Public Private Partnerships (PPP)

Cooperative models

NOVEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Special thanks to the NCSS experts group (https://resilience.enisa.europa.eu/enisas-ncss-project), We would like to acknowledge all the representatives from the Member States for their contribution to this study and especially:

Felix Antonio Barrio Juárez, Spanish National Cybersecurity Institute (INCIBE), SP

Raul Riesco Granadino, Spanish National Cybersecurity Institute (INCIBE), SP

François Thill, Ministry of Economy, LU

Stephen Rhodes, Department for Culture Media & Sport, UK

Lasse Laukka, Finnish Communications Regulatory Authority (FICORA), FI

Miikka Salonen, Finnish Communications Regulatory Authority (FICORA), FI

Klaid Mägi, Information System Authority, EE

Martin Mõtus, Information System Authority, EE

Jiří Průša, Czech Republic Domain Registry, CZ

Rogerio Raposo, National Cybersecurity Center, PT

Wolfgang Rosenkranz, Kuratorium Sicheres Österreich, AT

Heiko Borchert, Kuratorium Sicheres Österreich, AT

Uwe Jendricke, German Federal Office for Information Security (BSI), DE

Hans Oude Alink, National Cyber Security Center (NCSC), NL

G.J.P Peeters, National Cyber Security Center (NCSC), NL

Andreas Reichard, Federal Chancellery, AT

Maciej Pyznar, Government Centre for Security, PL

Marjan Kavcic, Ministry of Public Administration, SI

Jarosław Sordyl, CERT PSE, PL

Zuzana Halásová, Cyber Security Department, SK

Peter Grebáč, NSA Liaison Officer of Slovak Republic, BE

Bruce Nikkel, European FI-ISAC

ISBN 978-92-9204-241-7, DOI 10.2824/076734

Table of Contents

Executive Summary

One common objective of every European national cyber security strategy is collaboration. Collaboration to enhance cyber security in all different levels i.e. information on threats sharing, awareness raising is often achieved in two formal structures; the Information Sharing and Analysis Centers (ISAC) and Public Private Partnerships (PPP). This year ENISA has conducted a study on **Cooperative Models for Public Private Partnership (PPP) and Information Sharing and Analysis Centers (ISACs)**, collating information on best practices and common approaches. In 2011 ENISA conducted a good practice guide on **Cooperative Models for Effective Public Private Partnership (PPP)**[1], in order to collect information from the learning and experiences of existing PPPs. That study also provided information on how to set up and run a PPP. Taking again this year the topic of PPP, ENISA aims to analyse the current status of PPPs in the EU. The study identifies the main models of collaboration, the current challenges that both private and public sector face in the process of setting up and developing PPPs and provides recommendations for the development of PPP in Europe.

Even though many Member States have created PPPs, the titles used to name this collaboration model used are numerous. This study covers all types of cooperation and collaboration between public and private entities in the field of cybersecurity.

Building trust between public-private, private-private and public-public entities has been considered as one of the biggest challenges of PPP; eventually maintaining the same level of trust seems more challenging. Most PPPs define trust as an ongoing process, that involves personal relations and consumes a lot of time. In the evolution of a PPP, trust may be eroded, especially in the case of new members joining, or of the old ones not being active enough, or simply taking advantage of the services that a PPP offers without contributing to any of the defined duties.

The cultural dimension is one of the most important determinants of the way that public private partnerships are being established, developed and operated in Europe. Due to cultural differences, there is no universal scenario on how to create a successful PPP; a model followed in one country will not necessarily fit another.

Other challenges that are analysed in this report are the following:

- Lack of human resources in both the public and private sector.
- Insufficient public sector budget and resources fail to meet the private sector's expectations.
- The establishment of a common level of understanding and dialogue between the public and private sector.
- Promotion of the concept of PPP among SMEs.
- Lack of leadership and legal basis.

The main principles for setting up a PPP ecosystem in Europe are to provide adequate human resources, as well as a legal basis of cooperation. It is also important to ensure open communication between public and private sector. Involvement of Small and Medium Enterprises (SMEs) in the process of PPP building is also crucial, since they are the backbone of the European economy. At the end of this report, ENISA makes a few recommendations on how to set up and run a public private partnership, which are summarized as follows:

- Motivation for the private sector to participate should be a priority when establishing a PPP
- The participants should agree to a legal basis when creating a PPP
- Public institutions should lead the PPP or the national action plan for PPP

[1] https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps

- PPPs should invest on internal private-private and public-public collaboration
- PPP participants should invest on open communication and a pragmatic approach towards building a PPP
- The representatives of the government should be allowed to participate in the meetings with non-disclosure agreement
- Small and Medium Enterprises (SMEs) should also participate in PPPs

1. Introduction

A public – private partnership (PPP) is a long – term agreement/ cooperation/ collaboration between two or more public and private sectors and has developed through history in many areas.

The aim of this research is to analyse how PPPs in Europe are created, as well as to identify common challenges that highlight the need for future investment in PPP. Moreover, good practices and recommendations are provided to improve the effectiveness of collaboration between public and private stakeholders.

Two aspects need to be additionally highlighted at the very beginning. Firstly, PPP is not only about the private-public cooperation. It includes also private-private and public-public relations. To have a good interface between the government and industry, it is essential for both sectors to have good interfaces within their respective domains first. A common understanding of the PPP concept is necessary between governmental agencies, and the private sector (e.g. financial, energy, telecommunication).

The topic of *Information Sharing and Analysis Center (ISACs) Cooperative models* is covered in a separate document[2].

1.1 Objective and Scope

This study aims to indicate the current status of the existing Europe-based PPPs and to identify common challenges and best practices. It will result in supporting those countries who have not established or are in the phase of establishing a well-formed partnership for the first time or are experiencing barriers and looking for advice. The main objectives of this study are:

- **To provide information about PPPs in Europe** through collecting information and analysing the current status of PPP and to identify main models of this type of collaboration.
- To **identify current challenges** that both **the private and public sector face** in the process of setting up and developing PPPs.
- To **formulate and propose recommendations** for the development of PPPs in Europe

1.2 Methodology

To collect data for this study, a qualitative methodological approach was followed through desk research and a series of interviews with experts from EU Member States. The desk research was based on publicly available information, which built up the questionnaire that supported the interviews. The interviews covered 12 Member States representing stakeholders from both public and private sector. The validation of the findings was done through a workshop organised in The Hague together with NCSC NL and through the ENISA NCSS experts group.

1.3 Target Audience

The intended target audience are policy-makers and – in general – public and private organisations with an interest in NIS. This report should be used as a guide for any stakeholder who would be interested in launching and maintaining a PPP on cyber security.

1.4 Structure of this document

Chapter 1 presents the objectives of this report and the structure together with the EU policy context. Chapter 2 explains in a nutshell the driving forces of PPP creation, the motivation for public and private sector to participate in

[2] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/

these initiatives and the services that a PPP offers. Chapter 3 contains an analysis of common models for PPP. Chapter 4 presents the trust building mechanism within PPP. Chapter 5 explains the evolution of PPP through the years and provides and overview of the PPPs in the EU. Chapter 6 provides the main challenges that PPP face and Chapter 7 defines the principles for setting up, improving and maintaining the status of effective collaboration between public and private stakeholders in the EU.

1.5 EU policy context

DSM Strategy

In May 2015, the Digital Single Market Strategy (European Commission, 2015) was adopted[3]. It contains a number of initiatives, the implementation of which should open up digital opportunities for people and business and support Europe's position as a world leader in the digital economy.

Since "trust and security stand at the core of the whole DSM strategy" (European Commission, 2015), the Commission lead a number of projects aimed at enhancing internet trust and security, so that an appropriate environment for digital economy could be created.

Because DSM Strategy emphasizes the role of the digital economy, it concerns private sector and its interaction with public administration. Building proficient digital single market in Europe requires efficient ***collaboration*** *between industry and government. Mutual understanding of needs and constraints is also vital*.

In May 2017 the Commission has published the mid-term review of the DSM strategy (European Commission, 2017). It summarized the progress already made and called co-legislators to swiftly act on all proposals already presented, as well as outlined further actions related to online platforms, data economy and cybersecurity.

EU Cybersecurity Strategy

In 2013 European Commission presented the Cybersecurity Strategy of the European Union: *An Open, Safe and Secure Cyberspace* (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013)[4]. The document sets out the EU's approach on preventing and responding to cyber disruptions and attacks, as well as emphasizes that fundamental rights, democracy and the rule of law need to be protected in cyberspace. It was the first strategic document on the European level which referred only to the cybersecurity.

The Strategy points out achieving cyber resilience as a strategic priority, and it was recognised that the effective cooperation between public authorities and the private sector is absolutely crucial. "Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems". (European Commission, 2013, p. 2). Most of this systems are under the private sector control, so for the governments protecting the cooperation with the industry is absolutely crucial.

The Strategy encouraged Europe-wide discussions, that initially started with the Commission's 2009 communication on Critical Information Infrastructure Protection, about the need for ***private-public cooperation*** *in the field of cybersecurity.*

NIS Directive

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192
[4] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (European Parliament and Council of the European Union, 2016) (called "NIS Directive") was adopted in July 2016[5]. The implementation of the NIS Directive could be a vast challenge for the Member States, however PPP might support the process.

The following are the most important aspects of the NIS Directive which can be addressed by the PPP framework:

- **Awareness raising in the field of cybersecurity amongst the citizens and the essential services operators**: The NIS implementation should be accompanied by awareness raising in the field of cybersecurity. Only with the sufficient level of knowledge about cyber threats, the overall level of cybersecurity in Europe may increase. *This could be achieved in the PPP framework which allows knowledge exchange, sharing of best practice and creates a common level of understanding amongst all stakeholders.*
- **Setting up the cooperation between National Competent Authorities and operators of essential services:** Member States are obliged to identify essential services operators in the sectors listed in Annex II of the NIS Directive. Thus, the cooperation with both public administration and the industry is needed. The public administration and the regulatory bodies have the knowledge about specificities of particular essential sectors. Moreover, the supervisory institutions for critical infrastructure protection are important in this process, since many operators could be both the critical and essential services operator. Cooperation with the industry is essential as businesses will be affected by this regulation and they have the expertise about network and information systems that are in the scope of the Directive.

In addition to establishing thresholds for the reporting of cyber incidents, effective cooperation between the government and the industry is absolutely crucial. Nevertheless, no thresholds will guarantee that all incidents with a significant disruptive effect will be reported. Thus, close cooperation between private and public sector is essential. The same applies when the member states will identify operators of essential services.

- **Provide recommendations for the essential services operators and digital service providers**: The NIS Directive implementation is not only about adjusting the legislation, but also about delivering recommendations to the industry. While creating such recommendations it is crucial to have effective collaboration between national competent authorities and the entities in the scope of the Directive.
- **Cooperation with other important operators which are not in the scope of the Directive**: There are seven sectors defined as essential and three types of digital service providers in the scope of NIS Directive. This does not capture all stakeholders important for cybersecurity in the Member States (also telecommunication, food distribution and nuclear can be seen as critical sectors). Therefore, to achieve an efficient level of security in cyberspace, member states need to establish cooperation with other stakeholders as well, for example in order to gather information about the incidents.

Communication on Strengthening Europe's Cyber Resilience System

In July 2016, the European Commission presented the Communication on *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (European Commission, 2016)[6]. The document points out three goals: stepping up cooperation to enhance preparedness and deal with cyber incidents; addressing challenges facing Europe's cybersecurity Single Market; nurturing industrial capabilities in the field of cybersecurity.

The Commission recognised that the European cybersecurity industry (IT companies, cyber security companies as well as the end-users) needs to be supported. Because of that, a Contractual Public-Private Partnership, ECSO was created

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

in June 2016. ECSO (European Cyber Security Organisation) gathers representatives of national public administrations and industries to work together and provide advice to Commission in the development of directions in the field of cybersecurity market in Europe. ECSO's goal is also to use investments in research and development in the field of cybersecurity from the funds of Horizon 2020 co-financing the approved projects.

Joint Communication on Resilience, Deterrence and Defence

In September 2017, the European Commission presented the joint Communication on *Resilience, Deterrence and Defence*: Building strong cybersecurity for the EU[7]. This Communication aims at building a strong single market through an EU cybersecurity certification framework, through a blueprint plan for operationalising cybersecurity response, through investing in strong encryption and protection of fundamental rights, through strengthening ENISA's role and developing international cooperation for EU leadership on cybersecurity. The Communication recognises ENISA's role in the implementation of the NIS Directive and addresses a stronger role for the Agency through a proposal for a permanent mandate.

The Communication underlines the importance of cooperation and trust building through public-private partnerships and explains that the Commission will continue to support the establishment of public – private partnerships and cooperation mechanisms as it will be a further step to reinforce EU cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart.

[7] http://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PD

2. Setting and focus area of PPP

2.1 Driving forces for the creation of PPP

There are multiple reasons to create a PPP:

Economic interests. This is the most common reason to establish a PPP in Europe. It is the usual motivation for the private sector to participate. It may be the willingness to establish a body which will help identifying the barriers for the growth of the cybersecurity industry and create the conditions to export cybersecurity products. It could also be because the industry needs cooperation with the public sector, for example the finance sector in the field of fighting cybercrime. Finally, it could be due to a new legislation and industry welcoming the opportunity of influencing the process to protect its business from unnecessary or overly burdensome readjustments.

Regulatory requirements. PPPs are created as the implementation of a specific law whenever required and public administration decides that a PPP framework will be the best way to do it. This covers mostly the case of crisis management or emergency law. Regulatory requirements could also include a specific law for PPP, which provides a clear framework to the private-public cooperation and collaboration. Mostly this type of law deals with PPP in general, not only in the field of cybersecurity. It was created to stimulate the economy, but with cybersecurity becoming more and more an important issue on the political agenda, PPPs are focusing also on cybersecurity.

Public relations. In this case the government lets the private sector provide input to new legislation, as well as working together to develop a national cybersecurity strategy. For the private sector, the motivation lies in networking with the government and other private entities that share knowledge.

Social interests. When the social interest was named as a driving force, it was usually the motivation to discuss cybersecurity issues widely in the state, and set cybersecurity high on the political agenda. For the industry, the importance lies in promoting cybersecurity in general, so that the market could evolve without interruption.

It should be noticed that there are often more than one reasons to create a PPP. In most cases more than one reason needs to be met. The most common scenario is that economic and social interests exist which are accompanied by new regulation. This requires exchange of information and cooperation between private and public entities.

Other reasons. There are also other reasons to establish PPPs. In this category experts explained a number of reasons, namely the new EU regulations (NIS Directive and General Data Protection Regulation), which impose new requirements on the private sector. For this reason, the government decided to create PPP to help the industry implement the new regulations.

Below the diagram depicts the most common reasons for creating a PPP.

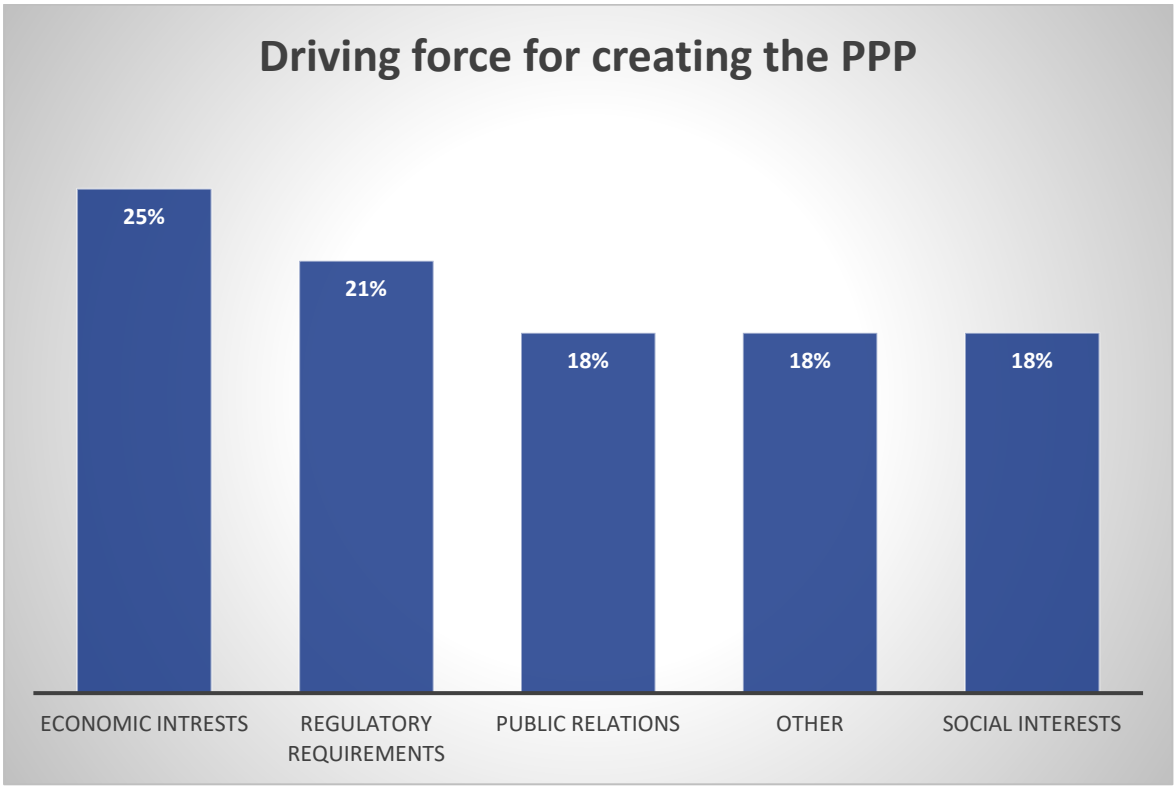

Figure 1: Driving force to create a PPP

2.2 Why join a PPP?

There is a common objective for the participation in PPPs, both of the private and the public sector: to raise the level of cybersecurity. However, there are also a number of different motivations, which are summarized in the Table 1 below.

PRIVATE SECTOR REASONS TO PARTICIPATE IN A PPP	PUBLIC SECTOR REASONS TO PARTICIPATE IN A PPP
Access to public funds	Better understanding of Critical Infrastructure Information Protection (CIIP) and industry in general
Opportunity to influence national legislation and obligatory standards	Possibility to create synergies between different initiatives of private sector
Access to public sector knowledge and confidential information (EU legislation, fighting cybercrime)	Access to private sector resources (e.g. valuable experts), which makes it is easier to set up standards and good practices
Assurance that the products delivered through PPP are of good quality, as it is guaranteed by the government	
Sharing knowledge, experiences and good practices	
Helping to achieve resilience in the cyber ecosystem	
Increase the trust between public-public, private-private and public-private – PPP allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis	
Getting direct and credible contacts with other organisations	

Table 1: Motivations to participate in a PPP

In a nutshell the combination of the reasons and incentives for both the private and the public sector to participate in a PPP are depicted below:

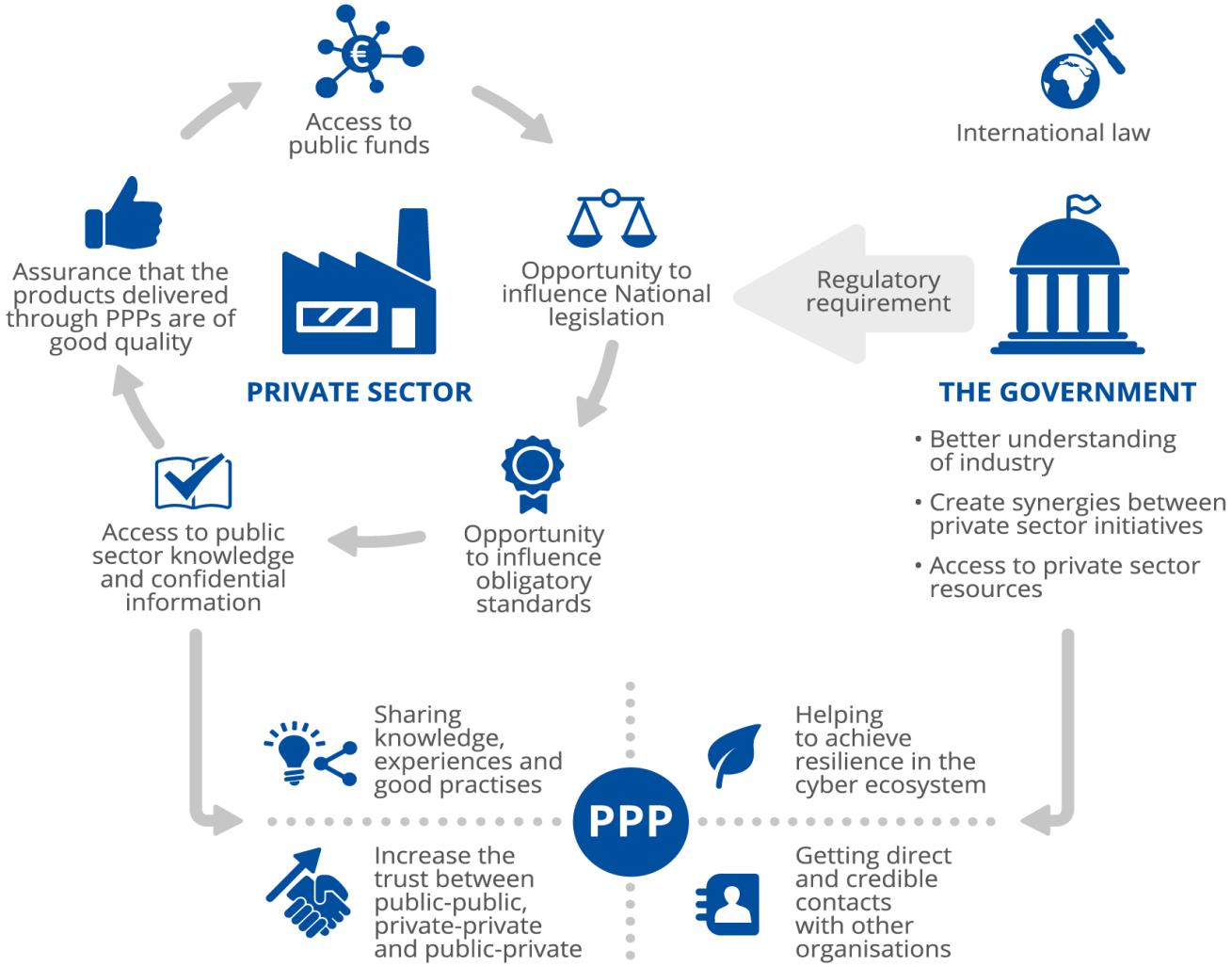

Figure 2: Reasons and incentives for both the private and the public sector

2.3 What PPP can offer

A PPP can offer many services to its members. A list of services together with PPP examples that offer such services in the Member States (MS) are described in the table below:

Services	Examples
Incident handling and crisis management	**UP KRITIS in Germany** supports its members during crisis **CSIRT.CZ in Czech Republic** is national CSIRT, which handles information about cyber incidents with its constituency

	Gov.CERT in Austria is governmental CSIRT, which handles information about cyber incidents with its constituency
Research and analysis	**Spanish Technology Platform on Industrial -** this PPP is focused mainly on research and development of new technologies to increase the level of security in the private sector **Security Made in Luxemburg (SMILE)** – SMILE is employing cybersecurity experts, who deliver services in the fields of behavioural, organizational and technical security.
Development of good practices and guidelines	**Cyber Security Platform (CSP) in Austria** – CSP delivers good practice to the critical operators **Government Centre for Security in Poland** prepares National Critical Infrastructure Program which contains a number of good practices and guidelines for critical infrastructure operators.
Information exchange	**CSIRT.CZ in Czech Republic** is national CSIRT, which exchanges information about cyber incidents with its constituency **Gov.CERT in Austria** is governmental CSIRT, which exchanges information about cyber incidents with its constituency **Cyber Security Platform (CSP) in Austria** was created as a platform to exchange knowledge and information between public administration and critical infrastructure operators **UP KRITIS in Germany** facilitates exchange information between private and public sector **Kuratorium Sicheres Österreich in Austria** facilitates exchange information between private and public sector
Early warnings	**UP KRITIS in Germany –** one of the established working groups works on Early Detection and Mitigation of IT Crises. **Information System Authority in Estonia** provides early warnings about threats in Estonian cyberspace
Exercises	**Kuratorium Sicheres Österreich in Austria –** KSO organizes war games – exercises where private and public sector can practice together in case of cyber events. **Information System Authority in Estonia** provides free training and exercises for private sector entities **Security Made in Luxemburg in Luxemburg** (SMILE) is preparing trainings and simulation platform to train the teams how to manage and notify the incidents, not only on technical but also on organizational level.
Awareness raising	**Kuratorium Sicheres Österreich in Austria** is providing a lot of awarness racing to both private and public sector. **CSIRT.CZ in Czech Republic** provides educational programs for the private companies
Technical evaluation	**Cyber Security Council in Netherlands** provides the government advice on new technological developments. **Spanish Technology Platform on Industrial Safety** helps both private and public sector to identify needs and demand.
Defining standards	**Cyber Security Platform (CSP) in Austria** - by working together critical infrastructure operators and operator and public sector develop security standards with a view of NIS directive implementation

	Kuratorium Sicheres Österreich in Austria facilitate defining standards for critical infrastructure operators **Government Centre for Security in Poland** prepares standards for critical infrastructure operators
Help desk	**Information System Authority in Estonia** provides help desk to its partners
Triage	**Information System Authority in Estonia** provides triage to its partners
Crisis management	**Government's Centre for Security in Poland -** RCB is a governmental institution, established in 2007 by Crisis Management Act (article 10), responsible for the crisis management and critical infrastructure protection. **Security Made in Luxemburg in Luxemburg** (SMILE) facilitate crisis management
Resilience planning	**UP KRITIS in Germany** supports its members in preparing resilience planning **Information System Authority in Estonia** handles resilience planning for Estonia **Security Made in Luxemburg in Luxemburg** (SMILE) facilitate resilience planning
Emergency planning	**Security Made in Luxemburg (SMILE)** supports its members in emergency planning **Information System Authority in Estonia** handles emergency planning for Estonia
Benchmarking	**Information System Authority in Estonia** delivers benchmarking to its members to critical infrastructure operators **Spanish Technology Platform on Industrial Safety** delivers benchmarking to its members
Statistics archiving	**Information System Authority in Estonia** develops statistic about incidents in Estonian cyberspace
Security audit	**Information System Authority in Estonia** provides free audits to the critical infrastructuyre operators. **AEI Ciberseguridad y Tecnologías Avanzadas in Spain** - members can send representatives to be trained by the PPP as auditors. **CSIRT.CZ in Czech Republic** is providing website scanner service, focused on penetration testing of NGO and government websites.
Strategic planning	**Cyber Security Commission (CSC) in Slovakia** helps to prepare state policy in the national cyber security as well during realisation of Cyber Security Concept of the Slovak Republic assesses and discusses drafts of strategic, conceptual, legislative, and methodological documents in the area of cyber security **Cyber Security Council in Netherlands** created to ensure that cybersecurity is discussed on the highest security level; the Council is a formal advisory council, which advices Minister about all kinds of the strategic issues in the cybersecurity (CEOs, professors, people from highest management level in public sector)

	The Cyber Growth Partnership in UK is providing strategic guidance and peer review to Government on innovation and growth initiatives to support the development of the UK cyber security ecosystem.
Risk analysis	**The Cybersecurity Initiative in Austria** in 2011 developed the first national Cyber Risk Matrix that was updated last year. **UP KRITIS in Germany** provides risk analysis about critical infrastructure

2.4 How do PPPs grow and evolve?

The information about how PPPs are started and how they evolve is valuable in understanding how to develop new partnerships. Different possibilities include:

Top Down - When a PPP has evolved top down there was often a key government directive or strategic plan that set out a requirement for the PPP and then members were recruited.

Bottom Up - when the evolution was bottom up, a community recognised a need and worked together to create the PPP and then more members joined.

Top Down then grown Bottom Up - Some PPPs have developed in a way that combines both previous categories. These PPPs started top down with a strategic requirement but then the membership and leadership developed bottom up.

Bottom Up then grown Top Down - An informal group came together and recognised a need and then approached a top level authority which endorsed the approach, maybe providing funding and authority and then the organisation grow top down.

Fire and Forget – A central body, often government led, creates a defining structure for a partnership, promotes its use but once the partnerships are created they are autonomous. A start-up kit may be supplied which may include tools and the ability to buy or register for services such as warnings or alarms.

Split or merge – PPP may recognise the need for a restructure. This can either result in splitting into two or more sub-groups in order to increase the specificity of the information and to reduce the size so that trust is developed or as interconnection of themes or skill sets are recognised PPP may merge.

Starting top down and then growing bottom up accounted for over two thirds of the PPP who responded. It was recognised that a bottom up approach, where industry sees a need, has a greater chance of gathering momentum and being successful.

Public sector organisations should consider the successful strategy used by many PPP, by starting with a top down approach and over time growing the PPP from the bottom up, so it is managed more by the private sector members.

3. Partnership Models

History note: In 1934, Ruth Benedict, American anthropologist, published her book "Patterns of Culture". The essence of this publication is that every culture has its own pattern – it starts, grows and develops in its own unrepeatable way. According to Benedict, "a culture, like an individual, is a more or less consistent pattern of thought and action" (Benedict, 2005). That leads to a conclusion that every culture is unique and special in its own way. Benedict concluded that every member of particular culture is determined by its pattern. That creates cultural personality – personal characteristics inspired by culture (and its pattern).

While analysing PPPs in Europe, it is evident that culture is one of the most important determinants of the way private-public partnership are being established, develop and work. There is no universal scenario of how to create a successful PPP; what works perfectly in one country can be tricky and challenging in another. That is mainly because of the cultural differences and the fact that the general relation between public and private sector differs amongst member states. In some countries formality is the most important part of PPP, while in the others pragmatism is more important.

In countries with a long tradition of strong public authority and strong public administration, there is a visible distance between public and private sector. Public administration is not so eager to enter in any type of cooperation and collaboration with the private sector. Even when industry expresses the interest in creating a PPP, there is still some hesitation. The rules must be well established and goals well defined, so that the public servants know exactly what can they expect from the industry. This is also connected with a highly hierarchical approach. There is usually a tendency to put the PPP in a hierarchical structure reflecting the hierarchy of public administration.

On the other hand, the member states with a long tradition of sharing power between the public authority and the citizens have different approach. Those countries usually have less hierarchical structures in public administration. The government has a very pragmatic approach to PPP and there is no need for a legal basis – non-disclosure agreements and traffic light protocols are sufficient to set up and grow private-public cooperation.

There is no universal, simple solution that applies to all the nations for creating and developing PPP. It is rather a national issue, connected with the culture and the way how the whole political and economic system works.

Based on the interviews conducted, the diagram below shows the types of organisations usually participating in PPP.

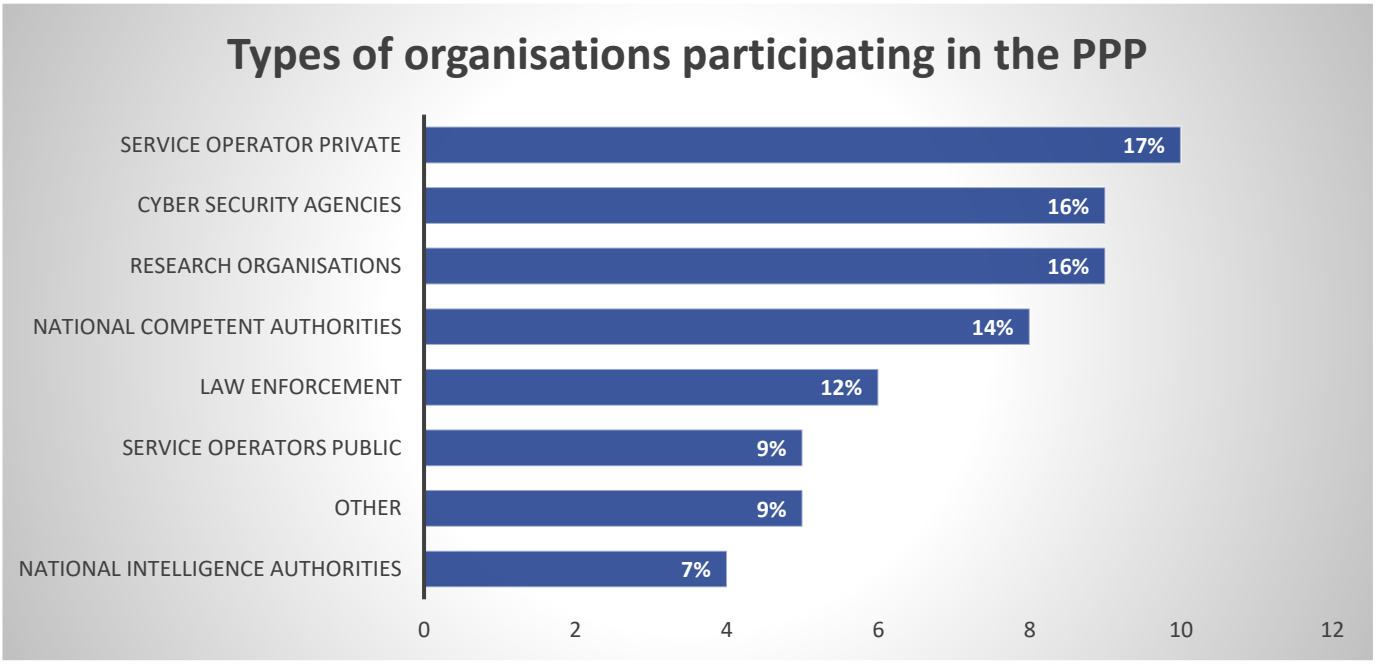

Figure 3: Types of organisations participating in the PPP

Based on the desk research, interviews and analysis of the collected information, four types of PPP have been identified:

- **Institutional PPPs.** In this type of PPP, the whole institution works under a PPP framework. Usually, there are many services that this type of institution delivers, such as research, analysis, development of good practices and guidelines, help desk, security audits and some more focused services. This type of PPP is usually linked with the critical infrastructure protection. This is because the institution is in charge of critical infrastructure protection by a legal act (e.g. emergency/ crisis management act). Common means of cooperation are working groups, rapid-response groups and long-term communities. The goal is to secure critical infrastructure in general, and cyber threats are considered important elements in the threat landscape.
- **Goal-oriented PPP.** PPPs of this type are created for the purpose of building a cybersecurity culture in the MS. There is usually a platform or a council established which brings private and public sector together to exchange knowledge and good practices. The objective for the members is to focus around one subject or a specific goal.
- **Service outsourcing PPP.** PPPs of this type are initiatives created by the government and the private sector. Their main task is to raise cybersecurity awareness and cybersecurity level among stakeholders. These PPPs can actually be considered as third parties for outsourcing services which address the need of industry and support the government in policy making process (e.g. NIS implementation, drafting of national cybersecurity strategies).
- **Hybrid PPP**. This type of PPP includes the CSIRTs operating under a PPP framework. In this case, governments decide to assign to an experienced entity – with already proven experience in operating CSIRT to deliver CSIRT services to the public administration or to the whole country.

All of the types have been analysed in details in the following subchapters and depicted in one view below.

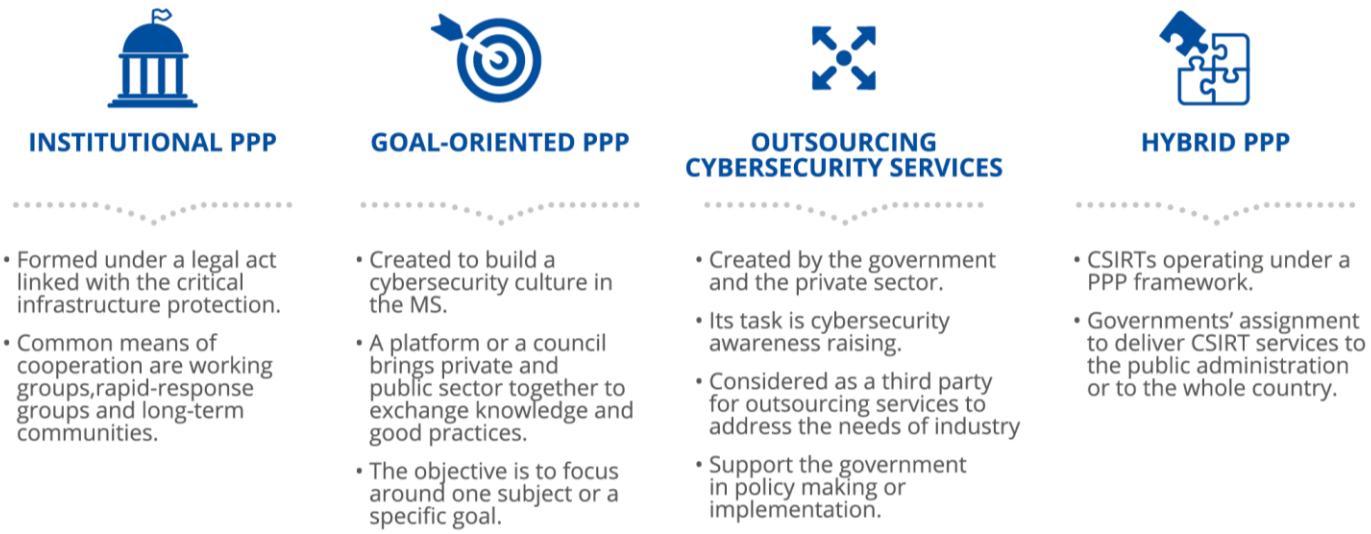

Figure 4: Partnership models

3.1 Institutional PPP

This kind of PPP applies to those public institutions which use public-private partnership frameworks to carry out activities related to critical infrastructure protection. These institutions have been assigned with the task of critical infrastructure protection by a legal act (crisis management/ emergency act). This creates the basis for cooperation with the industry and obligates the public sector to be more sensitive to the private sector's needs and challenges. Being assigned to protect critical infrastructure, public institutions understand that it is necessary to establish a strong and efficient cooperation with the private sector in order to address its needs. Firstly, because each industry has a deeper knowledge of the infrastructure and its specifications, and secondly, because thresholds established by law may not be enough for reporting incidents. Thus, cooperation is needed to share information about all important incidents. Two examples of institutional PPPs have been analysed. The first one is the **Information System Authority (Riigi Infosusteemi Amet, RIA) in Estonia**. Created in 2011, RIA is responsible for national cyber security and for the supervision over information systems used to provide vital services[8] and cybersecurity on the national level (CERT Estonia is part of RIA). The institution's legal basis is the Estonian Emergency Act from 2014[9]. The second example is the **Government's Centre for Security** (Rządowe Centrum Bezpieczeństwa, RCB) **in Poland**. RCB is a governmental institution, established in 2007 by the Crisis Management Act (article 10), responsible for the crisis management and critical infrastructure protection[10].

Institutional PPPs tend to be very dependent on their leaders. The commitment and openness of the public servants determines their success and the level of cooperation with the private sector. This kind of public-private partnership helps to ensure a higher level of security and the proper implementation of the regulatory requirements (e.g. standards and recommendations developed jointly by the government and industry). It also helps to establish an effective network of specialists in cases of crisis.

Main activities

Institutional PPPs provide many services:

- Incident handling and crisis management
- Research and analysis
- Development of good practices and guidelines
- Information exchange
- Early warnings
- Exercises
- Awareness raising
- Technical evaluation
- Defining standards
- Help desk
- Triage
- Crisis management
- Resilience planning
- Emergency planning
- Security audit
- Strategic planning
- Risk analysis

[8] 43 companies in the Estonia have been recognized as a vital service, but with the NIS Directive implementation the Emergency Act will be renewed in order to address the "essential service operators" identification.
[9] https://www.riigiteataja.ee/en/eli/525062014011/consolide
[10] http://rcb.gov.pl/en/about-us/

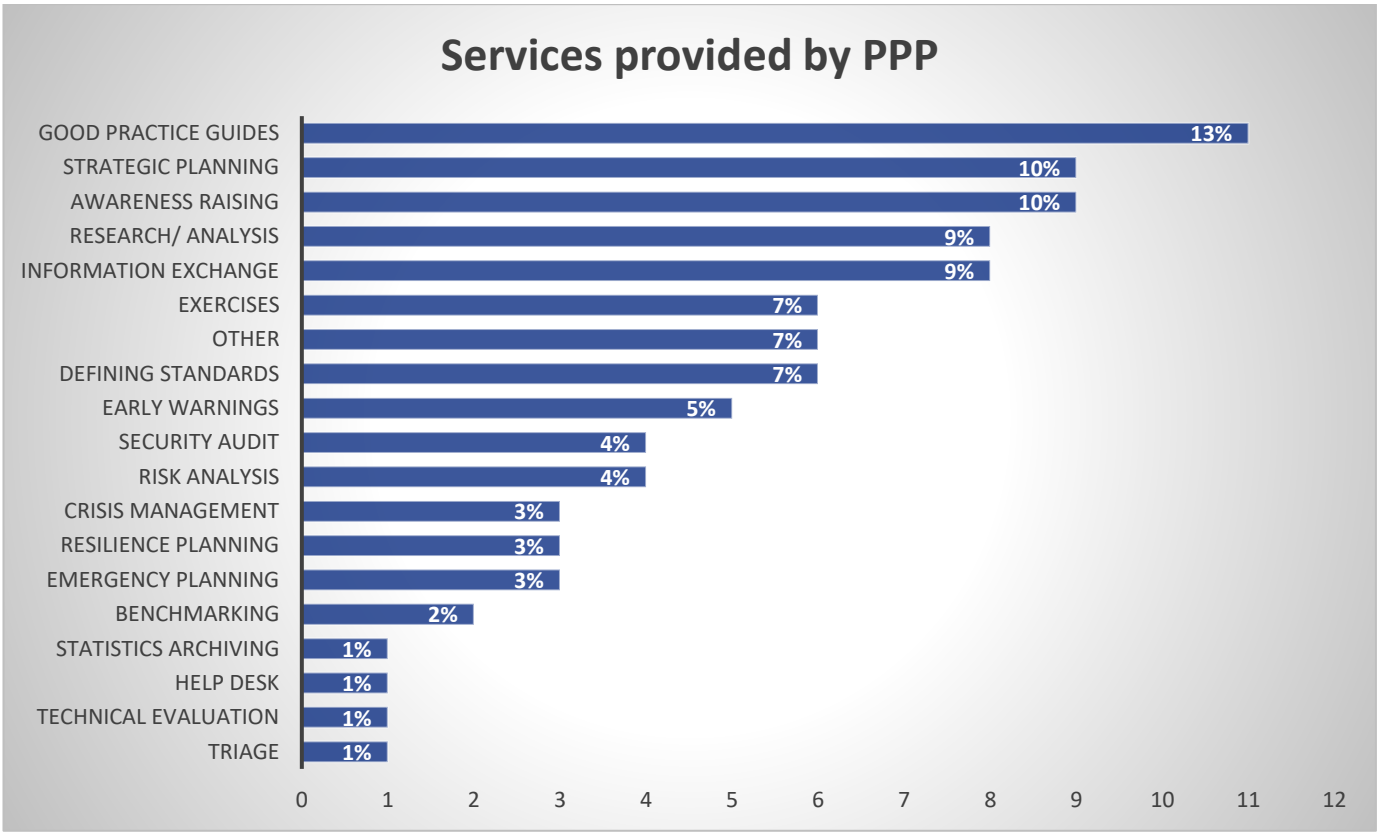

Figure 5: Services provided by PPPs

The diagram above presents data collected by the interviews. Some of these services are provided on a continuous basis, others as a rapid-response to meet expectations of the industry or to find solutions for new challenges that occur and are likely to influence critical infrastructure operators.

Actors involved

Institutional PPPs involve many actors from both the public and the private sector. From industry, all sectors identified as critical are typically involved: energy, drinking water supply and distribution, health sector, financial market infrastructures, banking, railway transportation, air transportation, maritime, road transportation, food distribution. Moreover, if the entity is a public operator but is identified as critical, it also participates in the PPP.

It should be highlighted that not all the sectors are involved on the same level. Some tend to be more interested in participating in the PPP than others. This is the case of the energy and financial sector, which are very aware of the cyber threats and recognize cybersecurity as a high priority. Therefore, they are willing to participate in any kind of activity which addresses challenges related to the cyberspace.

Institutional PPPs involve also public administration like:

- National competent authorities (NCAs) which are in charge of critical sectors. NCAs support the PPP by providing special regulations and recommendations which raise the cybersecurity level within particular sector. These recommendations and regulations are developed through private – public cooperation.
- Cybersecurity agencies that contribute to the PPP with expert cybersecurity knowledge.

- Law enforcement agencies are involved, so that the operators could be better protected against cybercrime.
- Academia is a part of institutional PPP – usually it is aimed at developing projects which help to support the operators in particular challenges.

The governance model

Institutional PPPs are governed in a hierarchical way, specific to the governmental institutions. However, when it comes to the specific initiatives, they tend to be more agile. For example, working groups which are created under the umbrella of this type of PPP are governed by the industry. The private sector makes the strategic decisions, which are then addressed by the public servants.

Funding options

Institutional PPPs are funded by the public sector. The government allocates money from the budget for operating the institution which is assigned with the task of critical infrastructure protection. The industry contributes to the PPP by voluntary contribution (appointment of an employee to cooperate with private sector).

A characteristic feature of institutional PPP is that usually there is not enough budget allocated for the provision of services needed for critical infrastructure protection. For this reason, the PPP framework is extremely useful. Instead of hiring extra personnel or buying services on the market, CIP is addressed by collaboration between government and industry (e.g. publication of the recommendations).

PPP interaction

Institutional PPPs are long-term communities. Most interactions are made by different working groups (both formal and informal) and systematic meetings (2-3 per year). Those activities are accompanied by seminars, workshops and conferences, which allow to address new problems and challenges.

3.2 Goal-oriented PPPs

Goal – oriented PPP are usually built, when cybersecurity is understood as a distinguished and specific task/objective of the economy, which needs extra support and interest from the government. This type of PPP is focused on providing strategic solutions, supporting the IT market and creating a framework for cybersecurity development in the country.

Goal-oriented PPPs and their specifications reflect to the highest extent the cultural differences amongst Member States. Starting from the initiative and reason for the PPP creation through its governance and interaction, it is clearly visible how cultural patterns and PPP's nature are linked – similar goals are achieved by very different approaches.

Six examples of goal-oriented PPP have been studied.

Cyber Growth Partnership (CGP) in UK[11] is the PPP created by the government in 2013 in order to identify the barriers for the growth of the cybersecurity industry in the country. The initiative came from the private sector, which wanted to work with the government. The goal of the CGP is to let the cybersecurity sector grow and to support its initiatives (e.g. a scheme which allows a company to publicly advertise that it sells solutions and services to the British Government). CGP also creates the opportunity for the industry to be promoted abroad and export its products and services. The PPP members are both national and international companies. The only criteria for participating is that the company must have a large cyber security presence/ investment in the UK. Every year the government carries out the process of membership renewal as only a limited number of companies are invited to join the PPP. The role of the Cyber Growth Partnership has now changed to provide only strategic advice and guidance to the government.

Security Made in Luxemburg (SMILE)[12] is the PPP created by the Ministry of Economy in 2010. It was created in order to provide services in the fields of behavioural, organisational and technical security. The government faced challenges in hiring experts with necessary skills and knowledge. For this reason, the SMILE was created to employ specialists to assist the Ministry in its most challenging tasks. Eventually, the government plans to use SMILE to create the PPP together with the industry and deliver specific services to support the GDPR and NIS legal acts. In this light, the Ministry of Economy is choosing nonexclusive partners who can deliver high quality services in the field of cybersecurity. They are to be cybersecurity-related companies, not necessarily from Luxemburg but also from other countries.

Spanish Technology Platform on Industrial Safety[13] was created in 2007 as the industry safety organisation. Currently due to the increase of cyber threats, it focuses on critical infrastructure protection, the Internet of Things and Industry 4.0. This PPP focuses mainly on research and development of new technologies to increase the level of security in the private sector. Cybersecurity is just one of the aspects of its activity The basis for this partnership is set up in third sector associations under Spanish law. The government uses this platform as a partner in creating strategy and initiatives in the field of cybersecurity in Spain.

AEI Ciberseguridad y Tecnologías Avanzadas[14] **in Spain** was created in 2008 by the industry in order to provide to the Spanish cybersecurity companies the opportunity to promote its services and products in Europe, as well as to get access to European funding. It is led by the industry itself and involves INCIBE (National Institute of Cybersecurity – El Instituto Nacional de Ciberseguridad) and the local government of Castilla y León.

[11] https://cyberexchange.uk.net/#/about
[12] https://securitymadein.lu/
[13] http://www.pesi-seguridadindustrial.org/index.php?option=com_content&view=article&id=31&Itemid=42&lang=en
[14] https://www.aeiciberseguridad.es/

Cyber Security Platform (CSP) in Austria[15] was created in 2011, when the government realised that cybersecurity is a very important issue. Thus, the country's first Cybersecurity Strategy was created. The platform is the implementation of Austrian Cybersecurity Strategy. The government decided that because the CI sectors will be affected by the new European legislation (minimum standards and mandatory incidents reporting) experts should be involved in the implementation process at the beginning. The cooperation was established to involve the CI sectors in drafting the cybersecurity law. They can provide input in the Austrian legislation. It was a new approach of the government. Before that it was usually the government that instructed the industry what to do.

Cyber Security Council in Netherlands[16] was created in 2011, when cybersecurity was also recognized as a priority by the government and the first Cybersecurity Strategy in the country was created. The Council is an element of implementation of the Strategy and was established in order to lift cybersecurity as a subject to a high political level and to start discussion about strategic issues. The Cyber Security Council is a formal independent strategic advisory council (it gives solicited and unsolicited advice to the Dutch government) and its main task are to monitor the Cyber Security Strategy implementation; give strategic advice on new technological developments; and contribute to research in the scope of the Dutch Cyber Security Research Agenda. It consists of highly-placed representatives of the industry, public administration and academia. It is governed by both the public and private sector (co-chairmanship) with the secretariat provided by the government.

Cyber Security Commission (CSC) in Slovakia
The Slovak Cyber Security Commission (CSC) was established in 2016 by the Cyber Security Concept and Action Plan. CSC is an advisory body of the National Security Authority´s Director. It is a platform created under the governance of the Slovak NSA and consist of the representatives of a public sector, private sector and academia and presents a very efficient and effective platform, that supports the NSA´s Director. It is a very important element for addressing the needs and knowledge from private sector and academia to the decision makers (NSA Director) mostly before the strategic issues are discussed at the political level.

Main activities

Goal-oriented PPPs have a high-level role in providing strategic guidance and consulting governments about innovation; providing guidance and recommendation for new law creation, and supporting the development of the cybersecurity industry.

Services delivered by this type of PPP are:

- Research and analysis
- Development of good practices and guidelines
- Defining standards
- Awareness raising
- Strategic planning
- Security audits

[15] As this initiative was created to support the implementation of the Austrian Cybersecurity Strategy it is marked as goal oriented. However, since it continues to exist through the next CSS, it could be also categorized as institutional. It depends on the initial motivation.

[16] Similarly, to the Austrian model, this was created in the light of the implementation of the NCSS. However, it exists even today after the 3rd version of the strategy.

- Cyber Exercises and drills
- Crisis management
- Emergency planning
- Resilience planning

Actors involved

Goal-oriented PPPs involve many stakeholders. The first actor is the cybersecurity industry (including cybersecurity companies, IT companies and other companies related to cybersecurity, critical infrastructure operators). Usually, the industry starts the initiative by expressing its needs to the public sector and by asking their support and assistance.

The second actor is the government, which addresses these needs and expectations by creating a PPP together with its structure that forms a base for mutual cooperation.

The last actor is academia, whose role is to create and develop solutions, jointly with the government and industry.

The governance model

All Goal-oriented PPPs have a clear structure and management model (chair, co-chairs), as well as supporting roles (secretariat). In general, the public sector has a stronger influence on the Goal-oriented PPP and co-ordinates the whole initiative. There are two exceptions: when the initiative is created by the industry itself, and when the industry has a dominant role. The government has only as an honorary member or observer.

- **Cyber Security Council in Netherlands**: governed by the public sector with the secretariat provided by the government
- **Cyber Security Platform (CSP) in Austria**: governed and coordinated by the public sector, with the secretariat provided by the government (Federal Chancellery)
- **Security Made in Luxemburg (SMILE)**: governed by the public sector, with the management board and the president both from the government
- **Cyber Growth Partnership in UK**: co-chaired by a government Minister and a CEO from large-scale company, with the board consisting of the industry members and secretariat provided by government
- **AEI Ciberseguridad y Tecnologías Avanzadas in Spain**: governed on an equal basis by members from the industry. The work of the of the whole initiative is organised in the working groups, where chairs are chosen during an election process. There is also the management board which keeps the proportional level of representation of all members.
- **Spanish Technology Platform on Industrial Safety**: led by private research entity, which also managing the office for the whole platform. The Ministry of Economy participates in the board.

Funding options

Goal-oriented PPPs are mostly founded by government subsidies (SMILE in Luxemburg, Cyber Security Council in Netherlands, AEI in Spain, Cyber Growth Partnership in UK, Spanish Technology Platform for Industry). Also, members own time and willingness to participate in PPP activities is important. Since the meetings are usually organised by the government or leading organisation and all members are invited to participate. Some of the Goal-oriented PPP are also funded by mandatory fees, depending on the size of the PPP member institution (both initiatives in Spain). Based on the interviews the diagram below shows the most common funding options (for all types)

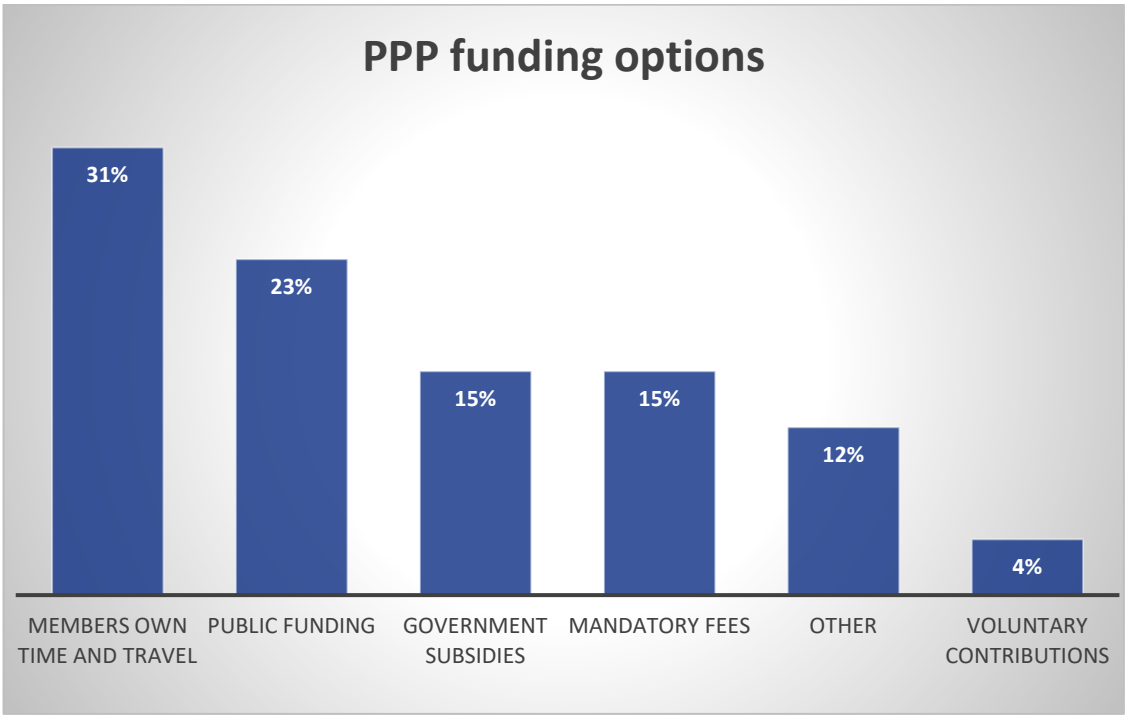

Figure 6: PPP funding options

PPP interaction

Goal-oriented PPPs are long-term communities that observe and provide advice on strategic development to governments. They interact through regular face-to-face meetings, and also use email and teleconferences to stay in touch between these meetings and to work in the forum of working groups, which are usually established during regular meetings and work on specific subjects (e.g. energy sector specific requirements). In one case, the so called "per rollam" meetings are being used, so that to ensure that the committee or board can vote in writing without covering face-to-face meeting.

Expert interviews resulted in a few findings regarding goal-oriented PPP' interaction. The first is to be open and collaborative with the industry. The industry views need to be recognised, otherwise their interest is lost and cooperation is in jeopardy. The second is that in this type of PPP it should be the government that keeps leading the initiative and ensures that the organization is to highest extent useful for its members.

3.3 Outsourcing cybersecurity services

Outsourcing cybersecurity services (OCS) occurs when the government recognises the needs of industry, but cannot address them. For this reason, the PPP becomes a stand-alone organisation that can offer services. PPPs which are outsourcing cybersecurity services address the industry needs and support the government in the policy making process (e.g. NIS implementation, drafting national cybersecurity strategies).

The main task of the outsourcing cybersecurity services is to raise the cybersecurity awareness and cybersecurity level amongst stakeholders.

Two examples of outsourcing cybersecurity services have been analysed.

Kuratorium Sicheres Österreich (KSÖ) in Austria.

Created in 1975 as a private association funded as a part of the Ministry of the Interior (MoI). In 2010 it became a self-contained, overarching umbrella organization with close relations to the Ministry. At the beginning the KSÖ focused on national and physical security. In 2011 the KSÖ and the MoI started a "Cybersecurity Initiative" and the KSÖ opened the way for a national cybersecurity dialog. The aim was to rise overall awareness in the field of cybersecurity (in particular to highlight that cybersecurity is not only a topic for the technical specialists, but an issue that concerns everyone). KSÖ's expertise was used in the national cybersecurity strategy and currently the organisation is contributing to cybersecurity law preparation (NIS Directive implementation). In 2015, the KSÖ created the "Cybersecurity Forum", which involved industry representatives (mainly critical infrastructure operators) who meet and discuss best practices and challenges in the field of cybersecurity. The KSÖ offers the "Cybersecurity Forum" as service for more enhanced information sharing. By 2018 the Forum will be transformed into a "Security Platform Digital Security" to include more actors from the private sector.

UP KRITIS in Germany.

UP KRITIS is the PPP created in 2007, which is a joint initiative of critical infrastructure operators and governmental agencies involved in critical infrastructure protection. At the beginning, UP KRITIS was created for the Implementation of the action plan for Critical Infrastructure protection, prepared jointly by the government and the critical infrastructure operators. Then, in 2013, when the implementation of the action plan was finished, the UP KRITIS as an acronym started to be used as the name of the PPP, which brings together the private and public sector experience and promotes cross-company and cross-sectoral communication and cooperation, so that the critical infrastructure protection in Germany could be enhanced (e.g. by preparing recommendations). UP KRITIS is also used as a platform for fast and reliable communication in crisis management. UP KRITIS involves 500 organisations from all over Germany.

Main activities

OCS is closely linked to the critical infrastructure protection. It delivers services which are supporting critical infrastructure operators and raises the overall cybersecurity level in critical sectors. These constituent services are:

- Research/ analysis
- Development of good practices and guidelines
- Information exchange
- Early warnings
- Exercises
- Awareness raising
- Defining standards
- Crisis management

- Resilience planning
- Emergency planning
- Security audit
- Benchmarking
- Strategic planning
- Risk analysis

Prepared jointly by the private and public sector, all these services support governmental policy and activities.

Actors involved

All critical infrastructure sectors are involved in OCS PPP along with governmental institutions, such as national competent authorities, cyber security agencies, national intelligence authorities and law enforcement. This provides for a unique synergy of knowledge and creates conditions to exchange the knowledge and develop solutions for upcoming challenges.

The governance model

There are different approaches to governing OCS PPP. The first one is when an organisation is appointed by the government to support the critical infrastructure protection. This organisation provides the secretariat and organises meetings for the whole initiative (amongst others prepares the agenda). The decisions are made on a consensus basis, so that the industry is certain that every voice is taken into consideration. The other when the public sector governs the PPP itself (including providing the secretariat) but some decisions are delegated to the industry.

Funding options

OCS PPP are funded by mandatory fees and government subsidies or a combination of both[17]. Worth to highlight is the fact that for the private companies it is not easy to pay membership fees. The cybersecurity specialists have difficulties in explaining to their companies the reason why it is profitable to pay for the membership in a PPP.

PPP interaction

OCS are long-term communities with working group set up to solve specific challenges. They interact by regular face-to-face meetings. Very important is their role of advisors to governments in creating cybersecurity policy and law.

3.4 Hybrid PPPs

Hybrid PPP is actually a combination of outsourcing cybersecurity services and institutional PPP. It occurs when the government does not have enough resources to deliver necessary cybersecurity solutions on a national level and starts cooperation with the private entity which has the appropriate expertise and can deliver these solutions. Hybrid PPPs are strongly connected to delivering CSIRT services on both governmental (i.e. public administration) and national (i.e. economic sphere) level.

Two examples of such initiatives have been analysed.

[17] For example, in Austria, there are not fees for the Cybersecurity Initiative as the projects are funded by the MoI; whereas the companies belonging to the Cybersecurity Forum pay a membership fee as they benefit from specific services exclusively available to them.

Governmental CERT (Gov.CERT) in Austria. When the government in Austria came to the conclusion that a governmental CERT was needed, the decision has been made to pay for this service. The best candidate was the national domain register – private company which was already operating the national CERT. The Gov.CERT and national CERT are actually the same entities with two different titles, but the head of the Gov.CERT is the Director of one of the Departments in the Federal Chancellery in Austria; apart from that, the Federal Chancellery is hosting the Gov.CERT. This is an interesting approach when the security-sensitive service is being outsourced to a private company. The obvious advantage of this approach is the fact that Gov.CERT has no "police functions".

CSIRT.CZ national CERT in Czech Republic, operated by CZ.NIC. CZ.NIC is a non-profit organisation established in 1998 by internet service providers and operates domain register in the country. It has 114 members. At the beginning, the CERT was operated on an informal basis, but the cybersecurity law established two CERTs – governmental and national. There was a public call to establish a national CERT and CZ.NIC won it.

Main activities

The core activities are CSIRT services both national and governmental.

Beside this, hybrid PPPs organise meetings for their constituencies and deliver presentations on specific issues, so that cybersecurity awareness could be raised. The other type of activity is supporting police authorities in cybercrime investigations, as well as website scanner services which focus on penetration testing of websites (CSIRT.CZ).

Actors involved

Actors involved in hybrid PPPs depend on the CSIRT constituency. National CSIRTs are teams which "have been granted a mandate from government to carry out tasks of coordinating and supporting incident handling within the state borders and acting as CERTs – of – last – resort domestically and official point of contact for n/g CERTs in other countries" (ENISA, 2016). At the same time, the governmental CSIRTs are teams which constituencies are public administration networks. Currently "in the EU, governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure as well as to ensure cyber-crisis management" (ENISA, 2016, p. 9).

The governance model

The governance structure is linked to the structure of organisation which leads the PPP. If the host has a hierarchical structure, also the PPP is governed hierarchically (Gov.CERT in Austria), and while the host have less formal approach, it applies also to the PPP (CSIRT.CZ – CZ.NIC is governed by the Collegium of three chambers elected from the members and three representatives appointed by the government).

Funding options

Hybrid PPPs are funded by hosting organisations. CZ.NIC collect entrance fee from its members (1 000 Euro) and allocates part of this money to the CSIRT, while the Gov.CERT in Austria is funded by the Federal Chancellery and public administration entities may participate in this PPP free of charge.

PPP interaction

Hybrid PPPs are long-term communities with a goal of increasing the cybersecurity level. They interact via face-to-face meetings twice a year, where new regulations (e.g. NIS directive) and case studies on the incidents, as well as best practices are being discussed. All members are welcome to participate in these meeting.

Sometimes hybrid PPP interacts also through mailing conferences in order to support the face-to-face meetings and to keep contact amongst PPP members also between the meetings.

4. Trust building

Building trust between public-private, private-private and public-public entities has been recognised as the one of the biggest challenges of PPP; yet maintaining it could be even more challenging. Most PPPs define trust as an ongoing process, that involves personal relations and consumes a lot of time. In the maintenance of a PPP, trust may be lost in the case of either new member joining, or members being inactive or taking advantage of the services that a PPP offers without contributing to any of the defined duties.

In many PPPs the whole process of trust building is starting from the very beginning. In many cases it happens that members tend to change workplaces or are being assigned to new tasks, so they no longer attend the meetings of the PPP. This means that trust is not always continuous and most of the times not stable. It was pointed out by many experts that trust is built mainly through common working experiences and long lasting cooperation.

There are several mechanisms which support trust building and used by PPP which are presented below:

- Face-to-face meetings: these meetings are defined as vital because trust between partners is built through co-ordination and exchanging information face to face. This type is one of the strongest interactions for effective information exchange.
- Regular meetings: Regular meeting is another form of building trust as all members are obliged to get involved in systematic and scheduled meeting over the year.
- Social events: the participation in social events is becoming required in a partnership as it will help all members to know each other and it will help build the relationship between them.
- Thematic conferences: the focus in a thematic area will help all experts to exchange their ideas and share information. Thematic conferences are taking place when members are all centred towards one definite topic.
- Thematic trainings: one of the instructional methods of bringing together experts from different topics to getting trained on a specific theme. This type of building trust is so creative that members are enabling themselves to notice the inter-relatedness of different subjects.
- Joint exercises.
- Governmental industry support (e.g. preparing recommendations and good practices).
- Value of the knowledge shared in real time incidents.

Face-to-face meetings, regular meetings and social events are considered as the most effective tools of trust building as they contribute to build long term partnerships. Personal qualitative interaction between the members of the PPP is considered as a key point for successful PPP.

In the process of building trust, the need for a “manager” would be considered catalytic as he/she would be someone who believes in the cause of, who is devoted to the presence and maintenance of it and by this attitude inspires others to get involved and to collaborate.

PPP with high level of trust are obviously more efficient – they recognise the needs of both public and private sector and they are able to address them through cooperation.

5. Overview of PPP in Europe

Evolution since 2012

Since 2012 more Member states invested in collaboration to enhance nationally cyber security. In 2012 the ENISA Good Practice Guide (GPG) provided insights on how to create a partnership; this report gives food for increasing sophistication and offers guidance on the formalisation of partnerships.

From one perspective this is foreseen in the adopted National cybersecurity strategies. Back in 2012 not more than 12 countries had a strategy, whereas today all 28 MS have published a national strategy plan for cybersecurity. From a different angle, it is evident that incentives for collaboration between public and private sector have been recognised by many stakeholders, such as economic and qualitative incentives deriving from information sharing. The creation of specific types of PPP, namely ISAC (Information Sharing and Analysis Centre) indicate an increase in sophistication.

Today more than 15 MS have an official PPP than the MS that had official PPPs in 2012. In many cases partnerships are created to conduct a specific project i.e. a national cyber security exercise or a cybersecurity awareness campaign (European Cybersecurity Month). It is very important to notice that since the first GPG, sectorial PPPs have been created in the EU following the approach of the US. This again is an indication of maturity and sophistication on the approach towards cybersecurity.

It is evident that partnerships require a clear framework specifying the roles of the public and private sectors, their relationships and the areas for co-operation. This topic is raised again as the scenery of cybersecurity is very volatile and has been through many changes the past years. If organisations are to face coherent, straightforward and effective regulatory and/or non-regulatory requirements, public-private co-ordination needs to be optimised. Moreover, the topic of trust is raised again, as trust is the adhesive power for a valuable collaboration.

This guide will feed back some of the experiences of those already involved with PPPs and provide advice to those setting up new PPPs or evolving/improving an existing one through presenting EU specific experience.

The map below presents an overview of PPP in Member States. In the annex more information on the status of PPP in each MS is presented.

Country	Examples of PPP
Austria	Cybersecurity Forum
Belgium	Flemish PPP Knowledge Center, Wallonian PPP Unit
Czech republic	CZ.NIC
Estonia	Information System Authority
Finland	National Emergency Supply Organisations' pool and sector system
France	CDC, MAPPP, CEFO-PPP, CPPP, Institute de la Gestion Déleguée
Germany	UTFP, Fondo PPP Italia
Ireland	Central PPP Policy Unit, Irish eTenders
Latvia	PPP Association
Luxemburg	Smile
Malta	MIMCOL
The Netherlands	Cyber Security Council and NCSC Council 'CEO Breakfast'
Poland	NASK, RCB
Slovak Republic	Cyber Security Commission, Slovak Association for Information Security
Spain	Spain
United Kindom	Cyber Growth Partnership, CiSP, Infrastructure UK

Figure 7 - EU PPP overview examples

6. Challenges and gaps

Lack of human resources in both the public and private sector.

Insufficient allocation of human resources in the development and evolution of PPPs is considered as a major challenge. Governments usually don't involve enough people as they don't consider PPP as a priority and the private sector resources are usually occupied with business-as-usual tasks. Because of this, many PPP are not as effective as they could be.

Insufficient public sector budget and resources fail to meet the private sector's expectations.

Lack of public sector budget and resources is one of the key challenges for PPP. The public sector resources and budget should be identified at an early stage. Governments often do not provide enough money for the development of PPP. At the same time, the public sector has a long-time perspective when developing the strategy and an action plan for the PPP. On the other hand, the private sector works in a dynamic framework, which means that strategy and action plans can be created only for a few years.

The establishment of a common level of understanding and dialogue between the public and private sector.

It is very difficult to create a common language to communicate clearly within a PPP. Different organisations use different language. Lack of common perception on things can create misunderstandings that are difficult to handle and solve. It is difficult to get common understanding on how the private sector works and how the public sector works. What is strategic, what is operational and what is technical might mean completely different thing in the different environment and work culture.

Promotion of the concept of PPP among SMEs. SME's usually do not have the resources or relevant experience to participate in PPPs. Encouraging SMEs to participate could be beneficial for them as they would gain experience from larger players.

Lack of leadership and legal basis. Hesitation in taking the leadership and disinterest of the government discourages private sector's participation. Sharing of knowledge and experience and actively participate in discussions and activities enhances the efficient development of the PPP. In addition, it is very frustrating for the private sector to witness disagreements between key public institutions and delays in taking decisions. The private sectors expect government to act. Having a legal basis will allow each party involved to know exactly their role and responsibilities, what kind of input must provide and what kind of benefit should expect.

7. Recommendations for effective PPP

Recommendation1: Motivation for the private sector to participate should be a priority when establishing a PPP.

What is clearly visible in every analysed model of PPP is the fact that to create successful and efficient PPP, resources are needed. These kind of collaborations need a driving force to stimulate them, so that it could be really vital. It is not enough to provide incentives and money. PPPs will not grow if there is lack of people who will work on them. A PPP really need someone who interacts with every member of the partnership; drives agenda, set up the meeting and keeps strategic perspective. PPPs need a whole group of people who prepare the action plans and work closely with both public administration and the industry. The most sophisticated PPPs are usually NGOs or institutions created only to build and strengthen cooperation and collaboration between public and private sector.

Recommendation 2: The participants should agree to a legal bases when creating a PPP.

As long as there is no legal basis for the cooperation, the whole process of creating and developing a PPP will be slow and not efficient.

Legal basis could be a national legal act or a Memorandum of understanding. Cybersecurity is cross-horizontal area in which many public entities are usually involved together with various private companies. Because of that, having specific rules which apply to everyone are very useful – they should set up the framework of the whole cooperation and every member should know what kind of input they should provide and what kind of benefits they may expect from PPP.

Recommendation 3: Public institutions should lead the PPP or the national action plan for PPP

It is very frustrating for the private sector representatives to witness disagreement between key public institutions. Private sector expects government to act. If the public sector could agree for the one contact point for PPP, that could be enormously beneficial for the overall PPP.

Since cybersecurity is highly interdisciplinary, there are usually many public bodies involved in PPP – Ministry of Internal Affairs, Ministry of Defence, Ministry of Economy or Development to name only a few. It is very important for public administration to communicate clearly and honestly their needs and limitations to the private sector.

The point of contact is perhaps just the most visible aspect, the tip of the iceberg. But what is much more important is the fact that government entities involved in a PPP should know in advance - ie, before inviting private sector partners to join - what they want to achieve, what their contribution is going to entail, and what the private sector should contribute. Or to put it shortly: get the strategy right before you join the PPP.

Recommendation 4: PPPs should invest on internal private-private and public-public collaboration

PPP is about private-private, public-public and private-public cooperation. Focusing only on the relationships between public and private sector could be very short-sighted for the PPP policy. The right level of dialog and understanding between public agencies is often the key to successful PPP.

The same applies to the private sector. The successful PPP integrates not only private administration and the industry, but also different entities among the industry (e.g. energy companies, banks, telecoms).

For this reason, the PPPs all over the EU should focus also on private-private and public-public cooperation and collaboration.

Recommendation 5: PPP participants should invest on open communication and a pragmatic approach towards building a PPP

If the members of PPPs do not communicate in an honest and open way, they can be victims of their expectations, which neither private nor public sector will be able meet.

It is crucial that both public and private sector are pragmatic and see the broader goal – increase the level of the cybersecurity – for the PPP to be more successful. Usually the industry as well as the public sector have specific, different expectations. It is very helpful if they speak openly with each other in order to understand and possibly meet each other's expectations, which usually requires compromise.

Recommendation 6: The representatives of the government should be allowed to participate in the meetings with non-disclosure agreement

Nothing discourages private sector as much as hesitation and disinterest of the government. For PPP to work and develop efficiently, public servants should not only participate in meetings but also get involved – share their knowledge and experience with the industry and openly take part in discussions and activities. The private sector strongly believes in reciprocity rule.

If the private sector participates and deliver knowledge/resources, the public sector should do the same as well.

Recommendation 7: Small and Medium Enterprises (SMEs) should also participate in PPPs

Usually, only big companies are involved in the PPPs. SMEs do not have enough resources to get involved and they do not recognise that a PPP could be helpful. It would be useful also from a societal perspective to involve other types of stakeholders like SMEs and start-ups in the PPPs to help them gain experience from larger players in the field. Promoting the concept of PPPs amongst SMEs would be also very beneficial for increasing the level of NIS in Europe and more especially when those SMEs provide third party services to larger organisations or/and critical service providers.

8. Bibliography/References

Andersen H., Cao F., Tvarnø C.D., Wang P., Public-Private Partnerships: An international analysis - from a legal and economic perspective, EU Asia Inter University Network for Teaching and Research in Public Procurement Regulation, August 2010. http://openarchive.cbs.dk/bitstream/handle/10398/8422/public-private_partnership.pdf?sequence=1

Asian Development Bank, Public-Private Partnership Handbook, ADB, Manila, 2008. https://www.adb.org/documents/public-private-partnership-ppp-handbook

Asian Development Bank, Public–private partnership operational plan 2012–2020: Realizing the vision for Strategy 2020—the transformational role of public–private partnerships in Asian Development Bank operations, ADB, Manila, 2012. https://www.adb.org/sites/default/files/institutional-document/33671/ppp-operational-plan-2012-2020.pdf

Benedict Ruth, Patterns of culture, Houghton Mifflin Company, Boston 2005, p. 46.

Carr, M., 'Public–private partnerships in national cyber-security strategies', International Affairs, International Affairs , vol 92 , no. 1 ., 2016, pp. 43-62 https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

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, July 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

Corrigan, Mary Beth, et al., Ten Principles for Successful Public/Private Partnerships, ULI - the Urban Land Institute, Washington DC, , 2005. http://uli.org/wp-content/uploads/2005/01/TP_Partnerships.pdf

CropLife International aisbl, Working together to help farmers: The benefits of the Public-Private Partnership, CropLife International, Brussels, May 2012. https://croplife.org/wp-content/uploads/pdf_files/The-Benefits-of-Public-Private-Partnerships.pdf

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

European Commission, Impact of the Energy-efficient Buildings Public-Private Partnership Workshop report April 2015 in Brussels, Publications Office of the European Union, 2015. http://www.streamer-project.eu/Downloads/Interview_PPP_Impact_Workshop_Report.pdf

European Commission, Impact of the SPIRE Public-Private Partnership Report of the Workshop held on 21-22 April 2015 in Brussels, Luxembourg: Publications Office of the European Union, 2015. https://www.spire2030.eu/uploads/IMPACT_WORKSHOP/KI0115513ENN_002.pdf

European Commission, 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, May 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192

European Commission, Guidelines for Successful Public–Private Partnerships, European Commission, Brussels, 2003.
http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf

European Cyber Security Organisation, European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for contractual Public-Private-Partnership (cPPP), June 2016 http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

European Investment Bank, The EIB's role in Public-Private Partnerships (PPPs), EIP, July 2004.
http://www.eib.org/attachments/thematic/eib_ppp_en.pdf

European PPP Expertise Centre, A Guide to Guidance Sourcebook for PPPs in TEN-Transport, EIB, May 2010.
http://www.eib.org/epec/resources/guide-to-guidance-in-ten-transport.pdf

Fraunhofer Institute for Systems and Innovation Research ISI, Public-private partnership in Research and Innovation – Case studies from Australia, Austria, Sweden and the United States, Fraunhofer ISI, Karlsruhe 2015. http://www.isi.fraunhofer.de/isi-wAssets/docs/p/de/publikationen/forschungscampus/Forschungscampus_case-studies_2015.pdf

Hall, D., Why Public–Private Partnerships Don't Work: The Many Advantages of the Public Alternative, Public Services International Research Unit, London, 2015
http://www.world-psi.org/sites/default/files/rapport_eng_56pages_a4_lr.pdf

Hamel P. J., 'Public-Private Partnerships (P3s) and Municipalities: Beyond Principles, a Brief Overview of Practices', INRS-Urbanisation, Culture et Société, Montréal, 2007
https://www.fcm.ca/Documents/reports/Public_Private_Partnerships_P3s_and_Municipalities_Beyond_Principles_a_Brief_Overview_of_Practices_EN.pdf

Instituto di Ricerche Sulla Pubblica Amministrazione, Global harmonization through public-private partnership: The case of pharmaceuticals, IRPA GAL Working Paper, Rome 2012/2. http://www.irpa.eu/wp-content/uploads/2012/01/IRPA.WP.2012.2.Dagron.pdf

International Monetary Fund, Public-Private Partnerships, 2004, IMF, Washington DC, 2004.
https://www.imf.org/external/np/fad/2004/pifp/eng/031204.pdf

Interreg Central Europe, Country report on the legal framework on Public-Private Partnership (PPP): SLOVENIA Version 1, November 2016. http://www.interreg-central.eu/Content.Node/RESTAURA/D.T1.2.1-Country-report-Slovenia-V1.pdf

Joint Communication to the European Parliament and The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, September 2017, http://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF

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, JOIN(2013), February 2013, http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

KS, Jomo, Anis Chowdhury, Krishnan Sharma, and Daniel Platz 'Public-Private Partnerships and the 2030 Agenda for Sustainable Development: Fit for purpose?', UN/DESA Working Paper. UN/DESA, 2016,.
http://www.un.org/esa/desa/papers/2016/wp148_2016.pdf

McKee M, Edwards N, Atun R. 'Public-private partnerships for hospitals.' Bulletin of the World Health Organization, 2006, 84(11):890-896.
http://www.who.int/bulletin/volumes/84/11/06-030015.pdf

McQuaid R. W., Scherrer W., Public Private Partnership in the European Union: Experiences in the UK, Germany and Austria, Uprava, letnik VI, 2/2008 http://uprava.fu.uni-lj.si/index.php/IPAR/article/viewFile/105/102

Ministry of Finance Singapore, Public private partnership handbook version 2, MOF, Singapore, March 2012 ttps://app.mof.gov.sg/Portals/0/Policies/ProcurementProcess/PPPHandbook2012.pdf

National Telecommunications and Information Administration, BroadbandUSA: An introduction to effective public-private partnerships for broadband investments, NTIA, Washington DC, January 2015 https://www2.ntia.doc.gov/files/ntia_ppp_010515.pdf

OECD, 'Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships', OECD Publishing, May 2012,
https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf

Rall, J., Reed, J. B. and Farber N.J. Public-Private Partnerships for Transportation: A Toolkit for Legislators. he National Conference of State Legislatures, Washington DC, 2010.
http://www.ncsl.org/documents/transportation/ppptoolkit.pdf

Sabol, Puentes, Private capital, public good. Drivers of successful infrastructure public-private partnerships. The Brookings Institution, Washington DC, December 2014
https://www.brookings.edu/wp-content/uploads/2016/07/BMPP_PrivateCapitalPublicGood.pdf

Scribner, M. The Limitations of Public-Private Partnerships: Recent Lessons from the Surface Transportation and Real Estate Sectors, Competitive Enterprise Institute, Washington DC, 2011
https://cei.org/sites/default/files/Marc%20Scribner%20-%20The%20Limitations%20of%20Public-Private%20Partnerships.pdf

Technopolis Group, Increased coherence and openness of European Union research and innovation partnerships final report, Technopolis group, June 2017 http://www.technopolis-group.com/wp-content/uploads/2017/08/eu_ri_partnerships_final_report.pdf

The World Bank, The Role and Impact of Public-Private Partnerships in Education, The World Bank, Washington DC, 2009 http://www.ungei.org/resources/files/Role_Impact_PPP_Education.pdf

United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), A guidebook on public-private partnership in infrastructure, UN, Bangkok, 2011
http://www.unescap.org/sites/default/files/ppp_guidebook.pdf

United Nations Educational, Scientific and Cultural Organization, A New Dynamic: Private Higher Education, UNESCO, France, 2009. http://unesdoc.unesco.org/images/0018/001831/183174e.pdf

United Nations Global Compact, The Role of Governments in Promoting Corporate Responsibility and Private Sector Engagement in Development, UN Global Compact, New York, 2010.
http://www.vub.ac.be/klimostoolkit/sites/default/files/documents/role_of_governments_in_csr.pdf

Verger, A., & Moschetti, M. Public-Private Partnerships as an Education Policy Approach: Multiple Meanings, Risks and Challenges. UNESCO - Education Research and Foresight Working Papers, 19., 2017.
http://unesdoc.unesco.org/images/0024/002473/247327e.pdf

Witters, Louis, Revital Marom, and Kurt Steinert. 'The role of public-private partnerships in driving innovation', The Global Innovation Index, INSEAD, Fontainebleau, 2012, pp. 81-87.
http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2012-chapter2.pdf

World Bank, Public-private partnerships : reference guide version 2.0., 2014. World Bank Group, Washington DC, 2014
http://documents.worldbank.org/curated/en/600511468336720455/Public-private-partnerships-reference-guide-version-2-0

World Bank, Toolkit for Public Private Partnership in Roads and Highways, World Bank, Washington DC, 2009.

Annex A: PPP in the Members States

Country	Austria
Cybersecurity system (main institutions)	Fenderal Chancellory, Ministry of Interior, CERT.Gov, national CERT
PPP	National CERT – CERT.at (https://www.cert.at/) Cybersecurity Forum

Country	Belgium
Cybersecurity system (main institutions)	CERT.be Cybersecurity Centre
PPP	Flemish PPP Knowledge Center, Wallonian PPP Unit

Country	Bulgaria
Cybersecurity system (main institutions)	CERT Bulgaria Ministry of Infrastructure
PPP	Ministry of Finance

Country	Croatia
Cybersecurity system (main institutions)	National CERT
PPP	Agency for Public-Private Partnership

Country	Czech Republic
Cybersecurity system (main institutions)	CZ.NIC https://www.nic.cz/ National Security Authority
PPP	CSIRT CZ https://csirt.cz/

Country	Cyprus
Cybersecurity system (main institutions)	National CERT
PPP	

Country	Denmark
Cybersecurity system (main institutions)	Centre for Cyber Security, Council for Digital Security The Centre for Cybersecurity operates as the national competent authority for network and information security in Denmark. It

	administrates GovCERT and acts as a central government repository of incident and cybersecurity data.
PPP	Danish Business Authority The Council for Digital Security is a security and privacy advocacy group comprised of 20 private sector and academic organisations. Furthermore, Dansk IT , a representative body for information technology professionals in Denmark, engages with cybersecurity in the course of its operations.

Country	**Estonia**
Cybersecurity system (main institutions)	Information System Authority https://www.ria.ee/en/ CERT Estonia
PPP	Information System Authority

Country	**Finland**
Cybersecurity system (main institutions)	Cybersecurity system (Main institutions) - National Cyber Security Center (NCSC-FI - National Emergency Supply Agency (NESA)
PPP	National Emergency Supply Organisations' pool and sector system

Country	**France**
Cybersecurity system (main institutions)	ANSSI (The National Agency for the Security of Information Systems) CERT.FR
PPP	Vinci, Bouygues, Eiffage, Spie Batignolles, Demathieu & Bard, NGE, Malet, Veolia, Dalkia, Egis CDC (Caisse des Depots et Consignations) MAPPP (Mission d'Appui aux Partenariats Public-Privé), CEFO-PPP (Centre d'Expertise Français pour l'Observation des Partenariats Public-Privé) CPPP (Club de Partenariats Public-Privé) Institute de la Gestion Déleguée (The French Institute for PPP)

Country	**Germany**
Cybersecurity system (main institutions)	BSI (Federal Office for Information Security) National CERT CERT-BUND
PPP	Lower Saxony: PPP Task Force North-Rhine-Westphalia: PPP Task Force UP KRITIS http://upkritis.de/, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.html

Country	**Greece**

Cybersecurity system (main institutions)	Ministry of Digital Policy National CERT
PPP	-

Country	**Hungary**
Cybersecurity system (main institutions)	National Security Authority Cyber Security Centre CERT-Hungary
PPP	-

Country	**Italy**
Cybersecurity system (main institutions)	CERT
PPP	Fondo PPP Italia, Unità tecnica Finanza di Progetto (UTFP) - Italian PPP Task Force

Country	**Ireland**
Cybersecurity system (main institutions)	CERT within one of the Ministry
PPP	Central PPP Policy Unit Irish eTenders

Country	**Latvia**
Cybersecurity system (main institutions)	CERT.LV
PPP	CFLA (Central Finance and Contracting Agency) Ministry of Finance PPP Association (Latvian)

Country	**Lithuania**
Cybersecurity system (main institutions)	CERT-LT State Information Resources Management Council
PPP	Not yet

Country	**Luxemburg**
Cybersecurity system (main institutions)	GOVCERT.LU https://www.govcert.lu/en/ Luxembourgish Cyber Security Board http://www.gouvernement.lu/

PPP	Smile https://securitymadein.lu/ http://www.luxembourg.public.lu/en/actualites/2015/06/09-cybersecurite/index.html

Country	**Malta**
Cybersecurity system (main institutions)	MITA (The Malta Information Technology Agency) CSIRT Malta
PPP	MIMCOL (Malta Investment Management Company Ltd) Ministry of Finance

Country	**The Netherlands**
Cybersecurity system (main institutions)	National Cyber Security Centre https://www.ncsc.nl/english
PPP	Responsible Disclosure https://www.ncsc.nl/security Strategic level: Cyber Security Council , and NCSC Council 'CEO Breakfast'; Tactical/Operational level: ISACs + Liaison officers + ICT Response Board + National Response Network + National Detection Network + Operational Incident Response Team network + 'Ecosystem' projects trade nexuses Port of Rotterdam and Schiphol Airport

Country	**Poland**
Cybersecurity system (main institutions)	Ministry of Digital Affairs Ministry of Internal and Police Department NASK – National Cybersecurity Center, CERT Polska Internal Security Agency – CERT.GOV.PL
PPP	NASK – Cooperation with essential services and digital services providers as well as CI operators RCB – Government Center for Security – cooperation with CI operators

Country	**Portugal**
Cybersecurity system (main institutions)	Centro Nacional de Cibersegurança Portugal The National Security Office (GNS) acts as the national competent authority for network and information security in Portugal. The GNS is directed by the National Security Authority, who is the sole authority with responsibility for the protection and safeguarding of classified information. The National Centre for Cybersecurity is run under the GNS and is the agency responsible for cybersecurity in particular.
PPP	There is no defined public-private partnership for cybersecurity in Portugal, however, the National Centre for Cybersecurity is tasked with liaising with the private sector in the course of its duties.

Country	Romania
Cybersecurity system (main institutions)	CERT-RO Intelligence Authority - CIP
PPP	-

Country	Slovenia
Cybersecurity system (main institutions)	SI-CERT
PPP	Cooperation between Bank Association of Slovenia and Police Department

Country	Slovak Republic
Cybersecurity system (main institutions)	National Security Authority http://www.nbu.gov.sk CSIRT.SK Ministry of Finance
PPP	Cyber Security Commission (CSC) http://www.nbu.gov.sk Partnership for Prosperity (PPP) http://www.p3.sk Slovak Association for Information Security http://www.sasib.sk Slovak PPP Association (Asociácia PPP)

Country	Spain
Cybersecurity system (main institutions)	CNPIC (National Centre for Critical Infrastructure Protection)
PPP	AEI Ciberseguridad y Tecnologías Avanzadas https://www.aeiciberseguridad.es/ Spanish Technology Platform on Industrial Safety http://www.pesi-seguridadindustrial.org/index.php?option=com_content&view=article&id=31&Itemid=42&lang=en SEITT (Sociedad Estatal de Infraestructura des Transporte Terrestre)

Country	United Kindom
Cybersecurity system (main institutions)	Department for Digital, Culture, Media and Sport– Digital Economy Minister National Cyber Security Centre https://www.ncsc.gov.uk/ Cabinet Office
PPP	Cyber Growth Partnership https://www.techuk.org/cyber-growth-partnership Infrastructure UK HM Treasury PPP Forum 'Cyber Information Sharing Partnership (CiSP) - www.ncsc.gov.uk/cisp '

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-06-17-317-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-241-7
DOI: 10.2824/076734