/11/2018 |
| Actual Date of Delivery | 14/12/2018 |
| Deliverable Security Class | Public |
| Editor | Atos Spain SA |
| Contributors | All *EUNITY* partners |

† The research leading to these results has received funding from the European Union H2020 Programme under grant agreement № 740507.

| | |
|---|---|
| Quality Assurance | Gregory Blanc, Marek Janiszewski |

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 |

# 1 Introduction

The EUNITY project has three main missions: to develop and encourage the dialogue between Europe and Japan on cybersecurity and privacy topics, identify potential opportunities for future cooperation and facilitate constructive collaboration of organizations in both areas.

Therefore, the main objective of this deliverable to describe the status and gaps of cybersecurity challenges in Europe and Japan and describe possible collaborations in the areas of legal, research and industry.

This document uses as basis D3.1, which presented an initial description of the different areas covered here: legal, policy, innovation, industry and standardization. Additionally, this deliverable formulates a preliminary set of topics in which EUNITY can engage the community further and align these cybersecurity topics such as ECSO and Cyberwatching.

Regarding the results obtained in the document, on the one hand the document presents a review of the existing cybersecurity challenges in both regions, focusing in the areas abovementioned: policy, research and industry. On the other hand, which is consider as a key point in this analysis, it identifies and analyzes opportunities for cooperation between EU and Japan, including reasons about why this cooperation is necessary and beneficial aspects for both Europe and Japan.

In order to present all this information in a proper way we have divided this deliverable in several sections, each one with a different focus. The sections are:

Chapter 2 (“Methodology”) describes the methodology we have followed for achieving the objectives and purpose of this document, including the mentioning of other CSA´s, their objectives and relation with EUNITY.

Chapter 3 (“Cybersecurity challenges in Europe”) focuses on the description of the three main sectors of cybersecurity (policy, research and industry) in Europe.

Chapter 4 (“Cybersecurity challenges in Japan”) focuses on the description of the three main sectors (policy, research and industry) in Japan.

Chapter 5 (“Cooperation opportunities”) describes the possible cooperation opportunities, and analysis of the commonalities between EU and Japan derived from the previous sections.

# 2 Methodology and knowledge sources

The development of this report about the challenges, gaps and possible collaborations among EU-Japan is a joint work that aims to cover not only different areas such as Europe and Japan but also different topics of cybersecurity: legal and policy, research and innovation and industry. We think using this structure for identifying the needs and collaboration opportunities in cybersecurity covers all the needs and opportunities we identified in D3.1. More specifically each of the topics aim to cover:

- Legal and policy: identification of policies and legal issues of data management, users, etc. legal bodies, law enforcement agencies, etc.
- Research and innovation: description of the areas for research mainly used in research centers, universities, public research and innovation centers, etc.
- Industry: identification of the needs and works in the context of cybersecurity, which was done by focusing in the needs and work of cybersecurity done in companies, industry bodies, technology-oriented areas of application, etc.

Therefore, using this structure, we defined a methodology for analyzing and researching the cybersecurity areas both in Europe and Japan that could facilitate the identification of their needs and collaborations. Additionally, the knowledge sources used for eliciting the requirements and challenges are very important in order to demonstrate the achievements and results we obtained. They are based in real work done by other European or Japanese organizations, public and private, for identifying needs and work in the area of cybersecurity. So, in the following subsections we describe the methodology we used for preparing this document and next a description of the knowledge sources used, which can be found in its full extension in the references of the document. In order to facilitate their access we included them as footnote so the information we used for eliciting the knowledge and describing challenges, recommendations, collaboration opportunities, etc. is very easy to access.

## 2.1 Methodology

In order to create this report the team of EUNITY, formed by members of different organizations and with cybersecurity expertise in legal, research and industry areas used the following information as the basis for start studying the current situation in Europe and Japan and define the best approach for the joint work:

- Use as basis the previous document D3.1 “Preliminary version of the cybersecurity Research Analysis Report” for the two regions. This was very important for the basis of current gaps and challenges that were identified early in the project.
- Partners from Europe and Japan defined the areas in which they would focus for analyzing the challenges and possible collaborations according to their expertise. For example KUL focused in the legal part, FORTH in the research area and ATOS in industry. NAIST collaborated with several entities in Japan for covering all the different cybersecurity areas of application due to its contacts and knowledge of specific Japanese partners.

Once this basis steps were completed we had a joint discussion about the methodology we could follow in order to align all the work in the different areas (Europe and Japan) and have all the possible information for the joint one: collaborations. The process is shown in Figure 1 and is the result of several iterations that were necessary for adapting the needs and work of the different partners of the project.

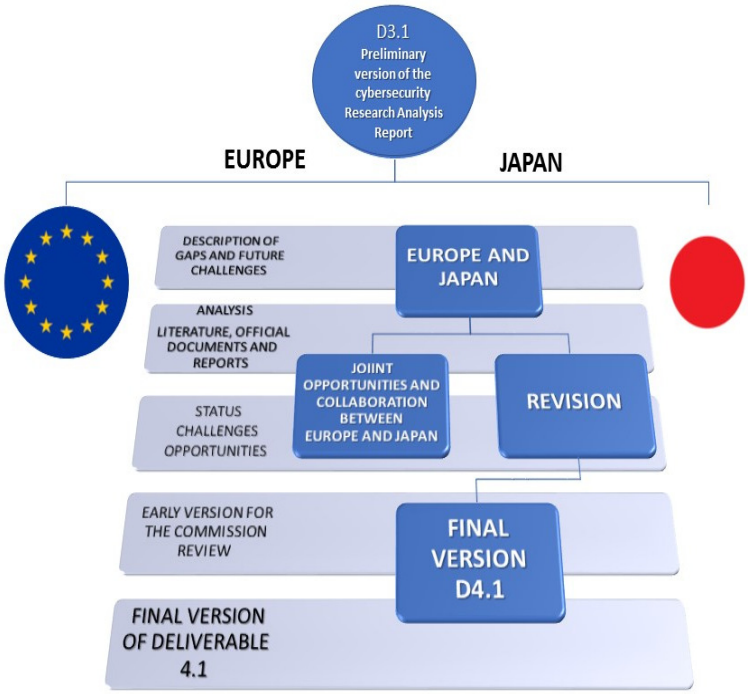


Figure 1. Methodology followed for the creation of this report

As we can see in the figure, the basis was D3.1 and the knowledge of the partners about the expertise they would focus in the report. The next step was to start working in an extended and improved version of the description of gaps and challenges in Europe in Japan, but focusing not only in the existing ones but also the future ones that are foreseen in both areas. This allowed us to not only describe the current possible collaborations (short term) but also the ones that will be possible in a medium-long term. The identification was done in the three areas in parallel: legal and policy, research and innovation and industry. Once we have an initial, and mature enough version, we did an analysis of them in order to provide feedback using our knowledge of cybersecurity. Being a cross-cutting issue, we all were able to provide valuable feedback for supporting in the identification of core areas.

As abovementioned, the identification of critical areas of cybersecurity in each sector was key to be fulfilled at the beginning of the process. Cybersecurity is a very wide area that affects technologies, businesses and legal topics. In each of the areas we identified several topics that are key and then extracted the ones we understood were the more important ones based on criticality, area of application, impact in Europe-Japan, adoption of new technologies, resilience, importance in the countries of Europe and Japan, size of the market, etc. The areas presented in the following sections are the ones that following this study we found more important for collaborations between Europe and Japan in each of the domains of application.

The next step was to start compiling, and analyzing, the knowledge material we were going to use for this work. For each sector we analyzed different sources such as reports of the European Commission and Japanese ministries, research journals and papers, whitepapers of cybersecurity, documentation about previous analysis of cybersecurity challenges, studies about future critical cybersecurity topics, etc. All this material is referenced in each of the sections and can be found at the end of the report. As

mentioned, the knowledge material used ranges from study of policies in Japan for artificial intelligence to challenging cybersecurity threats of the energy.

Once we had all the information analysed we prepared the report of the gaps, challenges, conclusions and recommendations in Europe and Japan. This was done in parallel for all the sectors in order to have an initial list of cybersecurity topics in short, medium and long term. This work was analysed by the partners of the project in order to align ideas and key areas of interest. Additionally, doing it for both regions allowed us to have very early an idea of the more important aspects in both Europe and Japan. Next, using this information as basis, we identified the joint work for recommendations of collaboration Europe-Japan. We did this in several iterations, starting with an initial view from Europe, completing it with the feedback from Japan and repeating till we had a good understanding and alignment of the collaborations. Additionally, we checked that this list of possible collaborations fulfilled the needs and challenges of the previous sections, so we could be sure the results presented were adjusted with the requirements of cybersecurity in Europe and Japan.

Finally, the document was provided for review for all the partners so we could check the work presented was a good representation of the challenges, recommendations and collaborations of the key cybersecurity topics in policy, legal, research, innovation and industry areas. The reviews helped us to improve the quality of the document, identifying the basis for the future research and innovation agenda of cybersecurity for Europe and Japan, which will be used in both areas for, hopefully, create more opportunities of joint work and increase results and adoption of cybersecurity.

## 2.2 Knowledge sources

For each of the three different areas we used the material listed in the references of the document (available in each section). More specifically, the legal and policy analysis was undertaken with the assistance of mostly three sources of literature review, namely (a) official policy documentation from EU agencies and institutions and non-official bodies (e.g. think-tanks, forums), (b) legal texts (upcoming and existing ones) like the General Data Protection Regulation, Law Enforcement Data Protection Directive, NIS Directive and Cybersecurity Act, (c) legal commentaries from doctrine and scholarship, particularly on AI, privacy and security. The analysis was then complemented by the results of unstructured engagement with cybersecurity professionals in the fields of public sector, private businesses, academia. Specifically, networking and participation to cybersecurity policy events, alongside with dissemination of EUNITY results, offered the chance for active engagement with such players, which enriched the analysis with best practice and sector-specific expertise.

Regarding industry, we used mainly information that could be classified in two different types: a) EU institutions and other governmental bodies (national ones) and b) industry and private organizations. This analysis was enhanced by having meetings with industry experts in the different fields identified as critical and collaborative workshops such as the ones organized by ECSO. Additionally, we analysed the main topics of research of cybersecurity in industry focusing in the areas with bigger future and impact in Europe and Japan. As we identified many areas of application we focused in the ones that are the more important ones due to the business opportunity they bring to companies, size of the market they move and technology adoption in both areas.

For the cybersecurity research and innovation areas the knowledge sources was obtained from (a) official reports provided by the European Union Agency for Network and Information Security (ENISA), (b) official study from European Economic and

Social Committee, (c) reports and press releases from EU' law enforcement agency, (d) official reports and white papers from industry and private organisations, (d) reports and articles from cybersecurity groups and international, nonprofit organisations and (e) CORDIS server and active EU-Japan collaboration projects. It is worth to note, that the following types of documents were used as additional information sources: (a) questionnaires collected during and after the first workshop in Japan, (b) cybersecurity strategies on the national and the EU level, (3) various information of strategies, projects and programs with regard to research and innovation in the area of cybersecurity and privacy collected during the creation of D3.1. We gathered all the topics referenced in the sources above, analysed and composed the main challenges, gaps and recommendation on cybersecurity.

# 3 Existing cybersecurity challenges in Europe

In this section we describe the three areas we are researching for the cybersecurity challenges, conclusions and recommendations in Europe and Japan: i) legal and policy, ii) research and innovation and iii) industry.

Regarding the gaps, challenges, and status we used as basis the information described in D3.1. This was extended here and aligned with the collaborations in both areas (Europe and Japan). This information will be further extended in the future D3.2.

## 3.1 Legal and policy in Europe

The following section focuses on the legal and policy aspects concerning the cybersecurity and privacy landscape across EU. It gives special attention to existing challenges and future issues. In particular, the initial description of the subsections deals with current (short and middle term) gaps and issues, whereas the second part looks at the same topics from a long-term perspective.

### 3.1.1 Status and gaps

#### Cybersecurity as a cross-cutting theme

Cybersecurity and privacy are an increasingly topical and urgent matter. What has been brought to the attention of many expert professionals in such fields is the fact that such a matter is entering the policy discourse at all levels and in all sectors. For this reason, it is pivotal that a common, comprehensive set of stable public policy directions is taken by the European Union, to be thus applied coherently and systematically at all levels of the political agenda. Whilst the European Union still recognizes cybersecurity as a national prerogative, more coordination and high-level instruments are yet still required in order to homogenize need and responses in all fields.

Laws and policies should therefore be aimed at harmonizing the European Union's approach to cybersecurity itself aiming to achieve both a secure single market and a prominent player in the international landscape, inter alia in order to enhance trust across the stakeholder and equalize approaches and responses in the deeply multi-layered world of information and network security.

By ways of example, a unitary European approach to cybersecurity as a policy item in the agenda would help solving the issue explained below with regard, for instance, to the legal boundaries between the military and the civilian spheres in the cyberspace, which are currently both tackling cybersecurity issues, but from potentially different perspective and different solutions.

The following section will unfold a number of topics identified during the research on legal and policy aspects undertaken within EUNITY. The analysis was driven by a number of approaches, unfolding a varied methodology therein. To start with, desk research was conducted on legal and policy papers produced by both decision makers and other interest groups (academia, industry); secondly, focused engagement with relevant stakeholders during our valorization activities (conferences and policy events) helped shaping and understanding the focus that will be outlined below. Finally, a review of the main topics analyzed in such events has confirmed the need for further research on the scenarios below.

For each of the policy scenarios enlisted below, two elements are identified and clustered in two separate sections (respectively, 3.1.2 and 3.1.3). Firstly, current and

future challenges arising from such scenarios (3.1.2). Secondly, policy recommendations aimed at addressing such challenges are provided in section 3.1.3.

The abovementioned scenarios that will be unfolded below are hereby enlisted:

- Software vulnerabilities
- The need for a pan-European institution on cybersecurity
- Cyber Defense: enhancing cooperation with third parties
- Harmonization of criminal law provisions
- Harmonization of criminal law treaties
- Improving police cooperation
- Regulatory certainty for certification schemes
- IoT security and crime
- AI crimes and ethical dilemmas
- Capacity building towards member states' public administration
- Capacity building towards neighboring countries and regions

### 3.1.2 Current and future challenges

#### Software Vulnerabilities

Software vulnerabilities is one of the main issues in today cybersecurity landscape[1]. They are invaluable assets for a number of stakeholders, and a considerable threat for others. Vulnerabilities are in fact considered as an inherent component of malware of any sorts.

On the one hand, governmental agencies tend to retain vulnerabilities for a number of legitimate purposes. For instance, they exploit them for defense or national security finalities, as well as for criminal investigations[2]. Cybercriminals have an interest in vulnerabilities, too, as deploying malware or ransomware enables the performance of a great and increasing number of criminal activities, including financial fraud and steal of intellectual property.

On the other hand, having structured regulation on responsible discovering, disclosure and patching of vulnerabilities is crucial for pursuing the need to keep online users and private industries safe.

Against this backdrop, it needs to be noted that the retention of vulnerabilities by public agencies results quite difficult to legislate at the European Union level, due to a number of reasons. To name the most compelling one, many of such processes are considered as falling under the exclusive prerogative of Member States, being it a national security competence.

#### The need for a pan-European institution on cybersecurity

[1] "E-Mail Vulnerabilities and Disclosure - Schneier on Security," accessed September 21, 2018, https://www.schneier.com/blog/archives/2018/06/e-mail_vulnerab.html.

[2] Trey Herr and Bruce Schneier, "Taking Stock: Estimating Vulnerability Rediscovery," *SSRN Electronic Journal*, 2017, https://doi.org/10.2139/ssrn.2928758.

Across the wide array of challenges identified in this report, the role of the European Network and Information Security Agency[3] is a prominent issue. Discussions on such topic seem to have created a governance impasse, which is improbable that will be addressed by the ongoing proposal for a Cybersecurity Act.

As we rapidly enter into the information age, the EU is in high need of an institution that takes the lead in most (if not all) the arising cybersecurity challenges.

Currently the European Union lacks of a comprehensive, structured agency which addresses the following topics coherently, systematically, efficiently and unitarily:

(a) Cyber diplomacy. Currently, diplomatic relations regarding the cyberspace are considered as a new-born discipline, and therefore the existing governance structures are still relying on the well-established offline protocols and institutions. Initiatives have started within the External Action Service of the EU and at Member States level. However, any operational cooperation, as well as executive decisions in the field of cybersecurity, demand for expert negotiations and diplomatic relations.
(b) Policy making on cybersecurity. It is quite clear that the current legal framework[4] establishing ENISA does not absolve this emerging need of a substantial broadening of capabilities, mandate and scope of the agency. On the contrary, to date such laws result quite limitative and reduce ENISA at a more consultative role.
(c) Operational role of the EU in the cybersecurity domain. Currently the EU has a CERT-EU which coordinates cyber-responses to threats against EU institutions. No central coordination with Member States' CERTs is established in its mandate, nor liaison with the abovementioned agencies (EEAS and ENISA) is efficiently satisfactory.
(d) Cyber defense (see below).

The abovementioned layers of action currently lack of common approaches and are derogated to three very different agencies. No allocation of such tasks is mandated to one agency only.

### Cyber Defense: enhancing cooperation with third parties

To date, the cross-border nature of online crimes leads cyber defense to be at a *structural disadvantage* to cyber incidents. The situation inside the European Union is particularly worsened by a twofold reason. Firstly, due to the highly differentiated nature of defense strategies, which are still considered a predominantly domestic matter. Secondly, for the current scarcity of mechanisms for cooperation amongst EU Member States in this field[5].

However, coordination is increasingly required, as it results in the interest of all individual Member States that the standard level of security in the cyber defense domain is kept equal and high throughout the entirety of the states. It would in fact take just one weak point to have a domino effect on all other Members.

---

[3] "ENISA Mandate and Regulatory Framework — ENISA," Page, accessed September 21, 2018, https://www.enisa.europa.eu/about-enisa/regulatory-framework.

[4] Regulation 526/2013/EU

[5] "Strengthening the EU's Cyber Defence Capabilities," Centre for European Policy Studies, March 6, 2018, https://www.ceps.eu/events/strengthening-eus-cyber-defence-capabilities.

## Harmonization of Criminal Law Provisions

A number of issues and challenges have risen over the last decade with regard to the application and enforcement of criminal law provisions, both at the substantial and at the procedural levels. As mentioned, in principle criminal law still remains in the Member State competence, although a number of instruments and domains can (and are) harmonized by European Union law.

The first issue with regard to cybersecurity and cybercrime is the legal uncertainty on the discipline regarding the exchange of electronic evidence (regardless of the fact that these are collected in the cloud or elsewhere) as well as its basic standard for admissibility. This issue pertains to two levels.[6]

To start with, there is an underlying lengthy and burdensome process with regard to law enforcement access to electronic data retained by EU-based foreign service providers[7]. As the discipline on data retention is extremely fragmented throughout the Union[8], uncertainty and the absence of efficient consolidated processes of data exchange undermines the need of promptness often requested to law enforcement and prosecutors, which in some cases see their investigation being significantly jeopardized by such a state of play.

Secondly, the discipline of exchange of electronic information and evidence between competent authorities (police-to-police), sees similar issues being poorly addressed by obsolete existing legal and procedural instruments which very often translate in an overly long process[9].

## Harmonization of Criminal Law Treaties amongst supra-national bodies

Unsurprisingly, the matter above has been subject of a recent initiative aimed at reforming part of the so-called Cybercrime Convention[10]. The Council of Europe has in fact announced and started the consultation process in order to complement the existing text with an additional protocol, addressing instruments for the exchange of electronic evidence and for mutual legal assistance at the international level.

Talks and negotiations are ongoing in parallel to the reform of the discipline on e-evidence of the European Union. Additionally, the existing legal instrument on the protection of personal data by the Council of Europe (Convention 108)[11], is being reformed, too[12].

## Improving Police Cooperation

---

[6] Frequently Asked Questions: New EU rules to obtain electronic evidence

[7] Nathalie A. Smuha, "Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency," *European Criminal Law Review* 8, no. 1 (2018): 83–115, https://doi.org/10.5771/2193-5505-2018-1-83.

[8] "Denmark Allows Massive Retention of Location Data for Mobile Internet," *EDRi* (blog), June 28, 2017, https://edri.org/denmark-allows-massive-retention-of-location-data-for-mobile-internet/.

[9] Electronic Evidence and Draft Convention On, "Draft Convention on Electronic Evidence," *Digital Evidence and Electronic Signature Law Review* 13, no. 0 (April 11, 2016): s1–11, https://doi.org/10.14296/deeslr.v13i0.2321.

[10] CoE, ETS No.185

[11] CoE, ETS No.108

[12] "Enhanced Cooperation on Cybercrime: A Case for a Protocol to the Budapest Convention | ISPI," accessed August 16, 2018, https://www.ispionline.it/it/pubblicazione/enhanced-cooperation-cybercrime-case-protocol-budapest-convention-20964.

Alongside a thorough reform of the legal frameworks for the exchange of electronic evidence, a significant challenge in the cybersecurity and cybercrime community is represented by the need of strengthening collaborations and cooperation channels across the various players involved, as well as establishing a solid normative framework for such practice.

It has made clear over the last decades that the imbalance of resources between public agencies and private industries, as well as within players belonging to the two sectors themselves, has led to consider a global response to cyber threats, were players are complementary one another[13].

**Regulatory Certainty for Certification Schemes**

The incremental push coming from the European legislator to develop a strong set of legal and policy mechanisms to address the security of the information systems across the continent is an undoubtable signal that the EU wants to be at the forefront in law making on these sectors. As already stated, whilst cybersecurity and privacy are two separate but complementary domains from the perspective of EU policy making, one of the most prominent legal initiative shared between such two fields is the inclusion in both legal frameworks of some sort of certification and code of conduct schemes.

**IoT Security and Crime**

The security of the Internet of Things is not anymore a long-term issue. Rather, we are entering in the fourth industrial revolution, also called the information age, where the internet has taken its third dimension, a more physical one.

Sensors and devices are nowadays connected with each other, and it is known to almost everybody that the expansion of devices with an internet connection could bring along serious and potentially catastrophic security threats[14].

Whilst the robust framework on privacy and the increasingly stricter one on cybersecurity could lead us think that the European Union is on the right track, yet a lot more to do is expected by EU policies to prevent and secure us from a dystopian future.

ENISA predicts[15] that IoTs will in fact be potentially misused in two different ways. On the one hand, pure cybercrime monetization activities[16]; on the other, exploitation for cyber espionage either by public agents or corporate sectors.

**AI Crimes and Ethical dilemmas**

---

[13] Fredesvinda Insa, "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study," *Journal of Digital Forensic Practice* 1, no. 4 (June 22, 2007): 285–89, https://doi.org/10.1080/15567280701418049.

[14] "Looking into the Crystal Ball: A Report on Emerging Technologies and Security Challenges — ENISA," Report/Study, accessed September 21, 2018, https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball.

[15] "Looking into the Crystal Ball."

[16] ENISA sums up the following specific threats: Data and available functions from IoT applications may be misused within cyber-threats such as phishing, ransomware, cyber-espionage, data breaches, identity theft, etc4 . • Ill-secured devices can be hijacked and misused in various attack scenarios, e.g. Botnets, Denial of Service, spam, etc. • Available ill-protected interfaces and processes owned by service providers may be misused to penetrate their systems. Moreover, the absence of product life-cycle functions (e.g. updates) makes the elimination of vulnerabilities impossible. • Available functions, processes and data can be misused with the aim of illicit profit. • Companies may be interested in data, practices and functions available to spy on their competitors. • Home appliances of single households or group of those can be misused by activists, terrorists, cyberwarriors, etc. to cause harm to entire areas. "Looking into the Crystal Ball."

Lastly, the mid-term challenge is certainly represented by Artificial Intelligence. Its rise is coming close to us, and the European Union has started investing on research and development of AI[17], wanting to become a landmark region for such innovation[18].

AI crimes therefore are being currently studied, conceptualized and analyzed thoroughly[19] at the theoretical level. It is not to be surprised if soon, practice will overcome theory[20].

**Capacity building towards Member States' public administration**

Cybersecurity has proven to be effectively disruptive when large-scale cyberattacks are conducted by malicious players towards a wide array of actors[21]. In particular, public agencies and public administrations are significantly affected by such crimes, and their resilience turns to be fundamental in critical situations. Let us think of instance at the emergencies generated by the attacks to the British National Health Center (NHS)[22], which reported massive consequences and potentially catastrophic damages.

For this reason, it is not only crucial that a common approach to such matters is guaranteed. On top of this in fact, the Union is in the advantageous position of coordinating a collective effort in order to enhance professionalism and reactiveness in the cybersecurity field.

**Capacity building towards neighboring countries and regions**

The importance of having a global response to cyber incidents as well as a harmonized approach towards resilience and deterrence forces any local and regional entity to broaden the scope of its capacity building, so to enhance neighboring regions' knowledge on cybersecurity for the benefit of the larger ecosystem.

During the exchange of views between Japanese and European partners in the context of EUNITY, the Japanese community described the successful capacity building missions undertaken by JP CERT in some African countries.

As an example, such missions implied training on malware analysis, environment analysis, anti-phishing development.

### 3.1.3 Recommendations

**Software Vulnerabilities**

The European Union can still play a role enabling its law-making processes in this subject matter. In pursuing the security of its Digital Single Market in fact, the Union

[17]European Commission, ICT-26-2018-2020 "Artificial Intelligence," accessed September 21, 2018, http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ict-26-2018-2020.html.

[18] Tim Skinner, "Ericsson's Big Black Box Full of AI Goodness Intrigues at MWC 2017," Text, Telecoms.com, February 28, 2017, http://telecoms.com/480122/ericssons-big-black-box-full-of-ai-goodness-intrigues-at-mwc-2017/.

[19] John Seymour and Philip Tully, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter," n.d., 8.

[20] Mariarosaria Taddeo and Luciano Floridi, "Regulate Artificial Intelligence to Avert Cyber Arms Race," *Nature* 556, no. 7701 (April 2018): 296, https://doi.org/10.1038/d41586-018-04602-6.

[21] Brooke Crothers, "Spectre, Meltdown: First Real Signs Of The Hit On Windows 10, Intel Performance Trickle In," Forbes, accessed September 17, 2018, https://www.forbes.com/sites/brookecrothers/2018/01/14/spectre-meltdown-first-real-signs-of-the-hit-on-windows-10-intel-performance-trickle-in/.

[22] "Investigation: WannaCry Cyber Attack and the NHS - National Audit Office (NAO) Report," *National Audit Office* (blog), accessed September 21, 2018, https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

is requested to take a stance towards keeping the online space a secure environment. Therefore, a coordinated legal and policy effort should be strongly recommended to codify the main principles of Coordinated Vulnerability Disclosure Policies, i.e. a set of measures aimed at establishing a collaborative channel between security researchers, CERTs and software producers, with the aim of smoothly and timely facilitate the exchange of vulnerability information and its prompt fixing[23].

Whilst some Member States are slowly implementing such practices, a pan-European approach towards this issue is still missing from the Union. Only a limited and marginal number of times vulnerabilities are included in the current EU legal framework (specifically in the NIS Directive[24], the ECI Directive[25], and the Directive Against Attacks at the Information Systems[26]). Moreover, the future Cybersecurity Act[27] seems not to address granularly the need of providing Member States with a set of clear principles on the basics of Coordinated Vulnerability Disclosure.

The importance of such an action is prominent, since it would address two elements. Firstly, it would give impulse to a reduction of the available vulnerabilities for both cybercriminals and governments. Secondly, this could counterbalance the current absence of transparent Vulnerability Equity Processes[28] across the Member States, which would outline the guidelines of a government on the handling of such vulnerabilities.

Secondly, a coordinated codification at the European level would facilitate a more unitary response to cybercrimes, serving as an impulse to a greater cooperation between different Member States and the private sector.

**The need for a pan-European institution on cybersecurity**

As mentioned already, an improvement might arrive within the Cybersecurity Act[29], currently still at its proposal phase. However, according to the research undertaken for the sake of the EUNITY project, tasks of the agency should include at least the following:

(a) Becoming a competence hub with leading tasks on policy and law making, as well as in capacity building. Such agency shall take leadership in establishing a permanent center for cybersecurity expertise, with the contextual allocation of responsibilities of training and development for EU officials, as well as Member States' public servants and private industries.

---

[23] CEPS – Center for EU Policy Studies, Task Force on Software Vulnerbility. Report: Pupillo, Lorenzo; Ferreira, Afonso; Varisco, Gianluca; 2018. Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges; 2018 Publisher: CEPS - Center for European Policy Studies

[24] Directive 2016/1148/EU

[25] Directive 2008/114/EC

[26] Directive 2013/40/EU

[27] "Cybersecurity Act: Build Trust in Digital Technologies | News | European Parliament," October 7, 2018, http://www.europarl.europa.eu/news/en/press-room/20180710IPR07605/cybersecurity-act-build-trust-in-digital-technologies.

[28] See also: Heather West, "White House Releases New VEP Charter," Open Policy & Advocacy, accessed September 21, 2018, https://blog.mozilla.org/netpolicy/2017/11/15/white-house-releases-new-vep-charter.

[29] European Commission, Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') 2017/0225(COD)

(b) Coordination and point of contact for the vulnerability assessment. In an hypothetical pan-European CVD policy codification, an important role shall be taken by the agency we advocate for. Similarly to what the NIS Directive establishes in terms of cyber incidents reporting, the same should be consolidated with regard to the exchange of information on zero-days vulnerabilities between software vendors, security researchers, CERTs and the EU. Such agency could therefore act as an independent trustworthy party, satisfying the need of having third impartial bodies participating in such processes, as well as developing periodical and updated statistics on the functioning of CVD policies[30]. Furthermore, CERT-EU tasks, with a widened mandate comprising coordination with European and international CERTs should be pivotal.

(c) Coordination role with non-EU regions in the area of cyber diplomacy. Whilst the foreign policy of the European Union is still prominently conducted by the EEAS, it needs to be noted that cybersecurity goes far beyond the principles of territoriality, sovereignty and attribution that are typical in a normal offline scenario of diplomacy. For this reason, such an agency shall take leadership in coordination with similar counter-parts in other regions. Incident response, reporting and vulnerability assessment are all subject matters which could fairly suit in this sui generis extra-territorial mandate, although the mandate to negotiate and train the negotiators for cybersecurity matters should be of utmost priority.

(d) Coordination with data protection authorities. As the cybersecurity legal framework of the European Union is complemented by the EU new data protection regime, it needs to be noted that from both disciplines a significant information sharing section is foreseen for instance in the case of cyber-attacks and data breaches. Whilst the competences of the parties involved are quite consolidated (particularly with regard to regulatory agencies and to ENISA itself), the further establishment of a formal network for information sharing could facilitate and ease the resilience of European information systems against such types of attacks. This line of communication does not only involve ENISA and the European Data Protection Supervisor, but also national data protection authorities tasked with the powers and the responsibilities of receiving data breach reports, under Article 33 of the General Data Protection Regulation[31].

To conclude, the EU should take the initiative to establish an agency with the above mentioned tasks, which will therefore coordinate an unitary effort towards the pursue of three plus one complementary tasks (cyber diplomacy in and out-EU, decision making support to the executive branch and operational/CERT plus cyber defense). It

[30] See also: CEPS – Center for EU Policy Studies, Task Force on Software Vulnerbility. Report: Pupillo, Lorenzo; Ferreira, Afonso; Varisco, Gianluca; 2018. Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges. Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges; 2018 Publisher: CEPS - Center for European Policy Studies

[31] Regulation 679/2016/EU

is therefore crucial that such policy areas are addressed coherently and by the same player, in order to ensure a common direction of the strategies therein.

### Cyber Defense: enhancing cooperation with third parties

The wide array of cyber criminals demands for a complex strategy to counter a multiple number of potential attacks. However, in spite it needs to be registered some step forward in this regard, for instance with the adoption of the PESCO-CSDP[32] initiative, supporting short- and mid-term objectives should follow and complement the overall strategy of the European Union on cyber defense.

For instance, an integration of the Common Security and Defense Policy with both long-term plans and short-term strategies, as well as an enhanced synergy between military and civilian (and broadly, public and private), is demanded by a number of factors, not least the dual use fashion of new technologies and the nature of security threats.

On a deeper level, this scenario certainly demands for more legal certainty on a number of basic principles of international public law applicable to cyber operations[33], where the European Union shall become a leading voice in the landscape. For instance, the principle of sovereignty has massive consequences with regard to the application of states' jurisdiction, opening to its ability to enforce the law and to retaliate. Whilst at the international level some efforts can be registered with the Tallinn Manual, yet the community has not reached a commonly accepted conclusion on such principles[34]. For this reason, the European Union should explore its own interpretations of the norms under scrutiny, in order to provide with further points of reflection the debate on the harmonization of the efforts on cyber defense currently undertaken throughout the continent.

Alongside such basic elements, institutional and organizational features shall be clarified in the pursuing of a well-ordered cyber defense strategy at the European Union level. A number of commentators and Think Tanks have tried to identify some of the most compelling challenges on this matter, namely:

- Considering Cyber Defense function as part of the EDA (European Defense Agency), or just going beyond a merely inter-governmental approach
- Re-assessing and strengthening the EU-NATO cooperation
- Creation of a European secure network for critical (information) infrastructure, along the lines of the USFirstNet

### Harmonization of Criminal Law Provisions

The regime of Mutual Legal Assistance results particularly time-consuming, sometimes taking up to ten months before the data is actually transferred to the

---

[32] Permanent Structured Cooperation (PESCO). Link: https://eeas.europa.eu/headquarters/headquarters-Homepage/34226/permanent-structured-cooperation-pesco-factsheet_en

[33] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, 2nd ed. (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.

[34] Oliver Kessler and Wouter Werner, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare," *Leiden Journal of International Law* 26, no. 04 (December 2013): 793–810, https://doi.org/10.1017/S0922156513000411.

requesting party. This could be particularly ineffective in the context of cyber terrorism or similar forms of crime.

Furthermore, the current regime does not provide for any form of effective fast-track MLA, which could be beneficial also in the case of serious risk for the public safety of the individual, regardless of the presence of crimes involved. For instance, in the case of emergency rescue, emergency teams and first responders are still bound to the foreign competent authority when there is a cross border electronic dataset to be analyzed or tracked.

In spite of the fact that an effort from the European Union to legislate on this matter is currently ongoing at the negotiation stage, some criticisms have been raised with regard to the protection of fundamental rights in the proposed texts[35]. A balanced approach seems to be a complex matter to achieve, although it is pivotal that the protection of certain civil liberties such as the right to personal data remain stable in their role of safeguard against arbitrary interferences, from both private and public sectors[36].

**Harmonization of Criminal Law Treaties**

It is clear at this point that both the European Union and the Council of Europe are taking legislative steps towards addressing the same issues. It will be up to both institutions then, to coordinate each other without ending their respective preliminary processes with conflicting provisions on similar scenarios. As repeatedly mentioned, cybersecurity and cybercrime are borderless issues, and tackling them with opposite approaches could end up undermining international legal certainty and most of all, cooperation amongst law enforcement and prosecutorial bodies both intra and extra EU.

**Improving Police Cooperation**

Recommendations from a policy perspective have been identified over three levels: intra-EU, extra-EU and multi-stakeholder cooperation.

*Intra-EU*

Firstly, the European Union is in high demand for more coordination between law enforcement agencies of the 28 Member States. Such a cooperation is of vital importance in cybercrime matters, as well as in the investigation of any other serious or organized crime having a digital information to be analyzed[37]. Alongside that, supranational shape of crimes demand for the participation of multiple agencies in a coordinated response.

Europol has in this scenario a crucial as well as advantageous position. Throughout the European Cybercrime Center and other SOC networks, the agency can actually ease the cooperative efforts amongst Member States.

---

[35] "Trust Issues and the Recently Proposed EU E-Evidence Framework," CITIP blog, accessed August 17, 2018, https://www.law.kuleuven.be/citip/blog/trust-issues-and-the-recently-proposed-eu-e-evidence-framework/.

[36] "EU 'e-Evidence' Proposals Turn Service Providers into Judicial Authorities," *EDRi* (blog), April 17, 2018, https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/.

[37] Ángeles Gutiérrez Zarza, "EU Networks for Administrative, Police and Judicial Cooperation in Criminal Matters," in *Exchange of Information and Data Protection in Cross-Border Criminal Proceedings in Europe* (Springer, Berlin, Heidelberg, 2015), 107–13, https://doi.org/10.1007/978-3-642-40291-3_6.

Similarly, a pan-European cyber agency can take a leading position in coordinating the response against cybersecurity incidents, channeling the information deriving from the different Points of Contacts designed under the auspices of the Network and Information Security Directive.

*Extra-EU*

Along the same lines of what has been stated above, it is crucial that collaborative efforts do take place also between EU Member States (and EU Agencies) and foreign countries, including international organizations.

Europol has, under its mandate, explicit statutory initiative to undertake strategical and operational agreements with a number of partners[38]. Whilst many important countries and international institutions have ongoing agreements with Europol (for instance, Interpol and the United States), the agency should nevertheless continue in its mission, to cope with a globalized response to cybercrime.

*Multi-stakeholder platforms*

Lastly, challenges derive from the absence of codification of platform for data sharing between police authorities and the private sector. In the European Union institutional structure, Europol is again at the forefront in this[39].

Over the last years, its business model has shifted adopting a more horizontal, collaborative approach with the private sector, acknowledging their importance and their resources. Some called it 'the *uberisation* of police work'[40], which starts to be seen as a potential effective way forward in the near future.

However, such model has so far operated under a number of challenges. Not least, the fact that the participation of the private sector is made on a voluntary basis. For this reason, both cybercrime and cybersecurity domains are looking at such model with interest mixed at some skepticism.

It would be down to the European Union therefore, try to explore policy and legal solutions to make such approaches more continuative and more formalized, verifying the potential extension of the *uberisation* model to other forms of law enforcement at national and international levels.

**Regulatory Certainty for Certification Schemes**

Policy sectors were recommendations have been identified pertain to cybersecurity and privacy, respectively.

*Cybersecurity*

The Cybersecurity Act mentioned above does not only carry on a substantive and expected reform of the European Union Agency for Network and Information Security

[38] Regulation 2016/794/EU

[39] "EU Should Build Trust Relationship with Crypto Business to Prevent Cybercrimes - Europol - Cryptovest," September 18, 2018, https://cryptovest.com/news/eu-should-build-trust-relationship-with-crypto-business-to-prevent-cybercrimes---europol/.

[40] "The 'Uberisation' of International Police Work | LinkedIn," accessed August 14, 2018, https://www.linkedin.com/pulse/uberisation-international-police-work-rob-wainwright/.

(ENISA). Rather, it also aims at introducing a robust set of certification schemes in the area of cybersecurity[41].

What is interesting to note at first, is that Member States will be obliged to adopt a governance on cybersecurity certification, although in turn, end-users (industries) should not in principle be obliged to abide to such schemes. The voluntary basis could be derogated only in exceptional cases and in presence of legal basis to be found either at EU level or domestic law. Such a chain of actions is quite unclear at the present moment and it might create some doubts in the future.

It comes quite clear that certification from third parties might create an extension of the time needed for a product to be launched on the market.

Furthermore, the delegation to the single individual Member State to make potentially mandatory certification schemes seems dangerous from a market perspective, as it would add burdens to companies and increase legal and regulatory fragmentation across the Member States of the Union, undermining the very essence of the Digital Single Market.

*Privacy*

Article 42 of the GDPR, as stated in previous deliverables, foresees a set of privacy certification schemes. In a 2017 report[42], ENISA sums up the following main elements of the certification schemes as enshrined in the above mentioned GDPR Article:

- Certification as an accountability-based mechanism
- Certification of compliance with GDPR provisions (not an exclusion of responsibilities)
- Key actors: Certification bodies and Supervisory authorities
- Accreditation of certification bodies:

a. accreditation by a Data Protection Authority (or the European Data Protection Board, in the case of the European Data Protection Seal)

b. accreditation by the National Accreditation Body on the basis of the Accreditation Regulation and the ISO/IEC 17065:2012 standard and additional requirements in the field of data protection provided by the Data Protection Authority, or

c. both authorities, namely the National Accreditation Body and the competent Data Protection Authority, collaborating in this task.

However, in spite of a more thorough discipline, uncertainty is still an element surrounding Article 42. Again, ENISA offers interesting inputs with regard to what open issues need for more clarification by the regulator as to how to interpret the following[43]:

- Terminology of the Article, for instance stating the difference between *criteria* and *requirement*

[41] "Standards and Certification — ENISA," Topic, accessed September 21, 2018, https://www.enisa.europa.eu/topics/standards.

[42] ENISA report on Certification (2017)

[43] "Recommendations on European Data Protection Certification — ENISA," Report/Study, accessed September 21, 2018, https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification.

- Subject matter of certification: processing operations only could lead to the a narrow interpretation of the scope of the article
- Diversity in accreditation models; the GDPR leaves Member States Authorities enough discretional room, although it does not lay down any cooperation process amongst them
- Approval of criteria for certification by Data Protection Authorities and/or EDPB, which means that such bodies should seek for consistency in the interpretation of such the relevant norms
- EU level vs. national certifications: risks of proliferation of national certifications
- Cross-border recognition of national certifications[44]

**IoT Security and Crime**

It will be fundamental that both industry and policy makers find synergies to address confidentiality, integrity, availability of IoT devices. What is important in this scenario, could be summed up in two very remarkable policy takeaways:

(a) Addressing security should not be narrowly focused at the micro-level, solely tackling a component or an element, or a device only. Rather, it is fundamental that the security of IoTs is conceptualized in the broader sense, with the larger environment in consideration

(b) The responsibility of tackling the potential threats of IoTs is not only limited at addressing safer and stronger security standards. Rather, a deep reflection should be done, at both policy and legal level, on whether the current structure of national criminal law frameworks are efficiently ready to include IoT crimes. The European Union has here a prominent responsibility to lead the debate.

**AI Crimes and Ethical dilemmas**

AI brings about substantial ethical questions. As many commentators and scholars say, there is an underpinning risk of robots silently having an impact on our self-determination[45]. In a future perspective, this point is key when assessing upcoming intelligent transport systems and similar technologies.

It thus becomes rather hard the role of both law makers and policy makers when it comes to Artificial Intelligence. Specifically, three areas might become a regulatory challenge with respect to AI:

- Definition of security standards
- Basic ethics principles on AI
- Harmonization and adaptation of criminal law frameworks.

[44] ENISA report on Certification (2017)

[45] Julia Fahrenkamp-Uppenbrink, "An Ethical Way Forward for AI," *Science* 361, no. 6404 (August 24, 2018): 763–65, https://doi.org/10.1126/science.361.6404.763-q.

**Capacity building towards Member States' public administration**

In particular, the following areas of the public administration are identified as in the need of continuous and incremental training and development of their civil servants' skills:

(a) CERTs

In the current cybersecurity structure laid down by the legal framework of the European Union, Computer Emergency Response Teams and Computer Security Incident Response Teams are increasing their importance and their role in coordinating resilience and responses to attacks. Particularly in the case of cross-border incidents, the information sharing network allocated to their lead is crucial. For all these reasons, it is needless to say how much a common approach towards training and development of CERT and CSIRT staff could help improving and sharing common approaches across the Union.

(b) Digital Transformation Teams

One of the most crucial challenges for the public sector is currently its digitization. From the handling of corporate business, to the offering of digital services to its citizens, local and central governments all across Europe are confronted with the need of transforming their practices as well as their institutions into efficient digital entities.

It is for this reason that the European Union has started a number of legal and policy initiatives aimed at introducing in the public administration a set of measures finalized at the increment of digital services.

However, this is certainly not sufficient for achieving a full digital transformation of public bodies, as the civil service still suffers of knowledge gaps across the different Member States and even within the different branches of the same Government.

(c) Law Enforcement Authorities

The rising allocation of tasks to law enforcement authorities with regard to cybersecurity and the fight against cyber-enabled crimes is becoming a primary challenge in the governance of police and competent agencies the like. European Union agencies therefore are the better suited to coordinate a common approach towards the development of skills in digital and computer forensics of national and local police officers.

(d) Judicial Bodies

Training and capacity building in this context does not only pertain to the development of a highly skilled prosecutorial community. Rather, the focus should be extended to courts and magistrates standing on the decisional bar of criminal cases. Research and commentaries have highlighted a knowledge gap in such bodies, with the alarming risk of superficial assessments of cases pertaining the cybersecurity or the cybercrime domains, particularly with regard to admissibility and evaluation of digital forensics tools and electronic evidence.

***Capacity building towards neighboring countries and regions***

Drawing from the examples mentioned in 3.1.2, the European Union could be the best suited institution to undertake a similar program, on a larger and more systematic scale. As stated above, the global state of cybersecurity is extremely important. For this

reason, resources and knowledge should be invested in a worldwide exercise of capacity building.

For the European Union, this would not only mean enhancing neighboring regions' security, but also benefitting of an indirect but inevitable positive impact towards people and industries of the Union itself. Africa and the Eastern Balkans for instance, are extremely strategic for the EU, both for security and trade reasons. It comes along that attention and investments on cybersecurity capacity building should and will have an effect on the relationship with countries located in such areas.

## 3.2 Research and Innovation in Europe

Current security measures are not sufficient and unaware of the challenges that new technologies will bring. In recent years there have been noticed an increased level of sophistication and "intelligence" in malware. Also, main security concerns lie in the importance and value of the user data (social media, IoT devices) that are increasingly exposed and being misused by cyber criminals and diverse companies. Adversaries seem to discover new ways of hiding their trails. The level of sophistication includes new updates in their malicious procedures in order to include new trends in anonymity, encryption and detection invasion. Moreover, the increase of the usage of digital currencies has given the advantage of anonymity to adversaries.

The extended spread of this phenomenon has mobilized governmental and commercial services to provide solutions to this important challenge. There is a plethora of national funding, European and international cooperation aiming to support cybersecurity research and education with main objective to tackle the challenges in the area of cybersecurity. Internationally as well as in the European Union there are framework programmes offering open competitions, as well as Special programmes such as Connecting Europe Facility (CEF) and Cybersecurity calls, the European Union Agency for Network and Information Security (ENISA). On national level there are national, state, regional, international joint programmes and PhD grant that support cybersecurity financially.

### 3.2.1 Status and gaps

The current R & I cybersecurity priorities and current directions include risk management and critical infrastructure protection, cybersecurity in emerging technologies (Internet of Things, Smart Cities, Industry 4.0, Cloud Computing and Big Data), threat detection and threat intelligence including new methods of detection of cyber-attacks and machine learning based threat detection, along with cryptology design, techniques, protocols encryption, network security and hardware and systems security. The main challenges in cybersecurity focus in malware, APT, network threats, lack of integration/cooperation between CERTs, poor cyber literacy, cyber-attacks for critical infrastructure, quantum cryptanalysis, social engineering and data theft.

Although the overall trend for malware in 2017 was stable, the new malware samples for the first quarter of 2017 reports 22 million, while the number are expected to increase even more[46]. According to a SANS report[47] and the *ENISA Threat Landscape Report 2017* [55], 48% of the web-based attacks in 2017 were introduced by web-based drive-by and downloads, while the overall trend of this kind of attacks was increased

[46] Link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, accessed October 2018

[47] Link: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910, accessed October 2018.

in 2017. Ransomware attacks have increased 36% this year[48], the Ransomware families have increased 4.3 times and the economical loss has doubled. Also, DDoS attacks still remain one of the top threats for business with online presence. The organizations that faced a DDoS attack to have increased to 33% in 2017 (17% in 2016)[49]. Meanwhile web application attacks were also increased in 2017, with 1.8 billion average daily attack volume[50]. The trend of botnets also increased in 2017, with a 69,2% increase in malware in the first quarter of 2017 and the counties infected most being China, India, Russia federation, Brazil, Vietnam, Argentina, Iran, Islamic Republic of, Thailand, United States[51].

### 3.2.2 Current and future challenges

The main challenges in cybersecurity are analyzed below:

1. **Malware.** The level of sophistication and complexity has increased. New malware attacks have reached 22 million samples in the first quarter of 2017[52]. According to a European Economic and Social Committee report[53], 98% of the companies have dealt with malware at some point, around the world. According to Microsoft's Security Intelligence Report[54], Trojans were the most important threat, followed by worms, viruses backdoors and Ransomware, for the first half of 2016.

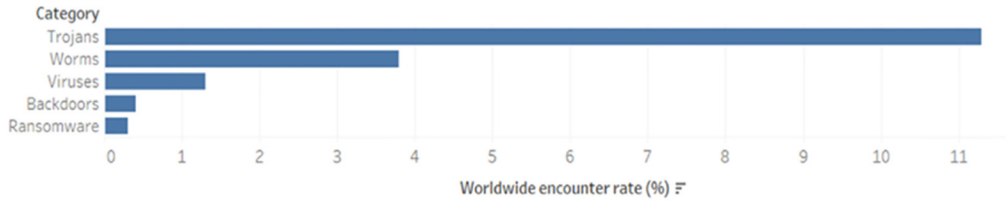


Figure 2. Malware Encounter Rate in the first half of 2016

New malware related challenges include the reduction or elimination of user interaction (e.g. number of clicks) to reach the malware (instead of using remote execution exploits & RDP brute force attacks), the usage of fileless malware using software, that is already installed on targeted computers (e.g PowerShell, PSExec, WMI) or is running scripts in memory, the revisiting worms to propagate infections, the wipers, the script based malware, the potentially unwanted programs (PUPs) (e.g. replacing a browser), the fake advertisements and ad networks, the hardware and firmware threats, the hybrid attacks which combine attack diverse methods (e.g. BrickerBot), the new evolving malware for MacOS and Linux, the domain generation algorithms and the supply chain

[48] Link: https://thebestvpn.com/cyber-security-statistics-2018.

[49] Link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

[50] Link: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Fortinet-Threat-Report-Q2-2017.pdf, accessed October 2018.

[51] Link: https://www.spamhaus.org/statistics/botnet-cc/, accessed October 2018.

[52] Ibid 4

[53] Link: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf, accessed 20 November ' 18

[54] Link: https://www.microsoft.com/en-us/security/intelligence-report accessed October 2018

attacks[55]. Other existing studies that identify malware as a crucial threat are from Verizon[56], Pandalabs[57], and Comodo[58] . Malware spread along Europe is shown in the Microsoft Security Intelligence Report.

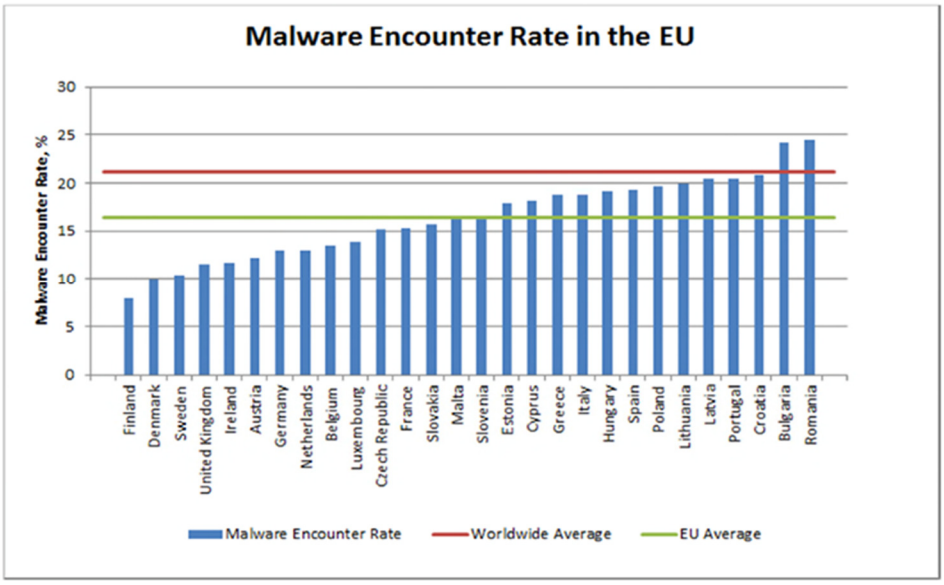


Figure 3. Malware encounter rate in the Europe

2. **Ransomware Evolution**[59] Ransomware remains a continuous challenge for cybersecurity, taking into consideration the increased level of sophistication and complexity. The challenge is expanded if we add new trends of adversaries to hide their trails, new malicious procedures in anonymity, encryption and detection invasions. EUROPOL along with the Dutch National Police, Europol, Intel Security and Kaspersky Lab have join hands against Ransomware[60]. Specifically, Europol has characterized Ransomware as 'dominant concern' for EU law enforcement, referring to the examples of CryptoWall, CTB-Locker, TeslaCrypt, and Locky.22[61]. Additionally, Google Research reports Ransomware as a multimillion-dollar business[62]. Some worth mentioning findings include the rise of ransomware as a service and the fact that ransomware targets server

[55] ibid4

[56] Verizon, "2017 Data Breach Investigations Report 10th Edition" (Verizon, 2017), 39. accessed October 2018

[57] Panda Security, "Pandalabs Quarterly Report Q1 2017," 2017, 14. accessed October 2018

[58] Comodo Threat Research Labs, "Comodo Threat Research Labs - Q1 2017 Report," Quarterly Report, 2017, 28. accessed October 2018

[59] Link: https://www.sophos.com/en-us/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en, accessed October 2018.

[60] Link: https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware, accessed 20 November 2018

[61] Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2016" (The Hague, Netherlands, 2016), 17. Accessed 20 November 2018

[62] Elie Bursztein, Kylie McRoberts, and Luca Invernizzi, "Tracking Desktop Ransomware Payments," accessed 10 November 2018, https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf, accessed October 2018

technologies. There is also an increase in the ransomware impostors and media impacts (WannaCry and NotPetya) as well as an increase of the complexity and the level of sophistication. Finally, it is worth mentioning the rise of mobile ransomware and the introduction of ransomware in medical devices.

3. **Increase of Web-based attacks.** Financial malware still depends on web-based attacks, browser extensions have been compromised as well and popular messaging applications (Telegram and WhatsApp) allow adversaries to break encryption. Finally, water-holing attacks seems to be increasing as well and the number of malicious URL's still remain very high.
4. **Web application attacks.** Attacks against specific available online applications, services and mobile apps are increasing. More specifically, SQL Injections and Content Management Systems vulnerabilities remain in the threat landscape, along with the well-known cross-site scripting (XSS).
5. **Phishing attacks.** They are deployed in massive campaigns while delivering malware. The phishing campaigns depend on multiple short-lived websites and have leveraged social media and legitimate websites, in contrast to direct emails used before. Another form of this attack is the *"Spear-phishing"*, targeting specific group of people (e.g Threat Group-4127, targeting Hillary Clinton's 2016 presidential campaign), the Clone phishing and the Whaling.
6. **Increase of spam.** The challenge of elimination of the traditional spam still remains important, as the level of sophistication and the quality of the obfuscation techniques has been increased. Currently, the techniques have included the combination of personalized information to lure users. Spam still remains 84% of the daily email volume and has expanded also in social media[63].
7. **DDoS.** New interesting characteristics introduced in DDoS attacks are: the "Pulse wave"[64] DDoS attacks, the multi vector attacks (using both UDP-TCP), the decrease of the cost for DDoS as a service, the DNS based attacks, the DDoS in bitcoin exchanges and last but not least it is interesting to mention that the DDoS attacks are used to cover other types of attacks. The European Economic and Social Committee report[65] mentioned Dyn, as the *"record-breaking of* 1.2 TB/s*"* DDoS attack that caused the temporary shutdown of companies like Facebook, Netflix, Twitter and Amazon. Studies from Nexusguard and Kaspersky Labs show that the geographical distribution of the attacks focus on Netherlands,
   Germany, France, UK and Romania[66] [67] while the victims are mainly located in UK, the Netherlands, and Germany[68].
8. **Popularity of botnets is increasing.** Botnets were the second most important threat in 2017. Virtual machines in the cloud infrastructures (Microsoft, Google) are used as zombies for further attacks. There was an

[63] Link: https://www.spamfighter.com/News_107-Flooded-Inboxes-84-of-All-E-mail-is-Spam.htm accessed October 2018

[64] Link: https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html, accessed October 2018

[65] Link: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf accessed October 2018

[66] Nexusguard, "Distributed Denial of Service (DDoS) Threat Report Q1 2017," accessed October 2018

[67] Alexander Khalimonenko and Oleg Kupreev, "Kaspersky Securelist DDOS Attacks in Q1 2017," www.securelist.com, May 11, 2017, https://securelist.com/ddos-attacks-in-q1-2017/78285/. accessed October 2018

[68] Imperva Incapsula, "Global DDoS Threat Landscape | Q1 2017 | Incapsula," www.incapsula.com, 2017, https://www.incapsula.com/ddos-report/ddos-report-q1-2017.html. accessed October 2018

increase in 2017 of malware tools like Ursnif, DELoader and Zeus Panda[69], which are used in fake advertising and massive IoT botnets**.**

9. **The artificial intelligence expansion.** The challenge to use new AI trends to serve cybersecurity[70], new machine learning techniques and deep learning neural networks are powerful tools against cybersecurity threats and vulnerabilities.
10. **IoT threat landscape.** The IoT landscape has expanded in the recent years adding millions of new devices as potential targets of the adversaries. The new IoT devices face serious security vulnerabilities. Insecure interfaces, lack of authentication procedures and users' security awareness make IoT threat landscape a huge cybersecurity challenge.
11. **Blockchain and new cryptocurrencies.** The popularity and spread of the cryptocurrencies have expanded in 2017. There are 402 new available cryptocurrencies[71] with first trade in 2017[72]. Blockchain technology and its complex structure can be used to protect users against potential frauds and data steal[73]. However, blockchain technology and the need for mining have increased the cybersecurity incidents, due to the need of computing power. The adversary, by using stealth methods, is determined to siphon off computing power, while the malware is running in the background harvesting bitcoins.
12. **Vulnerabilities in serverless applications.** Most serverless applications are used as web services and data processing tools, where the user is mostly responsible for defeating cybercriminals. The main problems that they face are that they need input validation, source repository systems can be revealing secrets of authentication, while there is too much access or limited access control. Moreover, old third-party libraries can be responsible for security vulnerabilities[74].
13. **Security and flexibility (resilience) in the Cloud.** As the popularity of cloud services increases, the challenge of offering security and resilience in this area arises. The challenge seems more difficult given the increasing complexity scale and interconnectivity of the various cloud ecosystems.
14. **Prevent cybercrime and cyber terrorism.** The complexity of facing cybercrime and cyber terrorism increases if we take into consideration privacy, considering surveillance and fundamental rights, leakage of data to adversaries as well as the final capture of cybercriminals.
15. **Trust Management in the Digital Society.** Assurance and accountability are mandatory values in the modern and future infrastructures. It is necessary to expand the self-certifications in order to include trust and accountability.
16. **Privacy.** Considering the exposure of private information of millions of users in the modern online social networks, privacy seems more and more challenging. This challenge is expanded if we add into account the millions of

[69] Link: https://en.wikipedia.org/wiki/Zeus_(malware), accessed October 2018

[70] Link: https://digitalbusinessblog.wordpress.com/2016/11/21/what-is-the-future-of-artificial-intelligence-a-i/, https://www.statista.com/chart/6810/the-future-of-ai/, accessed October 2018

[71] Link: https://bitinfocharts.com/cryptocurrency-list-2017.html, accessed October 2018

[72] Link: https://bitinfocharts.com/cryptocurrency-list-2017.html, accessed October 2018

[73] Link: https://medium.com/universablockchain/blockchain-is-all-about-security-8128a6e16afe, accessed October 2018

[74] Link: https://www.twistlock.com/2018/07/31/serverless-applications-security-risks/,accessed October 2018

IoT devices going online every day with a plethora of vulnerabilities that follow them.

17. **Big data.** The complexity and heterogeneity of Big Data including the IoT landscape, created the need to be approached in a holistic way. The characteristics that identify Big Data are the fast data insertion, the distributed redundant data storage, the parallel task processing and the different types of data. Also, when we refer to Big Data we have to mention the issues about scalability, large-scale analytics, hardware agnosticism, accessibility and cost effectiveness.
    The main key challenges are access control, authentication, secure data management and secure computation. Issues hard to tackle are also source validation, filtering, application software security and trustworthiness of devices. Finally, worth mentioning challenges for Big Data are the interoperability of applications, the distributed denial of service attacks and the heterogeneity in the protocols for communication[75].

### 3.2.3 Recommendations

## Conclusions

The increasing exposure of user data to new technologies, along with the expansion of the production of data from new devices, new applications and the general advance in digitalization, has made the protection of the user from cyberattacks even more challenging. The level of sophistication, the aggressiveness and the innovation in malware has increased and the cyber threat environment is even more complex putting in risk business transactions, ideas, technologies and infrastructure [79, 80]. This landscape seems to be continuous changing as relevant studies refer[76] [77] [78].

The most common risks seem to be malware and phishing[79] [80], although there are some new key players added to this battle like IoT technology, big data analytics, etc. Criminals are using analytics for the attacks, along with the misuse of the social media analytics[81] and the opportunities of Deep Neural Networks and Machine Learning approaches to handle the increasing amount of user data[81]. Along with the cyberattacks, this environment seems even worse if we take into consideration that the cybersecurity is not taken care in the time of development and deployment of these new technologies, creating weaknesses that may not be removed after the build[82]. The cyberattacks in the healthcare section seems to be important, in terms of user data exposure, if we take into account that it lags in alertness and preparation, in case of a

[75] Link: https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport, accessed October 2018

[76] Link: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf accessed November 2018

[77] Link: https://nakedsecurity.sophos.com/2017/11/03/2018-malware-forecast-learning-from-the-long-summer-of-ransomware/ accessed November 2018

[78] Link: https://cdn.securelist.com/files/2017/11/KSB_Predictions_2018_eng.pdf accessed November 2018

[79] Link: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf accessed October 2018

[80] ibid 31

[81] ENISA Threat Landscape Report 2017 15 Top Cyber-Threats and Trends, October 2018

[82] ibid 32

cyber threat[83]. SMEs seem to lack in preparedness for cyberattacks as well, while the fact that they act online, costs high[84].

**Recommendations**

The main efforts toward the handling of the threats in the cybersecurity sphere should initiate from the regulation and state support of the vulnerability discovery and the efficient cyberspace protection. There is a great need for programmes and frameworks towards the development of cyber threat intelligence. According to the ENISA threat landscape report[85] an initiative in the financial sector, which should be set as an example is the TIBER Threat Intelligence Based Ethical Red teaming[86]. Along with the development in the financial sector, policy makers should initiate the investigation of a methodology for transparency, as well as the feedback of the policies from the threat landscape[87]. In the political domain policy making should also include all related parties including civil, society and consumer groups.

The business factor will need to work on the defense strategy, training programs and better adaptation of CTI automation solutions[88]. Companies should be proactive in order to tackle the cybersecurity threats[89] and initiate public-private-partnerships that will also bring a broad selection of stakeholders united.

The mitigations mentioned above should work along with the necessary technical, research and educational resolutions. Educational programmes, including competitions, hackathons and prizes for public and private sectors[90]. New controls and emerging technologies should be developed accordingly to the new threat landscape. Germany, UK and Czech republic constitute ideal examples in the educational programs for cybersecurity.[91] The technical solutions should play along with lawful interventions while maintaining the user confidentiality, integrity and availability of data.

There seems to be a great need to tackle the issue of the fragmented regulatory environment, through harmonization of data protection rules and the development of *EU-wide regulations*. Additionally, a GDPR implementation strategy would enable level on control, in data flow.

The funding seems to be of great need in the training cybersecurity programs (from H2020 and ENISA) as well as the support of the small companies by the large ones.

The gap of national educational programs need to be covered with the expansion of skill sets introducing cybersecurity awareness from the early age, the adaptation of a multidisciplinary approach and the expansion of the cybersecurity education in non-

[83] Link: https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

[84] ibid 38

[85] Ibid 32

[86] Link: https://www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf, accessed October 2018

[87] Link: https://arstechnica.com/tech-policy/2017/03/group-sues-dhs-ic-over-digital-device-border-search-records/, accessed October 2018

[88] Ibid 31, October 2018

[89] ibid 38

[90] ibid35

[91] ibid35

technical academic domains as well as the end users and the increase of cyber experts in academia and civil society[92].

**Technical recommendations**

More specifically in technical terms, regarding malware, we have to ensure detection at all points (all inbound/outbound channels), security incidents management on all interfaces of malware detection activity, ensure security policies involving all relevant roles, always keeping up-to-date as well as regular monitor of antivirus test. Web-based attacks could be tackled by protecting web browsers (sandboxing, antimalware extension) and keeping them up-to date, avoidance of unnecessary plugins as well as blockage of malicious payloads through web traffic filtering and encryption (SSL/TLS). Updates should be made in CMSs as well and end points should be protected from unpatched software.

Web application attacks can be mitigated if we apply security policies in the development and operation of them. Authentication and authorization consists very important steps towards this direction, as well as the performance of traffic filtering an input verification. Education of staff concerning security and privacy and usage of specialized security email gateways should be the aim against phishing attacks and spam while usage of Artificial Intelligence and Machine learning techniques to detect anomalies. The moderation of spam in modern communication can be achieved by DKIM (Domain Keys Identified Mail), reputation filters, content filters and Real-time Blackhole Lists. DDoS attacks should be also handled with security policies as well as protection measures by ISPs and technical DoS/DDoS protection approaches[93].

Additionally, the Artificial Intelligence expansion and the use of new AI trends to serve cybersecurity, new Machine Learning techniques and Deep Learning Neural Networks are powerful tools against cybersecurity threats and vulnerabilities.

## 3.3 Industry and standardization in Europe

This section analyzes numerous cybersecurity challenges that we have identified in industry in Europe. It is organized in three parts:

1. Status, gaps and cybersecurity situation in Europe
2. Current and future challenges
3. Recommendations in industry and standardization areas

Innovation and transformation are not easy processes. During long time, the European Union has developed activities related to control security and electronic communications after faced with increasing numbers of cyber-attacks on different levels and critical infrastructures. The EU provided the strategy and started to realize the idea that societal reliance on technology constituted a huge growing security risk.

Digital technology in Europe has become an integral part of our daily life and industry in Europe is a main actor of this change, incorporating and creating new technologies for improving their business. This way, cybersecurity transformed from an “add-on” to be an integral core part of their technology, not only improving their work (e.g. industry 4.0) but also helping to create new business models.

[92] ibid35

[93] Link: https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf, accessed October 2018.

Following, we present an analysis that extends the work presented in D3.1 of status and gaps of industry in Europe covering the more important areas and the recommendations and conclusions we obtained from this work.

### 3.3.1 Status and gaps

Thought the Horizon 2020 research agenda, the European Union has invested more than $150 million in cybersecurity through research and innovation projects. The European Commission also plans to invest an additional finance active during the next 3 years in a new public-private partnership on cybersecurity. This plan will increase government-funded research programs and, therefore, public-private coordination is needed. This is more critical in the growing fields of data protection, big data and artificial intelligence[94].

As abovementioned, several organizations in Europe work in research and development of cybersecurity solutions, covering both public and private entities and needs. These organizations aim for European level of work and dissemination, in order to make the results and goals for all members states.

**European Union Agency for Network and Information Security (ENISA)**

The European Agency for Network and Information Security (ENISA) was originally established in 2004 and had its mandate renewed periodically. The current ENISA mandate is set out in Regulation EU No. 526/2013[95] (the 'ENISA Regulation') and is due to expire in June 2020.
Regarding to cybersecurity, ENISA has main objectives:

- Dependability of systems (avaibility, reliability, safety, confidentiality)
- Security of information (integrity, availability, authenticity)
- Resilience and Survuvability

**European Cyber Security Organization (ECSO)**

ECSO represents the industry-led contractual counterpart to the European Commission for the implementation of the cybersecurity contractual Public-Private Partnership (sPPP). ECSO members include a wide variety of stakeholders including many large companies, with the main objectives of[96]:

- Collaborate with the European Commission and national public administrations to promote Research and Innovation in cybersecurity.
- Faster competitiveness and growth of the cybersecurity industry in Europe as well as end users and operators through innovate cybersecurity technologies, applications, services and solutions.

**Electronic Components and Systems for European Leadership (ECSEL)**

ECSEL provides a partnership between public and private sectors for systems and electronic components[97].

Some of the goals they have are:

[94] Link: https://www.acm.org/binaries/content/assets/publicpolicy/2016_euacm_cybersecurity_white_paper.pdf

[95] Link: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1495472820549&uri=CELEX:32013R0526

[96] Link: https://ecs-org.eu/about

[97] Link: https://europa.eu/european-union/about-eu/agencies/ecsel_en

- to maintain smart systems manufacturing capabilities in Europe work in possibilities of growth
- provide access for all stakeholders to a world-class infrastructure for the design and manufacture of systems.

Due to this, they aim to benefit Europe by pushing industry to establish a strategic research and innovation agenda and support EU policies[98].

**Big Data Value Association (BBVA)**

BBVA represents the work of the private sector in the big data sector. Its main goal is to reinforce the European industrial leadership and capability to successfully complete on global level in the data value solution market. They plan to achieve this by advancing applications into new business opportunities. Its goal is to achieve a 30% of the market share by 2020 and provide solutions for major societal challenges.

**Cyberwatching**

Cyberwatching was funded under the H2020 programme[99] of the European Commission. This project aims to become the online hub for research and innovation in cybersecurity and privacy in Europe. It offers European citizens access to innovate and trustworthy ICT products, services and software. These solutions cover fundamental European rights such as privacy, trust, etc.

### 3.3.2 Current and future challenges

Cybersecurity is becoming an increasingly issue for business worldwide. Its financial and reputational cost of data breaches creates significant headaches for unprepared organizations. Innovation processes always mean adaptation, organizational structures and workforce for adopting the digital world. In terms of businesses it means taking risks by adopting new tools and adapting their systems as soon as possible. In this context cybersecurity challenges can affect many sectors. There are no limits or barriers that limit cyber-attacks. For example, an attack to a website of an organization could be used to penetrate the system and steal data of clients or encrypt the databases (ransomware). According to the Recommendations on Cybersecurity for Europe prepared by the European Cybersecurity Industry Leaders, the fragmentation of the European cybersecurity market is currently the main barrier to the creation of strong European businesses in the field[100].

On the other hand, the ECS itself defines industrial cybersecurity challenges such as[101]:

- Global cybersecurity and ICT market dominated by global suppliers from outside Europe
- European industrial policies not yet addressing specific cybersecurity issues
- Innovation not always properly funded due to a lack of a consistent transnational approach and global EU strategy.

[98] Link: https://ec.europa.eu/commission/sites/beta-political/files/communication-europe-chance-shape-future_en.pdf

[99] Link: https://www.cyberwatching.eu/about/project

[100] Link: https://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/2016-SWD-cPPP-Cybersecurity.pdf

[101] Link: https://www.chariotproject.eu/uploadfiles/04.%20CHARIOT%201st%20Workshop%20-%20ECSO%20Presentation%20and%20Activities%20of%20WG3.pdf

Other areas have been supported by initiatives at the political level in the European Union in order to ensure security and privacy are as follows:

**Energy infrastructures**

To cope with the global growth of energy demands and climate change, there is an increasing need for efficient and optimized use of energy, with the principal objective of saving energy. In the meantime, energy infrastructures are increasingly exposed to cyber threats. The attack surface is increasing due to the massive use of ICT and of new data interfaces, collectors, and other smart devices.

The main cybersecurity challenges identified in this area are:

- High level of complexity and very high volume of interconnected components deployed at country or continent scale.
- Energy systems usually have a long lifetime, sometimes remaining in the field for decades.
- Disaster recovery techniques are required in case of major disruption.[102]

Europe has to face the massive proliferation of IoT technologies, especially when its used in critical domain. Promoting IoT based services for energy efficiency and development would contribute to meeting European region to prevent climate change. The Research and Innovation topics contribute to the achievement of a more competitive, secure and sustainable energy system, with a plan for next decade according to Energy Strategy Frameworks[103].

**Internet of Things**

Many of our devices are connected to the internet collecting and sharing data. Its provides great benefits for the users. IoT represents the next step towards the digitization of our society and economy, where objects and people are interconnected through communication networks and report about their status.

According to a European Commission study the market value of the IoT in the European Union is expected to exceed one trillion euros in 2020[104].

Some of the current challenges limiting the adaptation of IoT[105]:

- Security vulnerabilities: privacy, sabotage, denial of service
- Regulatory and legal issues: banking, manufacturing equipment and infrastructure

**Big Data and Analytics**

Big Data will generate new business opportunities, helps to analyze the behavior of customers and evaluate our products to make better decisions and use that available information for providing a competitive advantage.

[102] ECSO Strategic Research and Innovation Agenda, 2017.

[103] Link: https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/2030-energy-strategy

[104] Link: https://ec.europa.eu/digital-single-market/en/policies/internet-things

[105] Link: https://www.gbnews.ch/the-iot-revolution/

Every year the amount of data is growing, and every person accumulate more and more data. Keeping a large volume of information requires particular conditions, specially space and possibilities. The biggest risks of data are privacy and security issues. Therefore, some of the challenges in this area are[106]:

- Access control and authentication
- Secure data management
- Source validation and filtering
- Application software security
- Infrastructure security

### Industry 4.0

Industry 4.0 is known for its innovation, product environment and all that is completely automated and computerized. This trend is forced by technological, societal and economical transformations where, on the one hand is increase demand for product customization, on another hand is technology push, known as rapid progress in digital intelligence, machine learning technology and increased flexibility of manufacturing infrastructure. In the same time industry in Europe is facing some of competing challenges which need to be addressed with cybersecurity concepts in mind.

The main cybersecurity challenges identified in this area are:

- Low level of maturity
- Difficult to execute
- Need of security infrastructures

### Smart Cities

More than half the world´s population currently lives in cities, and more than 60% will by 2030. Urbanization of the planet demands we learn more about making cities work for everyone. People all over the world are leaving farmland and flocking to cities where they see more opportunities and safety. In the same cities are wide open to cyber-attacks, which presents a real a danger.

The more technologically cities will be more vulnerable to cyber-attacks it is. The main challenges to face are[107]:

- Ensuring that the infrastructure is secure
- Conducting a security audit of technologies before they are implemented
- Preparing an action plan in the case of a cyber attack

### Healthcare

Over the last decade, the progressive adaptation of technology in health has brought about a significant revolution in the way health and health service delivery are viewed and in the means by which patients and health care providers interact with one other.

[106] Big Data Security, ENISA, 2015

[107] ECSO Strategic Research and Innovation Agenda 2017.

Security in healthcare systems, applications and services is positioned as key concern due to the high confidentiality requirements and privacy of sensitive healthcare data.

The impact of using new technologies will be reflected mainly in the following fields:

- mHealth. Use of technologies of mobile in medical practices
- eHealth. National health initiatives and reforms
- Telehealth. Medical services delivered from a distance

Some of the main challenges of the health sector include:

a. Data security and integrity. Its related to network elements and data storage.
b. System availability, business continuity for providing seamless electronic healthcare services and access to critical health information by authorized professionals.
c. Resiliency of all those services against cyberattacks together with prevention and their identification.

**E-services and Telecommunication**

E-services can provide numerous points of profits to citizens and business, including service availability and improved data transparency. This technology could increase participation of citizenship in political affairs.

Some of the main challenges for E-services are:

- Enhance the protection of public administration systems and real locals
- Necessity to cut cost and become more cost-efficient
- Secure exchange of data across borders

Regarding telecommunication, the main objective is fifth generation of mobile communication technologies. This is 40 times faster than existing wireless network. 5G will offer higher speeds of uploading and downloading content, and will help with many procedures in fields such as health or education

Despite having numerous beneficial points, challenges for this technology are still present[108]:

- Planning permission: local authorities need to approve the planning applications, and this takes time.
- High fees and charges to access street furniture: high fees to use street furniture charged by local authorities.

**Transportation**

The transportation situation of Europe in the past decade has progressed substantially and continues to make a notable involvement to European prosperity and employment. European countries have their local plans to improve traffic management with idea to reduce accidents. One of the objective is benefit from a better security, improve the quality of infrastructure and reduce the costs.

[108] Discussion Paper – Setting the scenes for 5G PDF, 2018.

The transportation cover some of specific transportation types including:

a. Smart cars and trucks
b. Maritime vessels
c. Aerial vehicles
d. Railway

The main cybersecurity challenges identified in this area are:

- Privacy is urgently to be protected due to the sensitivity of especially location and movement data
- Weakness in term of protection and detection of cyber-attacks
- High cost to protection of data and computers.

**Standardization**

Standardization is a key instrument for Europe and play an important action in improving approaches to information security across different communities and geographical regions. The main reasons include:

- Promoting effectivity and efficiency of key processes
- Facilitating systems integration
- Establish the approach to deploying new technologies or business models
- Provide economic growth

Digitalization is one of the cybersecurity challenges in this area which doesn't stop. Any standardization initiative at the European level should first reflect the global work of International Standardization Organizations such as: CEN, CENELEC or ETSI.

Industrial interest in standardization activities tends to be driven by areas of work that are in line with the core interests of service providers. Line of standards related to cybersecurity could be represented in different areas and cover technical standards, definitions and organizational tasks. The European Commission, for improving the approach to cybersecurity across Europe, recognized and responded to the need to bring different communities together.

Standardization of security requirements is a market-driven process. To ensure a convergent application of security standards, all European Member States should encourage compliance or conformity with specified standards to ensure a high level of security at the EU level. To this end, it might be necessary to draft harmonized standards.

### 3.3.3 Recommendations

Cybersecurity can make innovation possible and help emphasize data as a "new oil" of world economy. For the digital future and its security, it may need be necessary:

- Address threats to online platforms and allow them to contribute positively to society
- Support small and medium enterprises to be competitive in the digital economy
- Invest in the use of artificial intelligence and supercomputers in areas of energy, healthcare or transportation

Trust and confidence are essential points in the digital world. However, cybersecurity incidents cause important economic damage to European business, industry and the entire economy every day. Digital threats are habitually evolving and handling a large-scale cyber incident in diverse Member States simultaneously is a challenge for all of Europe.

Only a coordinated response based on cross-border exchange of information, can address such a risk in the most efficient way[109].

Industry is affected to all kinds of threats, that becomes very costly and inefficient when faced with a multitude of increasing risks. In many cases they come from international countries and affect more than one European country.

Europe must change its strategy and work together with other countries to improve cybersecurity. It is a more effective way than working in isolation. This would help us build a high level of trust in society for our digital economy. In collaboration with other countries, must establish a plan for responding to cyber-attacks and support global stability through international cooperation. One way to achieve this is to focus on big data and machine intelligence for discuss the business model of technology and innovations.

Despite an almost constant stream of media reports of cyberattacks and privacy incidents, there are still many devices that do not use encrypted communications or proper authentication, it is essential that smart home devices, or any IoT device for that matter, use authentication and mutual encryption[110].

Cybercrime is fundamentally an important concern for much markets, businesses and citizens. In many countries, not only in EU, societies have come to rely on cyberspace to do business, develop the industry, consume products and services or exchange information with other online. Regarding standardization some of the recommendations done by EU:

- Policy-makers should continue to encourage vendors to agree on the use of standards and encourage both private and public-sector organizations to include references to these standards in procurement processes.
- Incorporation of standards as part of national cybersecurity strategy for national governments.
- Use of standards as a point of reference in enforcing regulations from part of National Regulatory Organization.

Cooperation of countries and their governments for facilitate better work to define a broad certification scheme allowing end users to verify that products or services are complained with security standards[111].

[109] Link: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk5iif5wblzg?ctx=vhyzn0ikkwxq&v=1&tab=1&start_tab0=40.

[110] Link: https://ciberseguridad.blog/ciberataques-a-infraestructuras-criticas.

[111] Link: https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security.

# 4 Existing cybersecurity challenges in Japan

In this section, we analyze and document the cybersecurity challenges in Japan from three perspectives: legal and policy, research and innovation, and the industry and standardization. We benefited from bilateral meetings and e-mail exchanges with associate partners in Japan, namely Nara Institute of Science and Technology, University of Tokyo, Meiji University, Japan Advanced Institute of Science and Technology, JPCERT Coordination Center, National Institute of Information and Communications Technology, and NTT Secure Platform Laboratories. We also benefited from bilateral meeting with Ministry of Economy, Trade and Industry, and Ministry of Internal Affairs and Communications. These meetings and analysis was facilitated by the Nara Institute of Science and Technology.

## 4.1 Legal and policy in Japan

This subsection describes legal and policy challenges that were identified through bilateral meetings as well as e-mail exchanges between Japanese associate partners, in addition to bilateral meetings with key ministries and specialized agencies, as well as the analysis of key cybersecurity strategy documents in Japan. We begin with the description of status and gaps in the legal and policy area, followed by the current and future challenges for Japanese legal and policy instruments. Finally, we describe recommendations in the legal and policy area.

### 4.1.1 Status and gaps

Cybersecurity and privacy policies in Japan have been mainly led by two ministries, METI (Ministry of Economy, Trade and Industry), which is in charge of computing, as well as MIC (Ministry of Internal Affairs and Communications), which is in charge of communication. While the split of duties works for most of the time, both cybersecurity and privacy require consideration from both computing and communication aspects. Based on this kind of analysis, NISC (National center of Incident readiness and Strategy for Cybersecurity) was established under Cabinet secretariat as a cross-ministerial organization where it serves as the focal point for cybersecurity policy and legislation. Virtually every ministry is represented at NISC, thus its coordination capability has been the key enabler to harmonize cybersecurity and privacy policies. In addition to NISC, inter-ministerial coordination has been common in the cybersecurity and privacy issues.

Due to these strong cooperation mechanisms and the ongoing dialogue across government agencies, industry bodies and academia, Japan has been working on cybersecurity and privacy policies since its early days. Cybersecurity policies in Japan have been led by the Cybersecurity Strategic Headquarters under the auspices of Prime Minister and NISC, where government agencies, industry bodies and academia also participate in the deliberation. Privacy policies in Japan have been led by the IT Strategic Headquarters and more recently the Personal Information Protection Commission.

There are several other national strategic headquarters in addition to cybersecurity, such as one for IT, and another one for space policy. Although these topics are fundamentally linked with each other, the coordination among these strategic headquarters is left to higher level bodies.

Council for Science, Technology and Innovation (CSTI) serves as the key instrument in the innovation policy across all STEM-enabled fields, thus the Science and Technology

Basic Plan, which is drawn up based on the Science and Technology Basic Law and revised every five year, has broad implications to the cybersecurity and privacy policy. Most notably, Society 5.0 was proposed in the 5th Science and Technology Basic Plan as a future society that Japan should aspire to: "a human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space." In the Society 5.0 vision, cybersecurity is considered to be one of the key enablers.

### 4.1.2 Current and future challenges

A broad array of policy instruments exists to designate variety of tasks to specialized agencies, as one can observe in the Basic Act on Cybersecurity. However, Japan has limited number of specialized agencies with limited number of workforce, thus their effectiveness will be questioned over time. It is fair to say that the cybersecurity strategy and its annual update have been written with strong representation of ministries and underlying specialized agencies, thus such delegation of duties to ministries and agencies are intrinsic. Considering the growing importance of assumed responsibilities, it will be necessary to maximize effectiveness of each policy package by growing the ecosystems elsewhere, i.e., in the private industry and universities. While several countries established cybersecurity accelerators and academic cybersecurity centers and education programs, Japan did not actively pursue this avenue, resulting in the relative lack of cybersecurity start-ups and cybersecurity researchers.

In a broader context, cybersecurity is just one of the desirable features of IT, in addition to scalability, agility, ease of maintenance, reliability, cost efficiency, and automation. From the perspective of technology adopters, feature interoperability is clearly needed so that scalable, cheap and agile cloud can be secure, while in reality silo effect is intrinsic in the focused policy programs. As cross-fertilization is the key to any type of innovation, policy programs for cybersecurity can follow the cybersecurity strategy and break the barrier between "cybersecurity and others" so that we can benefit from scalable, cheap, automated and agile technologies that are also cyber-secure.

It is also imperative to recognize that the scale of cybersecurity investment in the private sector is much larger than that of public sector. Thus, cybersecurity strategy at national level should clearly indicate the ongoing dialogue with private sector, which implicitly forms the basis of current cybersecurity strategy in Japan. Such clear indication is essential in the broader context of international cooperation, as it is necessary to avoid confusion among developing countries that often refer to national cybersecurity strategies of several countries without access to the same degree of informed dialogue with private sector. As cyberspace is comprised of diverse stakeholders across private and public sectors, cybersecurity policy should continually reaffirm the fact that cybersecurity cannot be improved solely by the efforts of public sector.

### 4.1.3 Recommendations

Consider introducing policy instruments to facilitate innovations in the cybersecurity space, by analyzing the success of cybersecurity accelerators and academic cybersecurity centers in other countries. The Cybersecurity Strategy Headquarter compiled and issued the report[112] (in Japanese) entitled "cybersecurity workforce

[112] Link: https://www.nisc.go.jp/active/kihon/pdf/jinzai2017.pdf

development program" in April 2017, in which we can verify the lack of references to cybersecurity accelerators and academic cybersecurity centers.

Recognizing the fact that cybersecurity is only one desirable characteristics of IT, develop cybersecurity policy programs that also enable improvements of other desirable features such as scalability, agility, ease of maintenance, reliability, cost efficiency, and automation. This will be essential to promote cybersecurity and privacy in modern enterprises that are also interested in benefiting from latest technologies, such as cloud, IoT and big data. While a lot of public effort has been spent on the guidelines and best practices with specific focus on privacy and cybersecurity, businesses are in some cases prioritizing scalability, agility and cost efficiency over privacy and cybersecurity such that existing guidelines and best practices may not readily apply to the new breed of technologies. While one can argue that innovative technologies are largely coming from private enterprises with different security architecture and different technical instantiations, multi-stakeholder dialogue to obtain certain level of visibility into those emerging platforms will be crucial to assure privacy and security on top of them. Although certain technologies attracted enough level of interest to come up with technology-specific guidelines, e.g., IoT security guideline[113], multiple, often competing set of technical instantiations bear different security implications such that the guideline-based approach cannot address fundamental issues in each security architecture.

Recognizing the general preference of existing policy instruments to deal with platform-agnostic, catch-all approach to particular emerging technology, develop cybersecurity policy programs that deal with particular platform in order to minimize damage to privacy and security. This will be crucial, as several competing platforms tend to dominate the market while at the same time trying to avoid technical similarities. This phenomenon can be frequently observed almost everywhere, e.g., Android and iOS on smartphone, AWS and Azure on cloud, etc. Bearing in mind that each of these platforms are large enough and considerably different from each other under the same collective term such as smartphone and cloud, develop policy programs that deal with each dominant technical instantiation in order to understand the damage to privacy and security in each platform.

Recognizing the fact that cybersecurity investment in the private sector is much larger than that of public sector, elaborate the public-private partnership in the strategy documents such that other countries can avoid being blinded by the public sector efforts. While Japan does not possess explicit, contractual public-private partnership for cybersecurity like ECSO, it maintains a quite strong but implicit collaboration framework between private sector and public sector, as we can witness from the activities of Keidanren (Japan Business Federation) and JNSA (Japan Network Security Association) whose details are documented in D3.1. Such elicitation will be useful toward possible public-private partnerships across EU-Japan in near future, which will be eventually necessary to facilitate trade and cooperation across two major economies.

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

## 4.2 Research and Innovation in Japan

This subsection describes research and innovation challenges that were identified through bilateral meetings as well as e-mail exchanges between Japanese associate partners, in addition to bilateral meetings with key specialized agencies that are responsible for research and innovation in the cybersecurity and privacy domain. We begin with the description of status and gaps in the research and innovation area, followed by the current and future challenges for Japanese research and innovation ecosystem. Finally, we describe recommendations based on the above analysis.

### 4.2.1 Status and gaps

Japan has a strong research ecosystem for cryptography and information security, which still influences the basis of cybersecurity research and innovation programs. In contrast, system security, network security and human aspects of security were embraced by smaller communities such that research and innovation in these areas, particularly in academic sectors, have been rather limited. This can be partly attributed to the beauty of academic study in cryptography and information security, where mathematics and formalism have been mobilized to their fullest extent such that scientists exclude human factors in order to make the equations *solvable*. In the light of academic beauty, scientists have historically avoided network security, system security and human aspects, as these branches of study require one to deal with failures and adversaries with partial information and uncertainties.

Public funding to animate and grow cybersecurity research communities does exist[114] and will continue to foster young experts in this area, such as the Strategic Information and Communications R&D Promotion Program (SCOPE) and the New Energy and Industrial Technology Development Organization (NEDO). These funding programs however do not require cooperation between business entities and academic entities, sometimes resulting in direct competition among them. Therefore academic entities were less incentivized to work in this area.

Japan also maintains a strong research ecosystem for machine learning and deep learning[115], which can be more suitable to deal with partial information and uncertainties. Cybersecurity research in Japan is thus benefiting from its cross-fertilization with machine learning research. For instance, National Institute of Information and Communications Technology (NICT) employs machine-learning based analysis for improved visibility into network anomalies and smartphone malware[116].

Industry has business ecosystem to drive their own research and employ innovative technologies. According to the JNSA (Japan Network Security Association) IT Security Market Analysis Report 2016, IT security market in Japan was approximately 979 billion yen in 2017, which translates to 7.6 billion euros. Despite the large business ecosystem, large technology suppliers often seek public funding for their own research. Younger technology companies conduct research at enormous scale in the cybersecurity and privacy domain, whose details are not publicly available.

---

[114] See Section 3.1.2 of EUNITY Project Deliverable 3.1: Preliminary version of the Cybersecurity Research Analysis Report for the two regions

[115] 5 Countries Leading the Way in AI, https://www.futuresplatform.com/blog/5-countries-leading-way-ai-artificial-intelligence-machine-learning

[116] NICT Cybersecurity Laboratory, https://www.nict.go.jp/en/cyber/index.html

Specialized agencies such as NICT and IPA are also assisting research and innovation in the cybersecurity and privacy domain. Their scale of investment is limited in comparison with that of private sector, however.

### 4.2.2 Current and future challenges

While a lot of effort has been put into cryptography and information security, the ignorance of "human in the loop" and the academic pursuit to confine the problem into the domain of mathematics and formalism have dropped a large shadow on the safety of crypto-based systems. The record-breaking theft of crypto-currencies in Japan[117] is one such example where the extensive use of cryptographic methods blinded general public. Its lack of expertise on formal methods, system security and network security affected their assets at enormous scale either through faulty smart contracts, vulnerable software or vulnerable networking protocols.

It is thus imperative to overcome the compartmentalized structure of research and invite younger generations to obtain holistic understanding of cryptography, formal methods, system security, network security and hardware security. Many research laboratories, especially in the universities, specializes on particular branches of security studies such that young researchers in one laboratory can be specialists on hardware security despite sheer lack of knowledge on software security and network security. A crosscutting security education program did exist in Japan before[118], but is no longer funded.

Society 5.0 is effectively inviting researchers in diverse fields to explore human-centric approaches. As Cybersecurity Strategic Headquarter suggested in its 2017 cybersecurity R&D strategy[119], human-centric cybersecurity can be the next frontier of cybersecurity, although limited attempts for cross-fertilization have been made, e.g., psychology and cybersecurity, economics and cybersecurity, etc. Since major funding for cybersecurity in Japan comes from METI, MIC and their specialized agencies, non-technical branches of universities are normally oblivious of such opportunities for research. Since university does not automatically guarantee cross-fertilization, concrete and diverse approaches should be explored to animate the compartmentalized institution toward Society 5.0.

### 4.2.3 Recommendations

Recognizing the fact that specialized agencies and private sector are functioning both as R&D entities as well as sources of funding, develop funding programs that incentivize academic entities to work with private sector or specialized agencies in the cybersecurity and privacy domains. Unless strong incentives are introduced, academic entities will be less inclined to work in these domains due to their technical complexity, lack of operational experience, lack of real and latest dataset, in addition to legal complexities and ethical implications. While the business entities and government agencies prefer scale and realism, the pursuit for scale and realism may discourage younger generations to choose cybersecurity and privacy as their topic of study, since other branches of study such as data science and robotics already offer equally lucrative career without such complexities. Such tension for realism versus simplicity can be

[117] Japan's Coincheck suffers record $530m virtual currency theft, https://asia.nikkei.com/Spotlight/Bitcoin-evolution/Japan-s-Coincheck-suffers-record-530m-virtual-currency-theft

[118] Link: https://www.seccap.jp/gs/

[119] Link: https://www.nisc.go.jp/active/kihon/pdf/kenkyu2017.pdf

commonly observed in the academic setting. While industry experts may prefer to criticize simplified CTF (Capture The Flag) as *just a puzzle*, such simplified problem setting with clearly defined incentives has been functioning as an effective recruiting tool in many cybersecurity research labs.

Recognizing the general trend that platform technologies are eventually going to be black box with distinct security architecture, invite academic and public studies on the design and engineering of white-box counterpart with sound security architecture. Even if such white-box counterpart lacks scale and realism in terms of technology, business and compliance, it can serve as a useful instrument for scientific analysis, explorative engineering as well as for education in the engineering departments. We can find ample evidence in the computer science education, e.g., NachOS for operating system education. It is also worth noting that even the Internet architecture emerged out of academic research activities to overcome diversity in underlying, mutually competing network architectures, resulting in a globally embraced, common and simplified architecture that has fundamentally transformed the networking industry.

Reinvigorate crosscutting security education programs such that young talents can obtain holistic understanding of cryptography, formal methods, system security, network security and hardware security. While security education has been improvised with existing assets in the past, both government and industry have recently come up with reasonable definition of security professionals such that the coverage of any security education program in Japan can now be evaluated against predefined workforce requirements as set forth by both government and industry. Thus, each security education program can no longer be an arbitrary collection of theories, heuristics and tools.

Explore human-centric approaches to cybersecurity by cross-fertilization with social sciences, humanities studies and other fields that traditionally had fewer links to cybersecurity studies. In addition to being holistic in terms of security technology, security education programs should also seek to introduce human aspects as well as business aspects into the program by drawing inspiration from the 2017 cybersecurity R&D strategy. Likewise, research and innovation in this area should be actively pursued by reaching out to broader communities of social sciences, humanities studies and other fields such as economics, for instance by extending the scope of technology-oriented funding programs.

## 4.3 Industry and standardization in Japan

This subsection describes industry and standardization challenges that were identified through bilateral meetings as well as e-mail exchanges between Japanese associate partners, in addition to bilateral meetings with key industry experts who work for industry and standardization in the cybersecurity and privacy domain, as well as the analysis of key cybersecurity documents from Japanese industry groups. We begin with the description of status and gaps in the industry and standardization area, followed by the current and future challenges for Japanese industry and standardization activities. Finally, recommendations are made based on the above analysis.

### 4.3.1 Status and gaps

Japan has a strong ecosystem of technology innovation within technology suppliers, which can be observed by the large number of patents that are filed by these large enterprises. These large technology companies have been embracing cybersecurity through acquisitions of cybersecurity talents and start-ups in Japan, in addition to business partnerships with foreign cybersecurity companies.

Technology adopters, however, were slow to recognize the importance of cybersecurity due to their relative lack of technology expertise, as well as their lack of business and organizational expertise to deal with a new kind of risk that intrinsically requires cross-institutional cooperation.

Historically, there has been a clear split of technology suppliers and adopters within the industry, thus technology adopters largely entrusted and relied on the technology suppliers for all kinds of electronic equipment and communication device. Drawing on their past experience on the technology maturity process, technology adopters thus were reluctant to introduce new organizational instruments to deal with ongoing cyber risk, assuming that cyber risks will be eventually eliminated by the technology suppliers through their effort to mature the technology. Through painful lessons on malware incidents and data breaches over the past two decades, technology adopters eventually realized that cyber risks are intrinsically associated with the use of technology, thus the technology expertise cannot be entirely outsourced to technology suppliers.

Consequently, there is strong interest across industries to capacity building programs[120], in order to train their employees and managers at all levels. Technology suppliers are already providing multiple training programs, cyber-ranges and certification programs for their own employees as well as their customers. Technology suppliers and adopters also joined forces to analyze and define the types of cybersecurity workforce. Technology adopters are also benefiting from training programs that are operated by specialized agencies, such as the Industrial Cyber Security Center of Excellence (ICSCoE) operated by the IPA (Information-technology Promotion Agency).

Both technology suppliers and adopters are building cross-institutional cooperation through ISACs and other collaboration mechanisms. National CSIRT Association (NCA) is one such collaboration mechanism where CSIRT organizations across industries meet and share working practices among them.

### 4.3.2 Current and future challenges

Japanese industry recognizes the deep split between technology suppliers and adopters, which clearly needs to be addressed in a full-spectrum approach.

Japan has remarkably low mobility of cybersecurity experts across technology suppliers and adopters, thus technology adopters often have difficulty in understanding the cyber risk associated with their business. The low mobility is further exacerbated by the lack of *career path* within most technology adopters[121]. Technology suppliers, in contrast, are pretty much occupied with large enterprise customers who have been gaining competitive edge through advanced cybersecurity. Thus *digital divide* is manifesting in the cybersecurity adoption: skeptics are left unprotected without understanding the nature of the problem, while early adopters are more actively engaged in cybersecurity at all levels in order to remain competent.

Few technology suppliers are actually seeking economies of scale, thereby most of the latest technology offerings are only available to large enterprises. Consequently, most

[120] Japan Business Federation (Keidanren) – Second Proposal for Reinforcing Cybersecurity Measures, http://www.keidanren.or.jp/en/policy/2016/006_proposal.html

[121] There is an ongoing project to design career path for cybersecurity workforce under the auspices of Keidanren, which will eventually contribute to the improved mobility. http://cyber-risk.or.jp/sansanren/index.html

of small and medium businesses remain unprotected, although they are an essential part of the supply chain. Cloud computing has been widely embraced by small and medium businesses because of economies of scale, although the security of cloud computing varies from provider to provider, eventually recreating the market of lemons and generating certain degree of distrust and fear among skeptics, or overtrust and epic failures among optimistic technology adopters.

If technology suppliers and adopters fail to come up with realistic business arrangements that work for small and medium businesses, most of their businesses domains will be disrupted by the next generation of enterprises that act as both technology suppliers and adopters.

### 4.3.3 Recommendations

Recast cybersecurity adoption as an urgent digital divide problem that needs to be addressed at industry associations as well as regional industry groups, highlighting existing policy documents from ministries as well as guidance from Keidanren. Industry groups should analyze the root cause of skepticism that hinder cybersecurity adoption and devise awareness campaigns that originate from trusted sources in each industry and in each region, so that guidance and best practices can be embraced. While both government agencies and industry leaders have been actively promoting cybersecurity for many years, the originator of the message has been mostly limited to Keidanren, METI, IPA or NISC. Industry leaders should recognize the fact that trusted source of guidance is different from industry to industry. For instance, in order to effectively deliver message to the automotive sector, it should be originating from MLIT (Ministry of Land, Infrastructure and Transport) or from JAMA (Japan Automobile Manufacturers Association).

Technology suppliers are recommended to seek economies of scale and deliver affordable products and services for small and medium businesses, e.g., by obtaining hints from the cloud computing businesses. Cloud service providers have been innovating service offerings through latest virtual machines, containers, software-defined storage and software-defined networks that collectively enable on-demand IT infrastructure at nominal cost. While cloud enabled young programmers to deliver services that scale, they are often oblivious of entire technology stacks and associated security and privacy best practices in each technology layer, thereby leaving their cloud deployment prone to attacks such as JavaScript-based crypto-mining, or ransom threats on the cloud storage. Technology suppliers can contribute in this space by transforming their existing offerings to cloud or by introducing innovative products and services that contribute to improved cybersecurity and privacy in the cloud.

Consider forging business partnerships and strategic agreements among technology suppliers and adopters so that common understanding on cybersecurity can be fostered within particular business domains. Such partnerships and agreements can be conceived at multiple levels, ranging from large enterprises to small and medium businesses. In addition, regional business groups can also facilitate such dialogue across technology suppliers and adopters. While Tokyo accommodates a large number of seminars and business conferences for cybersecurity and privacy in general, technology adopters within particular business domain prefer to discuss in their business context, existing business priorities and domain-specific business language. Thus technology suppliers and cybersecurity leaders within each industry sector should reach out to regional groups and industry associations in order to facilitate dialogue and to explore partnerships.

# 5 Cooperation opportunities

## 5.1 Legal and policy opportunities

### 5.1.1 Existing collaboration

To date, the main current collaboration opportunities are listed hereby:

- On a broad sale, an EU-Japan trade agreement is in the pipeline to be voted by the European Parliament[122]. This concludes a six-years negotiation, which will impact all trade sectors and beyond. Such a big-scale deal will in fact facilitate the cooperation between the EU and Japan on all domains, becoming the first milestone achieved in the light of bringing the two regions closer.
- In the digital area, an adequacy decision is expected to be agreed very soon. As it will be explained below, this is going to be a very important deal for the digital community, as it will facilitate the exchange of personal data between the two regions, without any administrative burden[123].
- A number of minor initiatives have been set, which, collectively, indicate the strong reciprocal willingness to engage in further and more fruitful discussions on ways to collaborate with each other. For instance, the EU-Japan Cyber Dialogue[124] remarks the importance of negotiation and diplomacy in the cyberspace.

### 5.1.2 Perspective of cooperation in both regions

It first needs to be noted that the situation across the two regions is by nature substantially different for a number of reasons. To start with, Japan does not present vertical harmonization issues as it is a single country. Contrarily, the European Union, being formed by 28 Member States, presents a complex multi-level structure which makes the harmonization of laws and policies one of its biggest challenges.

Taken the two regions comparatively, however, and considering the need of bringing them closer, a number of elements to reflect on are hereby given. Overall, it is of EUNITY partner's opinion that a number of gaps could be filled on certain domains, thus enhancing and facilitating the cooperation of the European Union and Japan on privacy and cybersecurity policy matters.

To start with, the most imminent issue is the privacy framework as such[125]. Japan and the European Union have shown the strength of cooperating one another by coming very close to signing an adequacy decision[126], which would allow for cross border data transfers without overwhelming administrative burdens for who decides to undertake such a practice. The immediate effect of that could be that, given the limited resources of public sectors against a much wider financial availability of the private business, enabling personal data exchange between the two regions might help private-public

[122] Link: https://www.euractiv.com/section/economy-jobs/opinion/the-eu-japan-trade-deal-a-no-brainer/

[123] Link: http://europa.eu/rapid/press-release_IP-18-4501_en.htm

[124] Link: https://eeas.europa.eu/topics/security-defence-crisis-response/41330/3rd-eu-%E2%80%93-japan-cyber-dialogue-joint-elements_en

[125] Link: https://www.lexology.com/library/detail.aspx?g=242aba70-edd5-4d6c-b818-4938ea1a42a5

[126] Link: https://ec.europa.eu/info/sites/info/files/draft_adequacy_decision.pdf

partnerships with cross-regional nature, thus including both EU and Japanese public and private partners within the same umbrella.

The next challenge is and will be touching upon police and law enforcement cooperation. As the data protection framework within the EU was duly reformed also for personal information processed in the police sector, the transnational nature of certain types of crimes (specially cybercrimes) will require soon the decision maker to take a look at what data protection standards to apply when certain data are transferred to European partners like Japan. Japanese and European authorities might thus be engaged in a near future on the comparison and alignment of each other's policies, rules and procedures on such transfers. Any such discussion will foster the rule of law outside the borders of the EU, forcing all actors to have a fair, genuine and fruitful exchange of views on the basic principles of human rights, civil liberties and fundamental freedoms, alongside becoming an opportunity for strengthening the cooperation between the two regions.

On a cyber-security level, a number of policies might help collaboration between the European Union and Japan.

Firstly, as identified by both EU and Japan legal and policy outline in this report, IoT certification is one of the key elements that our decision makers will have to look at, as well as a crucial cooperation opportunity. Much has to be done in Europe with regard to vulnerabilities handling and disclosure policies, whilst Japan seems to have a more robust framework on this[127]. Harmonizing the two regions on such a pivotal issue would mean opening the chance to further develop basic certification schemes that are to be advanced in the cybersecurity sector. Whilst such certifications seem to go toward a generalist approach[128], rather than a sector-specific one, this wide stance could lead the two regions to align with each other, lifting their respective security standards on the uprising world of the Internet of Things.

On a governance level, the role of ENISA within the new cybersecurity framework should and could be aligned to the External Action Service (EEAS) tasks of bolstering international cooperation on digital matters. As it is now, the mandate and scope of the agency is to serve EU citizens and corporations only. However, given the internationalization of security standards and the need of a wider collaboration in the area of cybersecurity, a future harmonization between the two regions passes through the crucial role of ENISA in engaging with their Japanese counterparts (to be identified amongst METI, MIC and NISC) and thus leading the way of the technical discussions in such cooperation mechanisms.

Coming down to the soft policy domain, as the Japanese analysis outlined, the limited number of workforce in their agencies, enabling a strong collaboration would help training each other's staff and personnel on best practices and business optimization, thus harmonizing and reducing resources allocation in the cybersecurity field of the public and private domains. However, funding opportunities should also be combined. As the success of Japanese cybersecurity training projects in Africa has shown, a similar agenda should be jointly developed by the two regions to optimize the resources

[127] Link: https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

[128] Link: https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/#

and create a high-level series of training programs oriented to under-developed regions in the Balkans, Asia, Middle East and Africa.

A last point, on a much wider context, should be here made. It needs to be remarked that the collaboration opportunities should not be limited to cybersecurity only. Rather, what stated above should serve as a scalable example to be reproduced (with the due measures and exceptions), on other fields of information technology, such as agility, reliability or automation.

## 5.2 Research and innovation

Cybersecurity is very important in both regions, but some aspects can be found, which need special attention. Some of these aspects have been pointed out in Deliverable 3.1. One of the main similarities is the fact that both regions pay much attention to cybersecurity, seeking in this area many strategic opportunities for collaboration.

### 5.2.1 Existing collaboration

EU-Japan have collaborated in the previous Work Programmes (FP6, FP7) and they continue to collaborate and work together in a number of domains throughout the H2020 Work Programme. Existing research collaborations are not many in the cybersecurity domain although there are some coordinated calls specific for the cybersecurity every two years (EUJ-2016,2018). Many collaborations opportunities also exist in other, non-cybersecurity calls. Probably there is a need for broaden the cybersecurity related collaboration via other calls as well. In this paragraph we first present the existing/active collaborations that were realized via the coordinated calls and then we include information about collaborations performed in the context of other domains (e.g climate, materials etc.). Recently a new cooperation agreement has been signed between the European Commission (EC) and the Japan Science and Technology Agency (JST) to strengthen researcher's cooperation on 7th of October 2018[129]. Although the cooperation agreement between the two parties provide opportunities for Japanese researcher to collaborate with ERC funded researchers through mutual visits is a step forward for the joint collaboration of the two regions in other research aspects as well. Many research domains for possible collaboration were included in the 2016 and 2017 H2020 calls as described in the respective EURAXESS document[130]. There are EU-JP coordinated calls and calls where Japan is included and eligible to participate. The coordinated calls of the H2020 2016 present collaborations between EU and JP partners in the areas of 5G networks, IoT/Cloud/Big Data platforms, experimental testbeds and Novel ICT Robotics based solutions. Below we summarize the four 2016 coordinated calls and provide information about the participating partners for both regions although only one of the studied projects seems to address security related objectives (EUJ-02-2016 with project BigClout).

**H2020 2016 EU-JP coordinated calls[131] include:**

1. EUJ-01-2016: "5G – Next Generation Communication Networks" and the funded projects under this call are:
    a. 5G MiEdge: Millimeter-wave Edge cloud as an enabler for 5G ecosystem.

[129] Link: https://ec.europa.eu/research/iscp/index.cfm?pg=japan

[130] Link: https://cdn3.euraxess.org/sites/default/files/domains/japan/wp2016-2017_japan_calls.pdf

[131] Link: https://cordis.europa.eu/search/result_en?q=contenttype=%27project%27%20AND%20/project/relations/associations/relatedCall/call/identifier=%27H2020-EUJ-2016-1%27

   b. 5GPagoda: A network slice for every service.
2. EUJ-02-2016: "IoT/Cloud/Big Data platforms in social application contexts" and the funded projects under this call are:
   a. BigClouT: Big data meeting Cloud and IoT for empowering the citizen clout in smart cities**.** This is the only project out of the seven that has some security related objectives.
   b. City Platform as a Service - Integrated and Open.
3. EUJ-03-2016: "Experimental testbeds on Information-Centric Networking" and the funded project under this call is:
   a. ICN2020: Advancing ICN towards real-world deployment through research, innovative applications, and global scale experimentation.
4. SC1-PM-14-2016: "Novel ICT Robotics based solutions for active and healthy ageing at home or in care facilities" and the funded projects under this call are:
   a. ACCRA: Agile Co-Creation of Robots for Ageing.
   b. CARESSES: Culture Aware Robots and Environmental Sensor Systems for Elderly Support.

Table 1 Summary of the EUJ-2016 coordinated calls funded projects and partners for both regions

| Area/call | Project | Members | | |
|---|---|---|---|---|
| | | **Industry** | **Research** | **Other** |
| **5G Next Generation Networks** | 5G MiEdge[132] | EU:<br>1. Intel Deutschland<br>2. Telecom Italia SPA | EU:<br>1. Fraunhofer Germany<br>2. Sapienza University di Roma<br>3. French Alternative Energies and Atomic Energy Commission | EU: |
| | | JP:Panasonic Corporation | JP:<br>1. Tokyo Institute of Technology<br>2. KDDI Research | JP: |
| | 5GPagoda | EU:<br>1. Ericsson Ab Finland<br>2. Orange Polska S.A<br>3. Device Gateway SA Switzerland | EU:<br>1. Aalto-korkeakoulusäätiö Finland,<br>2. Fraunhofer Germany<br>3. Eurecom Institute France | EU:<br>1. Mandat International Switzerland |
| | | JP:<br>1. HITACHI, Ltd. Japan<br>2. KDDI R&D Laboratories, Inc. Japan<br>3. NEC Networks & System Integration Japan | JP:<br>1. The University of Tokyo<br>2. Waseda university | |
| **IoT/Cloud/Big Data platforms** | **BigClouT** | EU:<br>1. Engineering – SPA Italy<br>2. ABSISKEY CP France | EU:<br>1. French Alternative Energies and Atomic Energy Commission<br>2. Institute of Communication and Computer Systems | |
| | | JP: | JP: | JP: |

[132] Link: https://5g-miedge.eu

| | | | | |
|---|---|---|---|---|
| | | 1. Nippon Telegraph and Telephone East Corporation<br>2. Nippon Telegraph and Telephone corporation<br>3. Bristolisopen limited | 1. University of Tsukuba<br>2. Lancaster university –school of computing and communications<br>3. Keio university<br>4. National Institute of Informatics | 1. Grenoble-alpes metropole<br>2. Tsukuba city<br>3. Fujisawa city |
| | CPaaS IO | EU:<br>1. AGT international<br>2. NEC UK<br>3. Odins Solutions SE | EU:<br>1. Bern University of Applied Sciences(e-gov. Institute)<br>2. University of Surrey UK | EU:<br>1. The Things Network org. |
| | | JP:<br>1. Ubiquitous Networking Lab.<br>2. Microsoft<br>3. Access company<br>4. Ubiquitous Computing Technology Corp. | JP:<br>1. University of Tokyo | |
| **Experimental testbeds** | ICN2020 | EU:<br>1. Cisco Systems France Sarl<br>2. Ericsson AB Sweden | EU:<br>1. Georg-August-Universität Göttingen<br>2. Universita' degli Studi di Roma Tor Vergata<br>3. University College London<br>4. Institut de Recherche Technologique SystemX | |
| | | JP:<br>1. Kozo Keikaku Engineering Inc | JP:<br>1. KDDI R&D Laboratories Inc<br>2. Osaka City University<br>3. Osaka University | |
| **Novel ICT Robotics based solutions** | ACCRA | EU:<br>1. Trialog France<br>2. Buddy the Robot | EU:<br>1. Sant' Anna School of Advanced studies Pisa<br>2. Erasmus University Rotterdam<br>3. Dauphine University Paris | EU:<br>1. Opera di San Pio da Pietrelcina |
| | | JP:<br>1. ConnectDOT | JP:<br>1. Kyoto University<br>2. Kobe University | |
| | CARESSES | EU:<br>1. SoftBank Robotics France<br>2. Advinia Health Care UK | EU:<br>1. Universita Degli Studi Di Genova<br>2. Orebro Universitet<br>3. Middlesex University London<br>4. University of Bedfordshire | |
| | | JP: | JP:<br>1. JAIST: Japan Advanced Institute of Science and Technology<br>2. Nagoya University<br>3. Chubu University | |

Further summarizing the information in the table above the viewer can easily observe that the EU participates in those projects with **16 organizations from the industry** sector while Japan participates with **13 organizations**. The case is somehow similar in the research domain where **21 Universities participate from the EU side** and **14 from the Japanese side**. Moreover, in some projects, partners from the public sector (municipalities) consultancy companies (Mandat International CH) and standardization bodies also participate in these projects. From a geographical perspective the countries that collaborate with the Japan partners in the aforementioned projects are: Germany, Italy, Spain, France, Greece, UK, Finland, Poland, Switzerland, The Netherlands, Sweden. There are eleven (11) countries eligible for EU funding that are participating in these seven (7) collaboration projects. From a per country participation view in these 7 projects someone can see that France is participating in almost all projects (6/7) while Greece, Finland, Poland and Spain participate in one out of the seven projects (Figure 4)

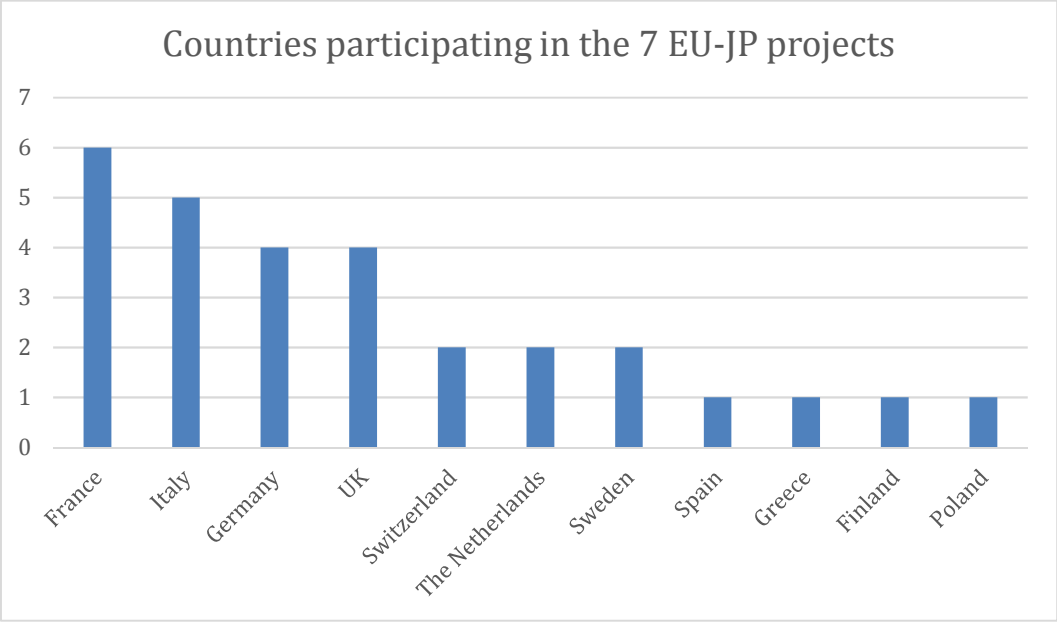


Figure 4 Countries participating in those 7 EU-JP projects

While counting partners per country, France is participating in these projects with ten (10) different organizations followed by UK, which participates with eight (8) organizations (Figure ).

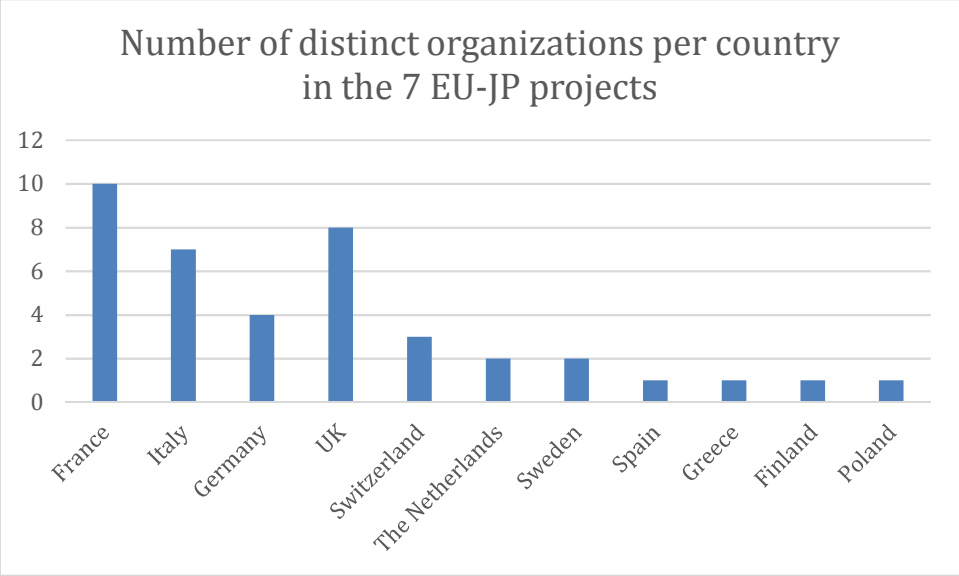


Figure 5. Number of distinct organizations per country

**H2020 2018 EU-JP coordinated calls[133] include:**

1. EUJ-01-2018: "Advanced technologies (Security/Cloud/IoT/BigData) for a hyper-connected society in the context of Smart City" and the funded projects under this call are:
   a. Fed4IoT[134]: Federating IoT and cloud infrastructures to provide scalable and interoperable Smart Cities applications, by introducing novel IoT virtualization technologies.
   b. M-Sec[135]: Multi-layered Security technologies to ensure hyper connected smart cities with Blockchain, BigData, Cloud and IoT.
2. EUJ-02-2018: "5G and beyond" and the funded projects under this call are:
   a. ThoR[136]: TeraHertz end-to-end wireless systems supporting ultra-high data Rate applications.
   b. 5G=Enhance[137]: 5G Enhanced Mobile Broadband Access Networks in Crowded Environments.

Table 2 Summary of the EUJ-2018 coordinated calls funded projects and partners for both regions

| Area/call | Project | Members | | |
|---|---|---|---|---|
| | | Industry | Research | Other |
| Advanced technologies (Security / Cloud / IoT / BigData) | Fed4IoT | EU:<br>1. Easy Global Market France<br>2. Odin Solution Spain<br>3. NEC Germany | EU:<br>1. KNIT University Italy | EU: |
| | | JP:<br>1. Panasonic Corporation | JP:<br>1. Waseda University | JP: |

[133] Link: http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_localsupp_japan_en.pdf

[134] Link: https://fed4iot.org/index.php/consortium/

[135] Link: https://www.msecproject.eu/

[136] Link: https://thorproject.eu

[137] Link: https://www.vtt.fi/sites/5g-enhance

| | | | | |
|---|---|---|---|---|
| | | | 2. IIJ Innovation Institute<br>3. Kanazawa Institute of Technology | |
| | M-Sec | EU:<br>1. Worldline Iberia SA<br>2. F6s Network Limited UK<br>3. Tecnologias Servicios Telematicos Y Sistemas S.A. Spain | EU:<br>1. Institute Of Communication And Computer Systems Greece<br>2. French Alternative Energies and Atomic Energy Commission France | EU:<br>1. Ayuntamiento De Santander Spain |
| | | JP:<br>1. Nippon Telegraph and Telephone East Corporation<br>2. NTT Data Institute Of Management Consulting, Inc. (NTTDMC)<br>3. Nippon Telegraph and Telephone corporation | JP:<br>1. Ubiquitous Computing Laboratory, Keio University (KEIO)<br>2. Research Center for Information and Physical Security, Yokohama National University (YNU)<br>3. GRACE Center, National Institute of Informatics (NII)<br>4. Waseda University / Waseda Research Institute for Science and Engineering / Institute for Advanced ICT Research (WU) | |
| **5G and beyond** | ThoR | EU:<br>1. Deutsche Telekom Ag Germany<br>2. Siklu Communication Ltd Israel<br>3. Vivid Components Ltd United Kingdom | EU:<br>1. Technische Universitaet Braunschweig Germany<br>2. Fraunhofer Germany<br>3. Universite De Lille France<br>4. Universitaet Stuttgart Germany | |
| | | JP:<br>1. NEC Corporation | JP:<br>1. Waseda University<br>2. Chiba Institute of Technology<br>3. Gifu University | JP:<br>1. HRCP R&D Partnership |
| | 5G=Enhance | EU:<br>1. Fraunhofer Germany<br>2. Accelleran Belgium | EU:<br>1. Teknologian Tutkimuskeskus Vtt Oy Finland<br>2. Oulun Yliopisto Finland | EU: |
| | | JP: | JP: | JP: |

| | | | | |
|---|---|---|---|---|
| | | 1. Ehime CATV | 1. Tokyo University of Agriculture and Technology<br>2. National Institute of Information and Communications Technology<br>3. University of Electro-communication | 1. Japan Cable and Telecommunications Association<br>2. Regional Wireless Japan (Previously, BWA Japan) |

Further summarizing the information in the table above the viewer can easily observe that the EU participates in those projects with **11 organizations from the industry** sector while Japan participates with **6 organizations**. Similarly, in the research domain, **9 universities participate from the EU side** and **11 from the Japanese side**. Moreover, in some projects telecommunication associations participate from the Japanese side and a regional unit from the EU side. From a geographical perspective the countries that collaborate with the Japan partners in the aforementioned projects are: Germany, Italy, Spain, France, Greece, UK, Israel, Finland and Belgium, thus nine countries were successful for EU funding and participate in these four coordinated projects. From a per country participation view in these 4 projects someone can see that France and Germany are participating in 3 out of 4 projects while Greece, Finland, Italy and Belgium participate in one out of the four projects (Figure 6).

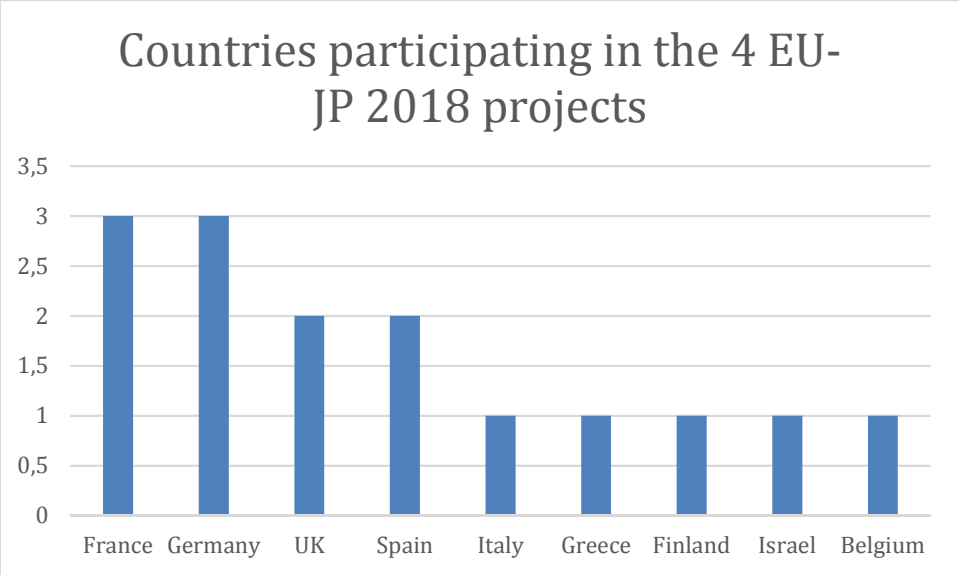


Figure 6 Countries participating in those 4 EU-JP 2018 projects

While counting partners per country, Germany is participating in these projects with five different organizations followed by France, which participates with three organizations (Figure 7).

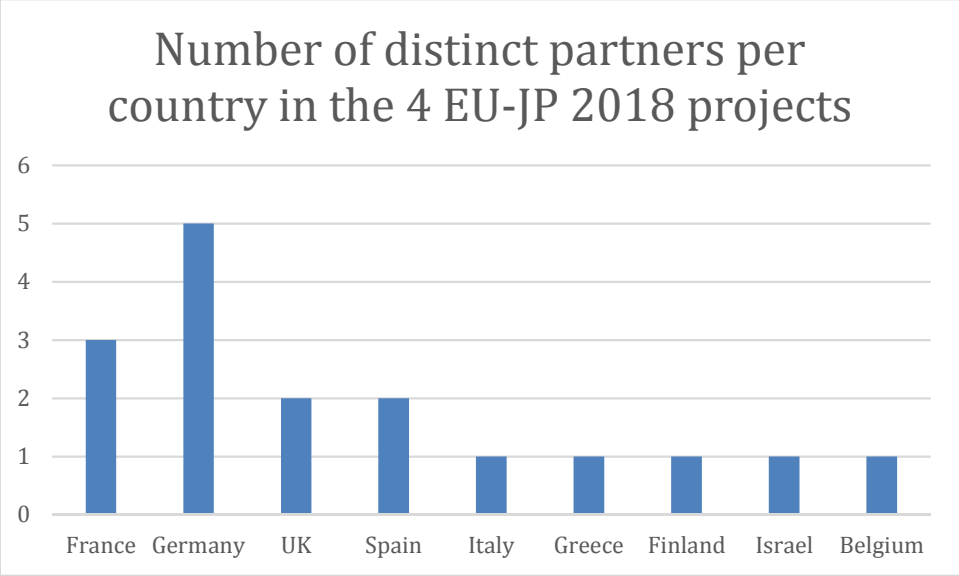


Figure 7 Number of distinct organizations per country

In a more graphical way JEUPISTE[138] project has created an interactive visualization for the Japan participation in H2020 calls. JEUPISTE is a "Japan-EU Partnership in Innovation, Science and Technology" FP7 project which was active from 2013 to 2017. The interactive map was created in 2017 and includes existing/active collaborations between EU and Japanese organizations. Figure 8 below is a screenshot of the interactive map created by JEUPISTE. Marie Curie program, LEIT space and climate related programs are the ones that Japan is mostly participating in according to JEUPISTE.

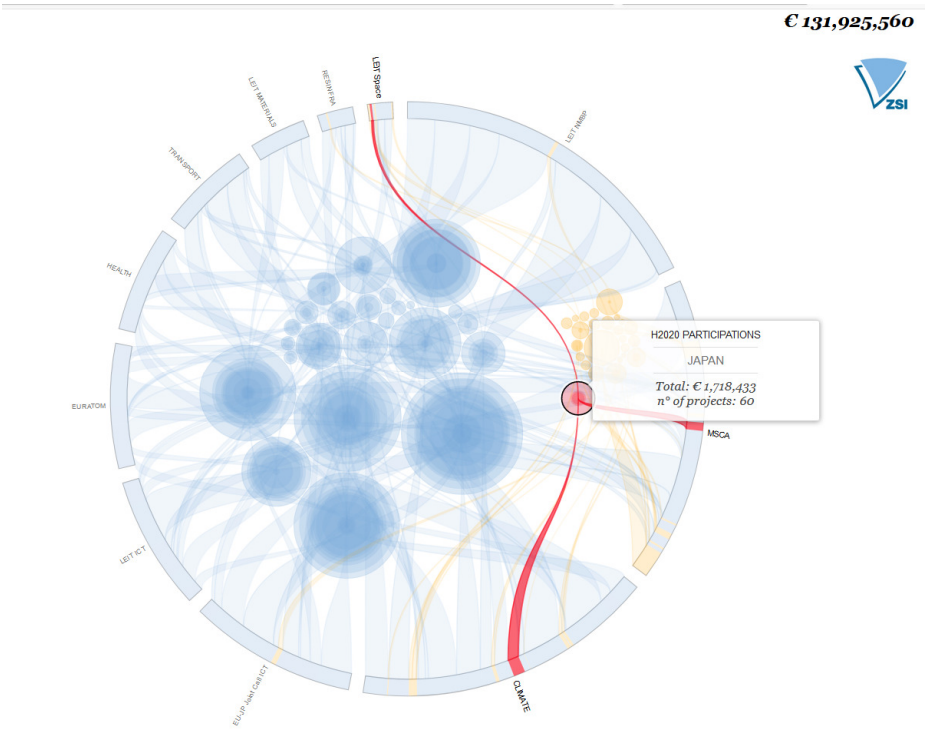


Figure 8 JEUPISTE interactive map. Japan participation in the H2020 calls from JEUPISTE (last update on 2017)

[138] Link: http://www.jeupiste.eu

Another joint initiative between the two regions is the EU-Japan Centre for Industrial Cooperations. It is a joint initiative between and has developed a Minerva Fellowship Programme[139] which among others is also eligible for scientists, academics and R&D. It is mainly focused on professionals related to trade, economic analysis, industrial policy, R&D etc.

**Other active H2020 collaborations between EU and Japanese organizations** (not via the coordinated calls), through calls/projects where Japan was included as one of the eligible countries to apply are summarized in the following table. Here we include the partners/collaborators from the Japanese side. The partners' related information in all these tables in this subsection of the deliverable can be really valuable for the reader who potentially wishes to apply/collaborate with partners from the other region in any upcoming EU-JP call.

| Project Name | Website | Partners/collaborators from Japan |
|---|---|---|
| CD-LINKS: Linking Climate and Development Policies - Leveraging International Networks and Knowledge Sharing | http://www.cd-links.org/ | 1. Center for Social & Environmental Systems Research<br>2. National Institute for Environmental Studies<br>3. The Research Institute of Innovative Technology for the Earth |
| my-AHA: My Active and Healthy Aging | http://www.activeageing.unito.it/ | 1. Tohoku University (TOU) Japan<br>2. JIN Co. Ltd. (JINS) |
| InRel-Npower: Innovative Reliable Nitride based Power Devices and Applications | http://www.inrel-npower.eu | 1. Kyushu University<br>2. Mie University |
| ZENCODE-ITN: Research Training through Zebrafish Genomics | http://www.birmingham.ac.uk/zencode-itn/about/index.aspx | 1. Deputy Director of the Center for Life Science Technologies<br>2. Director of Division of Genomic Technologies<br>3. RIKEN Center for Life Science Technologies |
| JENNIFER: Japan-Europe Network of Neutrino and Intensity Frontier Experimental Research | http://www.jennifer-project.eu | 1. Deputy Director, Institute of Particle and Nuclear Studies<br>2. High Energy Accelerator Research Organization (KEK) |
| MoDeRn2020: Development and Demonstration of monitoring strategies and technologies for geological disposal | http://www.modern2020.eu/ | 1. Waste Information Project<br>2. Repository Engineering & EBS Technology Research Project<br>3. Radioactive Waste Management Funding and Research Center (RWMC) |

### 5.2.2 Perspective of cooperation in both regions

Joint education programs (online and on-site) could be beneficial to both regions. Also exchange programs for students and employees that can facilitate the transfer of knowledge and experience between both regions, leading to quality improvement on both sides. This can also be perceived as a new motivational measure to improve awareness of cybersecurity.

International cyber exercises can also be very beneficial for building competences and procedures needed to fight cybercrime. Such exercises, in which the EU and Japan would be involved, could bring a broader view of global threats. The outcomes of such

[139] Link: https://www.eu-japan.eu/events/minerva-fellowship-programme

exercises could be an input to planning of conducting new research and new tools to synchronize activities on both sides.

Information regarding to cybersecurity (such as threats identification, vulnerabilities, monitoring of network at global level to indicate anomalies) are very valuable assets to assure cybersecurity. The development of new protocols and tools enabling the exchange of information is a very important aspect of activities leading to building situational awareness of such tools, especially in the EU and Japan. Despite the fact that some tools have been created (such as MISP – an Open Source Threat Intelligence Platform, formerly known as Malware Information Sharing Platform), there is still a need to work on new tools and also to enhance closer cooperation in the field of information sharing.

The information sharing environment could take into consideration the following areas:

- 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, e.g., industry ISAC[140].

In order to increase the efficiency of using public money and to increase synergy between both regions, as well as within the EU, the cooperation of research and development projects and programs in the area of cybersecurity should be significantly improved. The first step to achieve this is a creation of joint portal to share information about research and development projects. The portal should provide basic information about projects, as well as planned outcomes and contact information. Such an initiative within the EU exists in the form of cyberwatching.eu portal, but also Japan stakeholders should be encouraged to use it. The next step is a creation of joint EU-Japan programs which aim at conducting R&D&I projects on specific topics, such as indicated in this document.

A very important aspect which may be solved together is the case of risk management regarded to cybersecurity. One of the activities in this context could be the creation of assumptions and requirements of the cybersecurity risk management system, which could monitor the cybersecurity and threats on national and international level. The most important thing in this area is of course critical infrastructure protection, but the aim of such a system does not have to be limited to this context. Such a cybersecurity risk management system can perform a risk assessment for example based on information about incidents, such as malware infections, information leaks and so on, as well as information about vulnerabilities.

The most promising research areas in the context of cybersecurity, which can bring synergies in both regions are the as follows:

- Internet of Things
- Cloud Computing and cybersecurity in the cloud,
- cybersecurity in critical infrastructures,
- big data and cybersecurity

[140] ISAC stands for Incident Information Sharing and Analysis Center

Both regions have different experience in these domains and exchange of lesson learned could bring very positive results.

## 5.3 Industry and standardization

This section looks at the issues facing both regions in short, medium and long term of cybersecurity. More specifically we provide the following information:

- Existing collaboration between Europe and Japan
- Perspective of cooperation in both regions

At the same time this section will produce the analysis of the commonalities between Japan and the European Union using as basis the information provided before in the "existing cybersecurity challenges" in each country. Finally, it concludes with common topics of interest around cybersecurity needs for business and industry.

### 5.3.1 Existing collaboration

After analyzing the previous work of cybersecurity challenges, gaps and recommendations in Europe and Japan we can determinate that there are indeed common topics of interest around cybersecurity between these two areas from the point of view of industry and business.

Regarding existing collaborations in both areas in the field of cybersecurity for industry we have to specially mention two of them:

1) European-Japan technology transfer helpdesk[141]. This service provides a way for European companies to find Japanese organizations, research centers, etc. and help for doing joint work. In here people can specify the area of application where they would like to work and find organizations (or people). This way companies can search for industries that work in similar work, have interested in participating in specific topics or ways to enter the Japanese market with a partner with interest for working in the same area.

2) EU-Japan Business Round Table (BRT). This annual meeting was established from 1999 to foster communication between European and Japanese industries. Executive members from leading industry companies of both areas discuss about different needs and challenges for broad range of sectors of activity. The main objectives of BRT are to help develop trade and investment and encourage industrial cooperation in fields of common interest such as innovation and industrial standards[142].

3) EU and Japan sign Economic Partnership Agreement is the biggest ever negotiated strengthen cooperation by the European Union[143]. With help of this cooperation EU and Japan improve their data protection level. This should create the world's largest area of safe data transfers with a high level of data protection.

4) EU-Japan industrial policy dialogue, is particularly valuable as both Europe and Japan are confronted with similar challenge such as: which policies to adopt to accompany the digital transformation of industry and enterprises.

[141] Link: http://www.eu-jp-tthelpdesk.eu/about/

[142] Link: https://www.eu-japan-brt.eu/

[143] Link: http://europa.eu/rapid/press-release_IP-18-4504_en.htm

This dialogue serves 3 main purposes[144]:

- A forum for discussion on issues of mutual interest covering competitiveness and industrial policy. This is particularly valuable as both Europe and Japan are confronted with similar challenges.
- It reviews the work of the EU-Japan Centre for Industrial Co-operation and the activities of the business-led EU-Japan Business Round Table.
- It is the umbrella for 6 technical working groups that meet once a year before the plenary sessions of the dialogue and report to the annual meeting. The groups are: standards and conformity assessment, automotive, corporate social responsibility and robotics.

Finally, on July 17, 2018, the European Union and Japan agreed to recognize each other's data protection strategies for providing adequate support for allow exchange of data for specific areas of application. Once finalized, the "reciprocal adequacy" decisions will allow personal data to flow between the EU and Japan without being subject to additional safeguards[145].

In order to fight against the threats of cyberspace, cooperations are required between the different actors of the international market. Being aware and up-to-date against new attacks implies that both countries have to ensure their resources and activities in cyberspace, strengthening multilateral cooperation to defend against cyber threats. Industrial cybersecurity is a key to successful achievement of the connected industries in both areas.

### 5.3.2 Perspective of cooperation in both regions

The European Union and Japan are important trading partners from very long time. The main needs of both regions have a similar part: increase cybersecurity capabilities and cooperation with key partners in different technical areas of industry. Both have an initiative to establish a strong role in cybersecurity and mainstream cybersecurity in national policies.

International cooperation plays a key role for Europe and Japan. Therefore cybersecurity challenges and flow of cybersecurity information across borders is critical in order to fight against malicious hackers and cyberterrorists.

The strategy of Japan for addressing their challenges is heavily supported by the government, which launched a new cybersecurity strategy focusing in the needs of cybersecurity for industry and other business layers of the country. Among others, this strategy encourages industry to invest more in cybersecurity for business operations, risk management and innovation[146]. It also contains best practices for help companies better communicate and identify their cybersecurity risks.

From a global perspective, cybersecurity workforce is a scarce resource. In both regions the corporations are looking forward for prepared employees with expertise in cybersecurity so they can invest more in a "cybersecurity culture" in their day to day business. Unfortunately, in both regions, the combination of decreasing resources and increasing demand makes the professional employees to become a highly sought-after resource. This factor could be interesting for both areas for exchanging knowledge and

[144] Link: https://ec.europa.eu/growth/industry/international-aspects/cooperation-governments/eu-japan_en

[145] Link: https://www.skadden.com/insights/publications/2018/07/privacy-cybersecurity-update-july-2018

[146] Link: https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world

training in order to create more experts or for exchanging experts so they could taught their expertise to other cybersecurity actors. This possibility of exchanging information and resources would promote a better work in both regions and better creation of experts that could benefit both countries.

Big Data and Smart Cities are key in the growing of both areas. Big Data is one of the main technical areas of application of the future. This is due to the implementation and transformation of industry and cybersecurity sectors to digital services and the increase of personal and organizational data they work with now. Big Data has a huge potential for both regions and impacts different potential critical areas of technology with a very high presence in the industry market in both regions such as:

- Healthcare
- Public Sector
- Finance
- Energy and Transport
- Manufacturing and Retail

A successful data system between both regions could bring more collaboration between companies, professionals, and service providers in all industry. The cooperation in this sector can support the transformation of existing business sectors and could create new start-ups with innovative business models to stimulate growth in economic activity and cybersecurity. Data security and privacy must be fostered and integrated naturally in the system.

Another important moment in this cooperation is 5G. This technology is expected to drive Smart Cities through the deployment of a considerable number of low-power sensor networks in cities and rural areas. The need of the speech quality and communication security and less power consumption it's a great advantage.

One more aspect in perspective of collaboration is IoT. The Japanese IoT market will be worth around 250 billion in 2020. This technology really is transforming how many day-to-day business and industry are working in both regions. Also, IoT may change the content of some standards and create a need for meeting them. This way, the overall agenda to strengthen quality industry retails are147:

- Building the capabilities of quality assurance service providers
- Working towards the elimination of excessive technical regulations
- Stimulation demand from the private sector to adhere to quality standard by upgrading firm capabilities to produce higher-quality products

Finally, there exists a need for action in Europe and Japan for Industry 4.0 and Robotics, this last one being a key area in Japan and growing very fast in Europe. Some possible joint collaboration in these areas are:

- Identify the trustworthiness among organizations, people, systems, procedures, components and data.
- Develop a common roadmap with joint next steps and priorities and provide input for the ongoing international standardization work.

Cybersecurity is now one of the top security priorities for both areas. Though it is largely impossible to completely prevent attacks, working with cyberintelligence and

147 Mary Hallward-Driemeier – The future of manufacturing-led development, 2018.

allowing easy access to solutions and tools in Europe and Japan could facilitate that both of them are more protected against cyberterrorists. Finally, SMEs are a critical element in both Europe and Japan. In both areas they have difficulties for accessing cybersecurity solutions that can meet their special needs, both technical and business ones. In this sense, a way of joint collaboration could be to allow SMEs of both areas to share needs and have access to a joint market of cybersecurity solutions. This would increase the cybersecurity business of both areas and make more secure their small and medium companies, which would increase their impact and economic growth.

## 5.4 Beneficial aspects.

### 5.4.1 Economic and financial aspects

***Optimization of grants usage.*** Joint collaborative research grant programmes will allow to spend less money on R&D&I for a specific domain as both regions will focus their spendings on more qualitative proposals

***Economic bootstrapping.*** Joint focus on a specific domain will help bootstrap innovations in both regions by collecting more money, as opposed to the same domain being only one-sidedly funded.

***Co-development.*** Collaboration will also help connect and integrate complementary products developed in both regions.

***Market extension.*** Products developed by one region may also find customers in both regions, effectively extending the market of the vendors.

***Harmonized patenting and certification.*** Patenting is important for one business' sustainability and should be anticipated not only at a local level but also at a greater scale, which can be facilitated through cooperation between the two regions. Additionally, to resist and install more trust with respect to security solutions and their usage, the advent of a certification scheme is paramount. Obviously, joint efforts are at least expected, if not having a harmonized scheme across regions, which will alleviate the burden of having businesses being certified twice, for what it may cost.

***Institutionalization of funding strategy.*** Besides existing funding strategies with respect to a region's own priority, frequent cooperation will encourage policy makers to propose more joint funding opportunities.

***Cross-industry funding.*** Cybersecurity finds applications in many vertical markets which are impacted by security threats. Against this uniformized threat front, cross-industry cooperations through sectorial associations will allow to present a similarly uniform defense front.

### 5.4.2 Legal and policy aspects

***Joint workforce development.*** Collaboration between the two regions will enable at least harmonization, and even steer up the preparedness level of cybersecurity workforce across the regions. In particular, training on specific topics on which one region is more advanced will benefit not only the other region but could be disseminated unilaterally or jointly to under-developed regions. Additionally, joint exercises will allow to assess the progress in cybersecurity training on a regular basis.

***Exchange of cybersecurity guidelines.*** A tremendous amount of documentation exists not only in each region but is also available online. Obviously, all publicly available documentation should not be trusted, but government-certified documents that apply to Critical Infrastructures and Essential Services can benefit industries in

any region. Again, comparing guidelines from different regions or industrial sectors will lead to mutual improvement. In particular, technology-specific guidelines that may exist only in one region can be shared to the other region. Finally, in order to achieve technology-agnostic guidelines, it will be necessary to compare and abstract guidelines for technologies that may have different instantiations across the regions.

***Synchronized policy programs.*** Both regions have started implementing policies and strategies with respect to enforcing cybersecurity and privacy within the society. Addressing the impact of technologies is not always anticipated and is often considered once incidents have arisen. E.g., the dangers of social networks, in particular, cyber-bullying, have long been underestimated. Both regions may jointly evaluate impacts of technologies and design appropriate policies to prevent future cybersecurity and privacy incidents. In-progress policy plans that are shared immediately will allow early harmonization across regions, in particular, when it may harm businesses, e.g., GDPR.

***Benefits from public private partnerships.*** PPPs in cybersecurity revealed to be a driving instrument in advancing cybersecurity strategy and such impact should be acknowledged. Japan may actually benefit from the results of ECSO, which may lead to similar initiatives in Japan. Setting up a sister organization in Japan will enable to handle joint cybersecurity development in the future.

#### 5.4.3 Research & Innovation aspects

***Joint industry/academia funding programs.*** Academia may not always have the culture of tackling concrete problems posed to the industry. Successful past initiatives in both regions where industrial entities reach out to academia and research entities should be reproduced at a greater scale. Hackathons and cybersecurity competitions are a given instance that often offer new insights in the growing threat landscape. E.g., NTT usually shares malware datasets yearly within the Computer Security Symposium workshop on malware analysis. Carried out within a controlled legal and technological framework, such competitions or challenges can help industries scale out vulnerability and protection research. In general, joint training programs across regions, and bridging the barrier between academia and industry will improve quality and awareness. Additionally, joint exercises will benefit not only the experiences of each region, but present them with new perspectives, in particular with respect to threats, leading to the development of new research, new tools and new protocols (e.g., for information exchange).

*Human-centric approaches.* The human is a target of choice for cybercriminals as evidenced by the growing number of threats that affect society at the user level (ransomware, IoT malware, client-side web attacks, application-specific malware, spam, cryptocurrency stealing malware, etc.). Concurrently to education, focusing on how to protect users in a usable way will prevent the lack of adoption. However, cultural discrepancies may hinder joint initiatives but could also enrich and improve them. Approaches that were never attempted in one region may actually stem from the other region's culture and practices.

***Reducing the attack surface.*** Cybercriminals have now access to an ever-growing attack surface, due to the convergence of communication channels within the Internet. Data is increasingly present in IoT devices, and synchronized to cloud storage, which makes it harder to trace and protect. Obviously, a data-centered protection strategy should prevent most misuses, but because of the above-mentioned human aspect, some erros may lead to information leakage incidents, or worse, malware infection. In general, jointly addressing risk management, monitoring threats at the national and

international levels will allow to divide the efforts across the regions or allow double-checking. Specific avenues concern trust in devices, resilience of systems and compliance to policies.

***Considering cybercrime and cyber-terrorism.*** These aspects often raise dilemmas on privacy. Research that take into account these aspects when fighting cybercrime will prevent users from being denied their right for privacy. Such right should be uniformly recognized across regions.

***AI-driven cybersecurity and priority research domains.*** Sister initiatives have sprung between Japan and Europe for both cybersecurity and artificial intelligence. Not only, collaboration will be beneficial between Europe and Japan research communities, but also between cybersecurity & privacy and artificial intelligence research communities. In particular, the threat of AI-driven cybercrime should be anticipated, so as to not be lagging behind the attackers, for once. Other promising research domains will benefit from joint research such as cybersecurity in IoT, cloud computing, critical infrastructures and big data.

#### 5.4.4 Industry and standardization aspects

***Considering SMEs.*** A number of aspects should be considered with respect to small and medium enterprises in order to improve the overall level of security. Considering common needs and enabling their access to a joint market of cybersecurity solutions will make cybersecurity and privacy affordable, raising their adoption. Appropriate guidelines should be published, not only for critical infrastructures or essential services – that already enforce a certain amount of best practices – but also for the greater number of companies that may not be as cybersecurity-savvy as big companies.

***Engaging technology associations.*** Technology vendors/suppliers and adopters often gather nationally or regionally in technology associations, where technologies as discussed so as for suppliers to better satisfy the needs of adopters. Introducing cybersecurity actors in such associations will enable the introduction of best practices in technology development. These first two points are common across both regions.

***Involvement of online platforms.*** Online platforms attract most of the Internet traffic and are therefore a target of choice for cybercriminals. They therefore have a responsibility to protect and handle user data responsibly. The distribution of these platforms in different countries has also two advantages: 1) finding someone to talk to can be done through multiple channels in both regions; 2) joint pressure from both regions is possible.

***Incorporation of standards at different levels.*** Standardization is a worldwide effort and is not limited to Europe and Japan. But the involvement of both regions in standard bodies is not negligible and may enable joint lobbying for advancing proposals that matter. Both regions should also be leaders in adopting standards in companies and national strategies. Finally, certification is one medium to enable the industry to trust cybersecurity solutions, and it should be made affordable to both suppliers and adopters so as to improve the overall cybersecurity level of both regions. Therefore, joint efforts may help lower the costs of certification.

***Creation of new markets.*** A number of priority research domains such as IoT, Industry 4.0 or robotics will benefit from joint development creating new market opportunities, if not only by securing them. In particular, data being at the center of the IT world, and the main resource to exploit and/or protect, approaches in big data will be developed. Critical areas such as healthcare or the public sector will benefit from

the collaboration of companies, professionals and service providers, fostering the creation of start-ups with innovative business models, further stimulating the growth in economy and cybersecurity.

# 6 Conclusions

This document provides an analysis of the current and future gaps, challenges, recommendations and possible collaborations between Europe and Japan in the cybersecurity area. The reporting is composed of three different areas: i) legal and policies, ii) research and innovation and iii) industry.

The analysis conducted in this document on the legal, policy and regulatory aspects highlighted a number of opportunities for reciprocal collaboration and harmonization of existing and future legal landscapes.

Whilst to date, progress is being done at the general trade level (see for instance, the EU-Japan free trade deal) and at the data protection one (see the adequacy decision being currently finalized by Japanese and European negotiators), much seems to be done yet from a merely cybersecurity regulatory perspective.

Notwithstanding standards and codes, which are industry-oriented or sector-specific, progresses in the cybersecurity field still miss any mutual legal and policy action, which would definitely bring the two regions closer in an hypothetical extended version of the digital single market. Such opportunities do not only pertain the mere legal initiative, however, as we will see in the last part of this conclusion.

Whilst the legal scenario must and will expectedly still be very different between EU and Japan, given the nature of such two entities (a hybrid form of international institution vis-a-vis a sovereign country), efforts could still be in place to reduce the regulatory gaps therein. For instance, studies and analysis demonstrated how from both sides there is a high demand for legal clarity around vulnerability handling and disclosure, both at private sector and governmental levels. This domain ties up with the complete absence on both regions of comprehensive and wide IoT certification schemes.

The governance domain is taken over by the need for a substantial reform of ENISA. The EU needs an agency with a significant technical knowledge to engage in diplomatic and sector-specific discussions with the Japanese counterparts. For this reason, much progress is voiced by the cybersecurity community to the EU legislator to empower ENISA of external relations tasks, too.

On a judicial level, it was brought forward the idea that data protection and security standards will have to be agreed between two regions. Whilst terrorism, for instance, seems not to be a type of crime which equally affects the EU and Japan, network and information security-related ones (cybercrimes) have often a cross-border and transnational nature, sometimes involving EU Member States and Asian countries like Japan. For this reason, data protection standards on information sharing might expectedly be explored in the future.

Lastly, a wide series of soft policies initiatives should combine the efforts from both regions to develop effective capacity training in undeveloped countries, in order to enhance the level of awareness and security of the professions involved in the cybersecurity area.

From a research and innovation point of view this document provides the current status and gaps in cybersecurity, pointing out the new challenges that new technologies bring. These new challenges include the increasing privacy vulnerabilities of online social networks that continuously expose user's data, along with millions of new IoT devices, initiating the IoT botnets. Additionally, the existing cybersecurity threats have

increased in terms of sophistication and complexity, as adversaries invent new ways to hide their trails and remain anonymous. The artificial intelligence expansion and the popularity of Blockchain and new cryptocurrencies have raised the challenges of user protection from cyber threats.

Finally, regarding the status of cybersecurity in industry, we identified common gaps and needs in both areas. In the perspective of collaborations one of the main areas Japan is focusing is robotics, which is also growing fast in Europe. In Japan there exists an industrial revolution led by robots that covers almost all technical areas of application. This must be supported by Europe in order to take advantage of their knowledge and shared experience. Additionally, IoT is a key area in both areas. In Japan and Europe the IoT market is growing very fast and already exist collaborative opportunities for research projects regarding IoT devices for smart cities. Even already identified, it is a gold mine that will increase even more in time, so it is highly recommended that Europe and Japan join forces for taking advantage of this area of application.

Very related to the previous collaboration is the sharing of data. It is required mechanisms for international cooperation of cyberintelligence between Europe and Japan in order to increase the protection against cyberattacks in industry. This was also mentioned in the other two areas of research of this document: legal and research. Right now, it is very difficult to exchange cyberintelligence due to privacy of data and data protection policies, so a way to facilitate this exchange of data at different levels, for example using a EU-Japan information sharing platform, would increase exponentially the cybersecurity and business impact of industry in both areas.

Another of the more important topics for cybersecurity in industry in both areas are ways to increase the adoption of cybersecurity in companies. In Japan cybersecurity is still seen as an “add-on” while in Europe it is starting to get more importance as a key component of any product. Therefore, ways to increase the adoption of cybersecurity solutions in both areas would benefit them as they exchange of technologies and tools would be more fast and secure. Together with this, training and awareness of cybersecurity in several technical areas such as eHealth, IoT, cloud, etc. in Europe and Japan would benefit them both making the domains of applications more secure and allowing an easier exchange of information and solutions. This would be very beneficial for example in the area of eHealth, as the aging of citizens in both areas is getting more and more critical.

SMEs are a core in Europe and Japan and are identified with similar constraints. In both areas they have difficulties to access dedicated solutions, which reduces their cyberprotection, usage of digital services by customers, and impact in society. We think having a common strategy in Europe and Japan for facilitating usage of cybersecurity solutions for SMEs (both from a technical and business perspective) would make possible for both areas to enter a new market of cybersecurity solutions where both societies would benefit. Europe and Japan have a very huge market need for SMEs and it would allow the impact and their economy to grow very fast, creating new companies or facilitating the digital transformation.

Providing cybersecurity information at all levels of an organization is a key challenge in both areas. Cybersecurity is usually provided very technical and for experts in the area. This is an issue as management of the organizations, which have to take decisions of the business strategy of the company or decide about what cybersolution is more adequate to their economic strategy, have no idea about the risks and impact a cyberattack could have in their organization. Promoting joint collaboration for defining

ways to describe the impact, complexity and need of cybersecurity in the day-to-day of organizations would allow to expand the businesses in a more secure way and facilitate organizations of both areas can make business together.

Finally, 5G is a technology with a big impact in both areas. Even though there already exist discussions and plans for collaboration for this technology we think it should be more promoted as communications are nowadays key and having a joint collaboration for working in secure and trusted communication networks would have a high impact on the communications between Europe and Japan from a technical perspective and create new business opportunities for both national organizations and also at international level.

Therefore, and as presented in this document, we believe there exists several areas of possible collaboration that also are related to each other. This means that supporting joint work for cybersecurity in Europe and Japan would facilitate the technology transfer, business impact and creation, and cybersecurity expertise of both areas. Bearing in mind other countries such as USA, China, etc. are also pushing in the same direction, a collaboration between Europe and Japan could have a high impact in new technologies and make available a business market that is very difficult to access at the current situation.