EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Cybersecurity and privacy dialogue between Europe and Japan*  

Deliverable D3.1: Preliminary version of the Cybersecurity Research Analysis Report for the two regions

Abstract: This document contains a description of legal and policy aspects, research and innovation aspects as well as industrial and standardization aspects. It contains a review of the mechanisms used to finance research and innovation in Europe and Japan, a review of the main research directions in the field, and identification of the strong and weak points in the European and Japanese research landscape.

* The research leading to these results has received funding from the European Union H2020 Programme under grant agreement n° 740507.
<table>
<thead>
<tr>
<th>Contractual Date of Delivery</th>
<th>July 31, 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Date of Delivery</td>
<td>July 31, 2018</td>
</tr>
<tr>
<td>Deliverable Dissemination Level</td>
<td>Public</td>
</tr>
<tr>
<td>Editor</td>
<td>Anna Felkner (NASK), Marek Janiszewski (NASK)</td>
</tr>
<tr>
<td>Contributors</td>
<td>All EUNITY partners</td>
</tr>
<tr>
<td>Quality Assurance</td>
<td>Adam Kozakiewicz (NASK internal), all EUNITY partners, Gregory Blanc (IMT final), Christophe Kiennert (IMT final)</td>
</tr>
</tbody>
</table>

The *EUNITY* consortium consists of:

<table>
<thead>
<tr>
<th>Institut Mines-Telecom</th>
<th>Coordinator</th>
<th>France</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORTH</td>
<td>Principal Contractor</td>
<td>Greece</td>
</tr>
<tr>
<td>ATOS Spain SA</td>
<td>Principal Contractor</td>
<td>Spain</td>
</tr>
<tr>
<td>NASK</td>
<td>Principal Contractor</td>
<td>Poland</td>
</tr>
<tr>
<td>KATHOLIEKE LEUVEN UNIVERSITEIT</td>
<td>Principal Contractor</td>
<td>Belgium</td>
</tr>
</tbody>
</table>
# Contents

1. **Introduction**  

2. **Legal and Policy Aspects**  
   2.1. Executive summary  
   2.2. The European landscape  
      2.2.1. Privacy and data protection  
      2.2.2. Cybersecurity  
   2.3. The Japanese landscape  
      2.3.1. Privacy and data protection  
      2.3.2. Japan and the European Union: comparative aspects on privacy and data protection  
      2.3.3. Cybersecurity  
   2.4. Conclusions  
      2.4.1. Summary of Challenges and Gaps  

3. **Research and Innovation Aspects**  
   3.1. Mechanisms to finance cybersecurity research  
      3.1.1. In the European Union  
      3.1.2. In Japan  
      3.1.3. Summary  
   3.2. The main research directions in the field  
      3.2.1. Strategies and Research and Innovation Agendas  
      3.2.2. Programs and project calls  
      3.2.3. Projects  
      3.2.4. Other activities  
   3.3. The strong and weak points  
      3.3.1. Strengths
List of Figures

3.1. Schematic overview of the analysis . . . . . . . . . . . . . . . . . . . 56
3.2. The Red Book . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 80
3.3. The FORWARD blog . . . . . . . . . . . . . . . . . . . . . . . . . . . . 81
3.4. CONNECT2SEA website . . . . . . . . . . . . . . . . . . . . . . . . . 82

4.1. BDVA strategic Priorities (BDVA SRIA) . . . . . . . . . . . . . . . . . . 107
4.2. ARTEMIS SRA Matrix 2016 . . . . . . . . . . . . . . . . . . . . . . . . . 110
The goal of this deliverable is to establish a clear picture on the cybersecurity and privacy domain in both regions by analyzing existing roadmaps. It will first identify the appropriate methodology applicable to the information collected, then analyze the cybersecurity priorities in both EU and Japan, in order to produce a background document on the status and priorities of cybersecurity and privacy research and innovation activities in Europe and Japan.

The scope of the deliverable includes a review of the mechanisms used to finance research and innovation in Europe (both European and national funds, including non-EU level international cooperation) and Japan. It also includes an overview of the main research directions in the field, identifying the strong and weak points in the European and Japanese research landscape, looking for topics of common interest, where cooperation opportunity is clear, as well as topics where some aspects are covered asymmetrically, allowing even greater synergy.

The document also shows the analysis of the current role and activity of different units (SMEs, research institutions, CSIRTs, LEAs, etc.) in research and innovation in Europe and Japan, looking for possible asymmetries increasing the value of possible cooperation. An analysis of long-term research programmes at the national and international levels has also been carried out. The main objective of this analysis is to find thematic parallels between the EU and Japan which may create opportunities for either co-financing of joint EU-Japan projects or at least synchronization of efforts enabling cooperation between topically linked European and Japanese projects.

This document is mainly a collection of data, while a thorough analysis and drawing conclusions will be implemented in the deliverable "D4.1 Description of gaps and future challenges" and "D4.2 Strategic research and innovation agenda" documents. The purpose of the analysis here is only to indicate the most visible similarities and differences.
Elicitation of common topics of interest will establish a clear picture on the cybersecurity domain in both regions by analyzing existing cybersecurity and privacy roadmaps.

Chapter 2 (Legal and Policy Aspects) focuses on the analysis of regulatory documents, EU directives as well as laws and legal frameworks. It elicits the common regulatory aspects of cybersecurity and privacy, for example obligations for monitoring, certification, protection of personal data and information exchange. This mostly addresses the policy-makers and CERT communities, although the business community is certainly impacted.

Chapter 3 (Research and Innovation Aspects) focuses on the analysis of research agendas, programs, project calls and roadmapping projects as well as on showing the available mechanisms to finance cybersecurity research.

Chapter 4 (Industry and Standardization Aspects) focuses on the analysis of the output of clusters and industry associations. It also includes national strategic efforts to create or develop business strategies. With respect to standards, it covers the entire scope of standard bodies, as shown by the presence of the EUNITY partners and associate partners in standardization bodies.
2.1. Executive summary

The present section of this report will elicit the legal and regulatory landscape in the fields of privacy and cybersecurity in the European Union and Japan. With respect to the former, attention will be paid to the substantial reform on privacy and data protection brought forward mostly by the so-called GDPR (General Data Protection Regulation), while the cybersecurity analysis will focus on the cybersecurity strategy of the European Union and the NIS (Network and Information Security) Directive.

With regard to the Japanese landscape, privacy and cybersecurity will be analyzed through the lens of the Act on Personal Information and the Basic Act on Cybersecurity, respectively. Inter alia, such an analysis will try to draw parallels and differences with the above-mentioned European acts, so as to offer a comparative overview of the main legal concepts therein and of the possibilities created by both legislations to engage in cooperative efforts and information sharing.

As this report will outline, gaps and differences still persist amongst the two regions, in spite of the many similarities and overlaps. For instance, the approaches taken by the two Acts on cybersecurity delineate a fundamental gap between the two. Whilst the scope of the European NIS Directive applies to organizations and legal persons, the Japanese Basic Act includes a significant section dealing with the obligations on the security of the information systems that individuals should comply with. Similarly, the two laws on data protection have different approaches, namely within the sanctionatory regime (much stricter, in principle, in the GDPR), and in the inclusion within the definition of personal information of online identifiers such as IP addresses and alike (which have a wider protection in the European framework).

However, it must be noted that the legislative process still needs to be interpreted by the two jurisprudences, and a new EU Act (the Cybersecurity Act) is actually in the making. Such legal instruments, if taken and approached correctly, might actually decrease the legal gap between the two regions, facilitating the cooperation
and the information sharing, towards a more secure and sustainable future. This is why the present report aims at outlining a primer on commonalities and differences between EU and Japan in privacy and cybersecurity laws.

2.2. The European landscape

The present section aims at outlining the current and imminent landscape of EU law and policy as far as privacy, data protection and cybersecurity are concerned. The recent years were characterized by an intense effort by the European legislator aimed at reforming and modernizing privacy and cybersecurity laws, standards and practices across Europe.

The rise of modern technologies and new forms of human and digital interactions has brought into light the weaknesses of the existing legislation, which turned to be perceived by many as fragmented and outdated. This “obsolete” state of play was accompanied by the increasing number of cyber threats that European stakeholders are facing in both public and private sectors: growing security and privacy risks have become a landmark blocker for the achievement of a competitive and secure digital single market.

Against this backdrop, the above mentioned scenario triggered vibrant societal discussions which, ultimately, brought the political arena to initiate a long decision making process, leading to a substantial reform of the legislative and policy landscape in both data protection and cybersecurity fields. This section will therefore seek to outline the main legal and policy efforts by the European Union addressing such discrepancies. The first chapter will deal with the General Data Protection Regulation (GDPR) and the overall privacy reform package, while the second will focus on the legislative initiatives in terms of cybersecurity, namely the Network and Information Security Directive (NIS) and the EU Commission’s European Cyber Security Strategy.

Within the realm of the EUNITY Project, the analysis that will follow aims at supporting both European and Japanese partners (policy and decision makers, CERT representatives and businesses) in further understanding what major implications
for their business processes arise from the said evolving legal landscape. The objective of outlining such elements shall well serve to bring closer the two regions, thus facilitating a reciprocal comprehension of opportunities and boundaries inherent in the legal landscapes under scrutiny below.

2.2.1. Privacy and data protection

2.2.1.1. The General Data Protection Regulation

On May 25th, 2018, the General Data Protection Regulation (GDPR) entered into force, repealing the existing Directive 46/95/EC. A massive change for the European privacy landscape, mainly because of the legal instrument chosen to convey such novelties. As a Regulation, the GDPR has in fact binding legal force across all Member States of the European Union. Conversely, the Directive 46/95/EC rolled out a set of provisions that had to be implemented throughout the Union. It goes without saying that the GDPR aims therefore at a higher level of harmonization than the one previously in force, with less room for domestic interpretation and more legal certainty across the European territories.

Technology neutral. One crucial aspect of the GDPR is enshrined in Recital 15, stating that “in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used”. Firstly introduced in the EU law landscape in 2002 within the so-called e-Privacy Directive, for the sake of this analysis the meaning of this concept is that the principles enshrined in the Regulation shall apply regardless of the technological advancements, and that the same regulatory framework shall not influence innovation towards an intended outcome. Technological neutrality should therefore ensure an endurable application of the GDPR in spite of short and mid-term technological innovations.

Scope and grounds for processing

(Extra-territorial) Scope. One of the main changes from the existing legislation to the GDPR refers to the scope of application of the GDPR. Its provisions in

---

7Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.


fact apply with a broad interpretation of the principle of territoriality: Art. 3 pre-
scribes that the Regulation applies to personal data processing by those controllers
and processors\(^{11}\) (a) established in the European Union, irrespective of where the
processing activity takes place, or (b) process personal data of European citizens,
irrespective of their place of establishment. Such broad rules aim at a wider reach,
actually including non-European businesses and organizations processing data of EU
subjects, including the activities of behavioral monitoring and provisions of goods
and services (including free of charge).

**Grounds for Processing.** Article 6(1) provides for six legal basis that justify the
processing of personal data by controllers, namely:

- the data subject has given consent to the processing of his or her personal
data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data
subject is party or in order to take steps at the request of the data subject prior
to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the
controller is subject;
- processing is necessary in order to protect the vital interests of the data sub-
ject or of another natural person;
- processing is necessary for the performance of a task carried out in the pub-
lic interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued
by the controller or by a third party, except where such interests are overrid-
den by the interests or fundamental rights and freedoms of the data subject
which require protection of personal data, in particular where the data subject
is a child.

**Data Subjects’ and Information Rights**

The GDPR has broadened the scope of the rights of the data subjects towards
those controllers responsible for processing their personal information\(^{12}\). As a re-
sult, the Regulation aims at providing full control over personal data to European

---

\(^{11}\)See GDPR, Art.4.7 and 4.8: (7) ‘controller’ means the natural or legal person, public authority,
agency or other body which, alone or jointly with others, determines the purposes and means of the
processing of personal data; where the purposes and means of such processing are determined by
Union or Member State law, the controller or the specific criteria for its nomination may be provided
for by Union or Member State law; (8) ‘processor’ means a natural or legal person, public authority,
agency or other body which processes personal data on behalf of the controller; See also: De Hert, P.,
of the General Data Protection Regulation in its wider context. International Data Privacy Law, 6(3),
230-243.

\(^{12}\)Ausloos, Jef and Dewitte, Pierre, Shattering One-Way Mirrors. Data Subject Access Rights in
Practice (January 20, 2018). International Data Privacy Law, Vol.8(1), Forthcoming. Available at
SSRN: https://ssrn.com/abstract=3106632
citizens\textsuperscript{13}, thus protecting them against potential interferences or violations of their fundamental right to data protection\textsuperscript{14}. From the controller perspective, such data subjects’ empowerment leads to an increment of the obligations they need to observe and respect, from stronger rules deriving from existing rights to brand new legal requirements.

Table 2.1 provides a summary of the data subject’s rights as enshrined by GDPR.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|p{0.7\textwidth}|}
\hline
ART. & RIGHT & Brief description \\
\hline
12,13 and 14 & Right to Information & In light of an improved transparency of data processing, data subjects have the right to request (free of charge) for what purposes and by whom exactly (third parties included) their data are processed. \\
\hline
15 & Right to Access & The request may also pertain a copy of such data (see above), that must be provided electronically, in an easily-readable format and without undue delay. \\
\hline
16 & Right to Rectification & If personal data is inaccurate or incomplete, the data subject has the right to ask for them to be rectified. \\
\hline
17 & Right to Erasure (Right to “be forgotten”) & Data subjects have the right (under qualified circumstances) for their data to be erased from the controllers’ dataset.\textsuperscript{15} \\
\hline
18 & Right to Restriction of Processing & Controllers are bound by the right of the data subject to ask for their personal information to be suspended from the processing. \\
\hline
20 & Right to Data Portability & Data subjects have the right for their data to be transferred from one controller to another (or directly to the data subjects themselves) in an automatic and easily readable format. \\
\hline
21 & Right to Object & Right to contest the processing of personal data by controllers. \\
\hline
22 & Right not to be Subject to Automated Decisions & Data subjects have the right not to be subject to decisions based on solely automated means (including profiling), which leads to legal effects for the individuals. \\
\hline
\end{tabular}
\caption{Table 2.1: Summary of the data subject’s rights as enshrined by GDPR}
\end{table}


\textsuperscript{14}Article 8, Charter of Fundamental Rights of the European Union

\textsuperscript{15}C-131/12 - Google Spain and Google: Judgment of the Court (Grand Chamber), 13 May 2014 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González - Request for a preliminary ruling from the Audiencia Nacional

www.unity-project.eu 13 July 31, 2018
The increment in citizens’ control over their personal data also comes from the right to an effective remedy (Art. 79). It adds up to the abovementioned rights as a complementary one, and seeks to ensure citizens of having proper access to regulatory justice by means of the right to lodge a complaint to the competent supervisory authority, pursuant to Article 77, as well as to the ordinary justice.

Obligations on Certification and Codes of Conduct

Pursuant to the newly-introduced principle of accountability, the General Data Protection Regulation provides for a set of articles encouraging the establishment of codes of conduct and certification schemes. Additionally to the assessment of the Regulation, for the sake of this analysis, it is useful to look at ENISA’s Report “Concepts and recommendations on European Data Protection Certification mechanisms” issued in November 2017, where certification is considered as a “conformity assessment activity” performed by a third party (as opposed to a first-party self-assessment), including a set of rules and procedures (“scheme”) to perform such an exercise, resulting in a “certificate” or “seal” validating it. With a view to the future, a number of ENISA’s policy papers address certification as a major component of the next regulatory landscape on privacy and cybersecurity.

Article 42 of the GDPR asks Member States, the Commission, the EDPB to encourage, at the Union level, the creation of certification schemes as a way to ensure and promote compliance with the Regulation, as well as to disseminate good practice on privacy and data protection across all sectors within and out of European territories, particularly for SMEs and businesses alike. Among others, GDPR aims at ensuring through such certification schemes the existence of appropriate data protection safeguards in the case of personal data transfers to third countries or international organizations. Against this backdrop, the Regulation provides for a set of requirements to be taken into account by law makers and regulatory bodies when establishing such certification mechanisms, such as:

- The voluntariness of the certification for controllers and processors;
- A certification criteria to be set by EDPB;
- The maximum length (renewable) of certification shall be of three years;
- A publicly available register of all the “approved” certification mechanisms made publicly available by EDPB.

It is noteworthy to point out that the adherence to a certification scheme does not exclude or impact the potential liability of controllers or processors that are found in violation of the GDPR, nor does exclude capacities and responsibilities of data

---

16 Art. 24, GDPR
17 ENISA, Concepts and recommendations on European Data Protection Certification mechanisms, November 2017
18 Ibid. 17
19 See for instance ENISA, Looking into the crystal ball: A report on emerging technologies and security challenges, January 2018
20 The European Data Protection Board
2.2. THE EUROPEAN LANDSCAPE

protection authorities across Europe with regard to their enforcement and oversight powers.

With reference to third parties, as ENISA remarks in its report, Article 43 “explicitly requires accreditation for the certification body”\(^\text{21}\), thus pursuant to the rules laid down in Regulation 765/2008\(^\text{22}\) (Accreditation Regulation). Such bodies, which shall follow the principles of independence, reliability and competence\(^\text{23}\), may thus be created in the context of three different avenues, as unfolded in Table 2.2.

<table>
<thead>
<tr>
<th>AVENUE A</th>
<th>AVENUE B</th>
<th>AVENUE C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accreditation by a Data Protection Authority (or the European Data Protection Board, in the case of the European Data Protection Seal ex art. 70 GDPR).</td>
<td>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.</td>
<td>Both authorities, namely the National Accreditation Body and the competent Data Protection Authority, collaborating in this task.</td>
</tr>
</tbody>
</table>

Table 2.2: Three different avenues to create certification bodies

Following the assessment of the GDPR, ENISA identifies a number of challenges and open questions with reference to certification schemes as foreseen by the Regulation, followed by a number of recommendations aimed at mitigating such challenges. In particular, ENISA stresses that national DPAs and national certification bodies shall adopt a common and coordinated approach on “inception and deployment of GDPR data protection certification mechanisms”\(^\text{24}\), under the coordination of the European Commission and of the EDPB. This will help avoiding the proliferation of certification mechanisms with substantially and formally diverse angles and potentially conflicting approaches towards the same subject matters. Furthermore, it is encouraged that the same players shall work together to “stimulate the exchange of best practices and lessons learnt from certification practices in other well established domains (e.g. cybersecurity)”\(^\text{25}\).

As a complementary note, GDPR foresees in Article 40 the creation of sector-specific codes of conduct “intended to contribute to the proper application of this

\(^{21}\) Ibid. 17, p.11  
\(^{23}\) Ibid. 17, p.15  
\(^{24}\) Ibid. 17, p.6  
\(^{25}\) Ibid. 17, p.6
Regulation”, with particular reference to SMEs. At the time of writing, a number of industry organizations, business associations and various sectorial networks are in the process of starting to set up the basis for a sectorial code of conduct pursuant to the improvement of GDPR compliance by all actors (some of them are being amended, as already in place under the current Directive). Such codes of conduct will then need to be revised and approved by competent data protection authorities and the EDPB (in case the Code applies to organizations established in more than one Member State). The main points of the codes of conduct mentioned by Art. 40 shall address the following elements of GDPR: fair and transparent processing, grounds for legitimate interests of the controller, data collection activities, pseudonymization, information rights, protection of minors’ personal data, security, breach notification, data transfers and forms of alternative dispute resolutions. Interestingly, Paragraph 3 of Article 40 extends the possibility to adhere to such codes also to players not having to abide by the GDPR, for example “by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organizations”. It goes without saying that such clause seeks to enable GDPR-compliant relationships with non-EU countries, exporting European privacy standards as a baseline for the engagement of external partners.

Data Security: monitoring obligations and breach notifications

One of the points of contact between privacy, data protection and cybersecurity in the GDPR is certainly represented by the set of provisions regarding data security. Obligations, such as the duty to undertake monitoring activities identified in data protection impact assessments (DPIAs), provisions related to technical and organizational measures and breach notification obligations present elements of overlap between the two disciplines which will be further articulated below.

Monitoring obligations. One of the most important elements to highlight relates with the shift that the legislation imposes on controllers with regard to the assessment on whether a data processing operation results in a risk for individuals’ rights and freedoms, i.e. from a legally-based approach to a more iterative risk-based approach. Data protection impact assessments thus become a mandatory obligation within the GDPR26 auspices under a certain number of conditions. It is fair to point out that impact assessments were mentioned already in the existing legislation, but the move towards more compulsoriness supports the argument that, from the legislator viewpoint, data protection and information security compliance are getting close as never before: the rationale behind this choice is to bring controllers to reason about privacy according to a priority-risk mindset, an approach already in use in many cyber-security ecosystems.

26 GDPR Art. 35
Coming down to the Regulation, Article 35 demands data controllers to undertake DPIAs anytime they deem a data processing operation results in a “high risk to the rights and freedoms of natural persons”\textsuperscript{27}. A number of interpretative issues arise from the text of the Regulation, hereby briefly outlined.

With regard to the assessment of the so-called high risk, it should be noted that WP29\textsuperscript{28} provides further guidance for unlocking the concept; additionally, for the sake of this analysis, it is useful to point that a number of processing operations are subtracted from the arbitrary scrutiny of the data controllers, as they are considered not to necessitate a DPIA by default. As Article 35(5) states in fact, that data protection authorities may issue a public list of processing operations for which such exercise would not be required.

WP29 provides for a set of non-exhaustive operations to be evaluated as potentially risky and therefore falling under the DPIA requirement. The list includes:

- evaluation and scoring,
- automated-decision making with legal or similar significant effect,
- systematic monitoring,
- involvement of sensitive data,
- data processed on a large scale,
- datasets that have been matched or combined,
- data concerning vulnerable data subjects,
- innovative use or application of technological or organizational solutions,
- data transfer across borders outside the European Union,
- if the processing “prevents data subjects from exercising a right or using a service or a contract”\textsuperscript{30}.

**Security of processing.** It is important to note that GDPR promotes the use of Privacy Enhancing Techniques (PETs) as a way to achieve compliance and security in a given organization. For instance, tools and methods like encryption or pseudonymization are explicitly mentioned in the text of the law as a best practice.

However, GDPR expects data controllers to assess the data processing operation before it starts and, according to the potential risks for the security of processing itself, to implement adequate technical and organizational measures which are deemed as appropriate for the business case in question.

This means that the Regulation does not set a minimum standard for security, and it is fair to assume that such security measures are not scrutinized by regulators unless in the occurrence of a data breach, for which GDPR lays down explicit rules regarding notification and information.

\textsuperscript{27}Ibid. \textsuperscript{26}
\textsuperscript{28}Article 29 Data Protection Working Party, the panel composed by members of EU Member States’ privacy regulators, to be replaced by the EDPB under the GDPR regime
\textsuperscript{29}Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, p.7
\textsuperscript{30}Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, p.9
Notifications for data breaches. Data breach notifications represent a novelty in comparison with the existing Directive 95/46: on October 2017, Data Protection Working Party Article 29 issued guidelines on breach notification\(^{31}\), which will help us unlocking some of the basic concepts behind Art. 33.

Article 4(12) GDPR defines personal data breaches as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”. It goes without saying that the element of security here is strictly linked with the compromising of at least one of the three components of the so called CIA triangle, which in information security sciences refers to Confidentiality, Integrity and Availability\(^{32}\).

The above mentioned Article 33 requires data controllers and processors to have in fact 72 hours from the moment they became aware (i.e., when there is a “reasonable degree of certainty that a security incident has occurred”\(^{33}\)) of the breach to take actions towards the following stakeholders:

- Data protection authorities, unless there is the unliikelihood that the breach falls into the category of those incidents causing a risk for the freedoms of individuals.
- Data subjects, in the event that high risks for the freedoms of the individuals are likely to occur.

Interestingly, WP29 makes it clear that “an incident resulting in personal data being made unavailable for a period of time is a security breach (and should be documented), yet depending on the circumstances, it may or may not require notification to the supervisory authority and communication to affected individuals”\(^{34}\). This statement clarifies that controllers need to document a larger number of incidents than the ones for which they will need to initiate a notification to the DPA, thus applying Art. 33(5) which is clearly inspired by the principle of accountability. Furthermore, WP29 specifies that even incidents causing the temporary unavailability of personal data fall under the category of incidents ex Art. 33(5).

Furthermore, it is fair to assume that the reporting duty does not imply a one-end line of communication only. The aim of laying down security and personal data breach reporting in the GDPR is to enable a trustworthy relationship between controllers and competent data protection authorities, where the latter are expected to provide assistance in return to a notifying controller, possibly guiding them towards a situation of low-risk. Mutual updates and follow-ups are mentioned and welcome by WP29\(^{35}\), as a demonstration of the need for enhancing and facilitating smooth cooperation between regulators and controllers.

Another important point for data security is the obligation of embedding privacy by design in both development and deployment of a system processing personal

\(^{31}\)WP29 Guidelines on Personal data breach notification under Regulation 2016/679

\(^{32}\)Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, WP213

\(^{33}\)Ibid. 32, p.9

\(^{34}\)Ibid. 32, Opinion 03/2014 on Personal Data Breach Notification, WP213, p.7

\(^{35}\)Ibid. 32, p.13
information\textsuperscript{36}. Concepts of information security like data minimization, access control and access rights, activity logs, are all functional for meeting such requirement, and ultimately offer a paradigm of how the GDPR is actually influenced by features, elements and notions that are typical of a security context.

2.2.2. Cybersecurity

The EU Cyber Security Strategy in the Digital Single Market context. The Digital Single Market (DSM) is an initiative launched in 2015 by the European Commission with the aim of fostering the role of the EU as a global leader in the digital economy\textsuperscript{37}. The DSM has three major policy areas:

- Providing better access for consumers and business to online goods
- Creating the right environment and conditions for digital networks and services (telco reform, cybersecurity cooperation, audiovisual reform)
- Ensuring that economy, business and society are positively impacted by digitization.

Developing stronger cybersecurity rules constitutes a prominent objective in such context, as ensuring network security has a strong link with the growth of Europe’s competitiveness in the digital economy. To this end, within the mid-term review\textsuperscript{38} of the DSM initiative, a new Cyber Security Package (CSP) was presented, building on the previous 2013 EU Cyber Security Strategy. Amongst other initiatives, it is noteworthy to underline the following actions foreseen in the CSP, particularly aimed at fostering European cyber resilience:

1. The European Network and Information Security Agency (ENISA). The role of ENISA, established in 2004\textsuperscript{39}, is intended to expand and become the so-called “EU Cybersecurity Agency”\textsuperscript{40}. The ambitious proposal of the Commission is in fact to turn the agency into a centralized body that provides constant support to Member States and EU Institutions in key areas. Such initiative is rolled in a number of policy actions, including but not limited to the proposal for a “Cybersecurity Act”\textsuperscript{41}, currently under legislative discussion.

2. The Network and Information System Directive (NIS). After having adopted it in April 2016, the European Union aims at a swift implementation across its Member States. In order to do so, the proposed renewed scope of ENISA, along

\textsuperscript{36}GDPR, Article 25
\textsuperscript{37}Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy - A Connected Digital Single Market for All
\textsuperscript{38}The Digital Economy and Society Index (DESI) 2017 (European Commission)
\textsuperscript{40}European Commission proposal on a Regulation of the European Parliament and of the Council on the future of ENISA
with a proposal for a Commission Implementing Regulation\textsuperscript{42} laying down rules for application of the NIS Directive should serve the scope of harmonizing a common approach towards implementation and interpretation of the main provision of the abovementioned Directive\textsuperscript{43}. About the core principles of the NIS, more will be articulated in the next sections.

3. **Cyber Defense.** Under the Common Foreign and Security Policy (CFSP)\textsuperscript{44}, the European Union recently adopted a framework for a joint EU diplomatic response to malicious cyber activities (the “cyber diplomacy toolbox”) aims at harmonizing common responses to external cyber threats against the Union and its Member States\textsuperscript{45}.

### 2.2.2.1. The NIS Directive

As briefly mentioned above, the NIS Directive is the other crucial piece of EU legislation that is set to uplift the cybersecurity landscape alongside the GDPR. Differently from the latter, the NIS has no direct applicability within Member States (and does not strictly pertain to the protection of personal data, as we will see). This means that EU countries had an obligation to transpose the framework within a fixed amount of time (expiring in April 2018), with the consequence of resulting in twenty-eight potentially different interpretations of the same provisions. However, despite the legislators’ choice to adopt a minimum harmonization approach\textsuperscript{46}, the Directive has been long awaited and is supposed to lay down, along with its domestic transposing acts, those minimum requirements to ensure an acceptable and competitive level of cybersecurity, awareness and resilience amongst the Union\textsuperscript{47}. Specifically, it does roll out three goals to achieve:

1. Increasing EU-wide cybersecurity capabilities
2. Enhancing multi-actors cooperation
3. Laying down security measures and incident reporting obligations for certain players.

---

\textsuperscript{42}Ares(2017)4460501 - Commission Implementing Regulation pursuant Art 16(8) of NIS Directive

\textsuperscript{43}Europe emerges as global leader in cybersecurity law enforcement to protect critical infrastructure. (2016, Jun 16). PR Newswire Retrieved from https://search.proquest.com/docview/1797271801?accountid=17215

\textsuperscript{44}Annual report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament on the main aspects and basis choices of the CFSP, 2014

\textsuperscript{45}EUISS, Brief Issue, The EU Cyber Diplomacy Toolbox: towards a cyber-sanctions regime?

\textsuperscript{46}NIS Directive, Art. 3

The scope

The first category of stakeholders that are subject to the NIS Directive is the so-called "Operators of Essential Services" (OES), defined in Art. 4 as any private or public entity that cumulatively meets two requirements:
1. Falls under article 5(2), i.e. provides services depending on network and information systems which are essential for the maintenance of critical societal and/or economic activities and for which a potential incident would cause disruptive effects on the provision of that same service.
2. Is of a type referred to in Annex II of the same NIS Directive.

The second category refers to “Digital Service Providers” (DSP), again defined as those services meeting the following two requirements:
1. Delivering digital services as enshrined in Art. 1(1) of Directive 1535/2015.
2. The service is an online marketplace, an online search engine or a cloud computing service.

Two things are worth being noted on the scope of the NIS Directive. Firstly, a clause in the NIS provides for an exception for the referenced operators to be exempted from abiding to the Directive. It is in fact the case of players operating in particular areas which are highly sector-regulated and thus already meet in principle high security standards due to their compliance with other laws. Secondly, the Directive does not only address the categories mentioned above. Indeed, it also requires Member States to establish CSIRTs (Computer Security Incident Response Teams), pursuing a more coordinated pan-European resilience to information security incidents, as well as competent NIS-responsible authorities (the upcoming domestic transposition laws will clarify what will be each Member State’s designated body).

Security Measures and the role of standards

Similarly to what the GDPR requires, so does the NIS with respect to the security measures to be taken by OESs and DSPs separately. “Technical and organizational measures” are thus embedded in such security obligations laid down by Articles 14, 15 and 16. Beyond the mere legal analysis of such obligations, it is interesting to note the approach of the legislator when referring to the state of the art information security technology to be implemented by OESs and DSPs. Article 19 in fact, encourages the “use of European or internationally accepted standards and specifi-

---

48 Parameters and criteria for determining "disruptive effects" are further established in Art. 6
49 Annex II groups activities and businesses in seven macro-areas: energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructures
50 The definition includes the following description: “service” means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services
51 NIS Directive, Annex III

www.eunity-project.eu 21 July 31, 2018
cations relevant to the security of network and information systems” as a mean to promote a convergent approach to Art. 14 and 16 (respectively addressing OESs and DSPs). The reference to international standards reveals a technology-neutral approach which is pretty much mirroring the spirit of the GDPR, while maintaining a level of minimum harmonization as foreseen by the NIS Directive itself.

As a way of regulatory support to the reference above, the second paragraph of Art. 19 relies on the role of ENISA in coordinating the effort with Member States to roll out guidelines on the technical areas to be addressed and on the already existing technical standards to draw up from.

It needs to be highlighted here that compliance with a certain standard does not only permit an organization to demonstrate a certified and accountable conduct through the rules therein. The process of standards negotiations in fact (see below), does also enhance the cooperative efforts amongst various industry sectors, as well as horizontally throughout the supply chain. It provides for a line of junction between organizations, sectors and geopolitical regions which is vital in the context of cybersecurity, as very often the response to a threat is put in place at the global scale.

Irrespective of the presence of a legal framework in a determined sector, it should be noted that standards may address certain issues which could not be directly solved by legislation otherwise, since they very often pertain to problems and constraints that are perceived by a number of sectors but are not enough widespread to be included in a more high-level legal text with a much wider scope.

However, back in 2005, Weiss and Weber found more than 40 cybersecurity standards and put them in a non-exhaustive, paradigmatic list at margin of their paper. Ever since, the number has increased and today it comes as almost impossible to map all those relevant standards applicable in the information security domain. It is clear that fragmentation has the advantage of being sufficiently specific to tackle narrow and particular issues, while leaving the law to provide for a more high-level approach with a robust framework. The challenge observed within the EUNITY project is ultimately, to understand what is the best approach in order to achieve a cooperative cybersecurity relationship between selected trade partners like the EU and Japan. It is now too soon to give a consistent evaluation, as the NIS Directive will soon be in force in all 28 Member States, and the GDPR could be considered as a freshman in the legal landscape. What we can say however, is that the role of standards has not decreased over time and in spite of the existence of regulations and laws, it still provides for a normative rulebook to many industry fields.

Examples of cybersecurity standards are (non-exhaustively) listed below:

- ISO/IEC 27001

---


54 See also: Jenkins, J., Forsyth, C., & Amole, A. (2014). Should cyber security standards be imposed by regulation or left to discretion? Legal Week, 16(3), 10.


www.eunity-project.eu 22 July 31, 2018
- ETSI Cyber Security (CYBER)
- NIST 1.1 Cybersecurity Framework

 Processes
From a regulatory perspective, standards in Europe can either be seen as an alternative to “hard regulation” or an example of self-regulation. They can be either voluntary (market-driven), consensus-based or approved and recognized by a body (for instance, ETSI, NIST, ISO). According to the EU Regulation 1025/2012, “standard” means a technical specification, adopted by a recognized standardization body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following:
(a) “international standard” means a standard adopted by an international standardization body;
(b) “European standard” means a standard adopted by a European standardization organization;
(c) “harmonized standard” means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonization legislation;
(d) “national standard” means a standard adopted by a national standardization body.

The Danish Standard Foundation enlisted the five-step process with which a standard is developed:
1. Proposal and approval phase
2. Drafting and commenting phase
3. Public consultation and vote
4. Draft to formal vote
5. Final Publication

Legal effects take place by way of three different avenues, i.e. by incorporation in contracts, implicit legal significance or reference in normative or statutory text.

Breach notification and Incident Reporting

The NIS Directive (Art. 16) requires Member States to ensure that digital service providers notify the competent domestic authority of any incident resulting in a substantial impact on the provision of a service without undue delay.

---

58 K.Stuurman, Liability and the role of standards, 21.9.2015, TILT, LL.M Law and Technology
Firstly, the competent authority or CSIRT shall be provided by the breached organizations with all the information necessary to assess any cross-border impact of the incident. If an incident impacts more than one Member State, it will be responsibility of the first\textsuperscript{59} Member State’s authority to inform the second one about the breach. Secondly, it needs to be noted that the term “substantial impact” as expressed in Article 16 is further specified by a number of indicators, namely (i) affected users, (ii) length of the incident, (iii) “geographical spread” of the incident.

Because the Directive implements a so-called “light-touch approach”, providers will have to comply to just one of the implementing acts across the different Member States, which is the one of the Country where they have their main establishment.

With regard to the dividing line between OESs and DSPs, ENISA explains that “significant incidents affecting OES networks and systems caused by incidents affecting DSPs’ infrastructures are theoretically considered distinct incidents, therefore the reporting activities should also be distinct”\textsuperscript{60}. Interestingly enough, public awareness is not a necessary step to be fulfilled to comply with the NIS Directive. Differently from what was mentioned above with regard to personal data breach notification requirements under the GDPR, in the realm of the NIS Directive, there is no obligation to keep the public informed about the incident unless public awareness “is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest”\textsuperscript{61}.

In its guidance report\textsuperscript{62}, ENISA stresses the fact that the Directive requires incident reporting without undue delay. With respect to the adoption of information security standards (see for instance, ISO 27000) with a full set of protocols for incident handling and incident response, this approach might be on the one hand an additional layer of compliance and accountability, but on the other hand, following such protocols might be problematic with a view that incidents shall be promptly reported. Operators shall therefore try to strike a balance between reactivity in informing competent authorities of any incident without undue delay and complying with international standards that include incident management within their realms.

**Cooperation in the field of cybersecurity and cyber resilience.**

In order to foster the exchange of information and enhance effective cooperation across Member States of the Union, the NIS Directive foresees the establishment of a so-called “Cooperation Group”\textsuperscript{63}, composed by the European Commission, ENISA and representatives of the Member States, tasked to cooperate with several Union bodies for the provision of advice and best practice on network security. According

\textsuperscript{59}In chronological order

\textsuperscript{60}ENISA, Incident notification for DSPs in the context of the NIS Directive (February 2017)

\textsuperscript{61}NIS Directive, Art 16.7

\textsuperscript{62}Ibid. 60

\textsuperscript{63}NIS Directive, Rec. 4
to Article 1.2(b), the scope of the Cooperation Group should be to foster information exchange and to develop trust and confidence amongst the Member States.

Amongst the numerous tasks, the Cooperation Group is in charge of a number of responsibilities which include providing active support to Member States in determining the organizations that fall under the definitions of Operators of Essential Services and Digital Service Providers (adopting a pan-European “consistent approach”\textsuperscript{64}), hosting experts gathering for fostering the information sharing between actors.

With regard to the relationship between ENISA and the Cooperation Group, as stated in Recital 38, the two entities shall be deemed as “interdependent and complementary”. This means that ENISA, in line with its establishing Regulation 526/2013, shall provide policy and analytical support as well as in the development of sector-specific guidelines. Additionally, implementing powers are given to the European Commission to set up the procedural arrangements for the Group.

National cybersecurity strategies.

Important domains within the NIS Directive do not solely pertain to the obligations that Member States shall impose on digital operators\textsuperscript{65}. Rather, they also directly address Member States as such to start designing and developing a national strategy for cybersecurity (Art. 7), which, according to Art. 4(3), can be defined as a “framework providing strategic objectives and priorities on the security of network and information systems at national level”. The aim of Article 7 is to indicate a twofold objective for each national cybersecurity strategy, i.e. (i) achieving and maintaining a high level of security of network and information systems and (ii) covering at least the sectors mentioned above (Operators of Essential Services and Digital Service Providers). The Directive sets up four main points that shall be addressed within each of the national cybersecurity strategy. Firstly, high-level priorities and objectives with regard to the security of information systems. Secondly, a governance structure that enables the achievements of such objectives. It needs to be noted that such a framework shall be rolling out quite granularly what roles and responsibilities will be given to national and governmental bodies with respect to such strategy. Thirdly, each national strategy shall set forth a series of measures aimed at addressing preparedness, response and recovery. Within this realm, specific mention is dedicated to the elicitation of rules and procedures for smooth cooperation between public bodies and private entities. Fourthly, strategies shall lay down ways and measures enabling education, awareness raising and training, as well as research and development programs in the area of cybersecurity and information and communication technology. Lastly, risk assessment plans and a list

\textsuperscript{64}NIS Directive, Art. 5(6)

\textsuperscript{65}Europe emerges as global leader in cybersecurity law enforcement to protect critical infrastructure. (2016, Jun 16). PR Newswire Retrieved from https://search.proquest.com/docview/1797271801?accountid=17215

www.eunity-project.eu 25 July 31, 2018
of actors involved in the implementation of the domestic cybersecurity strategy shall be explicitly mentioned in the national drafts.

Obligations on the protection of personal data

Multiple overlaps can be identified not only between the NIS and the GDPR, but more broadly, between provisions, principles and obligations on privacy framework and cybersecurity. For instance, within the works of the Cooperation Group described above, the NIS makes explicit reference to the fact that, with regard to information and intelligence sharing between the Cooperation Group and amongst the various CSIRTs, the processing of personal data might be involved. Furthermore, as argued by many, national cybersecurity cooperation involving CSIRTs will help the governments to achieve a wider overview of the cyber threats scenarios, where such entities are considered as points of contact for an iterative exercise in the field of international cooperation. For this reason, interestingly enough, Recital 72 of the NIS Directive explains that any of such processing should be based on the standards imposed by a number of legal texts, namely:

- Regulation (EC) No 45/2001, to the extent that personal data are processed within the realm of European bodies and Institutions;
- Directive 95/46/EC, for any other personal data processing;
- Regulation (EC) No 1049/2001, for the application of the NIS with regard to access to documents;

As we are able to see, no reference whatsoever to the upcoming GDPR is made in the list above, and the data protection standards mentioned therein still refer to the previous framework. With regard to potential overlaps within the subject matter, it needs to be noted that the NIS Directive explicitly differs between data protection authorities (DPAs) as opposed to competent authorities. According to Recital 63, in fact, such two, apparently separate entities, are asked to cooperate in the case a cyber-security incident has an impact on personal data (thus leading to a data breach) in the exchange of meaningful information and intelligence sharing. Such reasoning is confirmed by Article 8(6) which states that competent authorities (under Article 8(1), defined as information security national centers with single points of contact) shall establish lines of coordination along with DPAs and law enforce-

---

67 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.
68 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
ment agencies. Narrowly speaking, such cooperation is further detailed topic-wise. Recalling Recital 63 above in fact, Article 15(4) explicitly provides the legal basis for a cooperative collaboration between competent authorities and DPAs in the circumstance of incident reporting involving data protection aspects, most likely personal data breaches.

2.3. The Japanese landscape

2.3.1. Privacy and data protection

The first recognition of the right to privacy in Japan comes with the jurisprudence in the Utage no Ato case where, based on an interpretation of the Civil Code, the Tokyo District Court stated that “The right to privacy is recognized as the legal protection of the right so as not to be disclosed of private life”.

Following the period of political and social chaos deriving from the Second World War and the so-called national disasters of the Sixties, in 1975 the first claims for the right to privacy consolidated across the Japanese territories with the aim of limiting potential government surveillance and to give a response to the defeated national ID-scheme policies. In the early 2000s, after the adaptation tendencies (with minor differences) of the Japanese legal landscape with parallel western countries, Japan realized that a legal approach to the right to privacy would have helped the nation’s success in commerce and trade, with a substantially consensual approach of all the players involved: “The early signs from the business community, the bureaucracy, the political elite and the populace at large are overwhelmingly supportive of the conclusion that the Privacy Act will be effective”.

The Act on Personal Information came eventually into effect in 2005, after its official announcement in 2003. The Diet, in that circumstance, received fierce opposition against the Act by the mass media community, and was constituted by two parts: basic principles (chapters 1 to 3), and general obligations (chapters 4 to 6).

---

71Judgment of Tokyo District Court, 28 September 1964, Hanrei-jihyo vol. 385, p. 12
72Carol Lawson, Japan’s New Privacy Act in Context, 29 U.N.S.W.L.J. 88 (2006)
74Ibid. 72
75The equivalent for the parliamentary bodies of Japan
The Japanese Reform on Privacy

The concept of privacy in Japan has rapidly evolved over the recent decades. As briefly mentioned, Japanese data protection laws pertain to a relatively newer tradition in legal privacy. Japan’s first Act on Privacy (APPI - Act on the Protection of Personal Information), is one of “Asia’s oldest data protection laws.”

The current privacy law got finalized in 2017 but started some years back with a couple of relevant steps that the Japanese Government had to go through before formally starting the amendment of the existing laws. As Harada states, “One of the main objectives of the amended Act is to create a framework that recognizes and addresses the fact that transfers of personal data occur on a global scale.”

Particularly relevant to this end are in fact the Law Reform Plan adopted by the Cabinet IT Strategic Headquarter in 2012 and the Policy Outline of the Institutional Revision for Utilization of Personal data (2014). In the same year the Amendment Outline of the Bill was presented, and in March 2015 the formal process officially started with the Cabinet Decision on the Amendments on the Acts. The purpose of the law reform was to foster innovation and to introduce new services as well as promoting people’s safety by ensuring an appropriate protection of personal information. The first law is the Act on the Protection of Personal Information, which included amendments regarding both the processing and protection of personal data. It also established the independent regulatory authority by means of a significant restructuring of the existing information protection Commission.

Furthermore, in September 2015 the so called “My Number” Act (ID Number Act) was set forth and included amendments on the promotion of the use of specific personal information (My Number) and on the numeration of the accounts, the use of numbers in the medical examination and health guidance, a link with vaccination records.

Japanese Privacy Act within the Japanese Legal System

It is important to note what is the structure of the Japanese legal system to better comprehend the role and the importance of the 2015 reform on privacy and data protection. To start with a top-down approach, the hierarchy of legal sources

---

78 Ibid. 72
79 Harriet Pearson, Julie Brill, Mark Parsons and Hiroto Imai (Hogan Lovells) for Lexology, Changes in Japan Privacy Law to Take Effect in Mid-2017: Key Regulator Provides Compliance Insights (1.2.2017)
81 From Wikipedia, Individual Number webpage: “An Individual Number, also known as My Number, is a 12-digit ID number issued to all citizens and residents of Japan (including foreign residents in Japan) used for taxation, social security and disaster response purposes. The numbers were first issued in late 2015”.

www.eunity-project.eu July 31, 2018
in Japan lists at its highest level the Constitution, under which a layer of so-called Fundamental Laws apply. Within such a cluster, the Act on the Protection of Personal Information can be considered as taking a similar role. The same act sees its sections 1, 2 and 3 standing a level below, where a number of legal principles are grouped, such as basic philosophy, responsibilities and measures of the State and Municipalities, or the establishment of the Basic Policy. Both acts on the Protection of Personal Information held by Administrative Organs and the one on the Protection of Personal Information retained by Incorporated Administrative Agencies occupy the lower levels, along with sections 4, 5, and 6 of the Act on Personal Information.

**Definition of Personal Information**

According to Articles 2-1 of the Act, personal information is an information that is identifiable of the individuals by names, birthdate and the other descriptions including documents, drawings, electromagnetic records or voices, motions and other means.

Personal identifiers are instead described in Article 2-2; they are letters, numbers, marks and the other codes which fall in (i) characteristics of the part of body for the purpose of use of electronic machines, which is identifiable for the individual or (ii) the individual user or purchaser designated, written or recorded in the service use or the sales.

Similarly to what we describe as “special categories of personal data”, Article 2-3 explains how personal information which include race, religious beliefs, social statuses, medical records, criminal offences, events related to victims or criminal offences are indeed sensitive data which require special care in order to avoid the injurious discrimination, biases and potentially subsequent disadvantages.

**Conditions for Processing**

It is noteworthy to highlight what the Japanese law says about anonymization. Specifically, Article 2-9 provides a definition for anonymous data as personal information which does not enable one to identify an individual. It further explains two ways to achieve such an event, (i) the deletion of all descriptions containing personal information and (ii) deletion of all personal identifiers containing such information. This clause is supplemented by Article 2-10 regarding the anonymous processing information entities as any entity that uses the anonymous processing database (easily searchable via electronic machines).

For such cases, businesses will not have to seek for users’ consent when it starts processing data. Accordingly, such a measure was advocated by the Japanese Gov-
ernment to ease the shift of many digital business models towards big data analytics use and to facilitate their legitimization within the Japanese legal framework\textsuperscript{82}.

**Data Broker Measures**

According to article 25 of the Japanese Act, based on the Commission’s rules on retention, (personal information handling) entities must keep records of the date and the third parties to which personal information are disclosed.

In the event that personal information handling entities receive the information from third parties, such entities shall check the basic details of the company (name, addresses and contacts of the representatives of the corporation), as well as the context under which such a transfer is made. Records shall be kept with regard to the date of data acquisition for a period of time set forth by the Commission\textsuperscript{83}.

In the event that personal information handling entities and / or their employees unlawfully acquire or steal personal information within a database for the purpose of making an illegal profit, the Act on the Protection of Personal Information provides for a punishment of up to one year imprisonment and up to 500.000 Yen under Article 83.

**The Personal Information Protection Commission**

Dating back in 2013, the My Number Act firstly established an independent oversight Commission with limited powers tailored for the monitoring and enforcement of such Act. The new Personal Information Act widens the scope of the pre-existing Commission as follows.

Chapters 4 and 5 of the Act on Personal Information provide for the basic rules and procedures of Japan’s privacy regulator, called PIPC - Personal Information Protection Commission.

With regard to its establishment (Chapter 5), it should be noted that the PIPC falls under the jurisdiction of the Prime Minister’s Cabinet Office, with a clear mission of ensuring the proper handling of personal data, taking into account the effective use of personal information. Article 52 enlists seven tasks of the Commission, namely:

1. Promoting the Basic Policy
2. Supervising the use of My Number
3. Assessing the impact of My Number
4. Actively engaging in public relations and education
5. Conducting necessary studies and analysis
6. Becoming a player in the international cooperation field

\textsuperscript{82}Harriet Pearson, Julie Brill, Mark Parsons and Hiroto Imai (Hogan Lovells) for Lexology. Changes in Japan Privacy Law to Take Effect in Mid-2017; Key Regulator Provides Compliance Insights (1.2.2017)

\textsuperscript{83}Article 26 Japanese Act on the Protection of Personal Information
7. Complying to the execution of other tasks provided for by law

The Commission performs its duties under the principle of independence of functions, particularly with regard to the President of the Commission and the Commissioners themselves. Having this in mind, it is useful to note that the governance of such body is constituted of the President and 8 Commissioners equally distributed in full-time and part-time posts. Such members are wholly appointed by the Japanese Prime Minister, with the approval of both Houses of the Diet (Japan’s bicameral legislature). Their background can be of different extractions, such as experts from Academia, consumer organizations, IT technologists, My Number Administrators, businesses and local organizations.

Their mandate lasts five years (renewable), and their status is guaranteed by immunity (unless they are involved in crimes related to insolvency, actions against the acts they supervise, crimes for which imprisonment is foreseen or they become mentally or physically disabled).

The Commission can establish specific expert committees to explore a particular issue or novelty, and has an obligation under Article 70 to report annually to the Diet. Section 3 (Chapter 4) of the Personal Information Act rolls out the main tasks of the Commission with regard to the supervision activities. According to such Section, the Commission has established powers of conducting on-site inspections and submitting reports. They can issue instructions and advices (Article 41), as well as recommendations and orders (Article 42).

Ultimately, the Commission has an explicit prohibition on non-interfering with some of the basic civil rights such as the freedom of expression, academic freedom, freedom of religion and freedom of political association. On a number of occasions, it can delegate activities and powers to the Competent Minister which shall report to the Commission upon finalization of the task. Conversely, on a number of residual cases, the Competent Minister can request the Commission to take necessary measures in a given issue.

2.3.2. Japan and the European Union: comparative aspects on privacy and data protection

Global Harmonization and Data Transfers

According to the Japanese Act, it is the task of the Government to take necessary measures to ensure the international harmonization with foreign states. Under Article 24, personal information cannot be transferred to a third party or a foreign country except in the cases of compliance with the Commission’s standards or transfers to countries with an equivalent level of protection of interests and rights.

Similarly to the Japanese Act, the GDPR presents similar grounds for international cooperation in the area of personal data transfers with third countries. Article 45 states in fact that a mechanism for data transfers without the need of prior authorization or particular safeguards by the controllers is in place with those countries
where an adequate level of data protection is ensured. Such an “adequacy decision” is the result of a relatively long assessment process (preceded by negotiations) undertaken by the European Commission, for which the following criteria serve as evaluation metrics: general (and specific) compliance with the rule of law and relevant civil rights, appropriate regulatory bodies in charge of supervision, enforcement and oversight and the international commitment the country has entered into by ways of any international public law instrument.

Currently, the European Union and Japan have entered into the negotiations towards an adequacy decision that is supposed to come at the end of the evaluation process by the European Commission84. Such a decision should allow the free flow of personal data, and the mutual recognition that each other’s territories abide to “essentially equivalent” standards for the protection of personal data. This process shall therefore comply to both the Japanese Personal Information Act (Art.24) and the GDPR (Art. 45 and broadly, Chapter 5).

The finalization of such evaluation process shall then lead to the issuing of an implementing act which, according to Article 45 of the GDPR, shall be subject to a period review aimed at assessing significant changes and transformations happened in the meantime.

The smooth and legally authorized personal data flow between regions is crucial for fostering the digital trade market between such areas85. However, it needs to be kept in mind that the adequacy decision does only allow for free flow of personal data. Compliance with the foreign country rules where personal data needs to be transferred to (or from) will still have to be met through additional operational efforts and regardless of any such adequacy decision.

Comparative Overview of GDPR and Japanese Privacy Act

Even if a mutual recognition of adequate standards for data protection is expected and likely to happen within the biennium 2018-201986, some differences between the two legal regimes still remain87. The comparison between the new reformed acts (GDPR and Japan’s Personal Information Act) that is carried out below elicits a number of differences which give an example of the potentially significant operational efforts and compliance demands on businesses and organizations wanting to make benefit of the opportunity of both European and Japanese data markets88. Nevertheless, the proximity of both reforms and the fact that both were

---

85 Julia Fioretti, EU sees data transfer deal with Japan early next year, Reuters, 15.12.2017
86 Kensaku Takase, GDPR matchup: Japan’s Act on the Protection of Personal Information, IAPP, 29.8.2017
87 Mark Scott and Laurens Cerulus, Europe’s new data protection rules export privacy standards worldwide, Politico.eu, 6.2.2018
88 Ibid. 86
approved over the last years supports the argument that “(...) the significance of the differences is less”\textsuperscript{89}.

**Territorial scope**

With reference to the territorial scope, the GDPR details the extraterritoriality principle\textsuperscript{90} (present in both jurisdictions) with an additional point. Such a principle implies that the legal standards set up within the territory by the GDPR do also apply outside such territories as long as foreign businesses and organizations offer goods and services to within the country or territory where the data protection laws apply. Thus, both territories of the European Union and Japan extend the applicability of their privacy laws to those established abroad but with the above-mentioned business interests within such regions. However, GDPR further extends such applicability also to those firms which are not established within the EU but monitor European data subject’s behaviors.

**Personal information**

Whilst the GDPR considers personal information as those relating to an identified or an identifiable person\textsuperscript{91}, the Japanese Act differs in such definition as follows. For such a concept in fact, the Japanese Personal Information Act provides a slightly divergent notion, i.e. those information relating to a living individual which can identify such specific individual by the description contained in the information.

Additionally, the Japanese Act adds up a definition of personal data, i.e. those personal information that are processed within a database (with dedicated rules\textsuperscript{92} and procedures for such cluster of personal information).

**Sensitive personal information**

The list of sensitive personal information under the GDPR is comprised of those revealing ethnic or racial origins, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic or biometric data for identification purposes. The Japanese Act includes in its list information concerning religion, social status or medical history, criminal records and the circumstance where a data subject has suffered damages from a crime\textsuperscript{93}. Such narrower interpretation of the category of sensitive personal information by the Japanese laws has allegedly caused some delays during the negotiations\textsuperscript{94}, since the European approach protects in this category trade union memberships and sexual orientations, whilst the Japanese Act does not\textsuperscript{95}.

**Information rights**

With respect to data subjects’ rights, the Japanese Act distinguishes between the duty of data controllers to provide for disclosure, rectification or cease of processing, added by the obligation of explanation of reasons (within the obligations chap-
The GDPR enlists a number of more systematic rights, such as the rights of information, access, rectification, erasure, object and explanation. On top of such basic rights, the GDPR improves user controls over his or her data by adding a new right at Article 20 (currently absent in the Japanese provisions): the right to data portability.  

**Data controllers and processors**  
Unlike the European Union, which has a longstanding tradition in the use of the term “data controller” within its privacy laws, Japan does not seem to have a perfectly overlapping profile. Such concept is in fact replaced in the Personal Information Act by the notion of “business operator,” which is the responsible entity for the handling of the information. No further distinction with personal data processors are made in the law.  

**Penalties and fines**  
The GDPR raises the bar for potential violation of its provisions up to 20M Euros or 4% of the global annual turnover. However, no criminal liability arises from the regulation. Conversely, the Japanese Act has a lower breach sanctions cap (for instance, for database stealing, the fine is up to 500,000 Yen, roughly 4,200 Euros), while explicitly foreseeing up to one year imprisonment.  

2.3.3. Cybersecurity  

Since the early 2000s, Japan has been an active player in the cybersecurity field. A number of initiatives are to be recorded in this section, to set out the background that led to the legislation on cybersecurity which will further be elaborated below.  

With regard to measures addressing government agencies, it needs to be noted that, in July 2000, a set of Guidelines on Information Security Policies was issued. Later on, between 2005 and 2014 a number of Common Standards for Information Security Measures for Government Agencies followed up the first Guidelines issued in 2000, with the 2014 edition published by the Policy Council in May 2014.  

With respect to the protection of critical infrastructures, the first initiative dates back to 2000 with the Special Action Plan on Cyber-terrorism Countermeasures for Critical Infrastructures, followed by two other Action Plans (respectively in 2005 and 2009) and the 2014 Basic Policy (3rd Edition), revised by the Strategic Headquarters in 2015.  

---  

96. “The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services”. The Information Commissioner’s Office (ICO), Right to data portability, www.ico.org.uk, last accessed 19.3.2018  
97. Ibid. 86  
99. Ibid. 98  

www.eunity-project.eu  

34  
July 31, 2018
2.3. THE JAPANESE LANDSCAPE

Regarding the governance model, in February 2000 the IT Security Office within the Cabinet Secretariat was established; after that in 2005 the National Information Security Center and the Information Security Policy Council were created\(^\text{100}\).

Out of the merely legal and strategic initiatives, it is noteworthy to underline that Japan has undergone a number of serious cyber incidents. For instance, a survey conducted by KU Leuven within the auspices of the first EUNITY Workshop Meeting held in Tokyo in October 2017 by means of a questionnaire circulated amongst Japanese partners and attendants revealed that incidents like the Benesse data breach\(^\text{101}\) (2014) had quite an impact on the cybersecurity community. However, the need for a structured and systematic response both at the strategic and at the legal level to cyber threats derives from a certain level of proactivity of the Japanese community towards the imminent Olympic Games, to be held in Tokyo in 2020\(^\text{102}\).

The Law

In November 2014, the Diet adopted the Cybersecurity Basic Act, amended in 2016\(^\text{103}\). The Basic Act has a number of principles and notions in it; amongst others, it provides for a definition of "cybersecurity" in a legal terminology, the basic principles of cybersecurity policies, stakeholders' responsibility, structure and functioning of the Strategy and the Cybersecurity Headquarters composition. All such topic areas were therefore strengthened within the Japanese legal system by being formulated in one and only systematic legal text\(^\text{104}\).

The Cybersecurity Strategic Headquarters for instance, introduces mandatory reporting from government bodies and agencies, as well as the NISC\(^\text{105}\) as a third, independent party which serves for auditing purposes and incident analysis. Furthermore, the Cybersecurity Strategy under the new Basic Act is no more an act adopted by the Information Security Policy Council (with no enforcement powers). Rather, it becomes a more accountable process, with the Act in itself being adopted with a Cabinet Decision and reported to the National Parliament, binding all governmental bodies and agencies and with clear enforcement powers\(^\text{106}\).

\(^{100}\)Ibid. 98
\(^{101}\)Nikkei Asian review, Customer data leak deals blow to Benesse, 10.7.2014
\(^{102}\)Reuters, Japan holds first broad cybersecurity drill, frets over Olympics risks. (2014)
\(^{103}\)Sayuri Umeda, Japan: Cybersecurity Basic Act Adopted, Global Legal Monitor (Dec. 10, 2014)
\(^{105}\)National center of Incident readiness and Strategy for Cybersecurity, established in January 2015
\(^{106}\)Ibid. 98
CHAPTER 2. LEGAL AND POLICY ASPECTS

A Legal Definition for Cybersecurity

First and foremost, the Basic Act defines cybersecurity within the realm of the Japanese Law. Accordingly, it is “consideration, maintenance and management of needed measures to prevent the leakage, destruction or damaging of information reported or transmitted or received by electronic way, magnetic way or other ways that human cannot recognize, or to manage safety control of that information, or to ensure safety and reliability of information systems or information and communication networks”\textsuperscript{107}. Interestingly, the European Union’s Network and Information Security Directive (NIS) does not define what cybersecurity is within the context of the Directive itself.

NIS vs Basic Act: the Citizen as an Active Stakeholder

It is important to highlight in this section a difference between the Basic Act and the European NIS Directive. Whilst the latter merely represents an attempt to coordinate efforts towards the security of European information systems by defining a set of rules that need to be implemented and that address a limited amount of players, Article 9\textsuperscript{108} of the Basic Act on Cybersecurity does actually mention the responsibilities of the citizens within the cybersecurity domain: “In accordance with the Basic Principles, the people are to make an effort to deepen their awareness and understanding of the critical value of Cybersecurity and pay necessary attention to ensuring Cybersecurity”\textsuperscript{109}.

It is not fully clear whether such a provision creates a positive obligation of a duty of care for the citizens or if it is merely a programmatic norm which pretty much remarks the concept summed by the Latin clause ignorantia juris non excusat (tr., ignorance of law excuses no one). However, what is striking in the Basic Act is the presence of the citizen as an active stakeholder, a player to whom some level of awareness is expected. To this end, one of the so-called Basic Principles, Article 3(2), invites all citizens to put in place voluntary actions aimed at preventing damages caused by cyber threats. This is not only relevant from a legal perspective. Rather, it reveals the level of maturity of a legislation and of a society which tends to include the citizen within the scope of such a legal text on such a specific domain, whilst its European alter ego (NIS), limits itself in addressing a restricted number of players. Notwithstanding the fact that there is a substantial difference in the two legal texts (one, the Basic Act, is directly applicable, while the NIS Directive needs an active implementation act by Member States), it should be nevertheless noted how the Japanese approach seems to mirror the general claim by the expert community that cybersecurity is a topic that has to be grasped and addressed also at the societal level.

\textsuperscript{107}Japanese Basic Act on Cybersecurity, 2014 (amended 2016)
\textsuperscript{108}Act No. 104 of November 12, 2014
\textsuperscript{109}Tr. “Japanese law translation”

www.eunity-project.eu 36 July 31, 2018
2.3. THE JAPANESE LANDSCAPE

Information Sharing and Incident Reporting

“Ahead of the 2020 Olympic Games in Tokyo, the government sees cooperation as necessary to better prepare for growing cybersecurity threats, recover from such damage and probe the causes”. This is how a government senior official was addressing the Japan Times\textsuperscript{110} on cybersecurity cooperation. As already mentioned earlier, the Japanese Government has proved to be willing to approach large events with potential cyber implications proactively.

In such circumstance, the point was that the Japanese Government was set to start filing a cybersecurity cooperation request according to the Basic Act, addressing 48 entities that were identified on the basis of the Basic Act itself, and for which it is foreseen a coordinated cooperative action to counter potential cyber threats before, during and after the Olympic Games.

With regard to information sharing, the Basic Act does not contain a coherent provision. Rather, it includes three different layers: Article 13, with respect to the measures to be provided to cybersecurity players such as administrative organs by the Government, which includes responses to cybersecurity threats and cooperation, communication and coordination with relevant domestic and foreign parties and sharing of information about cybersecurity across all sectors of the governmental machinery.

As a second layer, Article 14 of the Basic Act includes a provision requiring the Government to activate and set up the necessary measures in order to enable the promotion of information sharing. Lastly, Article 23 enlists a series of explicit areas where the Government is expected to carry out Japan’s role in the field of cybersecurity. These are measures like active participation in law-making of international norms, confidence and trust building towards the exchange of information with foreign countries, international technical cooperation on capacity building and cybercrime takedowns, awareness raising across the international community.

Over the recent years, Japan has signed a number of agreements on information sharing with regard to cybersecurity threat intelligence with a number of partners, which are not only located in the Asia-Pacific area, rather all over the world, as a symptom that this domain needs a global cooperative platform in which, for example, the relationships between the EU and Japan can be significantly improved. Examples of such partnerships are (non-exhaustively) listed hereby:

1. Japan-UK Joint Declaration on Security Cooperation, Tokyo, (2017)\textsuperscript{111}
2. Japan – India Cyber Dialogues, which lasts since 2012 and is at its Second Edition (2017)\textsuperscript{112}

\textsuperscript{110}The Japan Times, 48 infrastructure entities to get cybersecurity cooperation requests, 2015
\textsuperscript{112}For more information, consult: Joint Press Release Second Japan-India Cyber Dialogue, New Delhi, 2017
3. The Japan-ASEAN cybersecurity dialogues, which are rolled out in a number of different policy initiatives since 2009\textsuperscript{113}
4. Japan's first access to the US's DHS's Automated Indicator Sharing (AIS)\textsuperscript{114}.

### 2.4. Conclusions

The present report highlights the main aspects of the two regional entities in the scope of EUNITY project, the European Union and Japan, as well as their progress in the legal and regulatory area within the privacy and cybersecurity domain.

Both regions have undergone a period of substantial reforms and modernization of the existing legal frameworks with regard to privacy. In Europe, the GDPR entering into force in May 2018 brings up a significant update of the legislation with a strict compliance bar foreseen for its enforcement. In Japan, the Act on Personal Information was recently amended. However, in spite of a mutual recognition and the ongoing negotiations between the European Union and Japan towards the so-called adequacy decision for the free mutual transfer of personal data, it should be nevertheless noted that the two frameworks are not perfectly matching. For instance, the concepts of sensitive personal data, as well as some practical implications such as the diverging approach on the imposition of fines and sanctions might become a critical point for both Japanese and European businesses and organizations wanting to enter each other's digital markets.

In contrast, the cybersecurity domain is somewhat dissimilar from the one described above. At a first glance, differences might be spotted in the laws of the two regions, mostly pertaining to their scope and the stakeholders such laws apply to, thus diverging from one another in substantial elements. However, some lines of similarities can yet be pointed out. This can be observed in the room left by both policy and legal frameworks allowing EU, Member States and Japanese Government to engage in international cooperation, particularly in the fields of international norms settings and common strategy building, promotion and awareness raising of a cybersecurity culture within the respective territories and beyond.

### 2.4.1. Summary of Challenges and Gaps

This conclusive section provides for a number of points that have been identified as potential blockers or issues to be addressed in order to further strengthen the cooperation between the EU and Japan in the domains of privacy and cybersecurity.

(a) The **scope** of the two privacy legislations differ quite significantly in their application: whilst Japanese laws include the offering of goods and services only, the EU framework extends its scope to non-European organizations offering services in Europe and to those targeting market behaviors of data subjects.

\textsuperscript{113}Mihoko Matsubara, Japan's Cybersecurity Capacity-Building Support for ASEAN – Shifting From What to Do to How to Do It, PaloAlto Networks, 26.07.2017

\textsuperscript{114}Morgan Chalfant, US, Japan deepen cyber information sharing, Silicon Hill, 5.4.2017
2.4. CONCLUSIONS

For this reason, the imbalance stands on the European side, seemingly creating a burden on Japanese organizations wanting to monitor market behaviors of their potential customers.

(b) The concept of personal information is not aligned between the two regions. Whilst the EU takes a more protective and data-subject-driven perspective, (inter alia, by including within the definition IP addresses), the Japanese standpoint is more restrictive in the delineation of the contours of such definition, thus creating a potential gap. The result could be that Japanese businesses targeting EU data subjects will have to abide to data protection laws for processes that are normally excluded by such compliance in their country.

(c) Information rights result to be more articulated in the EU framework, entailing much more options for data subjects to control their personal data. For this reason, Japanese controllers would have to put in place processes to permit a number of actions (see portability for instance), which in contrast are not mandatory in the Japanese framework.

(d) The sanctionatory regime is significantly higher in the European legislation than the one in Japan. Therefore, assessment of the advantages in entering the other region’s market would definitely result more advantageous for Europeans offering services in Japan than vice versa, as far as the mere evaluation of the risk of being fined is concerned. However, the Japanese law entails some aspects of criminal liability (with prison penalties in some residual cases of privacy violations), which are not present in European law.

(e) With regard to cybersecurity, it is still too soon to provide an assessment of this sort. The draft Cyber Security Act is expected to provide substantial improvement to the current European legal framework on cybersecurity, which is currently solely constituted by the NIS Directive. However, one of the major differences observed in the comparison of the two frameworks is the fact that Japan actively addresses the conduct of the citizens with respect to cybersecurity. Such duty of care, lifts the burden of protecting information systems that in Europe merely stands on producers, manufacturers and other stakeholders in the supply chain. European businesses and the like will be thus conscious of such difference in their liability regime, which is potentially more advantageous in Japan.

(f) With regard to information sharing, a positive note is coming from the adequacy decision being signed between the EU and Japan. This will allow a mutual recognition of an equivalent level of data protection by the EU and Japan. Once adopted, this will cover “personal data exchanged for commercial purposes, but also personal data exchanged for law enforcement purposes between EU and Japanese authorities, ensuring that in all such exchanges a high level of data protection is applied” 115. The press release from the European Commission (17 July 2018) continues:

115 European Commission, Press Release “The European Union and Japan agreed to create the world’s largest area of safe data flows”
To live up to European standards, Japan has committed to implementing the following additional safeguards to protect EU citizens’ personal data, before the Commission formally adopts its adequacy decision:

a) A set of rules providing individuals in the EU whose personal data are transferred to Japan, with additional safeguards that will bridge several differences between the two data protection systems. These additional safeguards will strengthen, for example, the protection of sensitive data, the conditions under which EU data can be further transferred from Japan to another third country, the exercise of individual rights to access and rectification. These rules will be binding on Japanese companies importing data from the EU and enforceable by the Japanese independent data protection authority (PPC\textsuperscript{116}) and courts.

b) A complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority.\textsuperscript{117}

\textsuperscript{116}Japanese privacy regulatory body

\textsuperscript{117}Ibid. 115
This chapter contains the description of the most important research and innovation aspects regarding cybersecurity and privacy. Sections 3.1 and 3.2 have mainly descriptive character, and regard the area of research funding and the area of substantive research directions, respectively. Sections 3.3 and 3.4, in contrast, provide some conclusions regarding research in cybersecurity and privacy and also contain some suggestions about future common interests between the European Union and Japan.

3.1. Mechanisms to finance cybersecurity research

This section identifies and describes the mechanisms to finance cybersecurity research in both regions.

3.1.1. In the European Union

This subsection identifies and describes the mechanisms to finance cybersecurity research in the European Union. We start by generally describing the funding mechanisms in the European Union, followed by a detailed description of funding mechanisms in the countries of the EUNITY project partners.

3.1.1.1. European Union, International

Framework Programmes (now Horizon 2020) - open competitions
- Applicant: legal entities established in Member States, overseas territories linked to Member States, associated countries, or listed countries
- Project manager: not specified
- Duration: may be specified in topic
- Level of financing: 70-100%
- Budget
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- programme: specified in Work Programme
- call: specified per topic (per strand if applicable)
- project: specified approximated contribution per project but these are not required
- TRL: specified per topic (per strand if applicable)

Special programmes such as Connecting Europe Facility (CEF) - Cybersecurity calls
- Applicant: one or more Member State, international organisations, joint undertakings, public or private undertakings
- Project manager: not specified
- Duration: 24 months
- Level of financing: 75%
- Budget
  - programme: not specified
  - call: 12,000,000 EUR
  - project: CEF contribution up to 1,000,000 EUR
- TRL: not specified

ENISA-European Union Agency for Network and Information Security announces tender procedure for multiple framework contracts with re-opening competition. The budget for each framework contract period is specified in the tender. Successful tenderers sign framework contracts and are invited to submit their offers in specific tenders.

EUREKA has been created as an intergovernmental initiative in 1985 and aims at enhancing European competitiveness through its support to pan-European projects to develop innovative products, processes and services. EUREKA promotes and supports market-oriented international R&D&I project generation and facilitates access to finance for companies involved in its projects. The main aim of EUREKA is: "raising the productivity and competitiveness of European businesses through technology. Boosting national economies on the international market, and strengthening the basis for sustainable prosperity and employment."[1]

- Applicant: research centres, corporations, administrations, SMEs, universities
- Regions of applicants: European Union, Mediterranean countries, Switzerland, Balkans and other countries

EUREKA is a framework programme and is organized around 4 different instruments[2]:
- EUREKA Network Projects is an instrument focused on transnational, market-driven innovative research and development projects. Projects are supported

[2]Ibid. 1
3.1. MECHANISMS TO FINANCE CYBERSECURITY RESEARCH

by the public administrations and public funding agencies that represent EU-REKA. Projects aim to develop marketable products, services or processes.

- The Eurostars Programme is a joint programme between EUREKA and the European Commission and the first European funding and support programme to be specifically dedicated to research-performing SMEs. Eurostars stimulates them to lead international collaborative research and innovation projects by providing support and funding. Eurostars projects are collaborative, meaning they must involve at least two participants (legal entities) from two different Eurostars participating countries.

- EUREKA Clusters are long-term and strategically significant initiatives that develop technologies. A typical Cluster project is performed by 2-14 participants around 2-4 countries.

- EUREKA Umbrellas are an association of at least five national thematic networks in a specific field of technology or service. Umbrellas are comprised of experts from science and industry as well as representatives of national funding institutions. They are set up to support and advise project consortia on developing project ideas through international partnerships in their given field of technology.

Other forms of financing mechanism:

- Marie Sklodowska-Curie actions/grants and support for research infrastructures
- Projects of the European Strategy Forum for Research Infrastructures (ESFRI)
- European Structural and Investment Funds (ESIF)
- PRIMA initiative (Euro-Mediterranean cooperation)
- Euratom (European Atomic Energy Community) programs which support projects connected to nuclear energy (which could include cybersecurity aspects)

3.1.1.2. Financing mechanism in the countries of the EUNITY project partners

France

In France, the cybersecurity strategy is fixed by the Loi de Programmation Militaire (LPM) or “military planning law”. These programmes influence the amount of funding and the topics that are called by the three national funding entities that provide funding for cybersecurity research:

- Agence Nationale pour la Recherche (ANR) The French National Research Agency funds research projects under its yearly call for proposals. The projects funded by ANR are collaborative between academia and industry, with a strong focus on research. Projects are evaluated by committees of experts, usually from academia. In addition to the yearly global ANR research programme, there are several specific bilateral cooperation agreements that also include cybersecurity. ANR also funds projects under the CHIST-ERA European scheme.
• **Direction Générale des Entreprises (DGE)** The French Ministry of Economy under the enterprises directorate has several schemes for funding collaborative research between academia and industry. It also contributes to funding at the European cluster level through contributions to ITEA and CELTIC. These calls are jointly managed and funded by the Banque Publique d’Investissement (BPI France). The projects are partially evaluated (labelled in fact) by the French regional competitiveness clusters. Amongst these clusters, several label cybersecurity projects. The most relevant competitiveness clusters are Systematic, SAFE and Aerospace Valley.

• **Direction Générale de l’Armement (DGA)** The French Ministry of Defence hosts a procurement and research agency, that contributes to funding both academia and industry, with a specific focus on SMEs. These calls are generally jointly operated with DGE or ANR and have a dual-use objective. The projects are evaluated by ANR or DGE, following their specific rules for funding.

In addition, a few French regions provide funding for research, in general to support PhD grants. The most active in the area is the Brittany region, which hosts the *Pôle d’Excellence Cyber* (PEC). This cluster regroups the DGA research branch (located in the Brittany region) and industry to fund PhD research projects and chairs on cybersecurity.

The following programmes fund cybersecurity research:

• **ANR challenge 9 (ANR)** The ANR Challenge number nine, entitled *Liberté et Sécurité de l’Europe, de ses citoyens et de ses résidents*, mimics the Digital Security calls of the H2020 programme. It funds projects related to fundamental research (such as cryptography), crisis management and resilience, defense against organized crime and terrorism, cybersecurity and protection of critical infrastructure.

• **joint ANR-BMBF (ANR)** ANR has created a partnership with the german ministry of research funding agency BMBF to create a joint bilateral call for French and German teams to collaborate on security projects, including cybersecurity.

• **FUI and FSN (DGE)** The *Fond Unique Interministériel* (FUI) and *Fond pour la Société Numérique* (FSN) fund projects oriented towards industry, driven by industry but with academic collaboration. They aim at developing the digital society and are supported by excellence clusters. The yearly project call funds three to five cybersecurity projects each year.

• **PIA, PIA2, PIAVE (BPI)** The *Programme d’Investissements d’Avenir* (PIA) aims at funding the development of the French industry. Driven by industry and government needs, it funds three to four large cybersecurity projects that aim at a high TRL level, delivering working prototypes and close to market.

• **RAPID (DGA/DGE)** The *Régime d’Appui pour l’Innovation Duale* (RAPID) programme fund dual-use projects aimed at industrial research and prototype development. It funds the development of cybersecurity prototypes at an intermediate TRL level. The projects may include industry and academia, but they must be coordinated by an SME.
3.1. MECHANISMS TO FINANCE CYBERSECURITY RESEARCH

- ASTRID (DGA/ANR) The *Accompagnement Spécifique des Travaux de Recherches et d’Innovation Défense* (ASTRID) programme funds specific disciplinary or interdisciplinary themes, at a low TRL level, again for dual-use research.

In addition, many French institutions also participate in H2020 calls and are members of ECSO.

**Greece**

- National programmes / Government programmes
  - The Ministry of Education, Research and Religious affairs (MERRA)
  - The Public Investment Programme (PIP)
  - National Strategic Reference Framework 2007-2013 (NSRF)
- International, Joint Programming
  - Greece has engaged in 61 joint calls (past five years) and been part of international networks consisting of 43 institutions/stakeholders. From ERANETs: MARINERA, MARIFISH, PV, ERANET, ICT-Agri and ICT-Agri C-2, BS-ERA.NET, ERA.NET-RUS and ERA.NET-RUS Col, E-Rare 2 (JTC2011), ERACOBUILD, EMIDA, SEAS-ERA C-1, TRANSCAN C-1, ERA.NET FENCO and CAPITA and from joint calls of 6th and 7th Framework Programme networks: SEE-ERA.NET, COMPLEXITY NET, SEE-ERA.NET PLUS.
- Other
  - intergovernmental networks (e.g. COST), and the Joint Programming activities for current critical issues (e.g. action on immigration)
  - National Strategic Reference Framework (NSRF), providing funds under specific actions: Development proposals of Public Research Centers/Institutions - KRIPIS), EUs RTD Framework Programmes or other international programmes.

**Spain**

There are a few national mechanisms to finance research in information and communication technologies. These include cybersecurity as one of the areas. These mechanisms are framed in a larger program with four main objectives, which do not always include public funding of R&D activities, but which may also promote cybersecurity research by means different than public subsidies to research institutions. The following four programs make up the current Spanish 2017-2020 national plan for scientific research and innovation.

- State program for promotion of talent and skills
  - Programs for promotion of young researchers
  - Researcher mobility
  - Collaboration of researchers in industry, to strengthen training of researchers, targeting the preparation of a highly skilled workforce for industry.
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- State program for production of scientific and technological knowledge
  - Mainly through R&D projects
- State program for industrial leadership in R&D
  - Promoting private-public partnerships
  - Public funding of R&D projects
  - Geared toward producing disruptive knowledge and technologies
- State program for R&D targeting societal challenges
  - Multiple programs to achieve stronger impact and return on society of technological developments

Poland

In Poland cybersecurity research may be financed by various sources, both national and international.

National programmes
The National Centre for Research and Development (NCBR) - implementing agency of Minister of Science and Higher Education\(^3\), for example:

- **National Defence and Security Calls** (both open and closed) usually single-stage calls\(^4\). In each edition catalogue of eligible costs slightly differed from the previous ones.
  - call 2/P/2017 "MŁODZI NAUKOWCY 2017"
    - Applicant: research institution/ research consortium/ research-industrial centre/ entrepreneurs - project conducted by research team with young researcher as a Project Manager
    - Project manager: researchers under the age of 38 in the year of submitting project proposal
    - Duration: up to 36 months
    - Level of financing: up to 100% of the total eligible costs but project costs are part of evaluation
    - Budget
      - programme: overall (not just for cybersecurity) 100,000,000 PLN (60,000,000 PLN in 2016 and 40,000,000 PLN in 2018)
      - call: not specified
      - project: not specified
    - TRL: VI
  - call 8/2016
    - Applicant: research consortium/ research-industrial centre/ entrepreneurs
    - Project manager: not specified

\(^3\)http://www.ncbr.gov.pl/en/
3.1. MECHANISMS TO FINANCE CYBERSECURITY RESEARCH

- Duration: not specified
- Level of financing: up to 100% of the total eligible costs but own contribution and project costs are part of evaluation
- Budget: not specified
- TRL: VI

**CyberSecIdent** - CyberSecurity and e-Identity
- Applicant: research consortium
- Project manager: not specified
- Duration: up to 36 months
- Level of financing: up to 100% of the total eligible costs for research institutions, 40-80% of the total eligible costs for entrepreneurs depending on size and kind of work
- Budget
  - programme: not specified
  - call: 1st call - 70,000,000 PLN, 2nd call - 31,370,000 PLN
  - project: not less than 3,000,000 PLN of the total eligible cost and up to 20,000,000 PLN of financing
- TRL: not specified

**National Science Centre (NCN)** - government agency supervised by the Ministry of Science and Higher Education⁵ - calls mainly for researchers, mainly about basic research. Open calls:

- **PRELUDIUM 15**⁶:
  - Applicant: researchers who do not hold doctorate degrees
  - Project manager: researcher who does not hold a doctorate degree
  - Duration: 12/24/36 months
  - Level of financing: 100%
  - Budget
    - programme: not specified
    - call: 30,000,000 PLN
    - project: 70,000 PLN for projects with duration of 12 months /140,000 PLN for projects with duration of 24 months/ 210,000 PLN for projects with duration of 36 months
  - TRL: not specified

- **OPUS 15**⁷:
  - Applicant: research institutions, also consortia
  - Project manager: can indicate between 3 and 10 published research works
  - Duration: 12/24/36 months
  - Level of financing: 100%
  - Budget

⁵https://www.ncn.gov.pl/?language=en
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- programme: not specified
- call: 300,000,000 PLN
- project: not specified
- TRL: not specified

MINIATURA 2:
- Applicant: researchers with a doctoral degree obtained within the last 12 years prior to the submission of the proposal
- Project manager:
- Duration: 12 months
- Level of financing: 100%
- Budget
  - programme: not specified
  - call: 20,000,000 PLN
  - project: 5,000 - 50,000 PLN
- TRL: not specified

Grant-in-aid from national ministries (article 37 of the Act on research institute), e.g. The Ministry of Digital Affairs
- Applicant: research institute
- Project manager: not specified
- Duration: not specified
- Level of financing: 100%
- Budget: not specified
- TRL: not specified

Mixed
In that case part of the funding comes from the national resources, and part of the European funds.

Structural measures, i.e. Operational Programmes, e.g. Digital Operation
Operational Programme Digital Poland (OPDP) is funded from two sources: European Regional Development Fund, where the commitment amounts to EUR 2.2 billion, and National funds - public and private, where the minimum commitment amounts to EUR 394.4 million
- Level of financing: some projects may require beneficiary's own contribution
- Budget for priorities:
  - common access to high-speed Internet: EUR 1 020.2 million,
  - e-government and open government: EUR 949.6 million,
  - digital competences of the society, i.e. encouraging to use the Internet: EUR 145 million.

3.1. MECHANISMS TO FINANCE CYBERSECURITY RESEARCH

Belgium

Mechanisms to finance cybersecurity research may arise from different levels, due to the peculiar conformation and government system of the country.

National programmes  Belgium is an active country with regard to the increasing cybersecurity landscape. Research benefits can be, in the case of Flanders for instance, of a numerous kind. The Flemish Government in fact offers a number of incentives for research domains like cryptography, cyberintelligence, data analytics, security and forensics:

- innovation income deduction – up to 85% of a firm’s net earnings from innovation is tax exempt;
- investment deduction for R&D – 13.5% of acquisition value/qualifying asset or 20.5% of the depreciated amount;
- exemption of payment of 80% – of the personal income withholding tax of researchers in certain scientific fields10.

Regional programmes  Flemish programs Organizations establishing or managing their main business in Flanders can obtain funding opportunities depending on the source of the investment used:

- Start-up funding: acquaintances and relatives gain tax benefits if they have the intention of backing up a start-up of a close person
- SMEs loans: schemes like the so-called Win-win loan which allows for substantive tax benefits from the Flemish Government
- Bank financing: programs like Starteo, Optimeo, Impulsekrediten and GIGARANT are all aimed at helping startups with government support actions via the major banks of the country.
- Venture Capitals and Mezzanine financing: fully operational instruments, also allowed in the case of cybersecurity research.

Furthermore, the Flemish area benefits of the following funding programs

- VLAIO: Agentschap Innoveren & Ondernemen (Agency for Innovation and Enterprise) Stimulates and supports the innovation and entrepreneurial activities of Flemish companies11.
- FWO (FWO + SBO)
  - Research projects via grants for research projects, research teams can obtain additional resources to recruit scientists and technicians, to purchase equipment and to cover their operating costs
  - International mobility: The FWO promotes international mobility by giving researchers the opportunity to gain experience in international research groups, by attracting researchers from abroad

11https://www.vlaio.be/
• **International collaboration**: The FWO stimulates international collaboration via exchange agreements and (bilateral) scientific cooperations

• **SBO (Strategic Basic Research) projects (flemish companies [focus] + flemish research institutes)**: The Strategic Basic Research (SBO) programme focuses on innovative research which, if scientifically successful, will create prospects for economic or societal applications (e.g., a new generation of products, processes and/or services). The SBO programme breaks down into two finality parts: an economic programme part for projects with primarily an economic finality and a societal programme part for projects with primarily a societal finality. The available budget for the 2018 SBO call is circa €40 M*. 2/3 of this budget is reserved for projects with an economic finality and 1/3 for projects with a societal finality\(^1\).

• **Big Science Project\(^2\)**

• **The EOS-programme** wants to promote joint research between researchers in the Flemish and French-speaking community by funding joint fundamental research projects in any scientific discipline\(^3\).

• **imec ICON (flemish companies + flemish and imec research institutes)**: The imec.icon research program is a successful formula for demand-driven, cooperative research. Over a period of typically two years, multidisciplinary research teams of scientists, industry partners and/or social profit organizations work together to develop digital solutions that find their way into the market offer of the participating partners. The program has already resulted in over 100 completed projects in a wide range of ICT related application domains and markets\(^4\).

• **Flemish KU Leuven BOF (university fund) Special Research Fund (BOF)**

• **Flemish KU Leuven, CELSA\(^5\)** CELSA was founded in April 2016 by 7 old and famous universities in 4 innovative European cities: Budapest (Hungary), Leuven (Belgium), Ljubljana (Slovenia), and Prague (Czech Republic). In 2017, Tartu (Estonia) jointed the consortium, extending the alliance to the North. The Alliance aims at promoting collaboration between its members, to exchange practice at both policy and operational level, and together to find solutions for the major problems Europe is facing. The CELSA members’ mission is to educate Europe’s youngsters, to perform the best research in many scientific disciplines, and to reach out to society and economy with its talents and its state of the art research results.


\(^{15}\) [https://www.imec-int.com/icon](https://www.imec-int.com/icon)

\(^{16}\) [http://celsalliance.eu/about.html](http://celsalliance.eu/about.html)
3.1. MECHANISMS TO FINANCE CYBERSECURITY RESEARCH

Walloon + Brussels programs

- Projets du Fonds National de la Recherche Scientifique (FNRS) funds fundamental research.
- Projets d’Action de Recherche Concertée (ARC), where the university directly funds fundamental research.
- Innoviris\(^{17}\) (Brussels equivalent to VLAIO): offers support for research and development activities to companies and promotes their collaboration with academia. Companies in general, and SMEs in particular, are major stakeholders in the Brussels research and innovation system. It offers:
  1. Brussels-region,
  2. inter-regional and
  3. EU aid for companies.

3.1.2. In Japan

This subsection identifies and describes the mechanisms to finance cybersecurity research in Japan.

- Ministry of Internal Affairs and Communications (MIC) is primarily responsible for R&D spending for the communication aspects of cybersecurity, including mobile networks. Historically, MIC initiated some of the joint calls with European Commission on the FP7 and H2020 programme.
  - Strategic Information and Communications R&D Promotion Programme (SCOPE) is the research funding instrument of MIC. Normally, annual open calls solicit and adopt proposals based on their quality. Proposals and projects are evaluated by the committee of experts which is usually a mix of industry professionals and academia. Some of the past joint calls with European Commission are operated by building on top of this programme.
  - National Institute of Information and Communications Technology (NICT) is the specialized agency under MIC, which operates a limited number of commissioned research in addition to conducting research within its own research centers. Some of the past joint calls with European Commission are operated under the commissioned research programme of NICT. NICT drives its own research centers and allocates most of its resources to these centers, which normally do not initiate calls for proposals.

- Ministry of Economy, Trade and Industry (METI) is primarily responsible for R&D spending for the computing aspects of cybersecurity, including industrial control systems.
  - New Energy and Industrial Technology Development Organization (NEDO) is the research funding instrument of METI. Normally, annual

---

\(^{17}\)http://www.innoviris.be/en
open calls solicit and adopt proposals based on their quality as well as the impact to the industry.

- **Information-technology Promotion Agency (IPA)** is one of the specialized agencies under METI, which operates a broad array of programmes for cybersecurity as well as information technology in general. In contrast with other research-oriented specialized agencies, the IPA can be considered to be an operating agency. In order to run its broad array of programmes, IPA closely works with other businesses and research units through open calls, some of which may have elements of research.

- **Ministry of Education, Culture, Sports, Science and Technology (MEXT)** is primarily responsible for funding universities. It initiates calls for transformation of universities, e.g., for internationalization, and for more industry-oriented training programs including cybersecurity. Some of its past funding contributed to improve cybersecurity.

- **Japan Society for the Promotion of Science (JSPS)** is one of the specialized agencies under MEXT, which operates a broad funding program for academic research. Its Grants-in-Aid for Scientific Research program (Kakenhi) are competitive funds that are intended to significantly develop all scientific research. JSPS does not operate any funding program specifically for cybersecurity.

- **Cabinet Office (CAO)** is primarily responsible for promoting inter-ministerial and inter-sectional R&D efforts through the Cross-ministerial Strategic Innovation Promotion Program (SIP). SIP is a national project for science, technology and innovation, spearheaded by the Council for Science, Technology and Innovation, in order to accomplish its role in leading science, technology and innovation beyond the framework of government ministries and traditional disciplines. The SIP has identified 10 themes that will address the most important societal problems Japan is facing, as well as contribute to the resurgence of the Japanese economy. SIP designates Cyber-Security for Critical Infrastructure as one of the 10 themes so that research organizations engage in the development of core technologies and social implementation technologies under the guidance of the Cybersecurity Promoting Committee.
### 3.1.3. Summary

The following table summarizes the previous section and shows a comparison of the financing mechanism in the European Union (on the international and national level) and Japan.

<table>
<thead>
<tr>
<th>European Union, International</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framework Programmes (now Horizon 2020) - open competitions</td>
<td>Ministry of Internal Affairs and Communications (MIC)</td>
</tr>
<tr>
<td>Special programmes such as Connecting Europe Facility (CEF) - Cybersecurity calls</td>
<td>Ministry of Economy, Trade and Industry (METI)</td>
</tr>
<tr>
<td>EUREKA</td>
<td>Cabinet Office (CAO)</td>
</tr>
</tbody>
</table>

**EUNITY project partners countries**

- national programmes
- government, state programmes
- regional programmes
- national agencies
- international, joint programming
- structural measures, i.e. Operational Programmes
- funding for research, in general to support PhD grants
- other

<table>
<thead>
<tr>
<th>Table 3.1: Comparison of the financing mechanism in the European Union and Japan</th>
</tr>
</thead>
</table>

The table shows that in the case of member states of the European Union, we have a lot of financing mechanisms that support research and innovation in the field of cybersecurity. In addition to international funding, there are also national funding mechanisms that may vary depending on the partner country. However, on the Japanese side, we have three ministries that finance research and innovation in the field of cybersecurity and the SIP program.
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

Budget

During our research, we tried to obtain information on general funds invested in cybersecurity research in different ICT areas for both regions. Unfortunately, it seems that performing such an analysis – either in Japan or EU – is a major task requiring more resources than available within EUNITY due to the number and complexity of relevant documents and expert decisions involved, such as estimating the investment share in calls where cybersecurity is only part of the topic. This task involves a review of a very large number of documents, in many cases involving rough and difficult estimations (e.g. calls where cybersecurity-related issues are a significant part – but only a part of the topic). For example, we have analysed “A guide to ICT-related activities in WP2018-20” which was designed to help potential proposers find ICT-related topics across the different parts of H2020 in work programme 2018-20. This guide shows some of the priorities that have been raised, for example, “Boosting the effectiveness of the Security Union” (where EUR 1.08 billion was planned), which includes in particular cybersecurity activities. According to the H2020 calls, it was granted over 508.5 million euros for 2018-2020 (282.5 million in 2018, 179 million in 2019 and 47 million in 2020), but, as shown in Section 3.2.2, there are many other calls that are not only concerned with cybersecurity, but are connected. At the moment, some works are in progress. When publishing the cybersecurity package (September 2017), the EC announced more activities in the field of supporting Research and Innovation in cybersecurity. The legislative proposal on Cybersecurity, Industrial, Technology and Research Competence Center will be presented in September this year. At the same time, work is in progress on a new budget, where dedicated funds for Research and Innovation in cybersecurity are also to be allocated. However, this only refers to the European Commission’s funding activity. There are also many financing mechanisms other than that of the European Commission, at both international and national level, as described in previous sections. Finally, there are some major investments that are not part of the regular mechanisms we have identified so far, especially on national and multi-national levels.

According to the “Science and Technology budget overview for 2018” by the Council for Science, Technology and Innovation (CSTI) for year 2018, the planned expenditure on cybersecurity and related fields, that are visible on the CSTI budget overview, are as follows:

- Quantum cryptography for satellite communication: 310 million JPY
- IoT security comprehensive package: 600 million JPY
- AIP: AI/BigData/IoT/Cybersecurity integration project: 8560 million JPY
- Cyberattack countermeasure testbed: 1000 million JPY

This budget overview has significant problem however:

1. Most of the big cybersecurity projects known for the authors, are not included in the overview, each of which exceeds 10 million EUR/year;
2. Details of most of the big expenditures are not available, like AIP.
Although AIP’s funding is very big (exceeding 80 million EUR), its major constituencies are AI, big data and IoT with some links to cybersecurity, thus the precise amount of cybersecurity investment cannot be derived from publicly available sources.

Further evidence can be found in the FP7 JEUPISITE D2.6, “Update of the Inventory of the STI Programmes”, which states that the Japanese STI programmes landscape is rather fragmented as 319 programmes have been identified during a scan carried out in February/March 2016.

3.2. The main research directions in the field

A top-down approach is utilized in this section. The analysis of the main research directions in the field is started on the basis of strategic documents regarding cybersecurity, and in particular, Strategic Research and Innovations Agendas, and, on a limited scope, on the basis of national cybersecurity strategies. Although we try to take into account most of the important aspects of cybersecurity, a special emphasis is given the research and innovation aspect. This analysis is provided in Section 3.2.1. Section 3.2.2 is devoted to tactical aspects of implementation of the strategies, as it contains a brief, substantive analysis of programs and project calls regarding cybersecurity. Section 3.2.3 is dedicated to more detailed, and to some extent operational, aspects of cybersecurity, as it includes a brief review of the most important and recent projects in the area of cybersecurity. Section 3.2.4 includes activities other than projects, which are important from the perspective of research and innovation. Each analysis is performed at both the EU and Japan levels. Each analysis generally focuses on the EU perspective as a whole, but in some specific areas where it was especially relevant, we also considered the perspective of the individual member states of the EU. The schematic overview of the analysis is presented in Figure 3.1

3.2.1. Strategies and Research and Innovation Agendas

This chapter provides an analysis of the "strategic" perspective, which is done on the basis of strategic documents regarding cybersecurity.

3.2.1.1. European top-level strategic documents

**Digital Single Market (DSM) Strategy**

The fundamental assumption of the DSM Strategy is to remove regulatory barriers in digital affairs in a way which enables an introduction of a Common European Digital Market. The aim of the document is to facilitate faster development of digital services, and as a result, to improve competitiveness of European companies. The scope of this strategy is broader than only cybersecurity and privacy, but discussion of these aspects is an important part of the document. The document states that only secure digital services can be effectively used by citizens. The main aspect of
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

Figure 3.1: Schematic overview of the analysis
the document regarding cybersecurity is strengthening the trust in digital services and personal data processing and increasing the security of such services and data. The strategy was published on 6 May 2015 as *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe*[^18].

**Cybersecurity strategy of the EU**

The European Commission on 7 February 2013 has published the document *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*[^19]. This strategy is historically the first strategic document in the context of cybersecurity and is related to the NIS directive. The strategy indicates five main priorities:

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

In many cases, it emphasized that many of these efforts should be supported by research and development and by closer cooperation between governments, especially within the EU. This statement can be of course easily extended to ensure cooperation between the EU and other countries, for example Japan. The Commission stressed also the importance of cooperation in the area of cybersecurity between public and private sectors. The strategy states that all threats, incidents and crimes, made in cyberspace, cannot be easily affiliated with any borders (for example a specific country) and because of that the cooperation between bodies of information and network security, CSIRTs, telecoms, and so on should be established at the national, EU and also international level.

On 13 September 2017, as a part of the so-called “Cybersecurity Package”, the European Commission has published *Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*[^20], which is in fact a revision of the Cybersecurity Strategy of the EU. In the document, a strong emphasis is put on common response of member states in case of international incidents and on cooperation between civil and military sectors. In the opinion of the Commission, cybersecurity should be based on three pillars, and in each pillar, the description of the specific actions was presented in the document:

- Building EU resilience to cyber attacks

[^18]: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192
• Strengthening the European Union Agency for Network and Information Security
• Evolving towards a Single Cybersecurity Market
• Implementing the Directive on the Security of Network and Information Systems in full
• Building resilience through rapid emergency response
• Creating a cybersecurity competence network with a European Cybersecurity Research and Competence Centre
• Building a strong EU cyber skills base
• Promoting cyber hygiene and awareness

• Creating effective EU cyber deterrence
  • Identifying malicious actors
  • Stepping up the law enforcement response
  • Encouraging public-private cooperation against cybercrime
  • Stepping up the political response
  • Building cybersecurity deterrence through the Member States’ defence capability

• Strengthening international cooperation on cybersecurity
  • Cybersecurity in external relations
  • Cybersecurity capacity building
  • EU-NATO cooperation

Another interesting strategic document in the area of cybersecurity is Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry\(^2\), which was released on 5 July 2016. It can be perceived as an update to the Strategy and is strictly connected to the NIS directive (both documents were published around the same time). This document includes declarations of actions which will be taken by the Commission to strengthen the cybersecurity in the EU. The document states that the cooperation in the area of cybersecurity is truly crucial. The announcement of an action plan in the case of international cybercrisis is also included. For the very first time, the Commission announces actions for cooperation between cybersecurity and crisis management. Very important is the fact that the document announces the creation of a Joint Research Centre to gather expert knowledge, currently dispersed among member states and union agencies. The Joint Research Centre will be supported by ENISA and CERT-EU. The document also announces the setting up of an advisory group on cybersecurity composed of experts and decision-makers from industry, academia, civil society and other relevant organisations. The group would assist the Commission in preparing new regulations. The document also states that an education platform for cybersecurity will be built up. Promotion of cooperation at the EU level between sectorial entities and evaluation

\(^2\)https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52016DC0410
of risk of cyber incidents in similar sectors is also described. One very important conclusion of this document regards the fact that improving the cybersecurity level of small and medium enterprises (SMEs) and improving competences of SMEs as well as various forms of a contractual Public Private Partnership will be supported by the Horizon 2020 programme.

3.2.1.2. Strategic Research and Innovation Agenda

The main aim of the Strategic Research and Innovation Agenda is to suggest potential topics for calls of project proposals related to cybersecurity for the H2020 Work Programme 2018-2020. Because of that, the document cannot be perceived as a substitution of the initial cPPP Strategic Research Innovation Agenda (SRIA) v1.0. The main challenges described in the various ECSO documents regarding research and innovation in cybersecurity, are the following:

- Market fragmentation;
- Innovation led by imported ICT products;
- Need to mitigate cyber security dependencies from external sources and achieve strategic supply chain in the field;
- Less funding to research and innovation available and often dispersed due to a lack of transnational approach;
- European industrial policies not yet properly addressing specific cybersecurity issues;
- Weak entrepreneurial culture and lack of venture capital;
- Human factor and skills shortage.

All of the identified challenges need very concrete actions based on the harmonization of the European approach to all aspects of cybersecurity. Moreover, such actions should be based on a high-level cybersecurity policy.

The main aims of the outcomes of the Research and Innovation Agenda can be summarized as follows:

- Protect critical infrastructures and vertical sectors from cyber threats;
- Increase European digital autonomy;
- Provide security and trust of the whole supply chain;
- Invest in areas where Europe has a clear leadership or strategic needs;
- Leverage upon the potential of SMEs;
- Increase competitiveness.

The most important guidelines agreed in the cPPP SRIA, with regard to outcomes of the EUNITY project, are the following:

---

24 Ibid. 22
25 Ibid. 22
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- Allow funding of applied research and innovation, by focusing resources on fields that could maximize European competitiveness in the cyber security market;
- Concentrate efforts on cyber security sectors strategic to Europe (and its digital sovereignty);
- Foster continuous innovation also through further research for basic technologies and components as well as look forward for possibly disruptive technologies in order to keep medium/long term competitiveness for the products and services.\textsuperscript{26}

Overall strategy for the European cybersecurity market and industry

The fact is that the European cybersecurity market share is about 24%, which is less than the contribution of Europe to Global GDP (i.e. about 26%). It could be perceived as a result of the trends indicated in the previous paragraphs. Many activities should be performed to boost cybersecurity research. For example Strategic Research and Innovation Agenda (SRIA) states: “There is an increasing need to reduce the distance with the world-wide research communities dealing with cybersecurity and privacy issues. While there are currently several coordination actions, with US and Japan it would be useful to extend all the international activities to several other countries”\textsuperscript{27}. There is also a plan to identify and carry out many activities with other countries than US and Japan.

Scope

In the following paragraph we briefly describe the main areas identified as promising in the SRIA\textsuperscript{28}. In order to implement the research and innovation strategy and to align technical with cooperation and coordination aspects, five major types of mechanisms/projects are recommended:

- **Cyber Coordination (Coordination and Support Actions):** These projects will foster cooperation (also international) for the efficient sharing of information and coordination of activities.
- **Cyber Ecosystem:** Combination of organisational and technical elements – will allow challenges to be addressed in an interdisciplinary way and will serve as a hub for research, innovation, standardisation / certification, experimentation and transfer to market activities.
- **Cyber Pilots:** These projects, mainly innovation based, are devoted to piloting solutions in specific vertical domains. These pilots or demonstrators will possibly use the transversal cyber infrastructures and the capabilities developed in the technical projects to demonstrate how the developed innovations can satisfy specific requirements in key vertical sectors, garnering attention and the commitment of users and potential procurement bodies.
- **Cyber Infrastructures:** Large (lighthouse) projects that will help to develop large infrastructures in the cyberspace, mainly spanning across several domains with a

\textsuperscript{26}Ibid. \textsuperscript{22}
\textsuperscript{27}Ibid. \textsuperscript{22}
\textsuperscript{28}Ibid. \textsuperscript{22}
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

goal to create a direct competitive advantage to industry and of strategic relevance for European countries. It includes large scale projects which could be funded through a number of different channels, including Horizon 2020 and structural funds. They are specifically designed to raise awareness of the Partnership and give it increased visibility. These large infrastructures need to have a sufficient budget (between 10 and 20 M€ overall) to provide significant results and impact.

- **Technical projects:** Small or medium scale technical projects, often R&I activities for developing new cybersecurity capabilities and components. We should ensure that these projects contribute to develop the technical competences and contribute to the KPIs of the cPPP. These projects would be based on clearly defined technical priorities.\(^{29}\)

In the SRIA\(^{30}\) seven main priority themes for intervention are outlined:

- **Ecosystem for Education, training, market growth and SME support**
  - Cyber Range and simulation
  - Education and training
  - Certification and standardisation
  - Dedicated support to SMEs

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

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

- **Remove trust barriers for data-driven applications and services**
  - Data security and privacy
  - ID and Distributed trust management (including DLT)
  - User centric security and privacy

- **Maintain a secure and trusted infrastructure in the long-term**
  - ICT infrastructure protection
  - Quantum resistant crypto

- **Intelligent approaches to eliminate security vulnerabilities in systems, services and applications**
  - Trusted supply chain for resilient systems

\(^{29}\)Ibid. 22
\(^{30}\)Ibid. 22
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- Security-and privacy by-design
- From security components to security services
- Advanced Security Services

3.2.1.3. Other ECSO WG publications

The SRIA document, described in the previous section, was published by ECSO WG6. Moreover, other working groups of ECSO also have provided very important publications in the context of cybersecurity strategy for the EU.

Education, awareness, training, cyber ranges

The very important analysis describing gaps in European cyber education and professional training can be found in the ECSO WG5 Position Paper. The document states that there is clearly a lack of qualified cybersecurity professionals and there is a need for a rise in the overall level of cyber awareness. This statement is in line with the SRIA document’s findings.

3.2.1.4. National cybersecurity strategies in the EU Member States

The analysis of the cybersecurity strategies on national level, both in the EU Member States and in Japan was done on the basis of the methodology provided in Appendix A / 5.1 (in Section 5.1.1). This section only presents the most important findings of the analysis of Member States’ cybersecurity strategies, whereas the description of national strategies is provided in Appendix A / 5.1 (in Section 5.1.2). In the next section, a brief description of the cybersecurity strategy of Japan is provided.

It is worth noting that ENISA supports EU Member States in developing, implementing and evaluating their National Cyber Security Strategies (NCSS). Currently, all Member States have developed their NCSS, but the scope of the documents, as well as their actuality, are different.

Strategic vision

Different countries in different ways define their strategic vision. Most of them put an emphasis on gaining resilience to attacks and threats from cyberspace and creating a safe environment to make use of digital economy with respect to rights and freedoms of citizens.

The main aim

The main aim is defined in various ways, but almost every strategy tries to emphasize the importance of cybersecurity. For example in France, cybersecurity is

---

31Ibid. 22
32Position Paper, Gaps in European Cyber Education and Professional Training, WG5 – Education, training, awareness, cyber ranges, March 2018
perceived from the military point of view, whereas in other countries, the civil area seems to be more important.

**Specific aims**
Specific aims of cybersecurity strategies also vary, but the most common examples of specific aims in the EU Members States are listed below:
- gaining the ability to coordinate actions at the national level, and (in some cases) European or international level,
- gaining the ability to perform cyber threats intelligence and cyber threats prevention,
- fostering research and innovation actions in the area of cybersecurity.

**Areas of interest – research and innovation context**
In most of the strategies, the importance of research & innovation and privacy activities is noticed. Some of the strategies define a need for investing in the development of industrial and technological resources for cybersecurity. However, strategies, as very high-level documents, do not provide specific information regarding planned research and innovation actions, they outline main directions of such actions. It is very important that all analysed countries have prepared documents of the strategies although their granularity varies.

The most common areas of research in the field of cybersecurity and privacy which was identified in the strategies are the following:
- Internet of Things,
- Smart Cities,
- Industry 4.0,
- Cloud Computing,
- Big Data,
- methods of attacks and ways of counteracting these attacks,
- assessment of the effectiveness of response to threats,
- cyber risk management at national level.

It is worth noting that the similar areas of research were also identified as very promising in questionnaires received during and after the first EUNITY workshop. The very similar areas were listed both by European and Japanese responders.

**Areas of interest – legal, policy and organizational perspective**
Most of the strategies state that there is a need to improve organization and coordination of cybersecurity activities at the research level as well as at the operational level. Specifically the most common identified needs are the following:
- The need for legal changes, changes in the structure of cybersecurity system.
- The need for cybersecurity risk management at national level. The need for critical infrastructure, essential services and digital services protection.
- The need for enable military actions in cyberspace.
The need to build competences in the area of cybersecurity and building awareness in the area of cybersecurity.

The need to build public-private partnerships, stimulation of research and development.

It is worth noting that detailed regulations are scattered across different legal acts, on various levels, setting the prerogatives of different agencies or regulating the operation of relevant sectors of economy (e.g. energy). The current moves to harmonize and clarify the cybersecurity field (performed both at the level of the EU and Member States), are therefore both necessary and promising.

Areas of interest – financial perspective

In most strategies, there is no specific information regarding funding. However, some point out that specific planning and executive documents will be created. A few strategies also stress the need to prepare a research programme aimed at preparation and implementation of new cybersecurity methods or even the need to create a dedicated institution, which aims at coordinating or even at directly conducting research in the area of cybersecurity and privacy.

Fulfilled objectives

The description of the objectives and the methodology of analysis are provided in the Appendix A / 5.1 (in the section 5.1.1).

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>-/✓</td>
<td>Not all of the national strategies provide the strategic vision as well as the main aims with priorities.</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>-/✓</td>
<td>A few strategies state that development and implementation of a risk management system at the national level is one of the most important actions.</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>-/✓</td>
<td>In many strategies, there is no review of the existing regulations regarding cybersecurity and privacy. In many others, only a few of the existing regulations are taken into account.</td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✓/ -</td>
<td>Improving the structure of the national cybersecurity system is one of the actions defined by most strategies.</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✓/ -</td>
<td>see above</td>
</tr>
</tbody>
</table>
## 3.2. The Main Research Directions in the Field

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>-/✓</td>
<td>Only a few of the strategies state this objective in a direct way.</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✓</td>
<td>Most of the strategies satisfy this objective in a direct or indirect way.</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✓</td>
<td>Most of the strategies state that actions will be taken to improve cybersecurity of critical infrastructure operators.</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✓</td>
<td>Many strategies indicate the need for various types of cybersecurity exercises, such as: comprehensive exercises simulating nationwide incidents, smaller-scale exercises, including sectoral ones, exercises to carry out military operations in cyberspace and also international exercises.</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td>✓</td>
<td>Most of the strategies satisfy this objective in a direct or indirect way.</td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✓</td>
<td>Most of the strategies satisfy this objective in a direct or indirect way.</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>✓</td>
<td>In most strategies, objectives in the area of raising user awareness are defined.</td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✓</td>
<td>The need for many actions toward training and education are identified in most of the strategies.</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✓</td>
<td>Most of the strategies satisfy this objective in a direct or indirect way.</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✓</td>
<td>Most of the strategies satisfy this objective in a direct or indirect way.</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td>✓</td>
<td>In many strategies, various types of cooperation are listed, such as: at the European level, in the NATO and within the United Nations.</td>
</tr>
<tr>
<td>Establish a public/private partnership</td>
<td>✓/-</td>
<td>The goal of building cooperation mechanisms between the public sector and the private sector is defined in some of the strategies.</td>
</tr>
</tbody>
</table>
Balance security with privacy and data protection  ✓/-  Most of the strategies satisfy this objective in a direct or indirect way.

Institutionalise cooperation between public agencies  ✓  In most of the strategies, the objective is met by various proposed actions.

Foster R&D  ✓  Most of the strategies satisfy this objective in a direct or indirect way.

Provide incentives for the private sector to invest in security measures  ✓/-  A few of the strategies meet this objective partially by specific actions (such as creating innovation hubs).

Table 3.2: Fulfilled objectives by National Cybersecurity Strategies in the EU member states

3.2.1.5. National strategy in Japan

Brief description
In Japan, the Basic Act on Cybersecurity was adopted in November 2014 in order to designate responsibilities and authorities to specialized agencies. The National Cybersecurity Strategy has been adopted by the cabinet in September 2015, which predicates annual update of the cybersecurity planning by the Cybersecurity Strategic Headquarter. The Government of Japan has laid out this strategy as well as the annual plan as the platform for the common understanding and actions of relevant stakeholders. Japan has specific law regulating a certain industry, where mandatory standards and guidelines, including the mandatory reporting of cybersecurity incidents, are set forth by competent ministries for the purpose of critical infrastructures protection. Its National Cybersecurity Strategy clearly identifies the scope, whose details are further documented in the Cybersecurity Policy for Critical Information Infrastructure Protection.33

<table>
<thead>
<tr>
<th>Owner (responsible entity)</th>
<th>Government of Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publication</td>
<td>Government</td>
</tr>
<tr>
<td>Date of publication</td>
<td>4 September 2015</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cybersecurity Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>Japanese &amp; English 35</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
<tr>
<td>Scope (geographical or sectoral)</td>
<td>Japan</td>
</tr>
</tbody>
</table>

33 EUNITY Grant Agreement, Annex 1 Description of the action
#### 3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

<table>
<thead>
<tr>
<th>Scope (on the basis of merit)</th>
<th>All aspects related to cybersecurity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of stakeholders</td>
<td>All</td>
</tr>
</tbody>
</table>

**Table 3.3: Basic information about the National Cybersecurity Strategy in Japan**

**Previous strategies and related documents**

Previous strategies were published by the Information Security Policy Council, which has been transformed into the Cybersecurity Strategic Headquarters of the Cabinet in accordance with the Basic Act of Cybersecurity in 2015. Since 2015, the Cybersecurity Strategy has been augmented by the annual update issued by the headquarters. They are available as Cybersecurity 2015, 2016 and 2017, respectively.

National R&D strategy was initially adopted in July 2011 by the Information Security Policy Council, based on the recommendation of the 4th Science and Technology Basic Plan. The R&D strategy was subsequently revised in July 2014. The strategy reflected R&D activities of competent ministries and specialized agencies.

The latest R&D strategy was published by the Cybersecurity Strategic Headquarters as the “Cyberspace Research and Development Strategy” in July 2017. The strategy can be summarized by the following 7 points:

1. Consideration of business process in the cybersecurity R&D
2. Security consideration across the life-cycle of products and services
3. Holistic approach, including technology, legislation, psychology and management
4. Integration of cyberspace and physical space through IoT
5. Use of artificial intelligence and big data
6. Public-private partnership and the industry-academic collaboration
7. Facilitation of cybersecurity R&D through legal measures

**Strategic vision**

As Japan strives to become the world’s highest level IT-based society, reinforcing cybersecurity will be imperative not only for national security and crisis management, but also for bolstering Japan’s industrial competitiveness through the use of IT and data.

**The main aim**

The Cybersecurity Strategy identifies the following objective:

Ensure a free, fair, and secure cyberspace; and subsequently contribute to improving socio-economic vitality and sustainable development, building a society

---

[34]https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf

www.eunity-project.eu 67 July 31, 2018
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

where the people can live safe and secure lives, and ensuring peace and stability of the international community and national security.

Japan affirms the following basic principles in policy planning and implementation for reaching the objective: assurance of the free flow of information, the rule of law, openness, autonomy, and collaboration among multiple stakeholders.

Specific aims
The Cybersecurity Strategy outlines four detailed aims:
1. Improvement of Socio-Economic Vitality and Sustainable Development
2. Building a Safe and Secure Society for the People
3. Ensuring Peace and Stability of the International Community and National Security
4. Cross-Cutting Approaches to Cybersecurity

Areas of interest - research and innovation context
The strategy envisages the cyber-physical space in addition to cyberspace as follows: All kinds of physical objects and people have been interconnected by ICTs in a more multidimensional way, and the integration of physical space and cyberspace has become more intertwined. Attention should be paid to the fact that any event in cyberspace may affect society as a whole, producing a synergy effect with various events including those in physical space. Recognizing the transformational process leading to the unprecedented interconnected and converged information society, Japan will implement policies by precisely capturing such social transformation.

The 5th Science and Technology Basic Plan (adopted by the Cabinet on January 22, 2016) incorporated this recognition and coined the term Society 5.0, where smart energy, transport, manufacturing, services will be orchestrated in near future with smart management services such as HR, accounting, and legal services, as well as smart workforce such as the on-demand workforce and innovation, eventually leading to creation of new values. The plan specifically recognizes cybersecurity as the key enabler toward value creation and international competitiveness.

Areas of interest - legal, policy and organizational perspective
The legal basis of cybersecurity can be found in the Article 22 of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, which was enacted in December 2000. The Article 22 specifically requires that “Strategies developed to form an advanced information and telecommunications network society shall ensure that action is taken to achieve and maintain security and reliability of advanced information and telecommunications networks, to protect personal information and other actions necessary to enable citizens to use such networks without anxiety”, upon which basic principles for cybersecurity were later stipulated in the Basic Act on Cybersecurity. Diverse programs have been imple-
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

As cybersecurity measures are implemented by the balancing act of “freedom of expression” and “secrecy of communication”, the case of Japan can be an interesting example, as its Constitution mandates the secrecy of any means of communication in the Article 21 and further elaborated in the Radio Act, Wire Telecommunications Act, and Telecommunications Business Act.

It is worth noting that laws in Japan define minimum requirements, upon which associated guidelines are defined and published, in order to promote voluntary programs by both public and private entities. As cybersecurity measures effectively require public-private cooperation, the guideline-based approach of Japan can be useful in other countries.

NISC, directly attached to the cabinet secretariat, oversees and coordinates cybersecurity policy of all ministries. It also serves as the headquarter of cybersecurity policy, thus promoting integrated and strategic cybersecurity policy. Historically, NISC was founded in April 2005 as the National Information Security Center, subsequently renamed as the National center of Incident readiness and Strategy for Cybersecurity after the Basic Act on Cybersecurity was enacted. The Act assigns authority to NISC, enabling it to audit and give recommendations to government agencies.

NISC also promotes international cooperation. International Strategy on Cybersecurity Cooperation, which was published in 2013 by the Information Security Policy Council, outlines basic policies for international cooperation as well as priority areas. The document also puts focus on regional cooperation with ASEAN, as well as cooperation with EU, US and multilateral frameworks.

NISC has also been promoting public-private partnership. For instance, the Cybersecurity Policy for Critical Information Infrastructure Protection outlines information sharing to/from NISC through the CEPTOAR council (CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response), which exist for 13 critical infrastructure sectors.

Areas of interest - financial perspective

The Japanese government’s cybersecurity spending for 2018 was approximately 62 billion yen, which translates to roughly 485 million euros. The expenditure includes cybersecurity measures, basic R&D, and training programs. Current priorities on the budget are 1) IoT security, 2) critical infrastructure protection and the protection of government agencies, 3) investment onto national R&D agencies, 4) capacity building and R&D, and 5) investments toward the Tokyo 2020 Olympic and Paralympic games. As the cybersecurity investments are closely linked with the IT investments, coordinations among them are considered important.

As cybersecurity measures cannot be implemented by the government alone, it is considered important to promote private investments and engagements. In order
to promote cybersecurity activities across the private sector, a variety of measures are put in place, including issuance of guidelines and budget allocations.

According to the JNSA 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. It is anticipated to exceed 1 trillion yen in 2018.

**Fulfilled objectives**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✔</td>
<td>Basic Act on Cybersecurity</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✔</td>
<td>Review the cybersecurity strategy every three years.</td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✔</td>
<td>Basic Act on Cybersecurity assigns responsibilities to specialized agencies.</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✔</td>
<td>Basic Act on Cybersecurity, Article 4 to 9</td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>✔</td>
<td>Sector-specific information-sharing mechanisms, as well as cross-sector information sharing mechanisms exist.</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✔</td>
<td>Cybersecurity Strategy, the Cybersecurity Policy for Critical Infrastructure Protection (4th Edition) etc.</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✔</td>
<td>13 critical infrastructure sectors have been identified and are closely monitored and assisted by NISC.</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✔</td>
<td>Sector-specific exercises and cross-sector exercises are conducted on a regular basis.</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td>✔</td>
<td>Public sector adopts the common security criteria for the government. Private sectors adopt their own baseline security requirements with assistance and oversight of competent ministries.</td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✔</td>
<td>Basic Act on Cybersecurity</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>✔</td>
<td>Awareness programme has been organized by NISC and IPA.</td>
</tr>
</tbody>
</table>
### 3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✓</td>
<td>Educational programmes are managed by MEXT. Training programs for both private and public sectors are managed by specialized agencies.</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✓</td>
<td>GSOC (Government Security Operation Coordination Team), JPCERT/CC, and private-sector CSIRTs</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✓</td>
<td>National Policy Agency works with specialized agencies, private sector entities as well as the Japan Cybercrime Control Center to address cyber crime.</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td>✓</td>
<td>Agencies actively promote international cooperation, as documented in the International Strategy on Cybersecurity Cooperation.</td>
</tr>
<tr>
<td>Establish a public/private partnership</td>
<td>-</td>
<td>Keidanren (Japan Business Federation) engages in cybersecurity dialogue with the government.</td>
</tr>
<tr>
<td>Balance security with privacy and data protection</td>
<td>✓</td>
<td>The Act on Personal Information and the Basic Act on Cybersecurity outlines the basic framework. Guidelines by competent ministries augment the framework as necessary, which can be used to maintain the balance.</td>
</tr>
<tr>
<td>Institutionalise cooperation between public agencies</td>
<td>✓</td>
<td>Basic Act on Cybersecurity</td>
</tr>
<tr>
<td>Foster R&amp;D</td>
<td>✓</td>
<td>The 5th Science and Technology Basic Plan identifies cybersecurity as one of the four prioritized policy agenda.</td>
</tr>
<tr>
<td>Provide incentives for the private sector to invest in security measures</td>
<td>✓</td>
<td>Regulation and support from competent ministries, specialized agencies as well as NISC.</td>
</tr>
</tbody>
</table>

Table 3.4: Fulfilled objectives by Japanese National Cybersecurity Strategy

### 3.2.2. Programs and project calls

In this section, we provide an analysis of the “tactical” perspective.
3.2.2.1. European project calls

To implement the R&D and solutions to cope with the issues on cybersecurity and promote cooperation, the Horizon 2020 is the latest initiative of EU Research and Innovation programme with nearly 80 billion euros of funding available over 7 years (2014 to 2020) - in addition to the private investment that this money will attract. In the Horizon 2020 2014-2015 ICT Work Programme and 2016-2017 ICT Work Programme, there were a lot of research sectors which were prioritized to push the research and innovation. Those priorities are also present in the ICT Work Programme for 2018-2020. Some of them directly involve cybersecurity and some of them include the cybersecurity aspect in an indirect way. A brief summary of those calls is presented in the next paragraphs.

Information and Communication Technologies (ICT)

Cybersecurity can appear in almost every sub-item of ICT. Here we mention some of them. In the Horizon 2020 2014-2015 ICT Work Programme there were for example:

- ICT 32-2014: Cyber-security, Trustworthy ICT
- ICT 38-2015: International partnership building and support to dialogues with high income countries

In the Horizon 2020 2016-2017 ICT Work Programme there were for example:

- ICT-05-2017: Customised and low energy computing
- ICT-06-2016: Cloud Computing
- ICT-14-2016-2017: Big Data PPP: cross-sectorial and cross-lingual data integration and experimentation
- ICT-35-2016: Enabling responsible ICT-related research and innovation

In the Horizon 2020 2018-2020 ICT Work Programme there were three calls connected with cybersecurity: Information and Communication Technologies, Digitising and transforming European industry and services: digital innovation hubs and platform and Cybersecurity. The example of topics in that calls are:

- ICT-08-2019: Security and resilience for collaborative manufacturing environments (Joint with FoF)
- ICT-10-2019-2020: Robotics Core Technology
- ICT-11-2018-2019: HPC and Big Data enabled Large-scale Test-beds and Applications
- ICT-28-2018: Future Hyper-connected Sociality
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

Digitising and transforming European industry and services: digital innovation hubs and platform
- DT-ICT-01-2019: Smart Anything Everywhere
- DT-ICT-06-2018: Coordination and Support Activities for Digital Innovation Hub network
- DT-ICT-08-2019: Agricultural digital integration platforms

Cybersecurity
- SU-ICT-01-2018: Dynamic countering of cyber-attacks
- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems
- SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap
- SU-ICT-04-2019: Quantum Key Distribution testbed

Only some calls are listed above. There are many others that deal with the cybersecurity aspect, but this is not their main goal.

Joint Collaborations
Several of the Joint calls in International Collaboration are also interested in cybersecurity, such as
- EUB1-2015: Cloud Computing, including security aspects
- EUB2-2015: High Performance Computing (HPC), the priorities focus on the security aspects of all applications of HPC on societal challenges and in areas such as transport, energy, environment, climate, health, etc.
- EUB3-2015: Experimental Platforms, deals with the security related to the current tools and platforms in support of end-to-end experimentation.
- EUB-01-2017: Cloud Computing
- EUB-02-2017: IoT Pilots
- EUB-03-2017: 5G Networks

The other noticeable joint collaborations, namely “EU-Japan Research and Development Cooperation in Net Futures”, identified by H2020-EUJ-2014, also mention many cybersecurity issues. The 4 following topics consider security issues as top priorities:
- EUJ1-2014: Technologies combining big data, internet of things in the cloud, creates new challenges, especially for services and data hosted and executed across borders
- EUJ2-2014: Optical communications, cybersecurity should also be addressed and go side by side with the evolution of the network traffic speed and growth to enable the identification of potential threats
- EUJ3-2014: Access networks for densely located users, since those networks should be appropriately secured in order for the citizens to be able to access the provided services
EUJ4-2014: Experimentation and development on federated Japan-EU testbeds, the proposals should also investigate the related interoperability, privacy and security issues.

There is also one topic in which cybersecurity is a key issue in the Horizon 2020 2016-2017 ICT Work Programme under the “EU-South Korea Joint Call” and one in the Horizon 2020 2018-2020 ICT Work Programme under the “EU-Japan Joint Call”

- EUK-01-2016: 5G - Next Generation Communication Networks
- EUJ-01-2018: Advanced technologies (Security/Cloud/IoT/BigData) for a hyper-connected society in the context of Smart City

**Innovation In SMEs (INNOSUP)**

In the topic of “INNOSUP6-2015: Capitalising the full potential of online-collaboration for SME innovation support”, there are obviously security issues for online applications and services.

- INSO-9-2015: Innovative mobile e-government applications by SMEs
- INSO-10-2015: SME business model innovation
- SMEInst-01-2016-2017: Open Disruptive Innovation Scheme
- SMEInst-13-2016-2017: Engaging SMEs in security research and development
- SC1-PM-18-2016: Big Data supporting Public Health policies

**Secure Societies - Protecting Freedom And Security Of Europe And Its Citizens (DRS)**

There are a few calls where cybersecurity is addressed: Disaster-resilience: safeguarding and securing society, including adapting to climate change (DRS), Fight against crime and Terrorism (FCT), Digital Security: Cybersecurity, Privacy and Trust (DS). The cybersecurity issues are directly addressed within this call:

- FCT-1-2015: Forensics topic 1: Tools and infrastructure for the extraction, fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation
- FCT-3-2015: Forensics topic 3: Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials
- DRS-17-2014/2015: Critical infrastructure protection topic 7: SME instrument topic: “Protection of urban soft targets and urban critical infrastructures”

There are also many digital security topics that deal with cybersecurity and privacy (under the Secure Society priority) and we include them in the section below.

- Work Programme 2014-2015
  - DS-1-2014: Privacy
  - DS-2-2014: Access Control
  - DS-3-2015: The role of ICT in Critical Infrastructure Protection
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

- DS-4-2015: Information driven Cyber-security Management
- DS-5-2015: Trust e-Services
- DS-6-2014: Risk management and assurance models
- DS-7-2015: Value-sensitive technological innovation in Cybersecurity

**Work Programme 2016-2017**
- DS-02-2016: Cyber Security for SMEs, local public administration and Individuals
- DS-03-2016: Increasing digital security of health related data on a systemic level
- DS-04-2016: Economics of Cybersecurity
- DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation
- DS-06-2017: Cybersecurity PPP – Cryptography
- DS-08-2017: Cybersecurity PPP – Privacy, Data Protection, Digital Identities

Under the Work Programme 2016-2017 the “CRITICAL INFRASTRUCTURE PROTECTION H2020-CIP-2016-2017” focuses on critical infrastructure protection. There are several topics:
- CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

Under the Work Programme 2018-2020 the “Secure societies – Protecting freedom and security of Europe and its citizens” focuses on protecting the infrastructure of Europe and the people in the European smart cities, disaster-resilient societies, fight against crime and terrorism, border and external security and digital security. The specific topics for that priority are:
- SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
- SU-INFRA02-2019: Security for smart and safe cities, including for public spaces
- SU-FCT02-2018-2019-2020: Technologies to enhance the fight against crime and terrorism
- SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism
- SU-BES02-2018-2019-2020: Technologies to enhance border and external security
- SU-BES03-2018-2019-2020: Demonstration of applied solutions to enhance border and external security
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- SU-DS01-2018: Cybersecurity preparedness – cyber range, simulation and economics
- SU-DS02-2020: Management of cyber-attacks and other risks
- SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors

Under the Work Programme 2018-2020 the “Trusted digital solutions and Cybersecurity in Health and Care” focus area on “Boosting the effectiveness of the Security Union” had two topics connected with cybersecurity:

- SU-TDS-02-2018: Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures
- SU-TDS-03-2018: Raising awareness and developing training schemes on cybersecurity in hospitals

Inclusion of cybersecurity aspects is now required in many calls from various fields (not directly related to cybersecurity in itself), as for example:

- Future And Emerging Technologies (FET) - Cyber-security as an application field needs a lot of enabling technologies. The Future and Emerging Technologies (FET) programme has three complementary lines of action to address different methodologies and scales, from new ideas to long-term challenges. These are FET Open, FET Proactive and FET Flagships.
- European Research Infrastructures, Including E-Infrastructures (EINFRA) - cybersecurity is directly addressed in e-infrastructures.
- Societal Challenges - Secure, Clean And Efficient Energy (LCE)
- Smart, Green And Integrated Transport (MG)
- Marie Skłodowska-Curie actions (Individual Fellowships (IF): support for experienced researchers undertaking mobility between countries, optionally to the non-academic sector; Research networks (ITN): support for Innovative Training Networks)
- Climate Action, Environment, Resource Efficiency And Raw Materials (SC)

Brief summary
It is worth noting that there is an increase in the total number of calls in the area of cybersecurity. Cybersecurity does not only occur in project calls devoted to this issue but also in project calls from other areas in which cybersecurity is an important element. Inclusion of cybersecurity aspects is now required in many calls from various fields.
3.2.2.2. Examples of national project calls

**National Defence and Security Calls (Poland)** which regards national security and defence (in very wide scope – from weapons and other military applications to cybersecurity of critical infrastructure). Solutions in the area of cyber defence shall develop abilities of the Armed Forces of the Republic of Poland to provide cybersecurity of ICT and communication systems of the Ministry of National Defence and their ability to operate in cyberspace. These solutions may also be useful in systems connected with the security of critical infrastructures of the Republic of Poland, the crisis management systems and ICT systems used in Police, Border Guards, State Fire Service.

**CyberSecIdent (Poland)** – Cyber Security and e-Identity
The main goal of the CyberSecIdent programme is to increase security level of cyberspace of the Republic of Poland through the improvement of accessibility of software and hardware tools till 2023. The specific goal is to implement technological solutions to facilitate cooperation and coordination of activities in the area of security of cyberspace with special regard to e-Identity. The other specific goal is to implement methods and techniques of identification and authentication.

**NCN (Poland)** calls support basic research in Poland. Examples of calls:
- **PRELUDIUM** is a funding opportunity intended for pre-doctoral researchers about to embark on their scientific career
- **OPUS** is a funding opportunity intended for a wide range of applicants. The research proposal submitted under this scheme may include the purchase or construction of research equipment
- **MINIATURA** is a scheme offering funding for single activities that serve as part of larger basic research

**Grant-in-aid (Poland)** from national ministries (article 37 of the Act on research institute) – research institutes may be assigned tasks by their supervisory ministry

**Operational Programme Digital Poland** focuses on Internet access, e-government and general digital competence of the society

3.2.3. Projects
In this chapter there is an analysis of the “operational” perspective provided.
3.2.3.1. National and international roadmapping projects

The European Commission has led many coordination and roadmapping projects. The following ones have been identified as relevant and will bring their inputs to EUNITY. These projects are included in this section but it should be noted that they have very serious strategic meaning – to some extent they create a strategic plan for future activities in the area of cybersecurity and privacy (also in the research and innovation field). The most important projects in this context are the following:

- **CyberROAD, CAMINO, COuRAGE**
  Creating a research roadmap for a topic as dynamically changing as cybersecurity requires great predictive ability. This difficulty was recognized by the European Commission through decision to fund not one, but three separate CSA-type (Coordination and Support Action) projects in the FP7 call SEC-2013.2.5-1 - Developing a Cyber crime and cyber terrorism research agenda. The projects tasked with creating the roadmap were (a) CyberROAD – Development of the CYBER crime and CYBER terrorism research ROADmap (project no. 607642), (b) CAMINO – Comprehensive Approach to cyber roadMap coordInation and development (project no. 607406) and (c) COuRAGE – Cybercrime and cyber-errOrism (E)uropean Research AGEnda (project no. 607949). The three projects took different approaches to the development of the research agenda, from the information collection phase to the form of the final results. CyberROAD provides an interactive roadmap on its website, CAMINO summarizes its conclusions in a book while COuRAGE delivers a set of reports, concluding the work with the COuRAGE Brief. However, while the approaches were very different, the crucial results – the identification and prioritization of research topics – produced by all three projects were similar, giving the hope that the common findings of separate teams of experts in the field will likely be reliable predictions. The results of the three projects were compared and discussed during the joint conference on “Emerging and Current Challenges in Cybercrime and Cyberterrorism”, which took place in The Hague, Netherlands, in March 2016, and in a collective book, published by Springer. The results of the projects are likely to influence the future European research agenda in the field of cybersecurity.

It is worth noting that CyberROAD project priorities focus on the identification of cybercrime and cyberterrorism threats and the constitution of a strategic roadmap to handle them. The key directions that CyberROAD follows are built around the technological, societal, legal, ethical, and political aspects of cybercrime and cyber-terrorism.

- **SECCORD**
  Project SECCORD (Security and Trust Coordination and Enhanced Collaboration) was providing coordination and services for the Trust and Security (T&S)
research programme and its projects. One of the goals of the project is to map research results of FP7 security research projects to the ongoing ICT security industry (supply-side) priorities and offerings, market trends and demand-side needs and user priorities. One of the main objectives was to reduce the gap in the alignment of research to demand-side needs, besides supply-side priorities (often expressed in industrial research agendas) or market trends (found in different market analyst reports, hype curves, emerging technology radars etc).  

- **INCO-Trust and BIC**
  INCO-Trust and BIC (Building International Cooperation for Trustworthy ICT) were two coordination and support actions targeting expansion of co-operation between EU researchers and programme management with their peers in non-EU countries. While INCO-Trust focus was on highly developed countries, including Japan, BIC focus was more on ICT high-growth countries, specifically Brazil, India and South Africa, who represent emergent world-impacting information economies through the scale and sophistication of their growing ICT sectors.

- **CIRRUS**
  (Certification, Internationalisation and standardization in cloud Security) was bringing together representatives of industry organizations, law enforcement agencies, cloud services providers, standard and certification services organizations, cloud consumers, auditors, data protection authorities, policy makers, software component industry etc. with strong interests in security and privacy issues in cloud computing.

- **CAPITAL**
  (Cybersecurity research Agenda for Privacy and Technology challenges) was another CSA project that delivered Cybersecurity Research Agenda which provided 34 research clusters, defined areas of research critical for a EU Cybersecurity Strategy, and performed a rating of research clusters regarding impact, expected maturity and timeline.

- **SYSSEC**
  The SysSec Network of Excellence has produced the “Red Book of Cybersecurity” to serve as a Roadmap in the area of Systems Security. SysSec Red Book was realized by putting together a “Task Force” of top-level young researchers in the area steered by the advice of SysSec Work Package Leaders. The Task Force had vibrant consultations (i) with the Working Groups of SysSec, (ii) with the Associated members of SysSec, and (iii) with the broader Systems Security Community. Their feedback was captured in an on-line questionnaire and in forward-looking “what if” questions. The Task Force was then able to distill their knowledge, their concerns, and their vision for the future. The result of this consultation has been captured in the so-called Red Book which serves as a Road Map of Systems Secu-

---

38 Ibid. 33
39 Ibid. 33
40 Ibid. 33
41 Ibid. 33
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

The Red Book intended to initiate a more proactive approach in the way we stand towards cyber attacks and lead to the prediction of the threats and vulnerabilities rather than try to tackle the security issues after an attack. Towards this direction, SysSec targeted the advance of cyber defense by joining hands with Industry and Policy Makers while taking into consideration FORWARD initiative results. The main goals included the constitution of a European Network of Excellence that centralized the Systems Security research; the support of cybersecurity education; the introduction of a think tank to explore current threats and vulnerabilities and the initiation of an effective research direction in cybersecurity. Finally SysSec proposed to establish a collaborative working plan to promote synergetic research. Towards these directions, SysSec organized several workshops and summer schools, provided student scholarships, covering living and travelling expenses for visiting organizations in the SysSec Network of Excellence (including FORTH-ICS (GR), Vrije Universiteit Amsterdam (NL), Institut Eurecom (FR), IPP - Bulgarian Academy of Sciences (BG), TU Vienna (AT), Chalmers University (SE) and Politecnico di Milano (IT)), and created several courses covering Computer Security, Cryptography, Language-based Security, Network Security, Secure Programming, Algorithms and Architectures for Cryptographic Systems, Privacy and Security Engineering.

- FORWARD
  The main goal of the FORWARD project was to identify future attacks that threaten the security of the ICT infrastructure of Europe. It is clear that ICT infrastructures are no longer independent of societies and the economy, but they have evolved into the enabling and carrying platform that facilitates communication, production,

---

42Ibid. 33
trade, and transportation. Thus, attacks against ICT infrastructures have significant, adverse impact on the well-being of Europe and its people, and it is clear that adequate protection must be provided. By identifying future problems, Europe can take an active approach in defending against anticipated threats. In particular, one can prepare by setting a research agenda that provides solutions before threats become unmanageable. Main target of the project is to collaborate with international experts from academia and industry (both from Europe and the rest of the world) to identify future threats, and find those that are most pressing and that require the most immediate attention.43

Figure 3.3: The FORWARD blog

FORWARD main goals included the identification, networking and coordination of the research efforts in Academia and Industry in order to establish secure and trusted ICT systems and infrastructures. Towards this direction, three working groups discussing the best practices, progress and priorities in cybersecurity, were established: Smart Environments (WG-SE)44, Malware & Fraud (WG-MF)45, and Critical Systems (WG-CS)46. FORWARD created an online framework hosting the latest threat detection and prevention mechanisms. Additionally, industry, academia and policy makers organized workshops to explain the emerging threat landscape. The results of the project are presented in the FORWARD Whitebook47.

CONNECT2SEA

In the framework of the CONNECT2SEA project, a report was compiled on common priorities to promote cooperation regarding cybersecurity between Europe and ASEAN countries. The sources used to compile this report are, on the European side, the H2020 work programmes on cybersecurity, Information and Communications Technology (ICT), and data information that has been provided

43Ibid. 33
44http://www.ictforward.eu/wg/smartenvironments/
45http://www.ict-forward.eu/wg/malware-fraud/
46http://www.ict-forward.eu/wg/critical-systems/
47Available at: http://www.ict-forward.eu/media/publications/forward-whitebook.pdf
by CONNECT2SEA partners from ASEAN countries. The report determined the
top 12 R&D issues which are of the highest interest in ASEAN countries, includ-
ing new advanced R&D trends, such as Cloud Computing, Big Data, Internet of
Things, Cryptography, e-Services. The report also presented the results from the
two (2) Cybersecurity related workshops that were organized to gain feedback
from experts in the area, in particular regarding weaknesses in networking and
community cooperation to cope with cybersecurity in ASEAN.\textsuperscript{48}

Figure 3.4: CONNECT2SEA website

CONNECT2SEA as a follow up project to the SEACOOP, in a 30-months period,
established a strategic synergy between European Union and South East Asia
in the Information and Communication Technologies (ICT) research. Among
the achievements of the project, the transfer of knowledge and the policy dia-
ologue, between the two regions, were set at a high priority. CONNECT2SEA's
goals included the advancement of ICT R&D&I partnership, through the inter-
nationalization of EU and SEA research and innovation networks and frame-
works, the promotion of Horizon 2020 and cooperative research programmes
between EU and ASEAN, and the augmentation of EU-SEA ICT R&D policy di-
ologue. These goals have been accomplished through conferences\textsuperscript{49}, grants \textsuperscript{50},

\textsuperscript{48} ibid. 33
\textsuperscript{49} http://www.connect2sea.eu/news-and-events/news/details/Towards-new-avenues-in-EU-
ASEAN-ICT-collaboration-Highlights-and-presentations.html
\textsuperscript{50} http://www.connect2sea.eu/news-and-events/news/details/Newton-Institutional-inks-Grants-to-
Develop-Research-and-Innovation-Collaborations.html
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

funding fellowships\textsuperscript{51} \textsuperscript{52} \textsuperscript{53} \textsuperscript{54} and meetings focused on cybersecurity.\textsuperscript{55} \textsuperscript{56} The main outcomes of the project were the establishment of a common agenda and strategic cooperation between Europe and SEA countries, and the formulation of a knowledge network between the two regions.

- **ECRYPT-CSA**
  
  This CSA brings together the European cryptography community, involving academia, industry, government stakeholders and defence agencies. The project is coordinating ongoing research, develops a joint research agenda and foresight study, and identifies technology gaps and market and innovation opportunities and coordinate and strengthen standardization efforts; it also addresses governance of cryptographic standards at a European level. The project tackles through advanced training initiatives the skill shortage of academia and industry. The project intends to bridge the gap between academic research on the one hand and standards and industry innovations on the other hand, hereby strengthening the European industrial landscape in a strategic area. The project results in the availability of more trustworthy security and privacy solutions “made in Europe”, resulting in an increased user trust in ICT and online services and empowerment of users to take control over their data and trust relations. The work also results in more resilient critical infrastructures and services. The project intends to reach out beyond its constituency to the broader public and to policy makers.\textsuperscript{57}

3.2.3.2. European (Horizon 2020) projects in the area of cybersecurity

This section lists the most important recent European projects in the area of cybersecurity and privacy. This list is not intended to be comprehensive, but it aims at undertaking a review by providing the most reliable examples of Horizon 2020 projects:

- **Secure Hardware-Software Architectures for Robust Computing Systems (SHARCS)**
  
  SHARCS proposes a proactive response to cybersecurity instead of tackling cyberattacks afterwards. There have been an increasing number of cyberthreats in the past few years that need cooperation and anticipation. SHARCS intends

\textsuperscript{57}Ibid. 33
to constitute a platform that will be used to design, implement and demonstrate secure-by-design applications and services by analyzing the layers of hardware & software of a computing system and quantify the performance in real world applications. The application covers diverse domains including medical, cloud and automotive.

- **UNFRAUD**
  UNFRAUD is an advanced, online, anti-fraud, reliable software platform\(^{58}\) that detects fraudulent methods via deep learning neural networks.

- **CANVAS**
  Canvas consortium intends to build a community that will unify the distributed efforts by technology developers, legal/philosophical scholars and empirical researchers in the field of cybersecurity. The main goals of CANVAS focus on structuring the current knowledge coming from these different perspectives, designing a network of information dissemination across these different domains.

- **DISCOVERY**
  DISCOVERY intends to promote the dialogue and cooperation between Europe and North America (US and Canada) with regard to funding mechanisms, ICT policy and cybersecurity.

- **AEGIS**
  AEGIS (Accelerating EU-US Dialogue for Research and Innovation in Cybersecurity and Privacy) aims to strengthen international dialogues on cybersecurity and privacy in order to facilitate the exchange of viewpoints, policies and best practices to accelerate EU-US cooperation in cybersecurity and privacy research and innovation.

- **SAINT**
  SAINT plans to fight the cybercrime by analyzing the ecosystem of cybercriminal activity and revealing evidence on privacy issues and Deep Web practices. Additionally, SAINT plans to build a framework in order to advance the measurement techniques of metrics of cybercrime by adding innovative models and algorithms.

- **REDSENTRY**
  redSentry plans to build a real-time networking monitoring framework that will detect and manage any type of cyber threat faced by the financial services sector. The network monitoring of cyber threats will allow the financial sector to manage their responses automatically and proactively.

- **Cybersecurity Behavioral Toolkit (CLTRe)**
  The Cybersecurity Behavioral Toolkit - CLTRe intends to measure and correct the security level of an organization by checking the behavior of its employees. CLTRe will store these actions and will generate a trend analysis that will give insight into the behavioral change over time.

- **3ants**

\(^{58}\)http://www.unfraud.com/en
3.2. THE MAIN RESEARCH DIRECTIONS IN THE FIELD

3ants intends to build a cybersecurity framework against piracy and digital distribution of counterfeited goods by utilizing machine learning techniques. The framework is following crawler pirated contents in the Internet and forces the withdrawal of the goods by applying geolocation techniques.

- **CS-AWARE**
  CS-AWARE plans to tackle the issue of cybersecurity in commercial companies, NGOs, and governmental institutions regarding information sharing. They suggest a cybersecurity awareness solution for public administrations by applying analysis of the context. This analysis will give automatic incident detection and visualization and will promote exchange of information with EU level NIS authorities (CERTs).

- **CYBECO**
  CYBECO proposes to develop a framework for cyberinsurance, by combining multidisciplinary methods from Behavioural Economics, Statistics, Game and Decision Theory and build new models that will be coupled within a prototype software architecture (CYBECO Toolbox 2.0).

- **STORM**
  Storm is a Cyber Risk Management system which serves evidence based on metrics that can describe the cyber risk in real time, regarding business asset level. They leverage an efficient risk model, that enhances user experience and replies to queries like:
  - How much cyber risk do we have?
  - What should my customer pay for cyber insurance?
  Storm promotes collaboration on cyber risk management, by information sharing, advancement of analysis software, and interaction with current user involvement.

- **cyberwatching.eu**
  cyberwatching.eu intents to instrument and maintain an EU Observatory that will watch R&I initiatives on cybersecurity and privacy. Their main outputs include: the implementation of an online catalogue of services regarding cybersecurity and privacy, a cluster tool, webinars, annual workshops, concertation meetings, regional SME workshops, cluster reports, white papers, roadmaps and sustainability through cybersecurity and privacy marketplace.

- **Protection Beyond Operating System (ProBOS)**
  Protection Beyond Operating System (ProBOS) proposes a next generation cybersecurity protection system, by applying Artificial Intelligence approaches, that will offer a high level of protection to governments and private organizations.

- **Traditional Organised Crime and the Internet: The changing organization of illegal gambling networks (OCGN)**
  OCGN plans to examine online gambling and extortion networks and organized crime that is attracted around these. They aim to develop and validate tools and methods to simplify the management of cyberthreats in online
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

gambling; define standards of information management and dissemination of information to cybersecurity centres from online gambling sector in EU.

- **reliAble euRopean Identity EcoSystem (ARIES)**
  reliAble euRopean Identity EcoSystem (ARIES) intends to build a schema for reliable secure and privacy-respecting physical and virtual identity management by utilizing new technologies offering highest level of quality in eID. Their goal is to use virtual and mobile IDs cryptographically derived from eID documents that will not allow any identity theft by utilizing biometric features as well.

- **SISSDEN**
  Based on the experience of Shadowserver, known in the security community for achievements in the fight against botnets and malware and close cooperation with Law Enforcement Agencies, network owners and national CSIRTs, SISSDEN aims to improve the cybersecurity situational awareness of EU entities through building a large network of passive sensors, providing free-of-charge victim notification feeds, and developing innovative data collection and analysis tools, with a strong focus on effective botnet tracking.

- **CyberWiz**
  CyberWiz is determined to build a tool in order to understand cybersecurity levels across a large complex number of interconnected systems in ICT environments of critical infrastructure (energy distribution). The main goals focus on the proactive management of cybersecurity, the generation of a vulnerability "heat-map" for the configuration of the involved parts, along with a user friendly visual contrasting of diverse alternatives and a validation of the tool in two pilots (energy utilities in Sweden and Germany).

- **European Network for Cybersecurity (NeCS)**
  NeCS was structured to deal with the increasing needs for new, highly qualified researchers in the area of cybersecurity who are called to be challenged with the evolvable cyberthreats and information security vulnerabilities. The project will focus on a multi-sectorial/disciplinary approach including participants both from academic and non-academic sector.

- **Wide-Impact cyber SEcurity Risk framework (WISER)**
  WISER (Wide-Impact cyber SEcurity Risk) framework aims to build a cyber-risk management real-time framework that will estimate, oversee and mitigate cyber risks by implementing nine experiments (Early Assessment Pilots: EAPs). These experiments will be the basis to build an advanced risk management system that will be tested & validated in 3 Full Scale Pilots (FSPs).

- **LocationWise**
  LocationWise is a cloud based location verification system that intends to lower fraud costs acquired by banks. The idea is to get the user's location (through his mobile) and reduce the number of fraudulent transactions and false positives.

- **MEDIA4SEC**
MEDIA4SEC’s main intention focuses on the exploration of the challenges and ethical considerations social media use for public security. This will be done by communication and dissemination activities to make the public aware of all the cyber risks in social media like trolling, cyberbullying, threats, or live video-sharing of tactical security operations. Additionally, they plan to explore the usage of social media for public security purposes highlighting ethical, legal and data-protection-related issues.

- **Proactive Risk Management through Improved Cyber Situational Awareness (PROTECTIVE)**

PROTECTIVE is designed to improve an organisation’s ongoing awareness of the risk posed to its business by cybersecurity attacks. PROTECTIVE aims at the defense mechanisms of an organization towards incoming cyber attacks, malware outbreaks, and other security issues through two main actions: the development of the computer security incident team’s (CSIRT) threat alertness via security monitoring; and the ranking of critical alerts depending on the potential disturbance that can be caused. PROTECTIVE intends to give solutions to public domain CSIRTs and SMEs. For the evaluation process they will conduct two pilots.

- **Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP)**

C3ISP intends to create a cybersecurity, analysis and protection, management framework that will enable the collaborative and confidential sharing of information. The C3ISP will improve the detection of cyber threats while maintaining the confidentiality of information within a collaborative, multi-domain environment. They intend to enable the transitions from high level descriptions (close to natural language) to data usage policies which can be enforced in the system; in order to be able to work directly on encrypted data, they deal with the most applicable data protection schemes.

### 3.2.4. Other activities

This section provides examples of the “operational” (to some extent) activities, other than research and innovation projects. This section covers cybersecurity and privacy activities (undertaken in a given country among the EUNITY partners), which do not necessarily result from the national strategy, but are in some sense relevant.

In Greece, the Ministry of Digital Policy, Telecommunications and Media include in its missions the development and implementation of national policy, the contribution in the development of an appropriate institutional framework at European and international level, towards the development of high quality communication and digital politics. The ministry targets at the promotion of security in telecommunication, digital information and information media as well as the development of telecommunications’ market guidelines. The national cybersecurity strategy is
available through an online portal\textsuperscript{59}, along with updates on the implementation of the strategy. Some other resources that are currently available include information about the workshop on the role of Open Web Application Security Project (OWASP)\textsuperscript{60} \textsuperscript{61} in the protection of critical information systems and the implementation of the GDPR regulation in the public sector\textsuperscript{62}.

In Poland, the Research and Academic Computer Network - National Research Institute (NASK-PiB) has published a web portal, CyberPolicy\textsuperscript{63}. The CyberPolicy portal aims at providing knowledge about cybersecurity from the strategic, regulatory, organizational and practical perspectives. The main mission of the portal is to gather and disseminate information regarding new regulations, programmes, strategies, good practices and initiatives directly connected with the cybersecurity's ecosystem. However the portal is currently not very comprehensive and only available in Polish, but the dynamic growth of the portal is very promising.

In Belgium, The Cyber Security Coalition is a unique partnership between players from the academic world, the public authorities and the private sector to join forces in the fight against cybercrime. Currently more than 50 key players from across these 3 sectors are active members contributing to the Coalition’s mission and objectives.

In France, the OSSIR association (Information System and Network Security Observatory)\textsuperscript{64}, founded in 1996, gathers people interested in cybersecurity and fosters exchanges and scientific presentations through four regional working groups. Each year, it also organizes the JSSI (Information Systems Security Day) with conferences on a specific topic of cybersecurity. Another association, the CLUSIF (French Information Security Club)\textsuperscript{65}, gathers professionals from the information security area and aims at fostering exchanges of ideas through working groups, thematic conferences and publications, freely available on its website. As of today, the CLUSIF membership is comprised of more than 300 companies covering 15 different lines of business. Regarding cybersecurity evaluation, it is being delegated to CESTIs, which are independent IT Security Evaluation Centers. A CESTI must be authorized by the French national cybersecurity agency (ANSSI) in order to deliver certifications for specific domains, such as conformance to the Common Criteria model. Currently, a dozen companies in France have been authorized as CESTIs.

\textsuperscript{59}\url{http://mindigital.gr/index.php/kyvernoasfaleia}
\textsuperscript{60}\url{http://mindigital.gr/index.php/kyvernoasfaleia/2197-o-rolos-tou-owasp-stin-prostasia-krisimon-pliroforiakon-systimaton}
\textsuperscript{61}\url{https://www.owasp.org/index.php/Main_Page}
\textsuperscript{62}\url{http://mindigital.gr/index.php/kyvernoasfaleia/2085-efarmogi-tou-kanonismoy-gdpr-ston-dimosio-tomea}
\textsuperscript{63}\url{https://cyberpolicy.nask.pl/}
\textsuperscript{64}\url{https://www.ossir.org/}
\textsuperscript{65}\url{https://clusif.fr}
3.3. The strong and weak points

This section is the first part of a summary – it provides a general overview of strong and weak points for both regions. In this section, we provide conclusions drawn on the basis of available information. This section and the next section have been prepared on the basis of a number of sources of information. First of all, the outcomes of questionnaires collected during and after the first workshop in Japan have been deeply analysed. While the number of questionnaires collected is not very large (several dozens), their significance is very high, because of the fact that they were provided by high-level experts in the area of cybersecurity. In addition, every expert represents not only one’s own point of view, but also the point of view of her institution. Secondly, the observations and experience of all partners of the consortium have been used to broaden the landscape of the problems indicated in questionnaires and add the common ones. Another very important source of information is the review of the strategies, projects and programs with regard to research and innovation in the area of cybersecurity and privacy, as well as relevant financing mechanisms, which have been provided in the previous sections of this chapter.

It is worth noting that in many aspects of research in cybersecurity and privacy, the strong and weak points are common for both regions. In case of significant differences, the most important distinctive features are provided.

This section focuses more on the organizational aspects of research in cybersecurity and privacy. The second (and the last) part of the summary (which is provided in Section 3.4) focuses on more technical aspects of the area of cybersecurity and privacy, and states the main similarities and differences of both regions.

3.3.1. Strengths

3.3.1.1. Establishment of the cybersecurity strategy

During the review of the cybersecurity strategies, we analyzed strategic documents collected at various levels (EU, national, etc.). Some of them point out the most important technical areas of research. In general, the strategic vision of cybersecurity is an advantage both in the EU and Japan.

The table lists common areas in the field of research and innovation from the perspective of strategic documents.

For more detailed comments, refer to the earlier tables: Table 3.2 (EU) and Table 3.4 (JP).

<table>
<thead>
<tr>
<th>Objective</th>
<th>the EU</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.eunity-project.eu">www.eunity-project.eu</a></td>
<td>89</td>
<td>July 31, 2018</td>
</tr>
<tr>
<td>Objective</td>
<td>the EU level</td>
<td>the member states’ level</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Establish a public/private partnership</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Balance security with privacy and data protection</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Institutionalise cooperation between public agencies</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Foster R&amp;D</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
<tr>
<td>Provide incentives for the private sector to invest in security measures</td>
<td>✓</td>
<td>✓/- ✓</td>
</tr>
</tbody>
</table>

Table 3.5: The comparison of fulfilled objectives in cyber-security strategies between the EU and Japan

In the strategic perspective, there is a high level of awareness on both sides. Small improvements are only possible at Member States’ level for the EU side.
3.3. THE STRONG AND WEAK POINTS

Responses to the questionnaires were provided by many of the representatives of industry, government, research & academia and CSIRT community. The level of knowledge about national / international / sectorial research strategies, roadmaps and strategic agendas focused on cybersecurity or privacy is in general lower in case of representatives of the industry. As a consequence, it results, for example, difficult to encourage the industry to aim towards strategically relevant directions. On the contrary, many representatives state that such strategic directions pointed out by these strategic documents are well aligned with the needs of the industry. The most interesting are the following opinions:

- There is a need to have reliable metrics in cyber hygiene, for the common base of discussion and mitigation and therefore strategic documents are very important.
- Although the use of IT has already progressed widely in various fields, the regulation and the government policy are still able to have a great effect on the activities of the private sector and the citizens. Because of that, promoting public-private cooperation in the use of IT, cybersecurity and privacy protection will be critical for wholesome economic growth.
- Where there is absolutely no need, services cannot be sold on the market. However, if we are pursuing only needs, we will not be able to find an advanced business, and therefore strategic documents are relevant.
- Lately research strategies require programs to involve companies interested in technologies from the point of view of doing business. Those companies input the needs of the industry to the programs.

3.3.1.2. Declared focus on cybersecurity and privacy

Both EU and Japan are fully aware of the current importance of cybersecurity. Both regions emphasize the need to strengthen related areas, primarily in research, development and innovation contexts. At the level of the EU as a whole, as well as in Japan, a strong focus on research in the area of cybersecurity in strategic documents can be noticed. This is also evidenced by the growing number of funds dedicated to conduct research in these areas. But, due to heterogeneity in the EU at the Member State’s level, small differences could be perceived. First of all, not all EU countries put exactly the same emphasis on the area of cybersecurity. More importantly the way of financing research in this area can be also different at the national level. In general, however, many efforts have been made to encourage strategic investments in the area to foster progress, hoping to catch up with countries more advanced in this area (both in the case of research and industry in cybersecurity).
3.3.2. Weaknesses

3.3.2.1. Opposition between industry and research

This subsection discusses the obstacles in transferring outcomes of research into technologies and products as well as oppositions between industry and research. The analysis is based on the outcomes of questionnaires as well as on our own observations. The most interesting finding is that the main problems are common for both regions (the EU and Japan).

A very important problem is the ability and time needed to transfer the outcomes of research into technologies and products. This problem is not specific to cybersecurity, but in this area it can be especially challenging. The main indicated obstacles are outlined and briefly explained below:

- **Different focus.** Research and innovation usually focus on cutting-edge solutions, but the industry focuses on well-understood and tested solutions (also, often well supported) and, in many cases, widely-adopted solutions. In other words, the industrial side is becoming conservative, because there is a little consciousness to adopt new solutions progressively.

- **Different needs.** Even if research was able to provide a solution, which would be ideal in some ways, it could be still impractical. For example, a solution, which would be able to detect all network attacks, could be impractical if it was bounded to high level of false positives.

- **Different aims.** Sometimes it is really difficult to draw researcher’s attention to the hidden needs of existing solutions.

- **Different assumptions.** It is difficult to use outcomes of research in the real world, because outcomes of research are often effective only under certain circumstances, which are not always met in the real world.

- **Law limitations.** New solutions are often not legally viable because of the fact that existing regulation establishes limits to certain practices that would be necessary for such new technologies to be deployed and used. For example, data protection regulation represents a barrier to numerous data-processing based business models. Even cybersecurity solutions are affected by data protection regulations (IP addresses, normally managed in volumes for cyber threat analysis, are considered “personal data” and therefore they cannot be collected or stored as freely as it would be necessary). When it comes to research activities, GDPR allows the use of less stringent data protection rules for scientific data processing. However, the transformation of research outcomes into products may face the challenge of stricter privacy rules within the commercialization phases.

- **Fragmented regulations across the different markets.** Due to the fact that every solution has to be implemented in a certain environment, it is not strictly applicable to find a solution which will satisfy the needs of all potential adopters. For example, due to the various legal frameworks in different countries, there is a possibility that a solution, which is objectively very good (and proven by
research outcomes) cannot be adopted due to legal prohibition. It is worth noting that a fragmented European landscape with regard to cybersecurity and privacy somehow limits research exploitation, but this situation is changing due to efforts to harmonize regulations. For instance, in security-related projects involving law enforcement, the applicable legislation often differs between the research project phase and the end-use or exploitation, which generates loopholes. The disparate regulatory frameworks across Europe create much inefficiency and produce a fragmented market that makes it hard and costly for new technologies to thrive as viable businesses. A very important difference occurs between Japan and European markets. For example, in Japan, scanning tools like SHODAN or Shadowserver are in the grey zone of regulation, and because of that it is almost impossible for the industry to use such tools.

- **Conflict between theoretic model and reality.** Outcomes of research are in many cases based on a theoretical analysis that can actually lead to a conflict between reality and theory, due to the limitation of the model used.

- **Limited resources.** Even the best solution cannot be implemented in all situations because of various limits, for example due to the cost of such solution and lack of economic justification. On the other hand, in practice (in the industry) other parameters than only performance are also taken into account, for example user-friendly UI or ease-of-use.

- **Different limitations.** Outcomes of research can indicate that a solution should be deprecated, but in practice, due to various reasons, the solutions cannot be easily replaced by another solution (for example because that other solution does not exist or such replacement would be too costly). For example, even though outcomes of research recommend or even require immediate implementation of a more secure encryption algorithms, it is not adoptable because of the limitations of the existing system.

- **Time of adoption.** Every company has a business model. It is often difficult to incorporate new technologies into the business model smoothly. For example, even if a good new cyber attack detection technology has been developed, it is very difficult for existing monitoring companies to properly respond to detected alerts due to the lack of security knowledge. It usually requires hiring additional people understanding security, which is not taken into account in the current business model.

Interestingly, such obstacles are widely indicated by many of the surveyed experts. Some of these obstacles are also confirmed by the SRIA document\(^\text{66}\).

We can indicate the following propositions to reduce these obstacles:

- industry involvement in research,
- practical experience of the researchers,
- good definition of mutual expectations between research and industry,

CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- law harmonization, which can bring the effect of synergy, and because of that, research outcomes could be adopted and implemented more easily.

All of the above aspects are very important, but in the case of cybersecurity, industry involvement in research and good practical field-knowledge of the researchers are even more important than in other areas of industry.

Problems are in general very similar between the EU and Japan. One typical issue in both EU and Japan is the reliance of governments on foreign-made security appliances, in many cases exclusively.

3.3.2.2. High-level cybersecurity's personnel shortage

During the analysis, the lack of high-qualified personnel in the area of cybersecurity was highlighted. The analysis provided is based on the outcomes of questionnaires, the strategic documents regarding cybersecurity, as well as on our own observations. The most interesting fact is that both regions suffer from common deficiencies in terms of workforce (the EU and Japan).

On the basis of the received responses to the questionnaires, we can state that education remains very important at every possible level. For example, one expert states that there is often a need to perform courses from the bottom up, because sometimes even IT professionals lack basic knowledge essential to cybersecurity (for example, the basics of the UNIX command line and other related fundamentals). There is also an indicated need for education in handling information within an organization. On the other hand, many responders from both regions state that there is a very high need for education of average citizens to promote and improve awareness of cybersecurity. One of the responders also states that there is a need for more education on top of the research activities undertaken by academia and specialized centers. This is indeed particularly important as research and innovation should not be separated from education and professional training.

As a matter of fact, Working Group 5 (WG5) at the European Cyber Security Organisation (ECSO) is devoted to aspects of education in the area of cybersecurity. Specifically the working group focuses on the following issues67:

- Increase education and skills on cybersecurity products and safe use of IT tools in Member States for individual citizens and professionals.
- Develop cybersecurity training and exercise ecosystem leveraging upon cyber range environments
- Support awareness-raising and basic hygiene skills

As the WG5 Position Paper on Education and Professional Training68 states: there is clearly a lack of qualified cyber security professionals69 and a need for a rise in the overall level of cyber awareness. The demand for cyber specialists and experts is greater

---

68 https://www.ecs-org.eu/documents/publications/5ad725d06d33d.pdf
than the supply and this is making society and organisations increasingly vulnerable. Governments, associated with different stakeholders, should tackle the cyber security skills gap through more education and training accredited offers. This has become a very high priority for the European Commission, which is addressing this skills gap through several programmes, including: A New Skills Agenda for Europe: Working together to strengthen human capital, employability and competitiveness.

Moreover, the document also states that: with regards to cyber security, we are already in a crisis for not producing enough skilled experts that the industry is desperately looking for and stakeholders also lack the knowledge to understand the nature of the cyber domain.

Very similar problems have been noticed on Japan’s side, as the Cybersecurity Strategy of Japan states development and assurance of cybersecurity workforce as one of the aims, because of the fact that cybersecurity workforce development is a pressing task for Japan, as there is a critical domestic shortage of cybersecurity experts, both in quality and quantity.

Of course, the shortage of professionals affects all fields of cybersecurity, but it could be especially devastating in the field of research and innovation.

3.3.2.3. Lack of coordination of research actions on various levels

During the analysis of available materials (such as information about projects and programs, as well as financing mechanisms), including the review of questionnaires and on the basis of our own observations, the improper coordination of research actions in the area of cybersecurity at various levels (international, national, sectorial, etc.) has been noticed. Inevitably, the lack of coordination is more evident in the EU landscape (due to the larger market but not due to the lack of actions which aim at synchronization). In the EU cybersecurity landscape, research is conducted in a wide range of programs and is funded from different sources, as it has been indicated in Section 3.1. Unfortunately, there is a possibility that similar actions and projects can be pursued by various entities at the same time, which may lead to inefficiencies and wasted opportunities to achieve synergy. Contrary to other issues mentioned in this section, which are common to both regions, this problem is significantly more severe on the EU side.

3.3.2.4. Lack of strong global cybersecurity enterprises and solutions originating in the EU and Japan

During the analysis of questionnaires as well as on the basis of own observations, we have noticed that one of the main problems in the cybersecurity market is the insufficient presence of strong European or Japanese enterprises which could

---


[71]Ibid. 70

CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

provide globally competitive products. Because of that, the EU and Japan have to import such solutions from abroad. Of course, this is a problem in the context of industries, but it definitely has a strong impact on the research and innovation aspect as well (without high quality research with industrial or practical emphasis there is no chance to provide such solutions).

3.4. Common interests between the EU and Japan

In this section, we briefly describe the common interests between the EU and Japan which may create opportunities. During and after the workshop, the EU-NITY team has collected answers to many of the problems regarding research and innovation aspects of cybersecurity.

3.4.1. Main strategic directions in institutions

During the workshop, the EU-NITY consortium attempted to obtain information about strategic cybersecurity directions at the responders’ institutions, which are considered the most relevant. The respondents were quite prolific and cited a wealth of research topics including (research topics are grouped by the EU-NITY team):

- **cyber threat intelligence**
  - high performance data analytics for cybersecurity,
  - operational security including tools for CSIRTs,
  - information sharing,
  - cyber attack visualization,
  - threat analysis,
- **education, awareness and cyber range**
  - cybersecurity education and training,
  - security awareness training,
  - security testbed (cyber range),
- **data processing and privacy**
  - privacy and identity,
  - big data,
- **methods to enhance cybersecurity**
  - Artificial Intelligence for cybersecurity,
  - High Performance Computing for cybersecurity,
- **security services**
  - authentication/authorization,
  - digital certificate-based authentication infrastructure,
- **network security**
  - routing security,
  - file sharing methods,
- **cybersecurity in various domains**
  - IoT and cybersecurity in IoT,
3.4. COMMON INTERESTS BETWEEN THE EU AND JAPAN

- Cloud Computing and cybersecurity in the cloud,
- cybersecurity in critical infrastructures,
- legal/policy on IT, IP, privacy, cybersecurity and cybercrime,
- hardware security,
- cloud computing,
- social networks,
- other
  - cybersecurity technologies usable for the 2020 Tokyo Olympics.

In general, main topics listed by representatives of both regions are quite similar. It is worth noting that most of the listed topics are in line with general strategic cybersecurity objectives indicated in both regions, which puts the execution of the process of identification of needs performed during the development of the strategies in a very positive light. The interesting aspect is the fact that a few responders from Japan pointed out the topic of cybersecurity usability related to the 2020 Tokyo Olympic games.

3.4.2. R&I cybersecurity priorities and current directions

Based on the review of the strategies and research programs, as well as based on the experts’ opinion (e.g. collected using questionnaires) and on our own observations, the most important cybersecurity research topics and main current research directions in the field are the following:

- **risk management and critical infrastructure protection**
  - risk measurement,
  - risk management on national and international levels,
  - risk evaluation (on the basis of information on incidents, such as malware infection, information leakage and so on),
  - cybersecurity measures in critical infrastructure fields such as electric power and railway,

- **cybersecurity in various technologies**
  - Internet of Things,
  - Smart Cities,
  - Industry 4.0,
  - Cloud Computing,
  - Big Data.

- **threat detection and threat intelligence**
  - new methods of detection of cyberattacks,
  - machine learning based threat detection,

- **cryptology design, techniques and protocols**
  - encryption,
  - bitcoin and digital currencies,
  - blockchain-based identity management services,

- **network security**
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- routing security,
- IP security,
- security of radio networks,

- **hardware and systems security**
  - secure embedded systems,
  - secure products and services,

- **cybersecurity measures at the Tokyo Olympic Games in 2020.**

The main research directions are very similar in both regions. The only difference is the focus on the Tokyo Olympic Games in Japan.

3.4.3. **Identification of threats**

The most important common threats in both regions, which have been identified in majority by experts during the workshop, are the following (the threats were grouped by the EUNITY team):

- **malware**
  - advanced malware (including sophisticated IoT malware),
  - ransomware,

- **APT**

- **cyber terrorism**
  - cyber terrorism (including online radicalization),
  - state-sponsored hacking activities,
  - industrial sabotage and safety-related cyberattacks,

- **network threats**
  - botnets and DDoS,
  - BGP hijacking,
  - vulnerable radio communication systems,
  - bluetooth threats (blueborne, BT-enabled critical systems),

- **lack of integration/cooperation between CERTs,**

- **poor cyber literacy,**

- **cyber attacks for critical infrastructure,**

- **quantum cryptanalysis**
  - specific threats of various technologies,
  - IoT vulnerabilities,
  - drones,
  - 3D printers,
  - automotive,

- **data theft**
  - leakage of private information,
  - critical information theft and manipulation for economic activities,

- **social engineering**
  - identity theft/fraud,
  - spearphishing,
3.4. COMMON INTERESTS BETWEEN THE EU AND JAPAN

- fake news by strong origination, which leads public to misdirection.

It is worth noting that most of the threats are common for the EU and Japan. The most important and common areas are attacks targeting IoT as well as social engineering attacks. Big cybersecurity incidents are becoming increasingly frequent due to the massive appearance of IoT devices, which often include poor security features and weak infrastructures. Social engineering attacks (namely, attempting to attack the system by abusing the vulnerabilities of legitimate human users) are one of the most efficient paths to attack a system. Identity theft and ransomware are threats that make use of such social engineering attacks.

The issue of cybercrime attribution generates imbalances and issues in addressing foreign cybersecurity policy. Due to the difficulties in identifying hacking actors, homogeneous and common responses are often unachievable. Both regions are facing changes in terrorist threats, from cell/group-based terrorism to individual foreign fighters and lone wolves. For the latter, the Internet is a fundamental tool for dissemination, propaganda, radicalization and anonymous funding.

Some responders from Japan identify GDPR as a threat. When it comes to the invasion of privacy, the EU companies are required to report the details of breaches. However, there is no such regulation in Japan.

3.4.4. Examples of current collaborations

On the basis of the questionnaires, a very important fact is that a vast majority of institutions have foreign collaborations with the EU and with some other party than EU (it regards the EU side as well as Japan). It can be concluded that such collaborations could be strengthened. The highest number of examples of collaborations can be seen in the area of research and joint projects. Exchanging staff is also a popular way of achieving international collaborations. The examples of such collaborations include:

- JPCERT/CC has many bilateral MoUs with European national CSIRTs, and exchanges incident information when necessary,
- JPCERT/CC is a member of APCERT (https://www.apcert.org) since its founding, and has contacts with Asia-Pacific (especially South-Eastern Asian) countries/economies,
- JIPDEC cooperates with ETSI (European Telecommunications Standards Institute) in the field of Internet trust.

3.4.5. ICT areas which need collaboration between EU and Japan

The ICT areas other than cybersecurity and privacy which need collaboration, as indicated by responders are the following:

- communication technologies including 5G,
- NGN (Next Generation Network),
- IoT (Internet of Things) and cyber-physical systems, including drones,
- big data,
CHAPTER 3. RESEARCH AND INNOVATION ASPECTS

- HPC (High Performance Computing),
- AI (Artificial Intelligence) and ML (Microprocessor technology),
- computer science education,
- distributed OS,
- robotics,
- smart cities,
- NFV (Network Function Virtualization),
- VR/AR (Virtual/Augmented Reality),
- E-Health,
- interoperability between eID (government-issued digital certificate for citizen) in the perspective of EU and Japan (in regulation, policy and technical aspects).

One of the respondents mentioned something quite interesting: any systemic question that knows no borders (e.g., climate change, air/sea pollution) to which ICT may be part of the solution. On the whole the need for collaborations is a mirror of the identified threats.

3.4.6. Areas which need the most collaboration

In this subsection all the areas of cybersecurity which need collaborations are indicated:

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

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

- **information sharing**
  - sharing environments to monitor attacks,
  - sharing security intelligence among security vendors/organizations,
  - continuous information feeds on web sites ex. blog, whitepaper,
  - continuous exposure in conferences/exhibitions,
  - continuous workforce activities ex. industry ISAC.

Other activities which could be performed together are the following:

- Interpol-like cooperation and non-aggression treaties,
- improve communication, information/data sharing, legal framework,
- harmonize legal and penal frameworks to ensure effective prosecution of cybercriminals,
- reduce administrative procedures,
3.4. COMMON INTERESTS BETWEEN THE EU AND JAPAN

- intensify collaboration between CERT/CSIRT teams,
- promote joint initiatives (including meetings and workshops).

Certainly boosting the responsiveness of Europe as a whole and fostering cooperation and coordination in cybersecurity between Member States and Japan is a very important issue. There is a need of industry-government cooperation and global collaboration to exchange sensitive data and to enlarge the cooperation to as many countries and industry sectors as possible. Global collaboration shall not only be horizontal, i.e., limited to state entities, nations and international organizations. Rather, global cooperation should be horizontal and vertical, i.e. also involving private entities and other stakeholders (academia for instance).
4.1. Industry activity around research

In this section, the different efforts to create business strategies within the cybersecurity industry will be evaluated by analyzing numerous associations and clusters that operate at a European, Japanese and Member States levels.

In recent years, there has been an increasing concern of the companies about cybersecurity due to the growing threat of cyber-attacks. Furthermore, this interest has been supported by initiatives at the political level in the European Union in order to ensure security and privacy in critical Infrastructure and other sectors.

This has encouraged companies to invest part of their benefits in cybersecurity research and solutions, resulting in the emergence of industrial organizations and initiatives that analyze and collect the key priorities of industry in terms of research and innovation with a global vision.

Furthermore, published studies from agencies such as ENISA and others have provided also insight into cybersecurity challenges that industry will need to face in the mid to long term.

4.1.1. Methodology

This report is based on an analysis of the Strategic Research and Innovation Agendas (SRIA) of industrial associations and technology associations, as well as reports from ENISA, to understand the efforts and measures undertaken and challenges identified by the European Industry when it comes to cybersecurity. The analyzed initiatives have been chosen considering several criteria: scope of action (cross-cutting technologies and vertical markets), impact and activity level.

Several of these organizations were established to manage different contractual public-private partnerships (cPPP) on different topics. A cPPP is an instrument co-funded by the European Union for research and innovation activities in crucial sectors of Europe’s economy, bringing together companies, universities, research
laboratories, SMEs and other organisations. These cPPPs develop strategic research and innovation agendas where the R&I priorities and challenges of the industry are structured and defined.

These partnerships are essential for the cybersecurity market since they promote and generate a real dialogue between industry and the European Commission, driving R&I priorities in the future and, in doing so, fostering market approach of the innovative technologies. As a result, these partnerships improve European Cybersecurity Market competitiveness, making Europe a more attractive location for national and international companies to invest and innovate.

For the elaboration of this section, we have also analyzed the studies conducted by the European Agency for Network Information Security (ENISA) in various sectors. ENISA is considered an important player that provides recommendations on cybersecurity for several industries, working together with operational teams to implement strategies. ENISA works horizontally in multiple sectors such as Cloud, Big Data, CSIRT, IoT, Data protection, Intelligent Infrastructures, Risk Management and Trusted Services.

### 4.1.2. Associations and clusters at EU level

There are several associations of industry that include, among others, a strong focus on research activities. These are related with the ICT sector, and have ample capabilities to generate potential impact in the European Cyber Security market, regardless of their main topic of work or industry. The tables below summarize the associations we have considered for this study:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECSO</td>
<td>European Cyber Security Organization</td>
<td>Cybersecurity Service and product providers, operators of essential services (energy, telecom, finance)</td>
</tr>
<tr>
<td>BDVA</td>
<td>Big Data Value Association</td>
<td>Service operators, data management industry, technology providers, cybersecurity product providers</td>
</tr>
<tr>
<td>NESSI</td>
<td>Networked Software and Services Initiative</td>
<td>Software, Services &amp; Data</td>
</tr>
<tr>
<td>ECSEL (incl. Artemis)</td>
<td>Electronic Components and Systems for European Leadership</td>
<td>Smart Mobility, Smart Society, Smart Energy, Smart Health, Smart Production, Design Technology, Cyber-Physical Systems, Smart Systems, Safety and Security</td>
</tr>
</tbody>
</table>

Table 4.1: European technology associations
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

<table>
<thead>
<tr>
<th>Vertical sector</th>
<th>Industrial Associations and Organizations studied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet of Things</td>
<td>Alliance for Internet of Things Innovation (AIOTI), ENISA reports</td>
</tr>
<tr>
<td>(IoT)</td>
<td></td>
</tr>
<tr>
<td>Communication Infra-</td>
<td>5G Infrastructure Public Private Partnership (5G-PPP), European Telecommunication Network</td>
</tr>
<tr>
<td>stuctures</td>
<td>operators Association (ETNO)</td>
</tr>
<tr>
<td>Security</td>
<td>European Organization for Security (EOS)</td>
</tr>
<tr>
<td>Transport and Mo-</td>
<td>ERTICO, European Road Transport Research Advisory Council (ERTRAC)</td>
</tr>
<tr>
<td>bility</td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td>European Factories of the Future Research Association (EFFRA)</td>
</tr>
<tr>
<td>Health</td>
<td>European Federation for Medical Informatics (EFMI), MedTech Europe Association</td>
</tr>
</tbody>
</table>

Table 4.2: European vertical sectors studied

4.1.2.1. Technology perspective associations

European Cyber Security Organisation (ECSO)

ECSO is a non-profit organisation that represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security Public-Private Partnership\(^1\). ECSO is composed of 219 organisations (large companies, public administrations, SMEs, regional clusters, etc) from 28 countries. The main objective of this organization is to support all types of initiatives, that aim to promote European cybersecurity by protecting the European Digital Single Market from cyber threats, cooperating towards the growth of a competitive cybersecurity and ICT industry and developing cybersecurity solutions for the critical steps of trusted supply chains. ECSO defines 8 areas of interest: ICT Infrastructure, Smart Grids, Transportation, Smart Buildings and Smart Cities, Industrial Control Systems, Public Administration and Open Government, Healthcare, Finance and Insurance.

The members of the organisation are involved in 6 working groups with different task forces:

- **WG1**: Standardisation, certification, labelling and supply chain management. This working group addresses multiple issues such as labelling, standards for interoperability, increased digital autonomy, etc.
- **WG2**: Market deployment, investments and international collaboration. Aimed at supporting members to improve market knowledge, facilitating investment capabilities and promoting international trade.
- **WG3**: Sectoral demand. This group brings together cybersecurity stakeholders in order to engage directly with users, linking supply and demand.

CHAPTER 4. INDUSTRY AND STANDARDIZATION ASPECTS

- **WG4**: Support to SMEs, coordination with countries.
- **WG5**: Education, awareness, training, cyber ranges. This working group focuses on cybersecurity training.
- **WG6**: Strategic Research and Innovation Agenda. Coordination of cybersecurity results and activities of R&D projects.

In relation to the study we conduct in EUNITY, it is worth noting that working group 6 published its last Strategic Research & Innovation Agenda (SRIA) on June 2017\(^2\) where their priority challenges around research are presented:

- Remove trust barriers for data-driven applications and services: through data security and privacy technologies, distributed identity and trust management and user-centric security & privacy.
- Maintain a secure and trusted ICT infrastructure in the long-term: focusing on ICT infrastructure protection and quantum-resistant crypto.
- Intelligent approaches to eliminate security vulnerabilities in systems, services and applications: working on trusted supply chain for resilient services and security & privacy by design.
- From security components to security services: focusing on processes required to provide, manage, measure, certify and restore privacy and security.

**Big Data Value Association (BDVA)**

The BDVA is a non-profit organisation that implements the Big Data Value Private Public Partnership representing the private counterpart. The main goals of the BDVA are to boost European Big Data Value research, development and innovation and to foster a positive perception of Big Data Value\(^3\). The BDVA plays a crucial role in the implementation of the Digital Single Market Strategy in Europe, contributing to its different pillars.

The mission of the BDVA is to develop the Innovation Ecosystem, that will enable the data-driven digital transformation in Europe, achieving and sustaining Europe’s leadership in the fields of Big Data Value generation and Artificial Intelligence.

With its mission and vision in mind, the BDVA defines four different strategic priorities indispensable to achieve them. These priorities are shown in Figure 4.1.

By its nature, Big Data can deeply influence Cybersecurity and this relation emerges in the research and innovation efforts in the cybersecurity, in which the BDVA considers a number of topics:

- Homomorphic encryption
- Threat intelligence
- Assurance in gaining trust
- Differential privacy techniques for privacy-aware Big Data analytics
- Protection of data algorithms

\(^2\)ECSO, June 2017. *Strategic Research and Innovation Agenda*, s.l.: s.n.

\(^3\)Big Data Value Association, October 2017. *European Big Data Value Strategic Research and Innovation Agenda*, s.l.: s.n.
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

The industry around data intelligence realizes the concerns that exist around security of the data being processed, and the possibilities to deliver new security services based on data processing and analytics. This is why the BDVA has a specific task force working on data privacy and data protection.

**Networked Software and Services Initiative (NESSI)**

NESSI is the European Technology Platform that promotes software, services and data with the aim of helping to resolve European societal and economic challenges across all sectors such as manufacturing, transportation, healthcare and energy. NESSI’s vision is to allow European businesses and citizens to stay competitive by creating new economic value with new service offerings. The main objectives of NESSI are:

- Develop strategies and business-focused analysis of R&I
- Mobilise industry and other stakeholders
- Share information and enable knowledge transfer

The digital world is growing fast due to the convergence of the network of services, things and data. Key enablers for this transformation are technologies and developments such as cloud computing, social media, data analytics and mobile communication.
The organisation defines several Research and Innovation challenges\(^4\) classified by two criteria: Characteristics and Dimensions. The different challenges are defined in Table 4.3.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Characteristics</th>
<th>Secure Trustworthy Sustainable Computing</th>
<th>Smart Cognitive Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digital Infrastructures</strong></td>
<td>Computing Continuum</td>
<td>Dynamic policies and behaviour</td>
<td>Self-adaptable infrastructures</td>
</tr>
<tr>
<td>Software Technologies Data</td>
<td>Full-stack software</td>
<td>Programming policies</td>
<td>Self-aware programs</td>
</tr>
<tr>
<td></td>
<td>Data everywhere</td>
<td>Built-in protection of assets and actors</td>
<td>Knowledge and insight for decisions</td>
</tr>
<tr>
<td>Services</td>
<td>Software defined sectors</td>
<td>Regulation in societies of services</td>
<td>Digital business agents</td>
</tr>
</tbody>
</table>

Table 4.3: NESSI Research Challenges

**ECSEL Joint Undertaking**

ECSEL is a Public-Private Partnership for Electronic Components and Systems that aims at keeping Europe at the forefront of technology development. ECSEL supports the European industry, SMEs and research organisations by co-financing several projects and launching Calls for Proposal for research, development and innovation projects. The organisation is composed of multiple members:

- Three associations: EPoSS\(^5\), AENEAS\(^6\) and ARTEMIS\(^7\)
- European Union (European Commission)
- Member States and Associated Countries to the Framework Program H2020

The ECSEL SRA defines certain research and innovation priorities related with Cyber-Physical Systems, IoT and Industry 4.0 facilities. Below is a list of cybersecurity related ECSEL strategic priorities:

- Embedded software architecture modeling
- Security & privacy by design
- Security analysis and evaluation
- Safety and security patterns

\(^4\)NESSI, 2017. Strategic Research Innovation Agenda, s.l.: s.n.
\(^5\)European Technology Platform on Smart Systems Integration. https://www.smart-systems-integration.org/
\(^6\)Association for European NanoElectronics ActivitieS. https://aeneas-office.org/
\(^7\)ARTEMIS Industry Association, more information in next section. https://artemis-ia.eu/
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

- Harmonized and interoperable security evaluation & certification
- Formal methods for side fault analysis and fault attacks
- Fully homomorphic encryption: algorithms and attacks
- Simulation environments for security evaluations of components and systems
- Blockchain, post-quantum cryptography, quantum cryptography, fingerprinting
- New design tools: new security metrics, simulation techniques for safety and security analysis, verification and validation of security requirements
- Identity and access management
- Data protection
- Safe & secure execution platform
- Cryptography
- Trusted devices identities

ARTEMIS Industry Association

The ARTEMIS Industry Association is a private partnership that represents multiple actors of the European Embedded Intelligent Systems Market, Internet of Things Market and Digital Platforms Market. The association continuously promotes the research and innovation priorities of the members to the European Commission and Public Authorities.

ARTEMIS Industry Association pursues the ambition to strengthen Europe’s position in Embedded Intelligent Systems and other technologies related with IoT and Digital Platforms.

The strategy of ARTEMIS is based on the three following foundations:

1. Represent Research and Innovation actors in Embedded Intelligent Systems in Europe
2. Disseminate and support ECSEL Public-Private Partnership and Horizon 2020 projects
3. Support ECSEL Joint Undertaking with the community, involving the different members of the organisation: Industry, SMEs, universities and research institutes.

In the Strategic Research Agenda (SRA), the association defines a number of technological challenges and opportunities, defined as the ARTEMIS Priority Targets:

- Safety-critical Secure Systems
- Virtual World
- Big Data/ Data Analytics
- Systems of Systems
- Cloud Services
- Internet of Things
- Autonomous, Adaptive and Predictive Control

ARTEMIS Industry Association, 2016. Artemis Strategic Research Agenda, s.l.: s.n.
Computing & Multicore

In their last SRA, the association created a matrix where the technological challenges or building blocks and the applications priorities are defined in Figure 4.2.

4.1.2.2. Industry verticals associations

Internet of Things (IoT)

The Alliance for Internet of Things Innovation (AIOTI) is a European association formed by IoT industrial companies, European research centers, universities and public bodies. The different efforts are performed through vertical Working Groups which focus on several defined areas of impact. These key areas are defined in 2 different levels:

- Horizontal: IoT Research, Innovation Ecosystems, IoT Standardisation, IoT Policy
- Vertical: Smart Living for Ageing Well, Smart Farming and Food Security, Wearables, Smart Cities, Smart Mobility, Smart Water Management, Smart Manufacturing, Smart Energy, Smart Building and Architecture.

The association identified some barriers that might restrict the take-up of IoT in the Digital Single Market related with privacy, security and liability. Due to these
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

barriers, AIOTI is working on several topics such as: privacy, confidentiality of data, data authenticity, and integrity on IoT ecosystems.

According to the Baseline Security Recommendations for IoT report\(^9\), the deployment of IoT will be crucial for the European Smart cities and Smart infrastructures. In this context, the organization proposes some key technical areas to focus on in order to raise awareness for IoT cybersecurity:

- Hardware Security
- Trust and Integrity Management
- Data Protection and Compliance
- System Safety and Reliability
- Secure Software
- Authentication
- Access Control – Physical and Environmental Security
- Cryptography
- Secure and Trusted Communications
- Logging
- Monitoring and Auditing

**Communication Infrastructures**

The 5G Infrastructure Public Private Partnership (5G-PPP) is a joint initiative between the European Commission and the European ICT Industry that will deliver solutions, architectures, technologies and standards for the coming generation of communication infrastructures.

The objective of the 5G-PPP is to secure Europe’s leadership in the particular areas, where Europe has potential for creating new markets such as smart cities, e-health, intelligent transport, education or entertainment & media.

Key areas of research and innovation for 5G-PPP are related to the new 5G security architecture, defining the following challenges:

- A flexible architecture that integrates natively networking, computing and storage resources
- A secure and trustworthy network
  - Trusted and Trustworthy 5G Architecture
  - Multi-Domain and Multi-Layer Security
  - Security as a service
- A reliable and resilient network
- A quick end-to-end service deployment

**Security**

The European Organisation for Security (EOS) is an initiative that operates in 15 countries by providing security research solutions and services across many domains, including border, cyber, transport and crisis management. EOS’ activities

---

\(^9\)ENISA, November 2017. *Baseline Security Recommendations for IoT*
are distributed in several working groups such as Security Screening and Detection Technologies, Integrated Border Security, Cybersecurity, or Security Research.  

Regarding cybersecurity research and innovation, the EOS’ Cybersecurity Working Group includes the following objectives:

- Promoting the European cybersecurity and ICT security ecosystem.
- Collaborating with the European Commission and relevant stakeholders to promote R&I in cybersecurity.
- Fostering competitiveness and growth of the cybersecurity industry.
- Encouraging the implementation of European programs leading to the deployment of cybersecurity capabilities.
- Supporting the harmonization of EU Regulations.
- Setting up a stable regulatory environment with customers and administrations.

**Transport and Mobility**

ERTICO is an organization that brings together the interests of private and public European stakeholders. Its main objective is to bring intelligence into mobility for a safer, smarter and cleaner mobility by implementing deployment enablers and evaluating related technologies.

With this background, the organisation focuses their efforts on several areas:

- Connected and Automated Driving
- Urban Mobility
- Transport & Logistics
- Cross-sectors
- Innovation Platforms

ERTICO is also undertaking some challenging topics such as Blockchain technologies, eCall, Cybersecurity and Privacy. According to the European Road Transport Research Advisory Council (ERTRAC), the ongoing European activities towards security regulation will affect connected and automated driving. The organization outlines core activities proposed by the industry:

- Cybersecurity Risk management tools across the value chain with specific focus on automation use cases
- Standardization of this approach in the ISO AWI 21434 “Road vehicles – Cybersecurity Engineering”
- System Reliability and Security

ERTRAC highlights the importance of data collection and data sharing for the different mobility stakeholders.

**Manufacturing**

European Factories of the Future Research Association (EFFRA) is a non-profit association that promotes the development of production technologies in the man-

www.eunity-project.eu 112 July 31, 2018
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

ufacturing industry. The partnership aims to bring together private and public resources to create an industry-led programme in research and innovation with the aim of launching market-oriented cross-border projects throughout the European Union.

The association defines several areas where the manufacturing technology innovation should focus its efforts. One of these areas is highly related with the cybersecurity topic, and it is defined as “Interoperable Digital Manufacturing Platforms: Connecting Manufacturing Services”. Additionally, the document “Factories 4.0 and Beyond” outlines the HL26 standard: Security, Privacy and Liability – Cybersecurity and Industrial Safety.

From a technological point of view, the IoT related technologies adoption will increase the efforts in data security and protection, due to the decentralization of the data which is now distributed in computing and cloud environments. Within this context, EFFRA highlighted the following cybersecurity needs:

- New Information Security approaches and related standards
- Identify Security Service Level Agreements
- Develop security and privacy frameworks in the new digitized context
- Accountability and Trust Management
- Models on data exchange and trade among 3rd party suppliers

The organization also identifies needs on several specific technological enablers:

- Concurrent Control Systems
- Models for data ownership
- Computation on encrypted data
- Critical data-management components
- Metadata structure for new data frameworks
- Data architecture for the data marketplace
- Machine learning algorithms

Health

The European Federation for Medical Informatics (EFMI) is a non-profit organization which main objective is to research and develop medical informatics within the Health market. The association focuses its efforts through 14 different working groups. The one related to cybersecurity is WG12: Security, Safety and Ethics.

Nowadays the eHealth systems are increasingly prone to incidents that affect their availability. Considering this fact, the EFMI association has positioned itself towards a research group investigating security and privacy tools. Their main topics of research are:

- Interoperable and trustworthy EHR system solutions and personal health systems
- New healthcare and health management models for security and privacy
- Privacy and Security in the reuse and secondary use of health data

10Electronic Health Record

www.eunity-project.eu 113 July 31, 2018
CHAPTER 4. INDUSTRY AND STANDARDIZATION ASPECTS

- Solutions for trustworthy and interoperable EHR and personal health systems

According to the MedTech Europe Association, whose vision is aligned with the Global Medical Technology Alliance, safety is critical to the medical technology industry, and medical devices companies should take into account the critical need to assess security for their portfolio. The association exposes some principles that should be considered by the manufacturers when it comes to the production of medical technology devices:

- Medical device development and security risk management
- System-level security
- Coordinated disclosure
- Consensus standards, regulatory requirements and education

4.1.2.3. Summary

As a summary and after the wide evaluation of topics and efforts of associations in Europe dealing with cybersecurity research & innovation, we can sum up several priorities related to cybersecurity, proposed by these organizations in their Strategic Research and Innovation Agendas (SRIA). These priorities are listed in the following summaries.

Summary of horizontal association interests

- ECSO
  - Data security and Privacy technologies
  - Distributed identity and Trust Management
  - User centric Security and Privacy
  - ICT Infrastructure Protection
  - Quantum resistance Crypto
  - Trusted Supply Chain
  - Security and Privacy by design

- BDVA
  - Privacy-aware Big data Analytics
  - Threat intelligence
  - Assurance in gaining trust
  - Protection of Data algorithms
  - Homomorphic Encryption

- NESSI
  - Data Everywhere
  - Dynamic policies and behavior
  - Built-in protection of assets and actors
  - Regulation in societies of services

- ECSEL
  - Security & Privacy by design

www.eunity-project.eu 114 July 31, 2018
4.1. INDUSTRY ACTIVITY AROUND RESEARCH

- Fully Homomorphic Encryption
- Cryptography
- Identity and access management
- Data Protection
- Safety and Security Patterns
- Trusted devices identities

**Summary of vertical industries interests**

- **Internet of Things**
  - Hardware and Software Security
  - Trust and Integrity Management
  - Cryptography
  - Data Protection and Compliance
  - Authentication
  - Monitoring and Auditing

- **Communication Infrastructures**
  - Trusted 5G Architecture
  - Multi-Domain and Multi-Layer Security
  - Security as a service

- **Security**
  - Policy and EU Policy Regulation Harmonization

- **Transport and Mobility**
  - Blockchain technologies for security
  - Privacy
  - eCall
  - Risk Management
  - Reliability and Security
  - Standardization

- **Manufacturing**
  - Security and Privacy Frameworks
  - Trust Management
  - Cryptography
  - Machine learning
  - Critical data management
  - Data exchange and trade

- **Health**
  - Privacy and Security
  - Security Risk management
  - Trustworthy HER-system solutions

All the analyzed associations have a common interest in making their industries secure markets, and therefore all of them dedicate great efforts to promote research and innovation of cybersecurity solutions. This fact implies that cybersecurity is not just a common interest for the industries, but a requirement.
We see several common topics of interest across industries and associations: privacy, cryptography and risk management are referenced in several of these European-level groups.

4.1.3. Associations and clusters in Japan

There are a number of industry associations that influence research activities in Japan through reports, policy dialogue, representation at government subcommittees, as well as deliberations through working groups. In this section, we highlight key industry associations that are related with the ICT sector, with considerable capabilities to generate potential impact on the cybersecurity market in Japan.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keidanren</td>
<td>Japan Business Federation</td>
<td>All industries</td>
</tr>
<tr>
<td>JNSA</td>
<td>Japan Network Security Association</td>
<td>Network Security</td>
</tr>
<tr>
<td>VLED</td>
<td>Vitalizing Local Economy Organization by Open Data &amp; Big Data</td>
<td>Open Data &amp; Big Data</td>
</tr>
<tr>
<td>5GMF</td>
<td>Fifth Generation Mobile Communication Promotion Forum</td>
<td>5G</td>
</tr>
<tr>
<td>IoTAC</td>
<td>IoT Acceleration Consortium</td>
<td>IoT</td>
</tr>
</tbody>
</table>

4.1.3.1. Japan Business Federation (Keidanren)

KEIDANREN (Japan Business Federation) is a comprehensive economic organization with a membership comprised of 1,370 representative companies of Japan, 109 nationwide industrial associations and 47 regional economic organizations (as of April 1, 2018).

Its mission as a comprehensive economic organization is to draw upon the vitality of corporations, individuals and local communities to support corporate activities which contribute to the self-sustaining development of the Japanese economy and improvement in the quality of life for the Japanese people.

For this purpose, Keidanren establishes consensus in the business community on a variety of important domestic and international issues for their steady and prompt resolution. At the same time, it communicates with a wide range of stakeholders including political leaders, administrators, labor unions and citizens.

Keidanren implements diverse policy activities through its broad range of policy committees that also cover cybersecurity issues. It collectively contributes to the public-private policy dialogue through policy proposal documents as well as its representation at government committees. Regarding the innovation policy, a number of policy committees exist, such as the committee on information and telecommunication policy, committee on new industry and technology, and the committee on new business and medium enterprises.
Keidanren has published a number of policy proposals in the area of cybersecurity:

- A Call for Reinforcement of Cybersecurity to Realize Society 5.0 (December 12, 2017)
- Second Proposal for Reinforcing Cybersecurity Measures (January 19, 2016)
- Proposal for Reinforcing Cybersecurity Measures (February 17, 2015)
- Toward the Establishment of a Safe, Secure Internet Society through International Cooperation (October 17, 2006)

Furthermore, Keidanren has revised its Charter of Corporate Behavior on November 8, 2017 as part of its recent activities to embrace digital transformation and cybersecurity. Its Implementation Guidance on Charter of Corporate Behavior specifically invites members to “Strive to ensure cyber security” through organizational planning, risk management, resource allocation, information sharing and incident readiness.

4.1.3.2. Japan Network Security Association (JNSA)

The Japan Network Security Association is a non-profit organisation with industry membership, where different working groups develop different facets of the Association’s charter.

The objective of the JNSA is to promote the standardization of the network security technologies, contributing to better standards and measures in the field, and enhancing the public welfare through research and dissemination activities within the Network Security market.

JNSA is an industry association encompassing broad range of issues, ranging from awareness, education, membership services and investigation of standards. It has more than 20 working groups under 5 committees: social activities, survey and research, standards investigation, education, and marketing.

JNSA published a number of reports, checklists, guidelines and textbooks in Japanese. For instance, the following documents were published in 2017:

- Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT (Oct 30, 2017)
- Textbook for security incident response organization 2.0 (Oct 3, 2017)
- Security Body of Knowledge (SecBoK) skill map 2017 (Aug 21, 2017)
- Checklist for the introduction of identity management systems (Jul 12, 2017)
- Japan IT security market analysis report 2016 (Jun 20, 2017)
- Information security incidents in 2016 (Jun 14, 2017)
- Web application vulnerability assessment guideline (Apr 24, 2017)

4.1.3.3. Vitalizing Local Economy Organization by Open Data & Big Data (VLED)

General Incorporated Association "Vitalizing Local Economy Organization by Open Data & Big Data" is an organization established with views to promote the
public opening of the data owned by public service (public sector) entities, and to advance local vitalization (regional revitalization) and activation of economies, through utilization of such data in combination with the data owned by the national government and local public bodies, as big data.

4.1.3.4. Fifth Generation Mobile Communication Promotion Forum (5GMF)

The objectives of the Fifth Generation Mobile Communication Promotion Forum (5GMF) are to conduct research & development concerning Fifth Generation Mobile Communications Systems, research and study pertaining to standardization thereof, along with acting as a liaison and coordinating with related organizations, collecting information, and promoting education and awareness about Fifth Generation Mobile Communications Systems aimed at the early realization thereof, all with the aim of thereby contributing to the sound development of the use of telecommunications.

4.1.3.5. IoT Acceleration Consortium (IoTAC)

The IoT Acceleration Consortium was established in Japan with the aim of creating an adequate environment for attracting investment in the future with the Internet of Things (IoT) through public-private collaboration. The background is the possibility of a great change in conventional industry and structure of society with the development of IoT, Big Data, and artificial intelligence (AI) in recent years. While the development of IoT creates new services using data, it also generates concerns about existing businesses rapidly becoming obsolete.

The IoT Acceleration Consortium aims to combine the strengths of government, industry, and academia and build a structure for developing and demonstrating technologies related to the promotion of IoT as well as creating and facilitating new business models. The consortium promotes (1) the development, demonstration, and standardization for IoT-related technologies and (2) creation of various IoT-related project and recommendations such as regulatory reform to enable those projects.

4.1.3.6. Society 5.0: National strategic effort in Japan

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.” The term was introduced to inform broadest stakeholders that the next wave of industrial revolution is coming, after the hunting society (Society 1.0), agricultural society (Society 2.0), industrial society (Society 3.0), and information society (Society 4.0).\(^\text{11}\)

Since its introduction, the term has been widely embraced by both industries and government agencies as the generational conceptualization has been useful to

\(^{11}\)Cabinet Office, Society 5.0. [Online] Available at: http://www8.cao.go.jp/cstp/english/society5_0/index.html
signal industries that the next wave of innovation is going to transform our societies. Society 5.0 also implies that such next wave of innovation should foster balanced economic development, tackle societal challenges such as sustainable development, and nurture human-centered society.

Society 5.0 serves as a common thread to connect industry associations as it is driven by commonly accepted values, while at the same time proposes to incorporate enabling technologies such as IoT, big data and cybersecurity into people’s daily lives. Major industry associations thus adopt the term, in order to engage in the industry and policy dialogue to explore variety of innovation pathways toward Society 5.0.

4.1.4. Associations and initiatives at member states level

4.1.4.1. Spain

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEI ciberseguridad</td>
<td>The Spanish Cybersecurity Innovation Cluster</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>INCIBE</td>
<td>Instituto Nacional de Ciberseguridad de España</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>ISMS Forum Spain</td>
<td>Asociación Española para el Fomento de la Seguridad de la Información</td>
<td>Information Security</td>
</tr>
<tr>
<td>CCI</td>
<td>Centro de Ciberseguridad Industrial</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

Table 4.5: Associations and initiatives in Spain

Agrupación Empresarial Innovadora Ciberseguridad y Tecnologías Avanzadas (AEI)

The AEI is an organisation that brings together universities, research centers, companies and other organisations interested in promoting new technologies. The AEI is part of the organ of government of the European Cyber Security Organisation (ECSO).12 The AEI performs a large number of roles, such as:

- Promoting business and technical services implementation by engaging a dialogue between R&D entities, companies and professionals.
- Promoting new strategies for security of information technologies and cybersecurity.
- Developing collaborative exchange in innovative ICT industry projects execution.

AEI defines the following areas of strategic development related with cybersecurity technologies:

- Anti fraud
- Antimalware
- Technical and forensic audit
- Digital Authentication
- Firewall
- Event Management
- Visual recognition access and identity control
- Security on mobility
- Cryptography systems

**Instituto Nacional de Seguridad de España (INCIBE)**

INCIBE is a Spanish organism founded in 2006 and dependent on the Energy, Turism and Digital Agenda Ministry. Its main objective is to develop the Information Society through innovation and Cybersecurity project development with international view. INCIBE’s activity is founded on three fundamental pillars:

- Services: The organisation works for the user's protection and privacy by promoting mechanisms for the prevention of data security incidents
- Research: by addressing a wide range of complex projects with an innovative nature
- Coordination: participating in multiple partnership networks, giving the organisation immediate capabilities to execute operations in the field of cybersecurity.

The INCIBE defines 12 research and innovation strategic topics:

- Reliable and updatable systems
- Privacy
- Data processing
- Critical infrastructures
- Systems evaluation and Cyber Risks
- Attacks and defense against threats
- Identity Management
- Cryptography
- Safety awareness promotion
- Network Security
- Cloud Computing
- Internet of Things

---

Asociación Española para el Fomento de la Seguridad de la Información (ISMS)

The ISMS is a non-profit organisation founded in 2007 aimed at promoting the development, knowledge and culture of Information Security in Spain and benefiting the whole community within this sector. The association implements its activities through different initiatives:

- International journeys
- Data Privacy institute
- Cloud Security Alliance
- Cyber Security Center

The ISMS works in 5 different areas: Cybersecurity, Privacy, Mobility, Cloud, and Training. The Cybersecurity center promotes the exchange of knowledge between the key actors and experts in the sector to boost and contribute the Cybersecurity improvements in Spain.

Centro de Ciberseguridad industrial (CCI)

The Center of Industrial Cybersecurity is a non-profit organisation founded in 2013 with the mission to contribute to the continuous improvement of Industrial Cybersecurity.

The CCI does not define research trends or strategic topics, so any topic regarding or including industrial cybersecurity is of its interest.

4.1.4.2. France

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systematic FIC</td>
<td>Systematic Paris Region Digital Ecosystem</td>
<td>Multiple Sectors</td>
</tr>
<tr>
<td>ALLISTENE</td>
<td>The FIC Observatoire</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>L’alliance des sciences et technologies du numérique</td>
<td>ICT</td>
</tr>
</tbody>
</table>

Table 4.6: Associations and initiatives in France

Systematic Paris Region Digital Ecosystem (SPR)

Systematic is a Global Competitiveness Cluster that brings together more than 800 members connecting software, digital and industry players. Its main objective is to accelerate digital project through collaborative innovation, SME development and networking in several sectors: energy, ICT, Health, Transport, etc. For Systematic Ecosystem, the innovation for these markets is based on the development and continuous growth of the following key technologies:

- Digital Confidence & Cybersecurity
- Big Data & IA
CHAPTER 4. INDUSTRY AND STANDARDIZATION ASPECTS

- Digital infrastructures
- Free software
- Modeling, numerical simulation and HPC
- Embedded System & Internet of Things

FIC Observatoire (FIC)

The FIC Observatoire is a platform co-hosted by the national French Gendarmerie for debates and exchanges about cybersecurity and digital trust. The FIC aims at establishing a common framework for converging initiatives around supply and demand with two objectives:

- Understand and identify the needs of users
- Offer a prospective vision of the industrial sector

L’alliance des sciences et technologies du numérique (ALLISTENE)

Allistene supports the economic and social changes related to the diffusion of digital technologies. The organisation’s objective is to coordinate the various players in digital science and technology research in order to develop a coherent and ambitious research and technological development program. The mission is to identify common scientific and technological priorities and to strengthen partnerships between public operators (universities, schools, institutes), while creating new synergies with companies.

4.1.4.3. Poland

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSF</td>
<td>Fundacja Bezpieczna Cyberprzestrzeń / Cybersecurity Foundation</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>-</td>
<td>Mazowiecki Klaster ICT</td>
<td>ICT</td>
</tr>
</tbody>
</table>

Table 4.7: Associations and initiatives in Poland

Fundacja Bezpieczna Cyberprzestrzeń / Cybersecurity Foundation (CSF)

The Cybersecurity foundation is a non-governmental organization established in June 2010. The main objectives of the foundations are to educate and conduct cyber exercises and develop activities of research related to IT security and critical infrastructure protection. Its mission is to raise awareness on threats emerging from the cyber domain.

One of the most valuable initiatives of the foundation is the Cyber-EXE™ Polska, aimed at exploring the capacity and preparation of their members to identify and address the different threats in the field of ICT Security.
**Mazowiecki Klaster ICT**

The Mazovia Cluster ICT is a cluster established in 2007 and coordinated by the Association of Economic and Social Development “knowledge”\(^\text{14}\). The mission of the Mazovia cluster ICT is to bridge the gap between action and conditions for SME’s development by establishing and developing cooperation between computer science enterprises, telecommunication and electronic media R&D units, universities and business institutions.

Regarding cybersecurity and security aspects of ICT systems, the Cluster points out several challenges and areas of research:

- Public Key Infrastructure systems
- Safe systems of document circulation
- Identity Management systems
- Safety audits of IT systems
- Analysis and expertise in information security, electronic documents, identity cards, PKI

**4.1.4.4. Greece**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCC</td>
<td>Greek Cybercrime Center</td>
<td>Cybersecurity</td>
</tr>
</tbody>
</table>

Table 4.8: Associations and initiatives in Greece

There is not a wide range of Greek associations and clusters specialized in Cybersecurity. However there are existing projects and initiatives aimed at mobilizing Greek constituency in the area of cybercrime training, research, education and uptake of results.

**Greek Cybercrime Center**

The Greek Cybercrime Center is part of an European effort that has received funding from the Prevention of and Fight against Crime Programme of the European Commission.

This initiative combines partners from the industry, academia and law enforcement that together aim to promote the state-of-the-art in cybercrime prevention.


www.eunity-project.eu 123 July 31, 2018
CHAPTER 4. INDUSTRY AND STANDARDIZATION ASPECTS

4.1.4.5. Belgium

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Main Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC</td>
<td>Cyber Security Coalition</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>BELTUG</td>
<td>Beltug</td>
<td>Digital technology</td>
</tr>
</tbody>
</table>

Table 4.9: Associations and initiatives in Belgium

Cyber Security Coalition (CSC)

The Cyber Security Coalition is a partnership between entities from the academic world, private sector and public authorities from Belgium that join forces to fight against cybercrime. The coalition mission focuses on generating a cross-sector collaboration with various objectives:

- Share knowledge and experience
- Initiate, organize and coordinate concrete cross-sector initiatives
- Raise awareness among citizens and organizations
- Promote the development of expertise
- Issue recommendations for more efficient policies and regulations

To approach this mission, the cluster is organized in 4 strategic axes, with their own working groups.

- Experience Sharing. Trusted Platform to exchange knowledge and information on specific Cybersecurity issues. With specific themes distributed in multiple sessions: GDPR, Cyber heists, Cyber Ranges, etc.
- Operational Collaboration: Collective actions to fight cybercrime. Topics of discussion in this working group are:
  - Response & technical tooling to support incident response
  - Detection, future-proof monitoring & use cases
  - Working transformation, Cloud & Mobile Devices
  - Privileged Access Management, GDPR
  - Ransomware, awareness exercises, security by design
  - Threat-hunting activities
  - SSL interception
  - Wannacry-like incidents
  - PSD2 & API's
- Policies & Recommendations: Support sectorial bodies in setting policies and defining new ways to implement these policies.
- Awareness Raising: Dissemination campaigns, events and conferences.

---

4.2. COMMON TOPICS OF INTEREST

Belgian Association of Digital Technology Leaders (BELTUG)

Beltug is the largest Belgian association of the digital technology market. It is focused on breaking down the barriers that the companies face when building their digital strategy.

The association prioritizes on several topics related with the digital technology market, collected in their action plan:

- Blockchain
- Smart collaboration
- Digital Signature (eIDAS)
- IoT Security
- Enterprise mobility management
- Workable Security
- Managed Security Services
- Hybrid IT integration in ICT architecture
- 5G
- GDPR: Cloud Vendor assessment, HR Services assessment, Template consent, Special Interest Group, Corporate policy and privacy.
- E-archiving
- E-privacy
- CAPEX & Cloud
- Software CoC
- Access National Number

4.2. Common topics of interest

From this analysis we can conclude that there are indeed common topics of interest around cybersecurity between the Japanese and European industry needs.

Industry in both regions has identified a strong interest in areas like 5G and big data, with specific organizations created in both spaces to promote these technologies and to address cybersecurity challenges in these areas. In the EU, BDVA and 5GPPP have emerged, and in Japan the VLED and 5GMF were created with some similar objectives. There are IoT efforts also in both regions in the form of associations.

The Japan Network Security Association has also similar counterparts in some European countries, although a EU-level equivalent does not exist as such. Some of the EU-level organizations (such as ECSO) address some of the similar objectives as JNSA, to some extent.

In conclusion, we can see that several key areas of industry-led research around cybersecurity that are common in both regions can be found in applications and technologies around Big Data, 5G and IoT.

Common research interests include privacy of big data, availability and reliability of open data, security of 5G communication networks and protocols, cryptography,
CHAPTER 4. INDUSTRY AND STANDARDIZATION ASPECTS

and regulatory aspects of cybersecurity to enable new applications and technology developments.
5.1. Appendix A

5.1.1. Brief description of the methodology of cybersecurity strategies description

Strategies of selected EU member states are analysed in this chapter. National strategies of countries of EUNITY partners are analysed in a more detailed way, whereas analyses of strategies of other countries are based on information provided by ENISA on National Cyber Security Strategies (NCSSs) Map\(^1\). The description presents the state as at the date of the end of June 2018.

The most important questions to be answered on the basis of these analyses are defined as follows:

1. What research and innovation actions or objectives were defined in a national strategy?
2. What areas of research and innovation are defined in a strategy as especially important?
3. What are the goals beyond the strategy objectives defined by the ENISA (and briefly described below)?

In all of these questions we focus mainly on the research and innovation aspects. To enable making conclusions we briefly state the methodology behind these analyses and descriptions.

ENISA supports EU member states in developing, implementing and evaluating their National Cyber Security Strategies (NCSS). Currently all member states have developed the NCSS, but the scope of the documents, as well as their actuality, are different.

\(^1\)https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
CHAPTER 5. APPENDIXES

Objectives

ENISA has defined objectives and presented analysis of all countries’ strategies in a form of list of objectives which are met by each of the strategies.

The ENISA NCSS Map lists all the documents of National Cyber Security Strategies in the EU together with their strategic objectives and good examples of implementation. The information is based on publicly available material. More detailed information about the objectives and good practices is based on the NCSS Good Practice Guide that was published by ENISA in 2016².

In the context of the national strategies’ analysis, National Cyber Security Strategies: Practical Guide on Development and Execution³ and newer document: National Cyber Security Strategies: Good Practical Guide⁴, both prepared by ENISA, are very important and helpful. These documents, among other things, define the areas of interest of a cyber-security strategy. These areas are described in the documents mentioned above and can be briefly summarized as follows.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Description (based on⁵)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>The aim of a cyber security strategy is to increase the global resilience and security of national ICT assets, which supports critical functions of the state or of the society as a whole. Setting clear objectives and priorities is thus of paramount importance for successfully reaching this aim.</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>One of the key elements of a cyber-security strategy is the national risk assessment, with a specific focus on critical information infrastructures. Risk assessment is a scientific and technologically based process consisting of three steps: risk identification, risk analysis and risk evaluation.</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>Before defining in detail the objective of the cyber-security strategy, it is important to take stock of the status of the key elements of the strategy at national level. At the end of this activity important gaps must be identified.</td>
</tr>
</tbody>
</table>

⁵Ibid. 4
| Develop a clear governance structure | A governance framework defines the roles, responsibilities and accountability of all relevant stakeholders. It provides a framework for dialogue and coordination of various activities undertaken in the lifecycle of the strategy. A public body or an interagency/interministerial working group should be defined as the coordinator of the strategy. |
| Identify and engage stakeholders | Identifying and engaging stakeholders are crucial steps for the success of the strategy. Public stakeholders usually have a policy, regulatory and operational mandate. They ensure the safety and security of the national critical infrastructures and services. Selected private entities should be part of the development process due to the fact that they are likely the owners of most of the critical information infrastructures and services. |
| Establish trusted information-sharing mechanisms | Information-sharing is a form of strategic partnership among key public and private stakeholders. Owners of critical infrastructures could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of national security, including findings based on information collected by intelligence and cyber-crime units. |
| Develop national cyber contingency plans | A national cyber security contingency plan should be part of an overall national contingency plan. It is also an integral part of the cyber security strategy. |
| Protect critical information infrastructure | Critical information infrastructure protection (CIIP) is an integral part of many cyber and information security strategies. Cybersecurity covers a broad spectrum of ICT-related security issues, of which the protection of CII is an essential part. |
| Organise cyber security exercises | Exercises enable competent authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience. |
| Establish baseline security requirements | Baseline security requirements for a given sector define the minimum security level that all organisations in that sector should comply with. Such requirements could be based on existing security standards or frameworks and good practices widely recognised by the industry. |
| Establish incident reporting mechanisms | Reporting security incidents plays an important role in enhancing national cyber security. Incident reporting and analysis helps in adjusting and tailoring the security measures list, referred to in the previous section, to the changing threat landscape. |
| Raise user awareness | Raising awareness about cyber-security threats and vulnerabilities and their impact on society has become vital. Through awareness-raising, individual and corporate users can learn how to behave in the online world and protect themselves from typical risks. Awareness activities occur on an ongoing basis and use a variety of delivery methods to reach broad audiences. |
| Strengthen training and educational programmes | Unfortunately, universities and R&D institutions do not produce enough cyber-security experts to meet the increasing needs of this sector. Cyber security is usually not a separate academic topic but part of the computer science curriculum. Cyber security is also a continuously changing topic that requires constant training and education. |
| Establish an incident response capability | National/governmental CERTs play a key role in coordinating incident management with the relevant stakeholders at national level. In addition, they bear responsibility for cooperation with the national/governmental teams in other countries. |
| Address cyber crime | The fight against cyber crime requires the collaboration of many actors and communities to be successful. In this respect, it is important to address and counter the rise of cyber crime and to prepare a concerted and coordinated response with relevant stakeholders. |
| Engage in international cooperation | Cyber security threats and vulnerabilities are international in nature. Engaging in cooperation and information sharing with partners abroad is important to better understand and respond to a constantly changing threat environment |
Establish a public/private partnership

A public/private partnership (PPP) establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals. PPPs may focus on different aspects of security and resilience.

Balance security with privacy and data protection

Counter-terrorism measures and tools that tackle cyber crime often invade privacy in the most brutal ways and, at the same time, lack of personal online security leads to breaches of that same privacy. A cyber-security strategy should seek for the right balance between these two concepts.

Institutionalise cooperation between public agencies

Cyber security is a problem area that spans across different sectors and across the responsibilities of different public agencies. Therefore, close cooperation between these entities is an important pillar for the successful implementation of NCSS.

Foster R&D

Research and development in cyber security is needed in order to develop new tools for deterrence, protecting, detecting, and adapting to and against new kinds of cyber attacks.

Provide incentives for the private sector to invest in security measures

There are different ways how governments can ensure that businesses implement appropriate security measures. One way is to make certain standards mandatory by law. However, governments can also apply softer steering measures, for example by giving incentives to businesses to invest in certain security measures.

| Table 5.1: Objectives which should be defined in National Cybersecurity Strategies (NCSSs) |

In the context of research and innovation, the most important objective is “Foster R&D”, the more detailed description of this objective, on the basis of the document National Cyber Security Strategies: Practical Guide on Development and Execution, is as follows: Typical objectives of this phase include the following:

- Identify the real causes of the vulnerabilities instead of repairing their impact.
- Bring together scientists from different disciplines to provide solutions to multidimensional and complex problems such as physical-cyber threats.
- Bring together the needs of industry and the findings of research, thus facilitating the transition from theory to practice.

---

Find ways not only to maintain but also to increase the level of the public trust in existing cyber infrastructure. Typical tasks in this step comprise the following:
- Create a forum for industry and request R&D topics for consideration.
- Create an R&D agenda with topics that support the objectives of the cyber security strategy with a midterm horizon, of between four and seven years. For each topic the following should, at least, be described: the objective, the incentives and the challenges of the topic.
- Create a platform for bringing together high-level research and the private sector. This platform may take the form of a public/private partnership. Seek cooperation with similar European and international relevant activities i.e. the European Commission Research and Innovation programme (e.g. FP7/8).
- Create a coordination research plan in order to avoid overlaps between research activities undertaken by different institutions and programmes.
- Develop effective incentives to make cyber-security research ubiquitous. Both individuals and organisations might be the beneficiary of these incentives.

5.1.2. The EU member states’ national cybersecurity strategies

The national strategies of cybersecurity should, among other things, state the main research directions pointed out by the countries. Because of that, in this section we briefly describe each national strategy in the EU.

5.1.2.1. France

Brief description

In France, the law programming the defense strategy for 2014-2019 is the main framework for the development of cybersecurity. It includes many of the aspects that need to be covered in the strategic research and innovation agenda of EUNITY. It creates obligations for operators of sensitive (critical) infrastructure to investigate and report incidents, and to be equipped to resist and/or detect attacks. It defines priority areas for the development of products that are either innovative or that include sovereignty issues. It also outlines a budget and describes several mechanisms (R&I funding, national platforms, strategic projects, . . . ) to reach these goals. This law can be seen as a model for the strategic development of cybersecurity in Europe.\(^7\)

The content of this section is focusing on more recent developments than were included in the EUNITY Grant Agreement, Annex 1 Description of the action\(^8\). The two fundamental documents included here are the draft military planning law (published in January 2018, for discussion by the French parliament) including the associated report and the defense review of October 2017, and the cyberdefense review

\(^7\)source: EUNITY Grant Agreement, Annex 1 Description of the action
\(^8\)Ibid. 7
published in February 2018. These documents form a consistent set and the core of the French cybersecurity doctrine for the 7 years to come.

<table>
<thead>
<tr>
<th>Owner (responsible)</th>
<th>French Prime Minister</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publication</td>
<td>Government/Parliament</td>
</tr>
<tr>
<td>Date of publication</td>
<td>January 2018 (draft)</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Military planning law</td>
</tr>
<tr>
<td>Language versions</td>
<td>French &amp; English summary(^9)</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
<tr>
<td>Scope (geographical or sectoral)</td>
<td>French</td>
</tr>
<tr>
<td>Scope (on the basis of merit)</td>
<td>All aspects related to cybersecurity</td>
</tr>
<tr>
<td>Types of stakeholders</td>
<td>Industry, Critical infrastructure operators</td>
</tr>
</tbody>
</table>

Table 5.2: Basic information about the National Cybersecurity Strategy in France

**Previous strategies and related documents**

The military planning law is a 5-years exercise, that supports the long term planning of defense funding. As such, it is much wider than cybersecurity, and includes global security in its scope. Each law is usually created after the development of a strategic vision, developed in a “gold” book.

The laws have successively covered the 1997-2002, 2003-2008 and 2009-2014 periods. The 2009-2014 introduces a significant change, as it becomes the vehicle chosen by the French government to implement the cybersecurity strategy and the NIS directive. It includes in its scope a significant research effort of 110 million Euros. The current law covers the 2014-2019 period. Note that the spending planned in the law is usually adjusted in the yearly French budget. While the law provides a direction, its commitment to spending is weaker and usually not fully covered.

The law described thereafter covers the 2019-2025 period. It includes the text of the law, as well as a report evaluating the execution of the current period.

**Strategic vision**

The strategic vision is that the effort implemented by the 2019-2025 law aims at adapting the French Armed Forces to the needs of France and Europe in 2030. It dedicates almost 200 billion Euros for the years 2019-2023, reflecting the French presidency objective to increase military spending to 2% of the French GDP by 2025.

The vision can be summarized by the seven following points:

---

1. place a priority on protecting our information systems;
2. adopt an active stance of attack deterrence and coordinated response;
3. fully exercise our digital sovereignty;
4. provide an effective penal response to cybercrime;
5. promote a shared culture of information security;
6. help bring about a digital Europe that is safe and reliable;
7. act internationally in favour of a collective and controlled governance of cyberspace.

The main aim

The law is organized in four clusters, two short term and two long term. The first cluster aims at improving soldier’s life and training. The second cluster aims at improving and renewing aging military equipment. The third pole aims at guaranteeing France and Europe autonomy. The fourth pole focuses on innovation for future challenges. Cybersecurity is addressed in the last two poles.

Specific aims

The law asserts that cyberspace is rapidly evolving and is having a dual role. Attack attribution is extremely difficult. The damages created by an attack on the activity of nation states make cybersecurity a priority challenge in the law.

The law thus aims at offering improved operational capabilities to the French government in cyberspace, particularly focused on intelligence gathering and cyberdefense. The law supports the capability to operate and innovate in cyberspace, considering that this is a strategic industrial sector for France. Intelligence gathering must become actionable, particularly bringing in the capability for attack attribution with sufficient certainty. It should also enable the evaluation of cyberattack capabilities of potential adversaries, and of the necessary means to defend against these cyberattacks.

It also aims at protecting France, the French government, the French armed forces and the critical infrastructure operators, against cyberattacks. It must develop tools and techniques to improve the resilience of the digital society.

It aims at creating a fifth branch of the military, devoted to cyberspace, with significant operational capabilities. This includes a significant effort on cyberdefense and protection of military networks. This also includes training for professionals, both for operations and for adaptation to new techniques or new threats, such as artificial intelligence.

The law also aims at sustaining the European strategic digital autonomy. This aim should include strategic partnerships, that can leverage capabilities at the EU level to provide a cumulative effect.

The cyberdefense review aims at creating four operational chains related to cybersecurity:
5.1. APPENDIX A

- **The “Protection” chain.** Under the authority of the Prime Minister, ANSSI is tasked with ensuring national security in the event of a cyberattack. It is supported by the military.

- **The “Military Action” chain.** Under the authority of the French President (head of the armed forces), it can use active cyber-warfare for military operations.

- **The “Intelligence” chain.** Covers actions related to intelligence gathering in cyberspace.

- **The “Judicial Investigation” chain.** Under the authority of the French Government, it develops investigative frameworks and coordinate the action of police under the control of the judicial system.

**Areas of interest - research and innovation context**

The strategy is supported by the need for France to master digital technologies. The strongest research and innovation point in the French strategy is related to artificial intelligence and big data, seen both as an opportunity for defense and as a threat (tool offered to attackers to improve their capabilities).

Three key digital technologies are particularly highlighted:

- **Encryption of communications.** France has a strong background on cryptography. Of particular interest are the aspects related to cloud data protection.

- **Detection of cyberattacks.** Several research and development efforts have been carried out to develop sovereign sensors for detecting attacks.

- **Professional mobile radio.** This effort focuses on security for 5G networks.

**Areas of interest - legal, policy and organizational perspective**

The law defines an organizational basis for the French national cybersecurity agency (ANSSI) and the military central command (CALID) to monitor and protect cyberspace. It clearly states that international regulation is still very far away. While it acknowledges that negotiations have been ongoing since 2004, it also acknowledges the failure of the 2016-2017 expert groups meeting. One point of particular interest is the extraterritoriality of data, which is crossing French and European borders at will, and calls for new theoretical foundations for protection. It expresses a concern that this data is currently within the reach of the US judicial system only.

ANSSI is particularly tasked with improving the certification framework, in order to improve product security. The certification schemes, however, must become more practical than they are currently, and more visible to end-users. The European efforts related to certification provide an opportunity for EU-wide certification of products and services. However, these efforts must take into account the past history and ensure a high level of cybersecurity requirements.
Areas of interest - financial perspective

The fundamental ambition of France is to develop a strong industrial base for cybersecurity. Three areas of progress are particularly highlighted:

1. Encourage French industry leaders to develop their product offerings for cybersecurity in the civilian sector,
2. Promote the creation of ETIs by helping the best SMEs grow, this action being supported by national investment funds in the area of cyberdefense,
3. Encourage start-up creation in the area of cyberdefense, this action being supported by specific technology accelerators and incubators.

France also supports the emergence of a European cybersecurity industrial base, including the emergence of an EU cybersecurity market, protected from foreign investment if necessary.

It also supports the development of insurance schemes, to support the continuous improvement of the cybersecurity posture, and information sharing.

The military planning law requires that the cyberdefense forces should reach about 4000 personnel, to which one should add the 750 forces devoted to the protection of the military digital infrastructure, and the 400 personnel devoted to export support.

The funding level will be increased from 730 million Euros in 2018 to 1 billion Euros in 2022.

Fulfilled objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✓</td>
<td>White Book, 2013. Strategic review, 2018</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✓</td>
<td>Ongoing effort.</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✓</td>
<td>Focus on developing the industrial ecosystem.</td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>-</td>
<td>Information sharing happens at the French and EU-bilateral level, but is not formally engaged by law. It is encouraged through insurance mechanisms.</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✓</td>
<td>The current plans are focusing on government operations continuity.</td>
</tr>
</tbody>
</table>
5.1. APPENDIX A

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect critical information infrastructure</td>
<td>✔️</td>
<td>249 critical infrastructure operators have been identified and are closely monitored and supported by ANSSI.</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✔️</td>
<td>In particular, FR is participating in NATO exercises.</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✔️</td>
<td>PDIS requirements, supported by insurance mechanisms.</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>✔️</td>
<td>Awareness programme managed by ANSSI</td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✔️</td>
<td>Training certification programme managed by ANSSI</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✔️</td>
<td>PRIS requirements</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✔️</td>
<td>However the mechanisms have not been laid out yet.</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Establish a public-private partnership</td>
<td>-</td>
<td>Engagement with regional clusters and industry associations.</td>
</tr>
<tr>
<td>Balance security with privacy and data protection</td>
<td>✔️</td>
<td>Implementation of GDPR through CNIL, PDIS requirements</td>
</tr>
<tr>
<td>Institutionalise cooperation between public agencies</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Foster R&amp; D</td>
<td>✔️</td>
<td>Through all channels mentioned earlier.</td>
</tr>
<tr>
<td>Provide incentives for the private sector to invest in security measures</td>
<td>✔️</td>
<td>Regulation and support for critical infrastructure.</td>
</tr>
</tbody>
</table>

Table 5.3: Fulfilled objectives by French National Cybersecurity Strategy
5.1.2.2. Spain

**Brief description**

In Spain, there is already legislation that covers some security requirements to be mapped to risk levels, namely the classification of information and the handling of such information is covered by law 9/1968, Law 11/2007 and Royal Decree 3/2010. There is no legislation yet that requires mandatory reporting of cybersecurity incidents, such as the one proposed in EU NIS directive, but the National Cyber Security Strategy, adopted in 2013, states that enforced incident reporting is a line of action that Spanish government will pursue. The Spanish National Cyber Security Strategy consists of the following five chapters:

- Cyberspace and security
- Purpose and guiding principles of cyber security in Spain
- Objectives of cyber security
- Lines of action of National cyber security
- Cyber security in the National Security System

<table>
<thead>
<tr>
<th>Owner (responsible entity)</th>
<th>National Security Department, Presidency of the Government of Spain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publication</td>
<td>Government</td>
</tr>
<tr>
<td>Date of publication</td>
<td>2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>Spanish &amp; English[^10]</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
<tr>
<td>Scope (geographical or sectoral)</td>
<td>Spain</td>
</tr>
<tr>
<td>Scope (on the basis of merit)</td>
<td>All aspects related to cybersecurity</td>
</tr>
<tr>
<td>Types of stakeholders</td>
<td>Industry and research (All)</td>
</tr>
</tbody>
</table>

Table 5.4: Basic information about the National Cybersecurity Strategy in Spain

**Strategic vision**

The National Cyber Security Strategy[^11] provides a basis for developing the provisions of the National Security Strategy of cyberspace, with the following main principles:


National leadership
- Coordination of efforts
- Shared responsibility, Proportionality, Rationality and Efficiency
- International cooperation

The outlined principles underline the importance of a development plan of the current situation, emphasizing the constitutional values protection as a common element.

The main aim
To ensure that Spain uses Information and Telecommunications Systems securely, by strengthening prevention, defence, detection, analysis, investigation, recovery and response capabilities vis-à-vis cyberattacks.

Specific aims
The strategy sets up six specific objectives for different stakeholders. These specific aims are the following:
1. For the Public Authorities: Ensure an important level of security and resilience for the Information and Telecommunications Systems
2. For Companies and Critical Infrastructures: To foster security and resilience of the networks and information systems used by the business sector in general and by operators of critical infrastructures in particular.
3. In the Judicial and police field operations: Enhance prevention, detection, response, investigation and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace.
4. In the field of sensitisation: Raise awareness of citizens, professionals, companies and Spanish Public Authorities about cyberspace risks.
5. In capacity building: to gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all the cyber security objectives
6. International collaboration: To contribute to improving cybersecurity in the international sphere

Areas of interest - research and innovation context
The National Strategy defines several actions that could be analysed as areas of interest in research and innovation. In the line of action number 6, the document showcases the importance of promoting the training of professionals, giving crucial impetus to the industrial development by strengthening the Research and development efforts in cybersecurity matters. In these terms, the government created the Network of excellence on cybersecurity R&D+I, that brings together organisations such as INCIBE, dependent on the Spanish Ministry for Energy, Tourism and Digital Agenda, and others from the cybersecurity research ecosystem. This network set the following objectives:
- Boost the cooperation of expert agents in cybersecurity
CHAPTER 5. APPENDIXES

- Collect research resources
- Disseminate research results
- Promote the creation of projects
- Build incentives to attract cybersecurity experts

As a result of this initiative, the National Cybersecurity Cluster was created aiming at implementing several initiatives for coordination and knowledge transference between the R&D+I ecosystem and cybersecurity industry.

Areas of interest - legal, policy and organizational perspective
The plan defines several areas of interest regarding legal perspective:
- The focus on combating cyber terrorism and crime should have an effective legal and operational framework. In this context, the importance of incorporating legal framework solutions to problems that arise in connection with cybersecurity in order to establish the different types of criminal infringements is outlined.
- The action line 4 underlines the importance of the development of a framework for cybersecurity knowledge.

Areas of interest - financial perspective
The National Cyber Security Strategy does not define any topic regarding financial environment or funding for research.

Fulfilled objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Establish trusted information-sharing mecha- nisms</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Establish baseline security requirements (mea- sures)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
5.1.2.3. Greece

Brief description
With the recent advances in digitization, the tremendous increase in data, the big data analytics, the increasing use of IoT and sensors, we are walking into an era of new arising cyber-security threats. The National Cyber Security Strategy intends to build and establish a cyber-secure and resilient online interactive environment for the citizens, the public and the private sector, in alignment with international standards, rules and good practices. The National Cyber Security Strategy is comprised of two phases: the implementation and the evaluation phase, which actually settle an endless life cycle. The stakeholders are involved in the strategic and operational level. More specifically, at high political and governmental level, the National Cyber Security Authority monitors, implements and handles the overall responsibility of the strategy along with National Advisory Body/Forum. The National Computer Emergency Response Team (CERT) in cooperation with other entities, handles the operational level by dealing with the cyber attacks.

<table>
<thead>
<tr>
<th>Owner (responsible entity)</th>
<th>Ministry of Digital Policy, Telecommunications and Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publication</td>
<td>Council of Ministers (Government)</td>
</tr>
<tr>
<td>Date of publication</td>
<td>07/03/2018</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy</td>
</tr>
</tbody>
</table>
Strategic vision

This paragraph describes the national strategy concerning cybersecurity in Greece, setting the principles for the development of a safe online environment. The National Cyber Security Authority is implementing the National Cyber Security Strategy, that is called to fill the gap between the public and private sector. The National Cyber Security Strategy is basically a tool for assuring integrity, availability and resilience of critical frameworks, confidentiality of the transmitted information and subsequently advancement of online security.

The defence against cyber threats requires a set of principles and objectives in order to create a rule of law, ensuring high level of security and resilience, in alignment with principles like privacy, freedom, justice transparency and individual social rights.

The main aim

The aims of the National Cyber Security Strategy consist of the advancement of our protection mechanisms against cyber attacks especially for the critical infrastructures, as well as the components to handle, recover from and minimize the impact. Alongside, it is important to keep an informed user space in private and public sector, aware of the cyber threats and protections mechanisms available. To accomplish these goals, Greece should keep up with international cyber security initiatives; measures, decisions and technological advancements of the international organizations and EU directions that guard the cyber space.

Specific aims

- Increase effectiveness of national research systems: Enhancement of the level of prevention, assessment, study and recoverability of the threats against ICT systems including the strengthening of the public and private sectors with those capabilities

---


www.eunity-project.eu 142 July 31, 2018
- Enrich the job research market
- Equal gender opportunity market in research
- Dissemination of scientific knowledge (open access in data and publications), including at national level the social institutions
- Make use of international practices
- Optimally initiate and increase interaction, cooperation and competitiveness with countries around the globe towards the upgrade of national security

Areas of interest - research and innovation context
The actions that need to be undertaken include: the determination of the stakeholders that are part of the National Cyber Security Strategy in private and public sectors; the specification of the critical infrastructure in public and private sectors; the arrangement of the risk assessment study at national level including the identification, analysis and assessment of the impact of the risk. This will give the determination of the steps that can guard the critical infrastructure per sector/stakeholder that will be revised every three years. It should take in consideration risks associated with natural phenomena, technical problems or human error.

The fourth step includes the recording and enhancement of the existent institutional structures in order to be in alignment with the goals of the National Strategy. These include: the legislation, roles and capabilities of the stakeholders associated with Cyber Security as well as the administrative actions per sector; the structures, stakeholders and services in private and public sectors; the current emergency plans (Egnatia, Xenokrates etc.); and the European and international regulations on network and information security. Concerning the legislation enhancements, they should also cover the gaps in the constitutional freedoms and individual rights towards international Law.

Areas of interest - legal, policy and organizational perspective
After the first ERA (European Research Area) monitoring report of European Commission in 2013, each member state (MS) was obliged to prepare a national ERA for 2015-2020, which would define the financial research support of each country. The Greek government supported this decision and assigned to the Ministry of Education, Research and Religious affairs (MERRA) the task of capturing the current state of play, according to European objectives, setting future objectives (for 2020 and 2025) such as open access, building principles and policy directions.

A key instrument towards the ERA implementation is the Research and Innovation Strategy for Smart Specialisation 2014-2020 (RIS3). RIS3 includes the ERA principles and guidelines, the individual MS’s strategic agendas as well as the Horizon 2020 thematic priorities along with its targets for joint actions and synergy. Of course ERA is not limited to cybersecurity and privacy.

Areas of interest - financial perspective
Institutional Funding (public research organisations) - Project funding (jointly implemented by public and private bodies) State budget supports the permanent staff and other operating costs, as well as the payroll costs and operating expenses of public research institutions. They are calculated mainly by quantitative characteristics (non-competitive basis). On the other hand the public research organizations that constitute private law bodies and technological institutions are supported by the ordinary budget for their payroll expenses under the current legal framework. Here the programmatic agreements partly pay the operating costs.

In order to strengthen the funding structure described above there are several grants like the NSRF (National Strategic Reference Framework), which provides funds under specific actions ("Development proposals of Public Research Centers/institutions - KRIPIIS"), EU’s RTD Framework Programmes or other international programmes.

Fulfilled objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>✔</td>
<td>In order to implement the National Strategy, an important aspect is the exchange of information between the stakeholders, concerning their security threats and policies applied. This measure should be applied both in private and public sector stakeholders, in order to analyze the advancements in national cyber security, alongside with the development of partnerships in public and private sectors, so a common ground of goals can be established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Develop national cyber contingency plans</strong></td>
<td>✓</td>
<td>In case of important incidents in the critical information and the communication infrastructure of the stakeholders of the National Cyber Security Strategy, the national cyberspace contingency plan should define the arrangements, roles and competences of various stakeholders to deal with them.</td>
</tr>
<tr>
<td><strong>Protect critical information infrastructure</strong></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Organise cyber security exercises</strong></td>
<td>✓</td>
<td>The simulation of security incidents is an important mechanism for the development of a defense mechanism, and drafted contingency plans as well as, the dissemination of information and knowledge with the participating stakeholders. These national preparedness exercises take place at regular intervals, are administered by the National Cyber Security Authority and their plans are resolved on specific timetables roles, scenarios and goals.</td>
</tr>
<tr>
<td><strong>Establish baseline security requirements (measures)</strong></td>
<td>✓</td>
<td>All the stakeholders of the National Cyber Security Strategy should define the minimum security, technical and organizational measures, in order to establish an accepted level of security. Alongside, a common ground between the stakeholders should be established for the exchange of information, concerning the security incidents and measures to encounter them.</td>
</tr>
<tr>
<td><strong>Establish incident reporting mechanisms</strong></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
### Raise user awareness

A very important aspect of ensuring cyber security in Greece, is the awareness and enhancing the knowledge about security threats, of the users of stakeholders and citizens in general. The National Cyber Security Authority is responsible for the planning and supervision of the user-citizen awareness programme, which includes citizen campaigns (in primary and secondary education via the Ministry of Education) educational actions for users and administrators (cooperation with university institutes) and promotion via websites.

### Strengthen training and educational programmes

### Establish an incident response capability

Concerning the security incident, the stakeholders are obliged to react effectively, apply the necessary actions, in order to prevent the repetition of the event, and spread this information, so the rest of the participant can be prepared. The administration of these episodes should follow the National Cyberspace Contingency Plan, and special teams are responsible for this like: CSIRTs (Computer Security Incident response Teams), in collaboration with the national CERT and other CSIRTs on national and international level, who should as well, optimize the level of prevention, evaluation and analysis of the threats.

### Address cyber crime

<table>
<thead>
<tr>
<th>Raise user awareness</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>A very important aspect of ensuring cyber security in Greece, is the awareness and enhancing the knowledge about security threats, of the users of stakeholders and citizens in general. The National Cyber Security Authority is responsible for the planning and supervision of the user-citizen awareness programme, which includes citizen campaigns (in primary and secondary education via the Ministry of Education) educational actions for users and administrators (cooperation with university institutes) and promotion via websites.</td>
<td></td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✓</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✓</td>
</tr>
<tr>
<td>Concerning the security incident, the stakeholders are obliged to react effectively, apply the necessary actions, in order to prevent the repetition of the event, and spread this information, so the rest of the participant can be prepared. The administration of these episodes should follow the National Cyberspace Contingency Plan, and special teams are responsible for this like: CSIRTs (Computer Security Incident response Teams), in collaboration with the national CERT and other CSIRTs on national and international level, who should as well, optimize the level of prevention, evaluation and analysis of the threats.</td>
<td></td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✓</td>
</tr>
</tbody>
</table>
5.1. APPENDIX A

| Engage in international cooperation | ✓ | Concerning cyber security, Greece should be effective in terms of international collaboration in order to keep up with the global directions and strategies, exchange experiences and best practices, especially with countries with similar planning. In order to enhance the cyber security at national level and align with international multilateral negotiations and actions, Greece should be active in the contribution and establishment of relevant agreements with international organizations. |
| Establish a public/private partnership | ✓ |
| Balance security with privacy and data protection | ✓ |
| Institutionalise cooperation between public agencies | ✓ |
| Foster R&D | ✓ | Support of research and development programmes and academic educational programmes. Taking in consideration that cyber security is a constantly evolving cutting edge technology, it is very important to keep a high level of support to the academic community in terms of research and development. |
| Provide incentives for the private sector to invest in security measures | - |

Table 5.7: Fulfilled objectives by Greek National Cybersecurity Strategy

Evaluation and revision of the National Strategy
In order for the National Cyber Security Strategy to meet its goals, the National Cyber Security Authority should lead the evaluation and revision steps that will improve the Strategy. This evaluation will take into account the qualitative and quantitative efficiency alignment with international standards and practices within predefined time schedule.
5.1.2.4. Poland

Brief description
The National Cybersecurity Strategy has been a subject of heated debate for a few years, as aspects of security (monitoring of traffic) need to be balanced with proper privacy controls. The draft document has been published for public debate by the Ministry of Digital Affairs in February 2016, but after revisions it has been approved in May 2017 as National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022.

The basic information of this document is listed in the following table and outlined in the following paragraphs.

<table>
<thead>
<tr>
<th>Owner (responsible entity)</th>
<th>Ministry of Digital Affairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publish</td>
<td>Council of Ministers (Government)</td>
</tr>
<tr>
<td>Date of publication</td>
<td>9 May 2017</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022</td>
</tr>
<tr>
<td>Language versions</td>
<td>Polish(^{14}) &amp; English(^{15})</td>
</tr>
<tr>
<td>Status</td>
<td>In force (Accepted by Polish Government)</td>
</tr>
<tr>
<td>Scope (geographical or sectoral)</td>
<td>Poland</td>
</tr>
<tr>
<td>Scope (on the basis of merit)</td>
<td>All aspects related to cybersecurity</td>
</tr>
<tr>
<td>Types of stakeholders</td>
<td>All: from the formal perspective - only public administration, but the document affects in some way all types of stakeholders (public administration, enterprises, individuals) in Poland (also foreign enterprises which operate in Poland)</td>
</tr>
</tbody>
</table>

Table 5.8: Basic information about the National Cybersecurity Strategy in Poland

Previous strategies and related documents
The following documents related to the current strategy can be distinguished:


www.eunity-project.eu 148 July 31, 2018
5.1. APPENDIX A

- **National Security Strategy of the Republic of Poland** (2014) [available in Polish\(^ {16} \) and in English\(^ {17} \)] - concerns not only cybersecurity but also all other aspects regarding to national security and defence - type of document: National security and defence strategy.

- **Cyberspace Protection Policy of the Republic of Poland** (2013) [currently not available] - previously proposed strategy in the area of cybersecurity, the current strategy has superseded this document. The document presents more detailed strategy for coping with cyber threats.

- **Cybersecurity Doctrine of the Republic of Poland** (2015) [available in Polish\(^ {18} \) and summary in English\(^ {19} \)] - it is one of the documents which were taken into account during preparation of the current strategy. The document provides a high-level view of the cybersecurity landscape but it is set on a strictly conceptual level.

- **Cybersecurity Strategy of the Republic of Poland in years 2016-2020** (2016) [available in Polish\(^ {20} \)] - the previous version of the current strategy, this version has been never in force.

### Strategic vision

In 2022 Poland will be more resilient from attacks and threats from cyberspace. Due to synergy in internal and international actions, the cyberspace of the Republic of Poland will be a safe environment to make use of digital economy with respect to rights and freedoms of citizens.

### The main aim

Ensuring high level of security of the public sector, private sectors and citizens in the area of essential services and digital services.

### Specific aims

Four detailed aims are provided, such as:

1. Gaining the ability of coordinated actions at the national level, which aims at prevention, detection, fighting and minimization of impacts of security incidents.

2. Strengthening the ability of cyber threats prevention.

3. Enhancement of national potential and competences in the area of security in cyberspace.

4. Building of strong international position of Poland in the area of cybersecurity.

---

\(^{16}\)https://www.bbn.gov.pl/ftp/SBN RP.pdf  
Areas of interest - research and innovation context

In the strategy, actions are defined which aim at investing in the development of industrial and technological resources for cybersecurity, by creating the conditions needed for the development of enterprises, scientific research centres and start-ups in the area of cybersecurity. The creation of the Cyberpark Enigma programme, which aims at producing high quality hardware and software is provided as an example of such actions.

Another action, which is planned in order to increase the competence of research centres in the area of cybersecurity, is the creation of a Scientific Cybersecurity Cluster (SCC), which will be a scientific platform composed of higher education institutions and scientific research centres specialising in cybersecurity technologies.

The creation of innovation hubs, which will offer comprehensive services for companies and start-ups, including testing new solutions, market research, support in applying for funding for development of innovation solutions, advice on access to new markets and assistance in establishing cooperation with other entrepreneurs is also planned.

The areas of research in the field of cybersecurity which were identified in the strategy are the following:
- transformation from IPv4 currently used on the Internet to IPv6,
- the Internet of Things,
- Smart Cities,
- Industry 4.0,
- Cloud Computing,
- Big Data.

Specific research programmes will be also prepared in order to:
- prepare and implement new methods of protection against novel threats from cyberspace,
- assess the effectiveness of protections and resistance of Poland's cyberspace to cyberthreats,
- assess the effectiveness of response to threats,
- analyse new trends in cybercrime, cyberterrorism and methods of combating them,
- study methods of attacks and ways of counteracting these attacks.

Areas of interest - legal, policy and organizational perspective

The main areas of interest, described by the document, are the following:
- The need for legal changes, changes in the structure of cybersecurity system and improvements in effectiveness of interactions of institutions responsible for cybersecurity to outline clear areas of responsibility.
- The need for cybersecurity risk management at the national level. The need of critical infrastructure, essential services and digital services protection, as well as cybercrime and cyberterrorism prevention.
- The need for the ability to perform military actions in cyberspace.
The need to build competences in the area of cybersecurity: building public-private partnerships, stimulation of research and development and building awareness in the area of cybersecurity.

The document puts cybersecurity on equal level to the military security of the nation.

Areas of interest - financial perspective

In the strategy there is no specific information regarding funding, however the need of preparing a research programme aimed at preparation and implementation of new methods of protection against novel threats from cyberspace, which will be launched jointly with the National Centre for Research and Development, is indicated. Also other research programmes are to be developed with the scientific and academic community.

Fulfilled objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✔</td>
<td>The strategic vision as well as the main goal and four specific objectives are set, however the strategy itself does not provide prioritization of the aims.</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✔</td>
<td>Development and implementation of a risk management system at the national level is one of the defined actions in the first specific objective. The document states that a coherent risk assessment methodology, taking into account the specificity of individual sectors and operators of critical infrastructure, key services and digital service providers, will be developed.</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>✔</td>
<td>In the strategy only few of existing regulations (for example the NIS Directive) are taken into account. But one of the main purposes of the first specific objective defined in the strategy is conducting a review of sectoral and specific regulations in the area of cybersecurity.</td>
</tr>
</tbody>
</table>
### CHAPTER 5. APPENDIXES

| **Develop a clear governance structure** | ✓ | Improving the structure of the national cybersecurity system is one of the actions defined by the first specific objective. |
| **Identify and engage stakeholders** | ✓/- | In the strategy the need for identification and engaging stakeholders is not literally identified, however this objective could be satisfied on the basis of other defined actions (such as: increasing the effectiveness of cooperation of entities ensuring security). |
| **Establish trusted information-sharing mechanisms** | ✓ | The need for a system of cyberspace security management at the national level, which will allow threats and vulnerabilities to be reported, is identified in the strategy. The need to set up systemic solutions to exchange information between stakeholders and share knowledge about threats and incidents is also identified. |
| **Develop national cyber contingency plans** | - | This objective is defined only indirectly. |
| **Protect critical information infrastructure** | ✓ | The document states that the government will take action to improve the capacity and competence in cybersecurity of critical infrastructure operators. |
| **Organise cyber security exercises** | ✓ | The need for many types of exercises is indicated, such as: comprehensive exercises simulating the nationwide incidents, smaller-scale exercises, including sectoral ones, exercises of the Armed Forces of the Republic of Poland to carry out military operations in cyberspace and also international exercises. |
| **Establish baseline security requirements (measures)** | ✓ | One of actions indicated in the document regards the development of minimum requirements for ICT security, which will also cover the business continuity management. |
| Establish incident reporting mechanisms | ✓ | One of the main aims defined in the document is the development of the cybersecurity system at the national level, which also entails the further development of structures dealing with cybersecurity at the operational level, including CSIRT teams at the national level, sectoral incident response teams (sectoral CSIRT), information exchange and analysis centres (ISAC). |
| Raise user awareness | ✓ | Many objectives in the area of raising user awareness are defined. Users in this context are perceived as IT staff of companies, IT staff of public administration as well as ordinary citizens. |
| Strengthen training and educational programmes | ✓ | The need for many actions towards training and education is identified in the strategy. |
| Establish an incident response capability | ✓ | An incident response capability is to be established on the basis of CSIRT teams. |
| Address cyber crime | ✓ | The strategy defines a set of actions to enhance the capacity to counteract cybercrime, including cyberespionage, incidents of a terrorist nature and hybrid threats. |
| Engage in international cooperation | ✓ | Many types of cooperation are listed in the document: at the European level, in the NATO and within United Nations. The cooperation also at the operational and technical level is identified as an important action to carry out. |
| Establish a public/private partnership | ✓ | The goal of building cooperation mechanisms between the public sector and the private sector is defined. |
| Balance security with privacy and data protection | - | The objective is defined only indirectly. |
CHAPTER 5. APPENDIXES

| Institutionalise cooperation between public agencies | ✔️ | The objective is met by various proposed actions. |
| Foster R&D | ✔️ | Defined above |
| Provide incentives for the private sector to invest in security measures | ✔️ / - | This objective is partially met by specific actions (such as creation innovation hubs). |

Table 5.9: Fulfilled objectives by Polish National Cybersecurity Strategy

Next steps
The document provides only general aims, guidelines and declarations. Because of that current works are concentrated on preparing an Action Plan, which will implement these aims. After two and after four years from publishing this act there is a plan to conduct reviews and assessment of the effects of this act. The results will be presented to the Council of Ministers, and the Minister of Digital Affairs will be obliged to prepare propositions of corrective actions or a draft of a document which will be in force during the next 5 years.

Action plan
In October 2017 the Action Plan towards implementing the National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022 was published for consultation. Currently the document is available only in Polish. In the plan two appendixes were provided: the tasks catalogue towards implementing the National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022 and the action list towards implementing the National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022. Unfortunately, these documents are currently unavailable on the official government portals, however they are available on third-party portals, for example on the portal of Polska Izba Informatyki i Telekomunikacji (Polish Chamber of Information Technology and Telecommunication) a consultation website is available. Available documents include the Action Plan towards implementing the National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022, the tasks catalogue and the action list.

It is worth noting that a web portal cyberpolicy.nask.pl states that the Minister of Digital Affairs has published on January 18th 2018 the document of Action Plan, however this document is currently not available and not in force.

The Action Plan describes the following areas:

- Directions of interventions of public administration till 2022
- Tasks list towards achieving goals of the National Framework of Cybersecurity Policy of the Republic of Poland for 2017 - 2022
- Action list towards the realisation of identified tasks
- Rules of action financing
- Mechanisms of monitoring and reporting

Selected actions of the plan are presented below:

- **Preparing and implementing a National Cybersecurity System Act** - the aim of this action is to prepare a law which will be implementing the requirements of the NIS directive and will enable the creation of an effective IT system towards management of cyberspace of Poland. Currently, this action is at the final stage of legislation procedure.

- **Implementing a system of current management of security of cyberspace** - the aim of this action is to build a system, which will enable monitoring and event correlation of critical information services, which are important from the perspective of national security, citizens and private enterprises, enable real-time assessment of security level of Poland’s cyberspace and enable coordinated actions of incident response at the national level.

- **Building a governmental cluster of security** - the aim of this action is to build a secure infrastructure for information systems.

- **Building a national system of assessment and certification of IT products and achieving a full membership in SOGIS MRA** - the aim of the action is to gain an ability to certify IT products based on International standard ISO/IEC 15408 (Common Criteria).

### Belgium

**Brief description**

Belgium’s Cyber Security Strategy was adopted by the government in 2012. The strategy document, prepared by BelNIS (Belgian Network and Information Security; a national consultation forum on information security), identifies three strategic objectives which are to be realised through different initiatives in eight identified action domains. These three strategic objectives are 1) a safe and reliable cyberspace, 2) an optimal security and protection for critical infrastructures and governmental information systems, and 3) the development of national cybersecurity capabilities. The legal framework for cybersecurity in Belgium, however, remains somewhat unclear, and the information available on the implementation of the strategy is limited. Belgium also does not have a comprehensive critical infrastructure protection strategy or plan in place, but Section 3 of the Cyber Security Strategy addresses, in part, the need for the
government to work with entities engaged with critical infrastructure for the purposes of data protection and the development of improved incident management procedures.

On the other hand, Belgium does have an established computer emergency response team, CERT.be, and a well-developed cybersecurity incident-reporting structure. In the October 2015, Belgium’s federal government officially launched the Belgian Centre for Cyber Security. One of the organisation’s main missions will be to further educate all individuals and organisations in the importance of cyber security. Another aim of the organisation is to streamline and co-ordinate the various government and/or private initiatives around cyber security.

There is active support in the country for public-private partnerships, initially through BeINIS, nowadays through the aforementioned Centre for Cyber Security, on the one hand, and the Belgian Cyber Security Coalition (a partnership between players from the academic world, the public authorities and the private sector to join forces in the fight against cybercrime), on the other hand.25

<table>
<thead>
<tr>
<th>Owner (responsible entity)</th>
<th>Centre for Cybersecurity (Belgium)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level of public administration - acceptance/publication</td>
<td>Government</td>
</tr>
<tr>
<td>Date of publication</td>
<td>2012</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Strategy – Securing Cyberspace</td>
</tr>
<tr>
<td>Language versions</td>
<td>French26</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
<tr>
<td>Scope (geographical or sectoral)</td>
<td>Across the whole of Belgian territories</td>
</tr>
<tr>
<td>Scope (on the basis of merit)</td>
<td>All aspects related to cybersecurity</td>
</tr>
<tr>
<td>Types of stakeholders</td>
<td>All</td>
</tr>
</tbody>
</table>

Table 5.10: Basic information about the National Cybersecurity Strategy in Belgium

**Strategic vision**

To identify three strategic objectives which are to be realised through different initiatives in eight identified action domains. These three strategic objectives are 1) a safe and reliable cyberspace, 2) an optimal security and protection for critical infrastructures and governmental information systems, and 3) the development of national cybersecurity capabilities.27

25Ibid. 7
27Ibid. 7
The main aim
To ensure and secure the cyberspace for Belgian players.

Specific aims
Specific aims are hereby grouped: cyber threats, strategic objectives, approach and domains of action.

Areas of interest - research and innovation context
Stimulation of the development of new technologies via access to major hi-tech projects, fostering collaborative efforts in a multi stakeholder research agenda.

Areas of interest - legal, policy and organizational perspective
The legal framework for cybersecurity in Belgium, remains somewhat unclear, and the information available on the implementation of the strategy is limited. 28

Areas of interest - financial perspective
None to record.

Fulfilled objectives

<table>
<thead>
<tr>
<th>Objective</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>✔</td>
<td>Vision, goal and clear objectives are all well defined</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>✔ / -</td>
<td>Only indirectly mentioned</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>-</td>
<td>No mention</td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>-</td>
<td>No mention</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>✔</td>
<td>The strategy aims at reaching out to all stakeholders and engage with them</td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>-</td>
<td>No mention</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✔</td>
<td>Indirectly set forth</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✔</td>
<td>Annex on critical infrastructures included</td>
</tr>
</tbody>
</table>

28 Ibid. 7

www.eunity-project.eu 157 July 31, 2018
Organise cyber security exercises | - | No direct mention
Establish baseline security requirements (measures) | - | Establishment of guidance on policy settings rather than baseline security requirements
Establish incident reporting mechanisms | - | No direct mention
Raise user awareness | ✔ | Strategic goal to achieve
Strengthen training and educational programmes | ✔ | Raising awareness is within the main objectives
Establish an incident response capability | - | No direct mention
Address cyber crime | ✔ | Substantive section in the strategy
Engage in international cooperation | ✔/- | Indirectly mentioned
Establish a public/private partnership | - | Not directly from the strategy
Balance security with privacy and data protection | - | No mention
Institutionalise cooperation between public agencies | ✔/- | Indirect
Foster R&D | ✔ | Substantive section in the strategy
Provide incentives for the private sector to invest in security measures | - | No direct mention

Table 5.11: Fulfilled objectives by Belgian National Cybersecurity Strategy

Next steps
The strategy does not provide substantive nor granular explanations on the rollout of the strategy. The policy is quite short and high-level in the objectives is intended to set forth.

Action Plan
The implementation of the NIS Directive, particularly with regard to critical infrastructures, will be a crucial functional part in the achievement of the strategy.
CERT was established and now the next phases will be to enhance intra-national cooperation with private business as well as maximize the collaboration with CERTs from other Member States of the Union.

5.1.2.6. Other countries

Austria

Austrian Cyber Security Strategy is the main strategic document in the area of cybersecurity. The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Federal Chancellery of the Republic of Austria (Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>March 2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Austrian Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>Austrian &amp; English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
<tr>
<td>Types of stakeholders</td>
<td>All</td>
</tr>
</tbody>
</table>

Table 5.12: Basic information about the National Cybersecurity Strategy in Austria

Bulgaria

National Cyber Security Strategy “Cyber Resilient Bulgaria 2020” is the main strategic document in the area of cybersecurity. The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Council of Ministers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>18 July 2016</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy “Cyber Resilient Bulgaria 2020”</td>
</tr>
<tr>
<td>Language versions</td>
<td>Bulgarian</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.13: Basic information about the National Cybersecurity Strategy in Bulgaria

---

30https://www.digitales.oesterreich.gv.at/at.gv.bka.liferay-app/documents/22124/30428/Austria nCyberSecurityStrategy.pdf/35f1c891-ca99-4185-9c8b-422cae8c8f21
Croatia

The National Cyber Security Strategy of the Republic of Croatia is the main strategic document in the area of cybersecurity. The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>(Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>7 October 2015</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>The National Cyber Security Strategy of the Republic of Croatia</td>
</tr>
<tr>
<td>Language versions</td>
<td>English³²</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.14: Basic information about the National Cybersecurity Strategy in Croatia

Cyprus

Cybersecurity Strategy of the Republic of Cyprus is the main strategic document in the area of cybersecurity. The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>(Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>23 April 2012</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cybersecurity Strategy of the Republic of Cyprus: Network and Information Security and Protection of Critical Information Infrastructures</td>
</tr>
<tr>
<td>Language versions</td>
<td>English³³</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.15: Basic information about the National Cybersecurity Strategy in Cyprus

Czech Republic
National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020 is the main strategic document in the area of cybersecurity. The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>(Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>1 January 2015</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020</td>
</tr>
<tr>
<td>Language versions</td>
<td>English²⁴</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.16: Basic information about the National Cybersecurity Strategy in the Czech Republic

Denmark
The basic information of this document is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Ministry of Finance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>May 2018</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>The Danish Cyber and Information Security Strategy 2018-2021</td>
</tr>
<tr>
<td>Language versions</td>
<td>English²⁵</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.17: Basic information about the National Cybersecurity Strategy in Denmark

### Estonia

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Ministry of Economic Affairs and Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>2014</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.18: Basic information about the National Cybersecurity Strategy in Estonia

### Finland

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Security and Defence Committee - Ministry of Defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>24 January 2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Finland’s Cyber security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.19: Basic information about the National Cybersecurity Strategy in Finland

### Germany

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>(Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>2011</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Strategy for Germany</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
</tbody>
</table>

---


www.eunity-project.eu 162 July 31, 2018
### Hungary

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>21 March 2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy of Hungary</td>
</tr>
<tr>
<td>Language versions</td>
<td>English[^39]</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>


Table 5.21: Basic information about the National Cybersecurity Strategy in Hungary

### Ireland

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Department of Communications, Energy &amp; Natural Resources (Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>unknown</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy 2015-2017</td>
</tr>
<tr>
<td>Language versions</td>
<td>English[^40]</td>
</tr>
<tr>
<td>Status</td>
<td>Unknown (outdated)</td>
</tr>
</tbody>
</table>


Table 5.22: Basic information about the National Cybersecurity Strategy in Ireland

---

CHAPTER 5. APPENDIXES

Italy
The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration</th>
<th>Presidency of the Council of Ministers (Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>December 2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Strategic Framework for Cyberspace Security</td>
</tr>
<tr>
<td>Language versions</td>
<td>English$^{41}$</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.23: Basic information about the National Cybersecurity Strategy in Italy

Latvia
The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>(Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>unknown (implementation date: June 2014)</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Strategy of Latvia 2014-2018</td>
</tr>
<tr>
<td>Language versions</td>
<td>English$^{42}$</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.24: Basic information about the National Cybersecurity Strategy in Latvia

Lithuania
The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>29 June 2011</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
</tbody>
</table>


www.eunity-project.eu 164 July 31, 2018
5.1. APPENDIX A

<table>
<thead>
<tr>
<th>English name</th>
<th>Programme for the development of electronic information security (cyber security) for 2011-2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language versions</td>
<td>English⁴³</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.25: Basic information about the National Cybersecurity Strategy in Lithuania

Luxembourg

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>26 January 2018 (date of approval)</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English⁴⁴</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.26: Basic information about the National Cybersecurity Strategy in Luxembourg

Malta

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>unknown</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Malta Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English⁴⁴</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.27: Basic information about the National Cybersecurity Strategy in Malta


www.eunity-project.eu 165 July 31, 2018
The Netherlands

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Minister of Justice and Security (Government)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>unknown (2018)</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Agenda</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.28: Basic information about the National Cybersecurity Strategy in the Netherlands

Portugal

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>28 May 2015</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyberspace Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.29: Basic information about the National Cybersecurity Strategy in Portugal

Romania

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>23 May 2013</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
</tbody>
</table>


www.eunity-project.eu 166 July 31, 2018
### 5.1. APPENDIX A

<table>
<thead>
<tr>
<th>English name</th>
<th>- (Cyber Security Strategy in Romania)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language versions</td>
<td>Romanian</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.30: Basic information about the NGSS in Romania

### Slovakia

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>unknown</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Concept of the Slovak Republic &amp; Action Plan of Implementation of Cyber Security Concept of the Slovak Republic</td>
</tr>
<tr>
<td>Language versions</td>
<td>English</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.31: Basic information about the NGSS in Slovakia

### Slovenia

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>February 2016</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English &amp; Slovene</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.32: Basic information about the National Cybersecurity Strategy in Slovenia

---


---

www.eunity-project.eu 167 July 31, 2018
Sweden

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>22 June 2016</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy</td>
</tr>
<tr>
<td>Language versions</td>
<td>English\textsuperscript{52} &amp; Swedish\textsuperscript{53}</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.33: Basic information about the National Cybersecurity Strategy in Sweden

United Kingdom

The basic information of the strategy is listed in the following table.

<table>
<thead>
<tr>
<th>Level of public administration - acceptance/publication</th>
<th>Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of publication</td>
<td>2016</td>
</tr>
<tr>
<td>Type of document</td>
<td>Strategy</td>
</tr>
<tr>
<td>English name</td>
<td>National Cyber Security Strategy 2016-2021</td>
</tr>
<tr>
<td>Language versions</td>
<td>English\textsuperscript{54}</td>
</tr>
<tr>
<td>Status</td>
<td>In force</td>
</tr>
</tbody>
</table>

Table 5.34: Basic information about the National Cybersecurity Strategy in the United Kingdom

\textsuperscript{54}https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss

www.eunity-project.eu 168 July 31, 2018
5.1.2.6.1. Fulfilled objectives

Table 5.36 presents fulfilled objectives by the EU member states other than EUNITY partners.

<table>
<thead>
<tr>
<th>Objective</th>
<th>AT</th>
<th>BG</th>
<th>HR</th>
<th>CY</th>
<th>CZ</th>
<th>DK</th>
<th>EE</th>
<th>FI</th>
<th>DE</th>
<th>HU</th>
<th>IE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of objectives defined</td>
<td>12</td>
<td>3</td>
<td>7</td>
<td>10</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>14</td>
<td>9</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish a public/private partnership</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Balance security with privacy and data protection</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Institutionalise cooperation between public agencies</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Foster R&amp;D</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Provide incentives for the private sector to invest in security measures</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Objective</td>
<td>IT</td>
<td>LV</td>
<td>LT</td>
<td>LU</td>
<td>MT</td>
<td>NL</td>
<td>PT</td>
<td>RO</td>
<td>SK</td>
<td>SI</td>
<td>SE</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>Total number of objectives defined</td>
<td>0</td>
<td>9</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>7</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>Set the vision, scope, objectives and priorities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow a national risk assessment approach</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take stock of existing policies, regulations and capabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop a clear governance structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and engage stakeholders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish trusted information-sharing mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop national cyber contingency plans</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Protect critical information infrastructure</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Organise cyber security exercises</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish baseline security requirements (measures)</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish incident reporting mechanisms</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Raise user awareness</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Strengthen training and educational programmes</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish an incident response capability</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Address cyber crime</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Engage in international cooperation</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish a public/private partnership</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Balance security with privacy and data protection</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Institutionalise cooperation between public agencies</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Foster R&amp; D</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Provide incentives for the private sector to invest in security measures</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 5.36: Fulfilled objectives by NCSSs