# EP3R 2010-2013

*Four Years of Pan-European Public Private Cooperation*

FINAL, 1.0, November 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

## 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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

## Author

The Author of this report is

- Lionel Dupré, ENISA

## Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

## Acknowledgements

This report echoes conclusions and observations of a research project carried out by FORMIT Foundation on a call for tender issued by the European Network and Information Security Agency (ENISA), under the 'European Partnership for Information and Communication security and resilience (EPIC)' label.

The main contributors to this report are:

- Simona Cavallini, FORMIT Foundation
- Fabio Bisogni, FORMIT Foundation
- Margherita Volpe, FORMIT Foundation

Further support was provided by Giampiero Gasperini, Edoardo Limone and Sofia Scoglio from FORMIT Foundation.

## Legal notice



## Copyright Notice



ISBN : 978-92-9204-119-9

DOI : 10.2824/565581

## Executive summary

The EP3R (European Public-Private Partnership for Resilience) was established in 2009 and was the very first attempt at Pan-European level to use a Public-Private Partnership (PPP) to address cross-border Security and Resilience concerns in the Telecom Sector. The EP3R participants initiated many discussions, saw a lot of commitment, and produced interesting conclusions. It also revealed some further needs in the security and resilient field and also some gaps to be filled in order to reach a higher maturity level of the Telecom Sector.

The EP3R closed down in April 2013, after 4 years of existence and practically 3 years of operations. The impact of the very first European Public -Private Partnership for Resilience had to be assessed and lessons had to be drawn for future similar initiatives and other funded actions for improving European resilience.

Generally, the PPP approach is judged to be particularly appropriate for addressing complex cooperation problems within multi-stakeholder scenarios. The case of EP3R is mirrored overseas by the National Council of ISACs[1] (*Information Sharing and Analysis Centres*) and many other similar initiatives. This underlines the appropriateness of the PPP approach to address cooperation issues as complex as the security and resilience ones.

The large number of PPP experiences worldwide has confirmed the value of such approach also for its flexibility and appropriateness for today emerging challenges including cyber-attacks mitigation, critical infrastructure protection and security and resilience of information and communications.

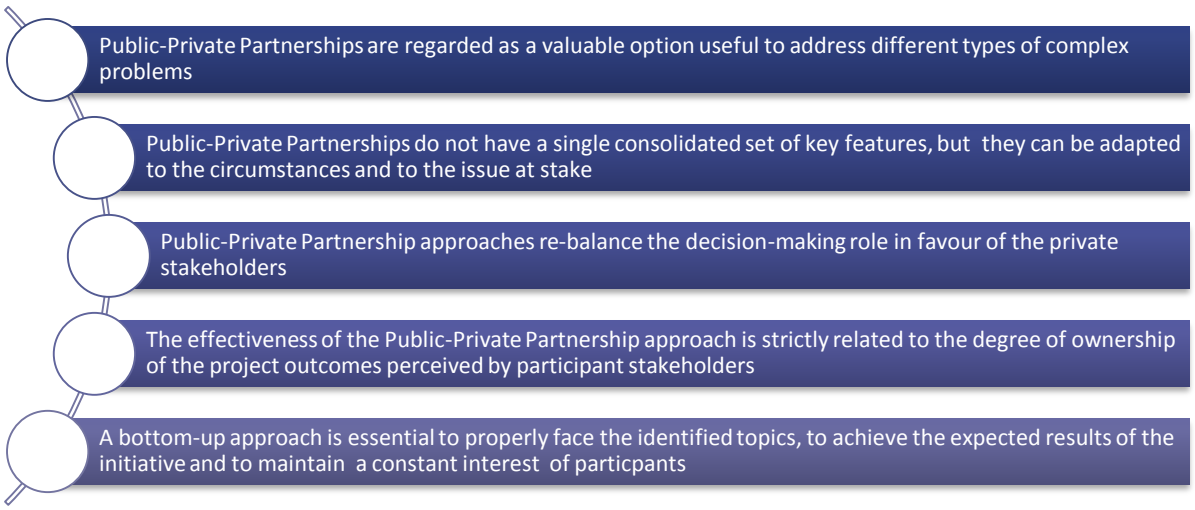
This study proposes to investigate the gap between expected optimal features of a Public Private Partnership for Resilience and its implementation in the EP3R, and bases its conclusions both on literature contributions and on a direct collection of information (i.e. interviews and surveys) with key EP3R actual and potential stakeholders (i.e. Chief information security officers, Security senior experts of both public and private European organisations).

The specific aim of this analysis was to:

- Review the experience of Public-Private Partnerships in the telecom and information technology sector;
- Understand how a PPP addresses the needs of improving the network and information security at Pan-European level;
- Assess how such cooperation platforms can positively impact on security and resilience.

[1] http://www.isaccouncil.org/aboutus.html

Involved stakeholders, both through interviews and questionnaires, have suggested several important observations:




Accordingly, the EP3R key drivers were "team building", "trust consolidation", "clear and focused objectives identification", and "tangible and specific outcomes definition", but a clearer definition of purpose and stable and agreed terms of reference were advocated by interviewees for a more effective, consistent and reliable cooperation mechanism.

In 2011 ENISA published a Good Practice Guide on Cooperative Models for Effective PPPs[2] and implemented the suggested features in the EP3R for the second half of its existence.

The main conclusions highlight that the PPP model for information sharing in the field of ICT security deserves to be considered as an experiment due to its different possible set-up combinations. The general perception among the respondents to the interviews carried out in this study is that the outcomes of the EP3R were "partially satisfactory". This can be considered as an encouraging outcome for a very first platform of this kind, and an incentive for adapting the setup of features in future PPP implementations. Some issues were raised by participants who stepped out after the first two years of the EP3R existence (2010-2011) not having the opportunity to actively participate when these issues have been addressed and to assist to the evolution of the platform in its last two years (2012-2013). Finally, a large majority of respondents demonstrated strong affinity of the additional value associated with such an approach and are supportive of such model.

The study allows to draw a number of recommendations:

- **Setup and use agile PPPs**: adapting rapidly to changes means that working groups should be small, their scope focused and detailed, and with a closed end-date;
- **Incentivise Industry initiatives and participation** by providing financial and human resources support;
- Define at the earliest stage simple but **formal rules and governance**;
- Publish and **advertise successful results**.

[2] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

## Table of Contents

# 1 Introduction

In the past few decades, information and communications became the backbone of today's society. Critical Information and Communication Infrastructures (CIIs) are a crucial component of economic and social systems worldwide and a fundamental asset for social life, private business and public services. As consequence the Telecom sector grew in size and complexity leading in Europe to a situation of market fragmentation where also main industry players operate in several countries.

In this context, a coordinated cross-border multi-stakeholder approach can help to address the challenges of the protection of CIIs. Such protection should be considered at three levels: Strategic level, Governance level, and Management (or Operations) level. While international regulations and national legislations refer to the strategic level, ICT providers are mainly interested in managing the CIIs lifecycle. This governance issue led to the development of a cooperation mechanisms including public-private partnerships (PPPs) at the European level to bridge the gap between the strategic and management levels. It is essential to improve resilience and security of the CIIs also taking into account the cross-border perspective.

In this study, many essential drivers have been identified in the ownership perception of the project outcomes of the participant stakeholders and in the PPP model:

- Addressed topics;
- Leadership approach;
- Effort for the involved stakeholders;
- Costs for the involved stakeholders;
- Geographical scope;
- Interaction model;
- Type of involved stakeholders;
- Profile of participants of the involved stakeholders;
- Expected outcomes;
- Inclusion rule;
- Participation rule.

Systematic cross-border cooperation may improve the effectiveness of security and resilience measures while lowering their cost. Market dynamics do not always provide sufficient incentives for private operators in the Telecom sector to invest in security and resilience of CIIs. Coordination among relevant public and private stakeholders therefore could be an important assets both at national and international level.

The development of a European culture of PPPs for security and resilience of CIIs is an iterative process. This report is a critical assessment of the experience collected in the first iteration of a PPP in the field, the European Public Private Partnership for Resilience (EP3R).

## 1.1 Objectives

This report analyses the opportunities and challenges of the first European public-private partnerships in the field of network and information security and resilience in Europe, the European Public-Private Partnership for Resilience (EP3R) in which mainly participated stakeholders belonging to the Telecom and Information Technology sectors.

The intention of this report is to draw a picture on:

- The affinity of respondents with security and resilience issues;
- The outcomes of PPPs in the Telecom and Information Technology sectors in comparison with those focused on other sectors (e.g. transport, energy, health, finance);

- The needs for a public-private partnership to improve network and information security and resilience;
- Other network and information security and resilience initiatives in the area of CIIs (different from the EP3R).

Moreover, given the role of Member States and the European Institutions aimed to guarantee an efficient and effective delivery of public utility services, the proposed analysis focus also on security and resilience issues related to CIIs as strategic assets of the European economy.

## 1.2 Methodology

In order to understand how the approach of PPPs contributes to increased security and resilience of CIIs, the following methods to collect information among stakeholders operating in the EU27 Member States were used:

- An on-line questionnaire submitted to Chief Security Officers, Chief Information Security Officers, directors/chiefs/responsible of the Security Department/Area and directors/chiefs/responsible of the ICT Department/Area belonging to operators in Telecom and Information Technology sectors as well as to operators of ICT-reliant sectors (e.g. transport, energy, health, finance).
- Telephone interviews with the EP3R participant stakeholders.
- Further telephone interviews with outsiders in order to determine which key characteristics of a PPP seem valuable to the ICT industry.

Finally, information and data collected from the respondents to the questionnaire and from the participants to the interviews were analysed in order to address the above mentioned research objectives.

## 1.3 Structure of this report

This report summarises the most relevant findings of the interviews and the questionnaires. Excluding the introduction, main contents are structured in four chapters aimed at:

- Describing the ICT industry perception of PPPs (Chapter 2);
- Analysing the EP3R Experience, its history and development (Chapter 3);
- Reporting observations from the interviews and questionnaires (Chapter 4);
- Providing recommendations for future cooperation initiatives in the network security and resilience such as PPPs (Chapter 5).

# 2 Industry perception of Public-Private Partnerships

Over the past few decades, ICT threats and concerns rose in complexity while resources available to handle them decreased. In this scenario, the traditional approach –i.e. delegating issues of collective interest to public management- has demonstrated some structural limitations. Public administrations, are not exposed to failure risks and provide collective services disconnected from any profit-making strategy. Private sector entities own and manage infrastructures of collective interest (such as CIIs) and cannot bear alone the cost of security and resilience.

The *New Public Management* theory has tried to overturn this tendency by introducing a market-oriented management notion into the public sector. The basic assumption is that a market-oriented management would have led to greater cost-efficiency for governments, without producing negative effects in terms of objectives and outcomes[3].

Since then Public-Private Partnerships have been used to introduce market practices in areas traditionally dominated by non-market players, e.g. the delivery of infrastructural services and the provision of public goods[4]. When establishing PPPs for project-financing, public administration representatives are aware that the private partners will run the project under a profit-maximising strategy.

For this report, cooperation mechanisms have been considered and investigated which all those that fit the broad scope as defined in the report on *Cooperative models for effective Public-Private Partnership*:

> *"[A PPP is] an organised relationship between public and private organisations, which establishes common scope and objectives. It uses defined roles and a work methodology to achieve shared goals."*[5]

Furthermore, as one of the essential benefit of the PPP approach is its flexibility, one of the main goal of this work is to identify which PPP model would be the most effective to improve CIIs security and resilience according to the indications of participant stakeholders.

## 2.1 Types of cooperation mechanisms

The dialogue established with the stakeholders from industry revealed that information sharing and cooperation on specific issues were common activities for the most of their PPP experiences.

As the interactions get global and increasingly complex, approaches based on multi-stakeholder involvement become the sole option to effectively address horizontal issues related to security and resilience. Thus in this field, the nature of cooperation has evolved from problem solving to shared strategy building. The main purpose remains the creation of economies of scale.

Results of the direct interaction with participant stakeholders belonging to Telecom and Information Technology sectors confirm this pattern. As shown below, respondents to the questionnaire declared that cooperation initiatives are present and based on information sharing (37%) or on cooperation on specific issues (53%).

[3] HOOD C., "A Public Management for All Seasons.", in *Public Administration*, 69 (Spring), 3-19, 1991
[4] MENARD C., "Is Public-Private Partnership obsolete? Assessing the Obstacle and Shortcomings of PPP.", in *The Routledge Companion to PPP*, 2012
[5] ENISA, *Corporative models for effective Public Private Partnership: Good Practice Guide*, 2011

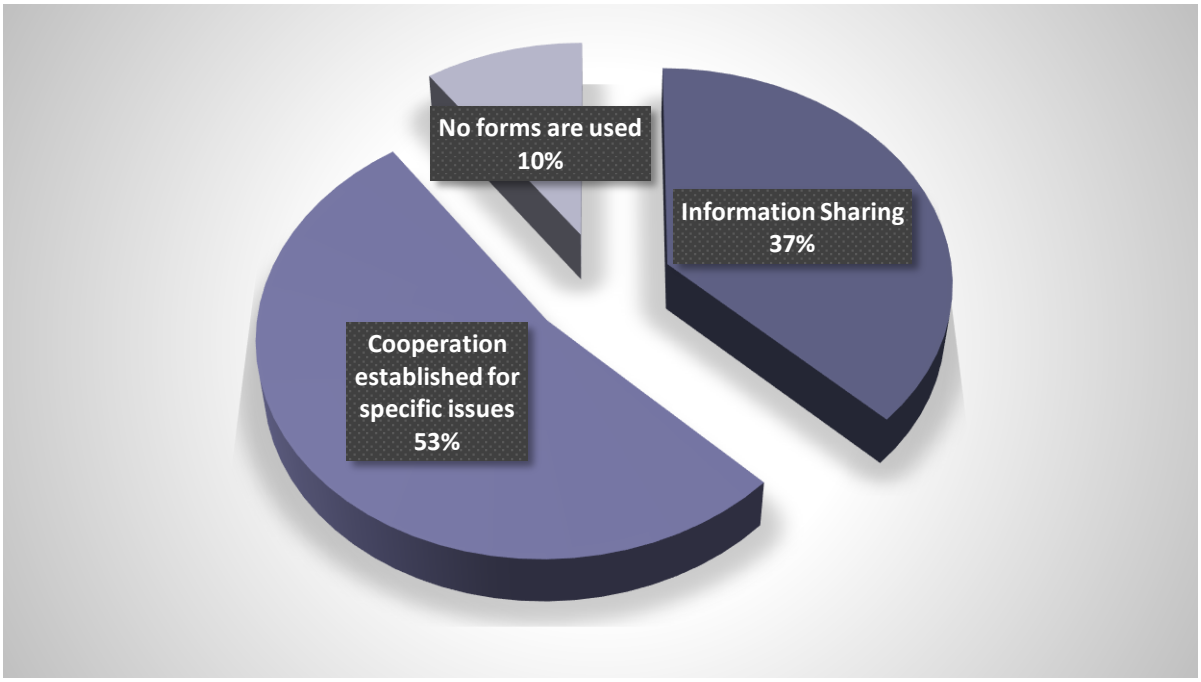



**Figure 1 – The main PPP types used among ICT respondents**

## 2.2 Previous experience of the respondents in PPP Initiatives

An overview of various PPP experience allows a preliminary assessment of differences and similarities with the investigated cooperation model; a synthesis of recurrent weaknesses and strengths related to each PPP approach and an identification of connected good practices and lesson learnt. In order to achieve these goals, the questionnaire has been designed to include all type of public-private initiatives regardless of their types and aims.

As the majority of respondents declared to have had experience with PPPs in the last 5 years (65%), a reasonable assumption is that in the Telecom and Information Technology sectors PPP initiatives can be considered as a well-established cooperation mechanism.

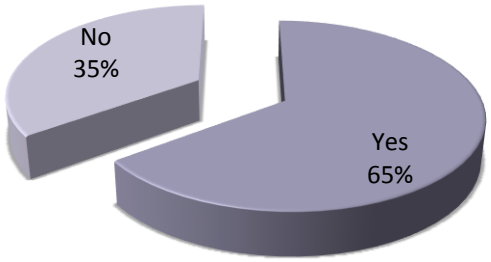



**Figure 2 – Answers to the question *"Has your Organisation been involved in any kind of PPP in the past 5 years?"***

As shown in Figure 2, new types of PPP emerged. The original project financing approach (i.e. delivery of large infrastructures) is no longer the sole model used. PPPs in the Telecom and Information Technology sectors for information sharing (29%) and ad-hoc cooperation on specific issues (35,5%) can be considered as a well-established collaboration mechanism[6].

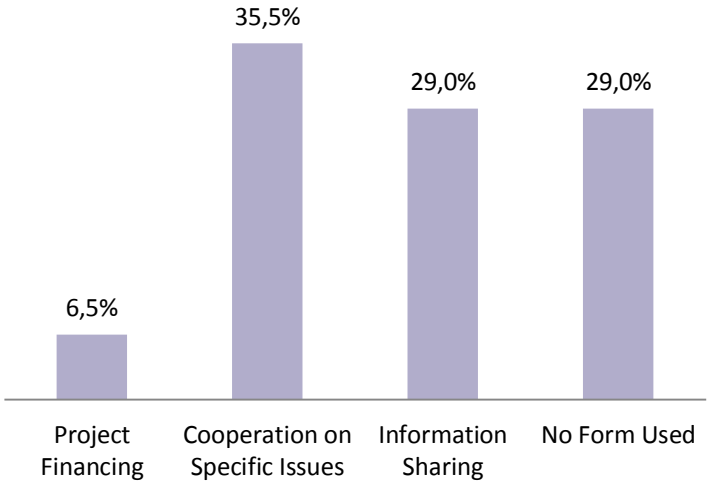



**Figure 2 - Respondents' previous PPP experiences[7]**

## 2.3 Industry indications on PPP needs

The information collected through the questionnaire allows also to draw indications of the desired features of a PPP for network and Information security and resilience. A key element is that **regional cooperation** could be a fundamental driver to enhance European competitiveness. Furthermore, industry representatives felt that significant results in this domain can no longer arise from private stakeholders or public actors alone. In this context, PPPs become a pillar in network and information Security and Resilience **good practices**.

In order to achieve these goals, human and relational capital should be considered an essential asset to be exploited in PPPs.

[6] A clarification on the low value related to the number of PPPs in project financing is needed. As PPPs for project financing are commonly used for the creation of large physical public infrastructures (e.g. roads) or provision ofcollective services (e.g. healthcare assistance), opportunities to adopt this type of interaction are structurally less than those to create "soft infrastructures" (e.g. cooperation tables for security and resilience).
[7] Questionnaire, Question 3.1 "*Which form of PPP is usually used in your activity sector?*"

According to the information collected from the respondents belonging to the Telecom, Information Technology, Transport, Energy, Health, Finance sectors, the following features of a PPP should be included in an effective European PPP for network and information security and resilience:

1. **Leadership** would be effective if based on a management approach agreed among participants. The establishment of a responsibility structure is essential also to monitor participants' effort.
2. **Funding** should be based on participants' efforts and time. Incentives such as ownership of project objectives, reduction of threat exposure, benefits from a multi-stakeholders approach may be used to increase to benefit/cost ratio of participants.
3. **Expected outcome** of the initiative should be at European level, even if potential benefits could arise from addressing the issue at national level. Several issues related to security and resilience *in se* seem to require an approach as wider as the national one.
4. **Inclusion Rules** should be properly defined taking into account also feasible options for enhancing participation both on invitation and on spontaneous candidatures or expressions of interest.
5. **Participation** should be limited to effective and proactive contribution to the general effort in order to ensure coherence between goals and results of the partnership.

As shown in Figure 3, five main questions (Why, Where, how, What, Who) were used to identify the key features for an effective PPP and represent them in a simplified scheme.

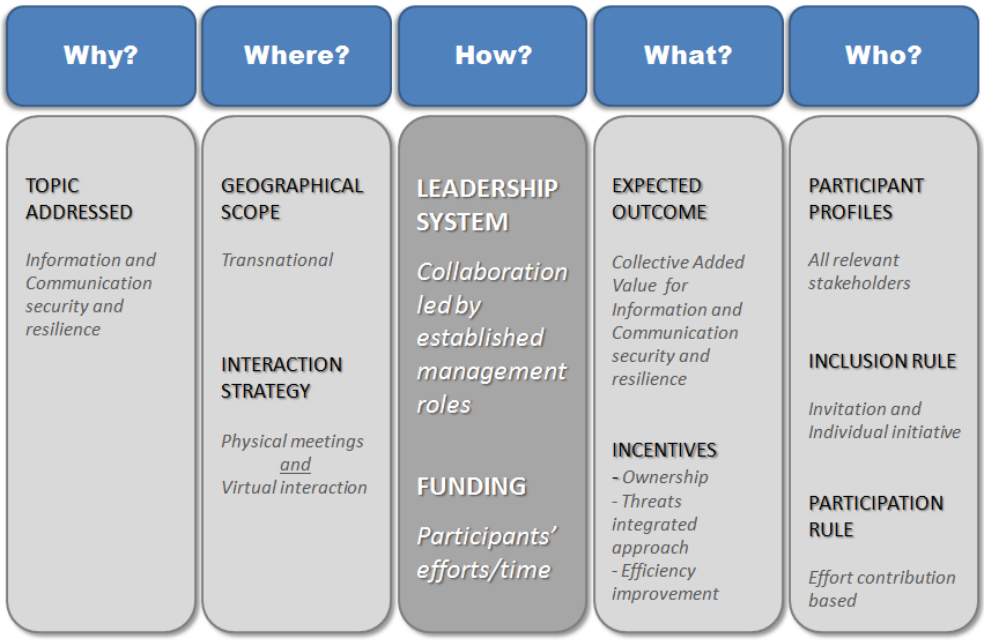



**Figure 3 – Key features of a PPP for network and Information security and resilience**

## 2.4 Benefits of PPPs

Over the past 20 years, the roles and responsibilities of the industrial players of Telecom and Information technology sectors have remained abstract. A gap existed between the perception of the industry players' security and resilience duties for provided services and the existing regulatory indications.

In this respect, PPPs could be also a bridging solution between industrial players and public authorities enabling four advantages in this cooperation mechanism:

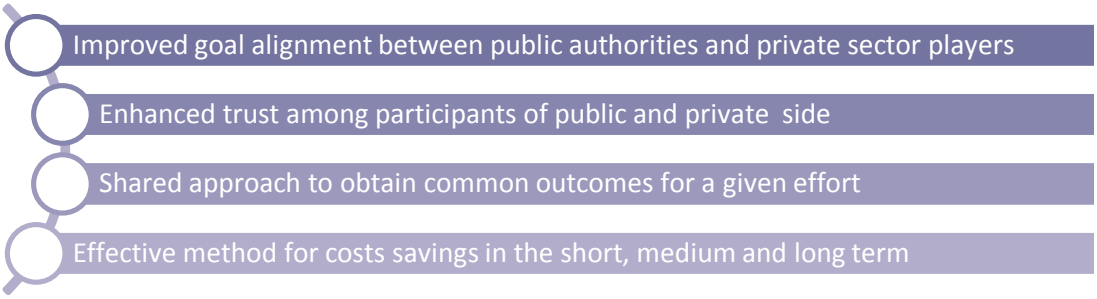



**Figure 4 - Key Objectives of a PPP with industrial players of the Telecom and Information Technology sectors**

Within this mechanism, private sector players may act in line with public needs and requirements and interact for the decision-making process, while the public sector players increase their awareness of emerging challenges and market dynamics. Mutual input from the public and private side gives the opportunity to create synergies and improve resource allocation also in light of a more rational selection of priorities leading to a so-called "soft regulation".

According to the answers provided by respondents, the most relevant advantage of a PPP approach is the opportunity to exchange information, knowledge, expertise and good practices (25%). The opportunity to influence the decision making process is perceived by the 16,10% of the respondents which considered PPPs also effective for networking opportunities (17,90%) .

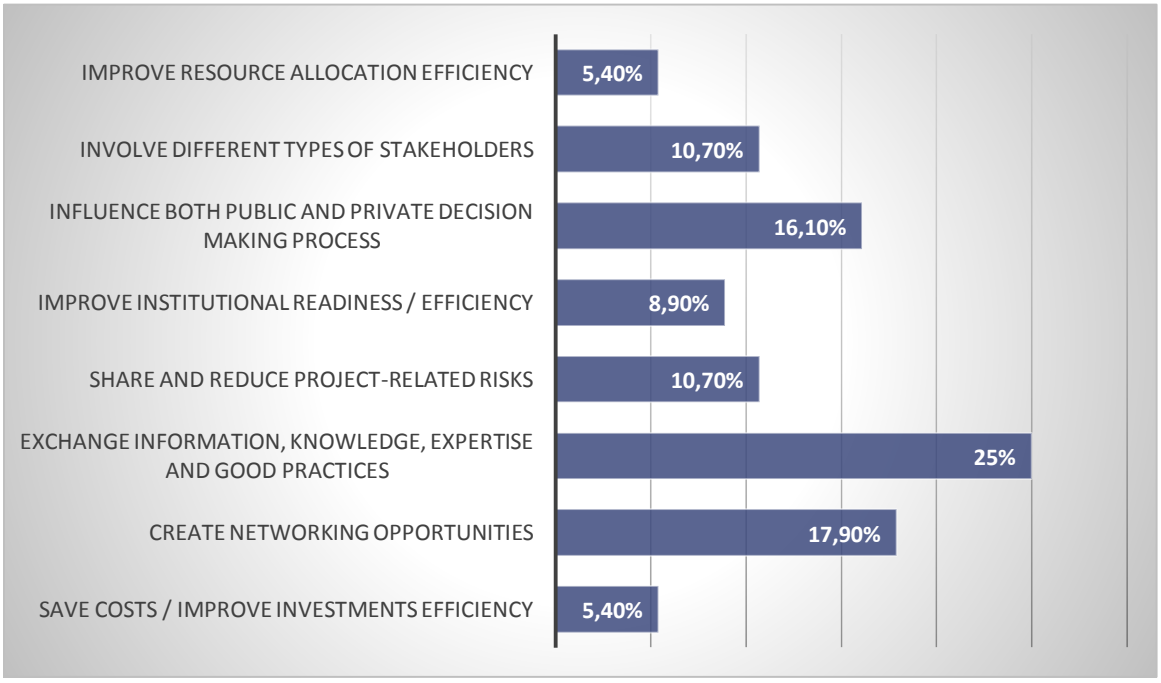



**Figure 5 – Answer to the question "Which could be the most relevant advantage of the PPP approach?"**

In particular, additional considerations should be mentioned also taking into account qualitative indications collected:

- PPPs set up the opportunity to have a direct insight on specific issues by the point of view of the participant stakeholders in a trusted environment instead of relying on second hand information.
- Networking opportunities are crucial for interactions inside and outside PPPs opportunities of direct peer-to-peer dialogue may represent an important added value for participant stakeholders
- Potential gains in human and relational capital are considered the most relevant advantage coming from this type of interaction.

According to the results of the questionnaire, existing PPP models and objectives need to be further developed. A wide majority of respondents declared that their expectations were fulfilled only partially (60%). No one reported that the public-private interaction was a failing approach that has to be discouraged and unsatisfied respondents provided several suggestions to improve their outcomes.

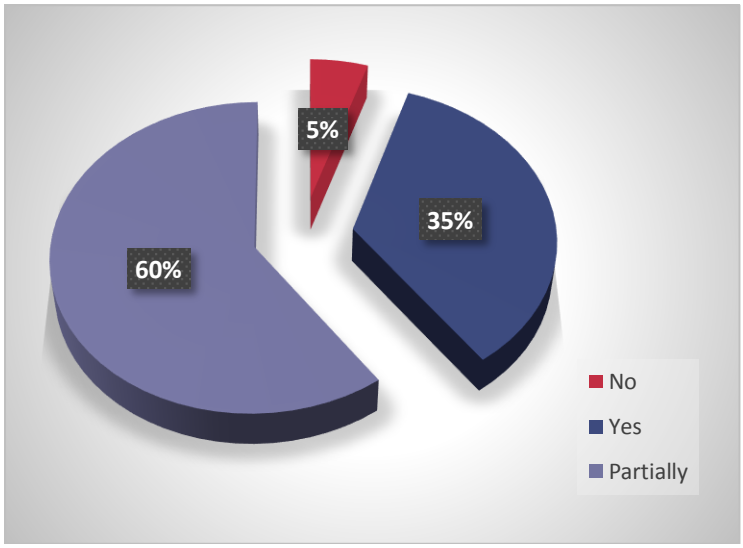



**Figure 6 – Answer to the question "Have PPPs produced expected positive outcomes for your organisation?"**

The overall result is of particular interest because it represents a paradigm shift. The added value of PPPs relates not mostly to the consolidation of human relations. The objective has shifted from maximising the immediate revenue to ensuring long term opportunities based on cooperation activities.

## 2.5 Purpose and European perspective

Examples of the effective PPP approaches in the Telecom and Information Technology context already exist at national level. In fact, different types of PPP mechanisms have experimented and tried with different purposes. Successful examples[8] were mentioned:

- The *Superfast Cornwall*[9] project (UK);
- The *Asturcorn*[10] (ES);
- The public outsourcing provision of broadband infrastructures realised by the Auvergne Region[11] (FR);
- The *Metroweb* project for the management of internet physical infrastructures and routes has been established as a joint venture between a public subject (the A2a publicly owned electricity company) and a private actor (F2i and Intesa Sanpaolo). Metroweb network covers a 2700 km metropolitan area (almost the entire municipality of Milan), and its operations is leased to different telecom companies (IT).[12]

As these examples confirm, the project financing PPP type has been applied with success at national level and it will probably become one the main drivers for the achievement of the objectives of the Digital Agenda. On the other side, the realisation of similar initiatives at European level remains extremely complex.

On the contrary wider-scope PPPs focusing on information sharing and specific cooperation targets may be easily set up at the European level. They would allow participants to share experiences which public authorities and private actors can directly adopt and exploit, and further develop also later on at National level. Due to the sensibility of the topics relating to security and resilience (both for national public authorities and private companies) cooperation PPPs is the most promising approach.

## 2.6 Reasons preventing participation in PPPs

When considering information collected from other sectors (transport, energy, health, finance), respondents declared that they have not been involved in any sort of PPP in the last 5 years. They identified which factors impeded their direct involvement in these cooperation initiatives. The question had a double purpose: to understand why respondents was not involved in a PPP and, if involved before the last 5 years, to understand why they left the initiative.

[8] Examples have been selected on the base of an EPEC study on the theme which includes a wider sample of case studies, e.g. EPEC, *Broadband. Delivering next generation access through PPP.*
[9] Private Design Build and Operate PPP for the provision of Next Generation broadband (FTTP and FTTC) in the Cornwall area. For more information, see http://www.superfastcornwall.org
[10] Public Design Build and Operate PPP for the provision of FTTP infrastructures in the Asturias region; to the date EUR 55 million have been invested.
[11] Public outsourcing PPP for the provision of high-speed broadband (at least 512kbit/sec) for a period of 10 years, basing on a 38,5 million EUR budget.
[12] For further information, see http://www.metroweb.it

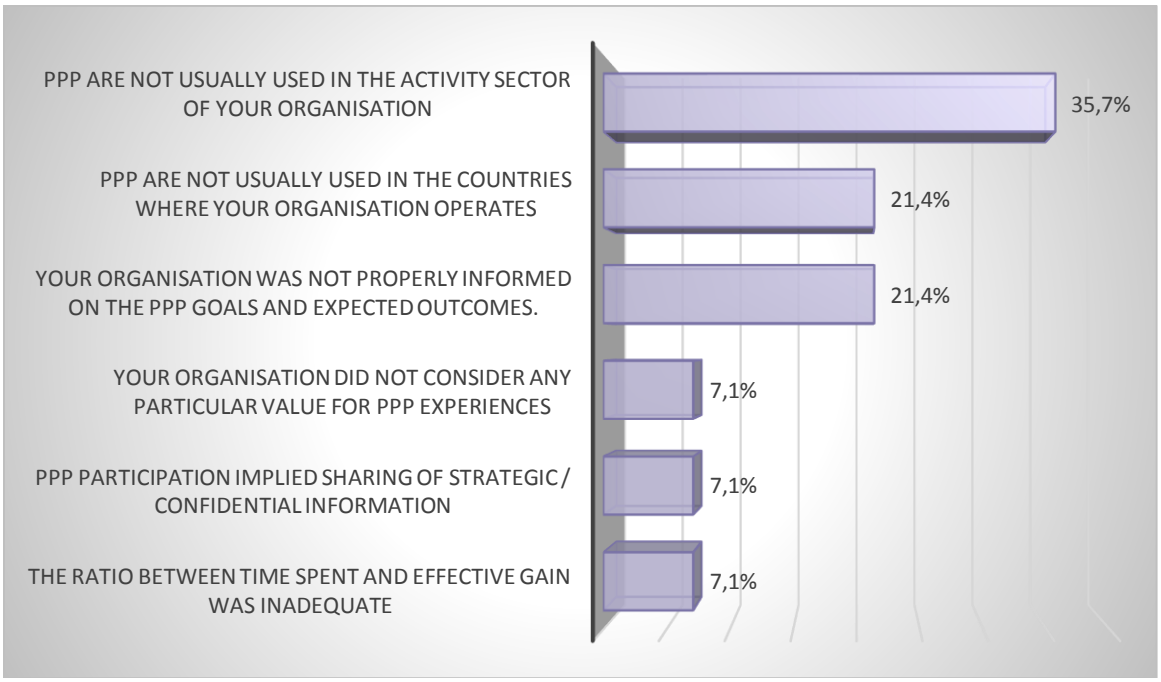



**Figure 7 – Answer to the question "Which were the reasons impeding the participation to PPP?"**

As shown in Figure 7, a large majority of respondents did not participate to a PPP because these type of initiatives are not common in their sector of activity. More than 20% of the respondents declared that these initiatives are not used in the countries in which the organisation operates. These results confirm that the PPP approach is not equally distributed both in considered sectors and in the Member States.

The opinion that PPP initiatives are useless also remains. Several respondents claimed that:

- The lack of information or visibility on the PPP initiative itself or of its specific objectives/expected outcomes;
- Difficulty in sharing of confidential information.

The perception that information sharing is a deterrent factor should not be considered as a structural weakness of the PPP approach. Trust building is arguably one of the most crucial issues to be addressed either by consolidated relationships or by establishing formal guarantee systems.

Mechanisms to improve cooperative behaviour of public and private stakeholders should be identified in order to create PPP initiatives which address common issues and benefit from a multi-stakeholder approach. Furthermore an increased awareness of current PPPs initiatives may enable cooperation and interest in shared management of common goals.

# 3 EP3R: a European PPP on Networks Resilience

### Initiation (2009)

The EP3R (*European Public Private Partnership for Resilience*) was established in 2009 in COM(2009)149 on *Critical Information Infrastructure Protection (CIIP)* [13]. otherwise known as *CIIP Action Plan.* The initial aim of this partnership was to establish a sustainable cross-border co-operation devoted to address the CIIP Action Plan fundamental pillars. The objectives of the EP3R were:

*"- Encourage information sharing and stock-taking of good policy and industrial practices to foster common understanding;*

*- Discuss public policy priorities, objectives and measures;*

*- Baseline requirements for the security and resilience in Europe;*

*- Identify and promote the adoption of good baseline practices for security and resilience."*[14]

The *CIIP Action Plan* represents an important milestone in the implementation of the strategy for a Secure Information Society, COM(2006)251[15]. The approach chosen by the Commission was mainly to engage the public and private sector in a multilateral, open and inclusive dialogue for partnership and empowerment in order to achieve the five pillars of the *CIIP Action Plan*:

- *Preparedness and Prevention*
- *Detection and response*
- *Mitigation and recovery*
- *International Cooperation*
- *Criteria for European Critical Infrastructures in the ICT sector*

The overall goal of the EP3R was to cope with the *CIIP Action Plan* prescriptions (with ad-hoc working groups organized to address specific issues) and the EP3R scope itself evolved over the years in order to better fit needs and policy evolutions.

### Early days (2009-2011)

Bearing in mind these objectives, in 2010 the EP3R was devoted to information sharing and stock taking of good policy and industrial practices. It aimed at improving the consistency and the coordination of policies for security and resilience in Europe.

It was originally structured on three *Working Groups* (WG). Security Experts were invited from National and pan European Telecom operators, Internet Service Providers, industrial associations, Standardisation Bodies, Competent National Authorities, manufactures and solution providers. EP3R intended to reach a regional scope (initially, EU27) with the participation of a number of selected operators chosen among the categories mentioned previously.

[13] Commission of European Communities, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS*, *on Critical Information Infrastructure Protection* "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149, Brussels.

[14] As stated in the ENISA web page http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[15] Commission of European Communities, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGION, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, COM(2006)251, Brussels

Adopting the simplified scheme based on the five main questions (Why, Where, how, What, Who) already used to describe the key features for an effective PPP, the EP3R set up can be summarised as follows (see Figure 8).

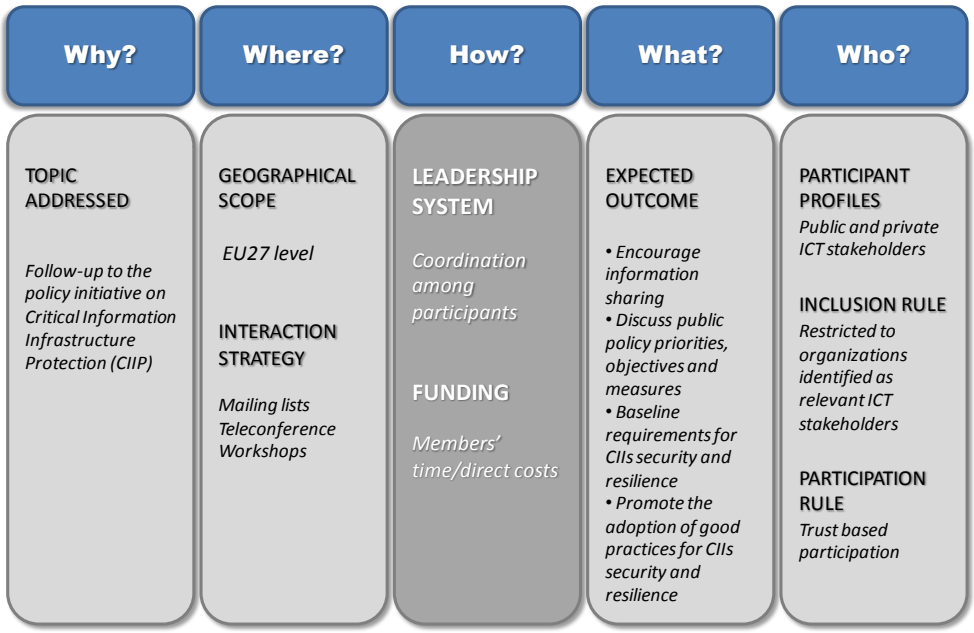



**Figure 8 – Main key features of the EP3R**

With respect to the five key elements identified as to be included in an effective European PPP for network and information security and resilience, EP3R presented:

1. **A leadership approach based on coordination** among participants that were sked to join thematic working groups working mainly on a virtual basis using online collaboration, mailing lists, call conferences or remote workshops.
2. **A funding** scheme based on **time and efforts of the involved stakeholders**.
3. An **expected outcome** strictly related to **information sharing, policy priority identification, CIIs security standards definition and promotion of CIIs' security and resilience good practices.**
4. The **participation** (of involved stakeholders) was **voluntary, inclusive and based on trust**
5. **Inclusion rule** was set up on a **profile of the stakeholder.** Stakeholders admitted had to belong to security sectors of National and pan European Telecom operators, Internet Service Providers, industrial associations, Standardization Bodies, Competent National Authorities, manufactures and solution providers.

### An Improved model (2012-2013)

The evolution of participants' needs for a more topic-focused and impact-oriented approach led to implement structural changes after mid-2012. Since early 2012, also the management mechanism of working groups was already modified significantly: EP3R introduced nominated Moderators, organised frequent teleconferences and provided alternative additional meeting opportunities (e.g. combination of plenary sessions with working group sessions the day before or after). These came to force from April 2012 (in Rome).

According to the EP3R Activity Report 2012. Between August 2011 and March 2012 several discussions were on-going in each working group:

- Working Group 1 addressed the Critical Information Infrastructure Protection approach and delivered recommendations within the ICT Criteria Non-Paper. Relevant considerations came also on a methodology to classify assets supporting CIIs infrastructures;
- Working Group 2 gathered Hardware Manufacturers, Supply Chain operators, and Telecom Operators to define "quick wins" to improve reliability, resilience and default security levels of equipment;
- Working Group 3b proposed to implement a pan-European botnet-fighting programme, along with key recommendations on how to proceed;
- Working Group 3e reflected mainly on the preparedness for a Preliminary Emergency Communication and recommended the establishment of a European Crisis Coordination Contact list.

Several topics emerged from each of the 3 initial areas and gradually evolved into smaller sub-groups.

The Work Programme 2013 acknowledged those observed changes, and already in September 2012, Task Forces were created to address those emerging topics. The EP3R Work Programme 2013 reports that *"Much progress was achieved during the April 2012 Experts Meeting which was held in Rome. Four position papers have been produced and have been consolidated in a general Working Groups' Yearly Statement. [...] Several conclusions arose after the Rome Meeting, to allow for a maturing of the work organisation, and therefore achieve a higher degree of reflection during the working sessions. The natural next step was to divide each topic into smaller tasks assigned to 5-6 Experts maximum, and later have them reviewed in an EP3R plenary session. [...] Such a model presents a series of advantages:*

- *Shorter Time to Delivery for recommendations;*
- *Greater flexibility in addressing current issues, and prioritising the work based on its natural dependencies;*
- *Sense of ownership of the topic by Experts working on it;*
- *The opportunity to address the trust related issues of effective information sharing in EP3R and beyond;*
- *Better use of Subject Matter Experts' time and better focus on issues based on their level of knowledge.*

*[...] While keeping the coverage of the initial Terms of Reference (ToR), the structure of the Working Groups [has] gradually been replaced by smaller Task Forces."*

The organisational change was implemented to allow a better trust building and to improve stakeholders' commitment in the overall collaboration environment.

### Overall perception of the initiative

A set of Interviews addressed EP3R participants from both early and later years. Another set of interviews was also conducted with persons who observed the development of the EP3R or were indirectly involved. The overall experience of EP3R participants was considered positive and appreciated. Several aspects of such cooperation initiative have been indicated *to be improved in order to actually achieve impacts and reach effective outcomes.*

Among the questionnaire respondents only 23% participated in the EP3R. Almost half of them participated to more than one working group (13%).

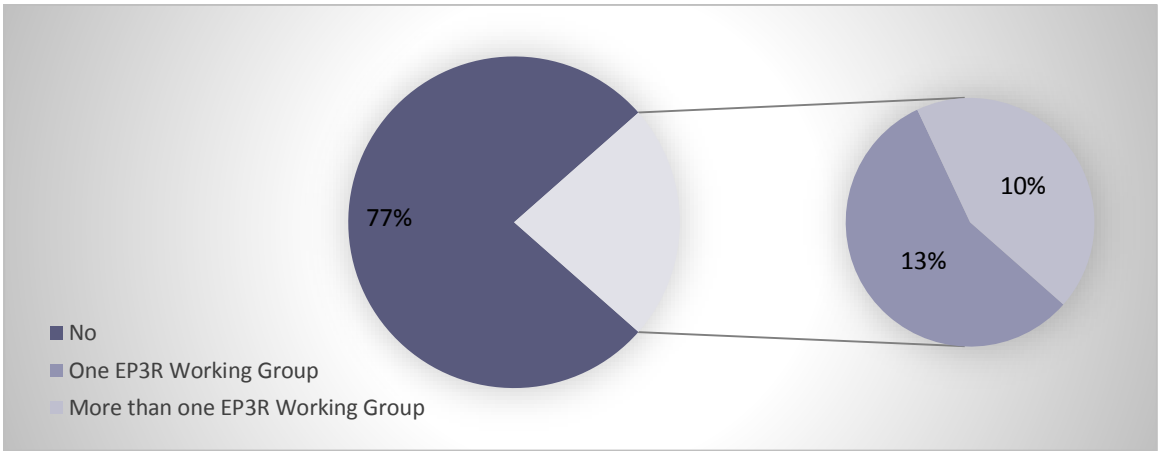



**Figure 9 – Answer to the question "Have you ever been involved in the activities of the EP3R?"**

Taking into account the fact that the EP3R was exclusively dedicated to Telecom and Information Technology sectors, most of participants reported a general lack of information on the initiative, its goals and outcomes.

No respondents reported that reasons to leave EP3R were related with the confidentiality of the information to be shared despite the presence of competitors or due to an inappropriate selection of stakeholders to be involved. 15% of the respondents did not consider the EP3R activities of particular interest, while 8% of them clearly stated that the ratio between the effort required and the effective gain was underbalanced. Another 15% of respondents reported that the EP3R was not opened to operators of their sector.

In light of these results, it seems that EP3R participants partially validated the outsider perception that the actual experience was not fully coherent with the initial objectives of the EP3R establishment.

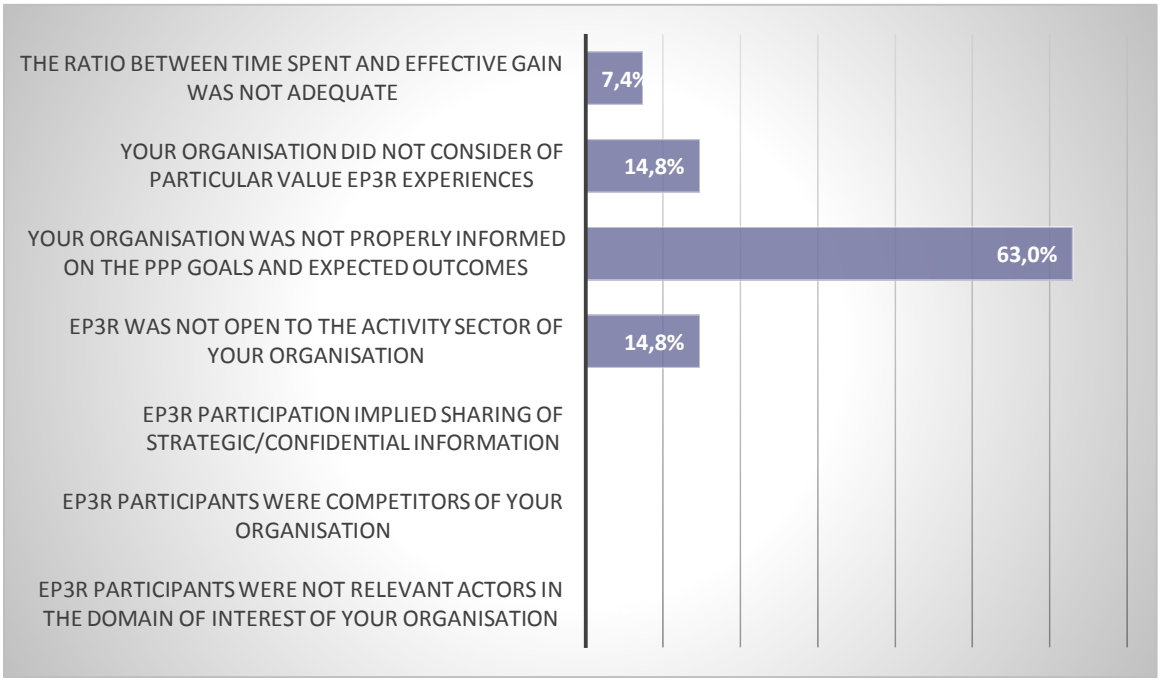



**Figure 10 – Answer to the question "Which were the reasons impeding the participation to EP3R?"**

The actual assessment of the EP3R initiative does not correspond to the objectives of its creators. Also taking into account interview answers, many criticalities explicitly emerged:

1. Lack of participants,
2. Unclear perception of the objectives, and
3. Instability of both the organizational structure and the core set of involved participants.

Focusing on the eleven key feature taken into account, in the analysed PPP model, the "Addressed topics" feature received the best average score confirming that network and information security and resilience was a concrete need for the majority of the involved stakeholders. On the opposite, the feature "Expected outcomes" was the lowest in the score suggesting that, on average, participants were unsatisfied with the results achieved.

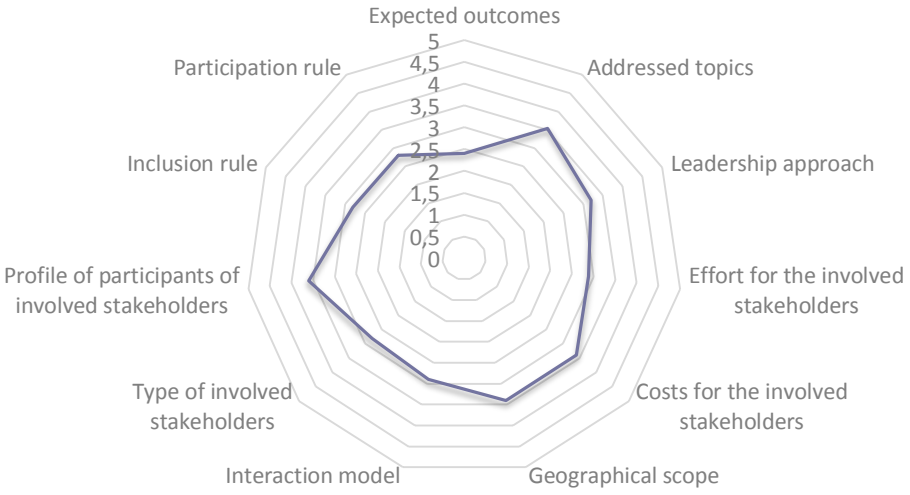



**Figure 11 – Assessment of the EP3R experience**

## 3.1 Addressed topics

Even if Network and Information security and resilience were considered on average the most appreciated aspect from the EP3R respondents.

Many of them however reported that the general objectives and the topics themselves were not initially properly detailed. EP3R participants declared that pre-defining a set of topics and asking them to select the most interesting one was different from an expected bottom-up approach; the proposed flexibility of choice in a limited set of options was perceived as a lack of vision regarding the concrete objective of the proposed interaction.

The implementation of the Task Forces attempted to address that issue in 2012, but some respondents saw this as another way to obtain the same pre-defined outcomes. Actual perception of EP3R participants is the opposite of the desired effect: during an interview, one participant pointed out that "*Prioritisation was correct but there was a need to find ways to cope with the settled objectives and to avoid important on-going changes".*

The build-up of the Task Forces on top of the existing initial areas was supposed to achieve the goals of the ToR initially agreed by the EP3R constituency in June 2010 and reach a final outcome.

Among participants there was also a dichotomy of opinions: some reported that topics were pre-defined and some others that they were unclear or not fixed. In 2012 EP3R suffered an important turnover of participants and major changes in its approach. Several "new comers" felt that topics were predetermined since they simply inherited them as result of the suggestions of the early participants.

**Observation 1: Objectives should be appropriately selected and clearly stated.**

**Observation 3: A bottom-up approach enhances participants' ownership and engagement**

**Observation 4: Preliminary feasibility assessment of the expected outcomes can improve the effectiveness of the strategy selected to reach them**

**Observation 8: Addressed topics should be selected among those related to protection of Critical Information Infrastructures**

## 3.2 Leadership approach

According to the literature overview, the leadership approach is one of the most relevant criticalities in each PPP experience.

In the specific case of EP3R, the lack of the evidence in influencing and in having a direct role in the regulatory and policy environment of the European institutions was perceived as a major obstacle to achieve any reasonable impact and a *"Lack of authority and ability to enforce the outcome in local environment".*

In other words, the management approach based on the definition of objectives by the public actors and on their achievement relying on cooperation activities among (private) stakeholders, was perceived as a potential limitation for the impact of the EP3R activities at policy and regulatory level.

**Observation 5: Management with defined roles enhances responsibility and commitment**

**Observation 6: Action sharing can be preferable to information sharing under certain circumstances**

**Observation 11: Leadership approach should be based on coordination among public and private stakeholders**

## 3.3 Effort for the involved stakeholders

The effort requested to each EP3R participant was based on their time and active commitment in the activities mainly during the meetings (both virtual and in presence) and in contributing to shared documents. The perceived lack of potential impact of EP3R affected participation and started a high membership turnover. This prevented the creation of stable personal networks and led most of the respondents to declare that the initiative was not valuable from the economic point of view.

**Observation 12: Funding strategy should provision for participants' time and effort investment.**

## 3.4 Costs for the involved stakeholders

Participation to EP3R activities led to direct costs (i.e. travel costs to attend the meeting in presence). Cost-opportunities (i.e. time of the human resources working for a company invested in contributing to the EP3R debate) were based on resources of the involved stakeholders. A general perception among participants was that funds available to sustain direct costs may have had a positive impact on the number of participants and their commitment.

**Observation 12: Funding strategy should provision for participants' time and effort investment**

## 3.5 Geographical scope

To the question about the appropriate geographical scope for a cooperative initiative such as the EP3R, none of the respondents has reported a geographical perspective different from the regional one.

There is much needed attention to be paid to coordinate efforts at regional level in order to reach in Europe economies of scale results in security and resilience comparable to those obtained in the most advanced countries (i.e. the USA, Japan).

On the other side, respondents mentioned also that an effective coordination of national initiatives could have a greater and more concrete impact than one at regional level. In this perspective, one of the participants to the interviews suggested that *"a multiple approach, combining national PPPs with a regional/multinational coordination initiatives would be desirable".*

**Observation 7: Regulatory provisions should be established at regional level**

**Observation 9: Geographical scope should reach regional coverage involving all the EU28 Member States**

## 3.6 Interaction model

The interaction model proposed for the EP3R initiative was based on both in presence and virtual meetings.

The general aim of such interaction was to identify a trade-off between the need of building stable personal networks and trust among stakeholders and the intention of containing effort in time and direct costs of participants. Answers provided by respondents revealed that the relevance of face to face meetings in building a trust environment was underestimated. Respondents generally requested as a need more frequent in presence meetings, although in 2012 EP3R hosted 4 meetings (3 combined plenary/TF meetings) and in 2013 participants kicked off face to face in Task Force meetings.

**Observation 10: Interaction model should necessarily include regular meetings in presence**

## 3.7 Type of involved stakeholders

The EP3R experience was limited to public and private stakeholders of the Telecom and Information Technology sectors operating in Europe.

Nevertheless a significant number of respondents mentioned a lack of presence of the larger players from the private sector. This fact had in turn a negative impact on the attractiveness of the initiative also for small and medium stakeholders.

Among the respondents to the questionnaire, Figure 12 shows participation in different types of PPP initiatives including EP3R. 65% of the respondents were involved in some forms of PPPs in the last 5 years. Almost all of them participated in cooperation initiatives focused on information and communications security and resilience but less than half of them experienced the EP3R.

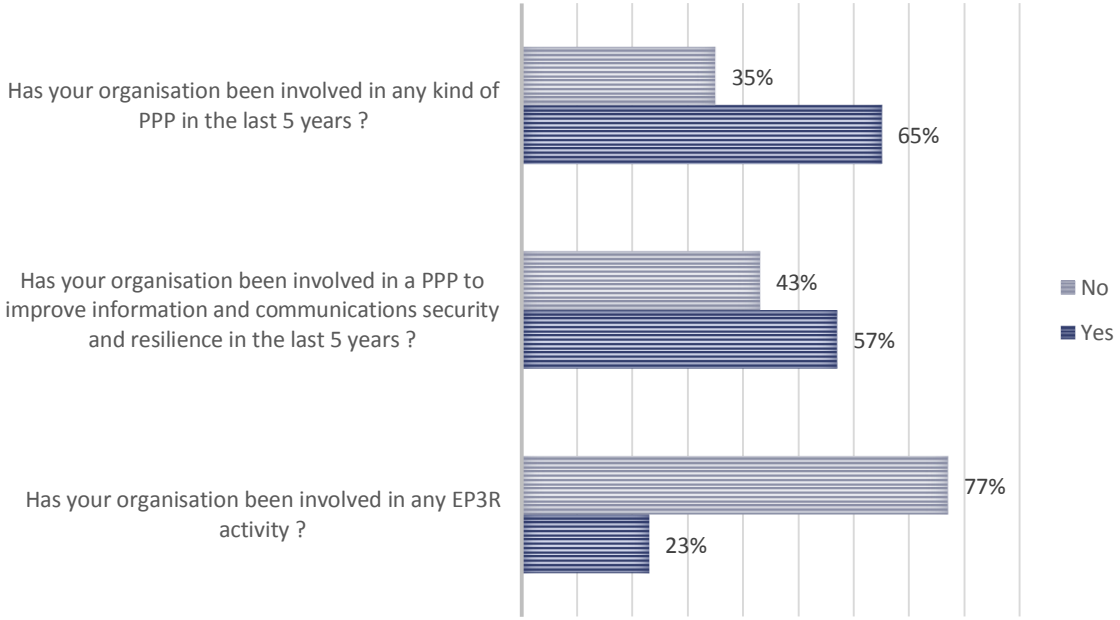



**Figure 12 – Involvement in different types of PPPs of the respondents to the questionnaire**

This result provides indications on the involvement of the same stakeholders in initiatives similar to the EP3R which were organised at national level. It reveals existing engagements in **cross-sectors**

**cooperation activities**. For this reason, in order to increase participation and commitment, it seems more appropriate to better specify objectives and expected outcomes rather than to enlarge the set of types of stakeholders that can be involved.

**Observation 2: Ownership of the underlying project is a fundamental driver of the participants' commitment**

## 3.8 Profile of participants of the involved stakeholders

The EP3R involved by invitation stakeholders of the Telecom and Information Technology sectors but participants were directly appointed by the involved organisations.

Suggested profiles of participants were high profile professionals such as ICT Manager, Security Managers, Information Security Managers, Chief Security Officers, and Chief Information Security Officers, directors/chiefs/responsible of the Security Department/Area and directors/chiefs/responsible of the ICT Department/Area of the involved stakeholders. The appointed representatives were asked to take part in the Working Groups (in the first EP3R period) or in Task Forces (in the second EP3R period) activities. The open and inclusive nature of EP3R allowed several members of each stakeholders to participate in different Working Groups or Task Forces. Some participants to the interviews stressed that in the cases in which more than one person was involved in the EP3R activities there was a loss of the knowledge in the working team in case of alternance of the persons and an additional lack of trust in case of frequent change of the representative. As a final result, contribution of stakeholders and consequent commitment was partially fragmented and dispersed.

**Observation 14: Participants' profile should include both public sector decision makers and private sector high level security managers**

## 3.9 Expected outcome

Respondents to the questionnaire felt that the objectives selected within EP3R were initially not aligned with the needs of private sector stakeholders. The three initial investigation areas defined in the Terms of Reference of EP3R were set-up in June 2010 during the EP3R plenary meeting.

Later, participants' turnover led to a partial disconnection between those initial goals and requirements of new participants to the EP3R activities. This observation was shared among participants and, in February 2012, an entire EP3R plenary meeting was again organised to re-open the discussion around the Terms of Reference. Discussions were held and the development of a new, specific and detailed Work Programme was approved, leading in December 2012 to the publication of a series of Position Papers.

In any case, all participants reported that EP3R was lacking a way to enforce the desired outcomes in a way or another. Several respondents mentioned that the lack of knowledge of the regulatory environment at national level affected the understanding of the potential barriers and, ultimately, the provision of effective recommendations.

**Observation 1: Objectives should be appropriately selected and clearly stated.**

**Observation 6: Action sharing can be preferable to information sharing under certain circumstances**

**Observation 7: Regulatory provisions should be established at regional level**

**Observation 13: The most desirable outcome would be the delivery of technical/organizational solutions**

## 3.10 Inclusion rule

The involvement of participants was based both on individual invitation to targeted operators and on open expression of interest of stakeholders belonging to the selected types.

Such inclusion mechanism had an adverse effect: the EP3R appeared as informally established. This affected the commitment of the stakeholders resulting in a lack of a stable group of participants. This observation was already made in 2011; new rules were adopted to mitigate this negative effect with the creation of the Task Forces. The process took time to become really visible and EP3R activities were closed before reaching the desired results.

**Observation 15: Involved stakeholders should be organizations with specific predefined characteristics and approved by a relevant part of the PPP participants**

## 3.11 Participation rule

Participation in EP3R relied on voluntary commitment with no formal obligations for participants to effectively contribute to the proposed activities proposed. As considered a weakness point, most of the respondents proposed several ideas to address this point:

- The establishment of a guarantee system to improve commitment and trust among participants (see Annex C);
- The obligation of participants to agree on a detailed commitment, in particular related to the confidentiality of the shared information.
- The definition of an access rule based on the proof of an actual, effective and active participation

In light of the 2012 structural change of the EP3R, commitment was expected to continue. The actual behaviour seemed to be slightly different: as already shown in Figure 9, half of EP3R participants took part in more than one Working Group. This created an organisational issue: since working sessions in presence were held in parallel, these participants took part in the end to the group which was the most interesting for them. No indications were provided on the reason of their choice and if it was a behaviour led by the topic discussed in a specific meeting or by other factors. In any case the effect was negative on the creation of a shared trusted environment and on the achievement of the expected outcomes themselves. Also according to other respondents' experiences in cooperation initiatives, trust was pointed out by all respondents as the fundamental requirement on which to build up fruitful interactions.

**Observation 16: Participation rule should be based on formal membership and subordinate to active involvement in the working groups**

# 4 Observations

The aims and the relevance of the EP3R experience is appropriately understood and effectively reported in the answers of the questionnaire and in the participants' interviews. The initiative was terminated as organisational features started to maximise the expected outcomes of the interactions among the participants of the public and private sectors.

Along the years, EP3R has changed its configuration both in terms of internal organisation and participants' involvement: in these evolutions, participants were contingently asked to declare their willingness to participate in cooperation activities and to take decisions on which activity to support. As the participation was set on voluntary basis and on individuals' time investment, the EP3R key governance features should be considered correct from the theoretical point of view.

The presented results should not discourage from establishing later new PPP approaches but rather encourage refinements and improvements.

In particular, the overview of an existing PPP allows the identification of considerations for an effective PPP and in particular:

1. The public-private partnership model is strongly exploited among different sectors for its added value in relational capital and for its contribution in information sharing;
2. Effective public-private partnerships are based on trust building which can be achieved by establishing guarantee systems or by creating participants' consolidated relations;
3. Sharing of objectives and expected outcomes among the involved stakeholders helps to build a working community able to face the emerging challenges in an integrated manner.

Accordingly, the assessment of EP3R initiative leads to the following general remarks:

1. The application of a wide-scope PPP model for the EP3R experience was the first valuable attempt to involve relevant stakeholders belonging to the Telecom and information Technology sectors on the issue of Network and Information security and resilience.
2. Creation of thematic Working Groups, in the first period, and Tasks Forces, in the second period, aimed at building restricted groups in order to give to opportunity to focus on topics of interest and to enhance trust building among participants
3. Perception of participants of the EP3R and its expected outcomes was far from the original intentions; the main weakness points of the initiative were the lack of well-defined participation rules, the soft leadership approach, the limited interaction opportunities and the unclear definition of expected concrete outcomes.

This results encourages future PPP implementations which could refine the model through an ad-hoc tailoring of its key features.

Respondents provided in addition to the structured answers several additional comments that composed a set of observations. The following table synthesises the most relevant and important ones, i.e. those which should be considered in the creation of future initiatives.

| | | |
|---|---|---|
| **1.Objectives should be appropriately selected and clearly stated** | Both literature review and telephone interviews confirmed the relevance of clear set of well specified and properly selected objectives. Participants are more motivated to invest their time and effort if the goal to be achieved is concrete and in light with their needs. | **Advantages**<br>Enhancement of participants' commitment<br>Concrete and achievable outputs<br>**Pitfalls**<br>Fragmentation of the general objective in multiple and too specific goals with problems to rebuild a general framework |
| **2. Ownership of the underlying project is a fundamental driver of the participants' commitment** | The degree of commitment of participants is strictly related to the perception of the ownership of the underlying project; a proper selection and sharing of the outcomes to be achieved and the output to be produced can avoid any lack of commitment from participants. | **Advantages**<br>Stronger participants' commitment<br>**Pitfalls**<br>Potential difficulties in conciliating public and private interests in a unique shared and common project |
| **3. A bottom-up approach enhances participants' ownership and engagement** | The involvement of participants in the selection of objectives and expected outcomes is a crucial factor for the success of a PPP, guaranteeing participation and commitment. | **Advantages**<br>Enhance participants' commitment<br>**Pitfalls**<br>More complexity in the decision making process |
| **4. Preliminary feasibility assessment of the expected outcomes can improve the effectiveness of the strategy selected to reach them** | A preliminary feasibility assessment analysis can improve PPP effectiveness by defining whether the proposed approach can provide added value, and by identifying the most convenient specifications of the identified key features. | **Advantages**<br>More effective selection of the specification of the PPP key features<br>Improvement of resources allocation<br>**Pitfalls**<br>Additional time and effort costs |
| **5. Management with defined roles enhances responsibility and commitment** | Management with defined roles can enhance the responsibility perception among participants, making clear to whom they are liable to. In addition PPP activities should be led by participants of recognised professional reputation. This directly and indirectly affects participants' responsibility and commitment. | **Advantages**<br>Enhanced responsibility perception<br>**Pitfalls**<br>Dependency paths respect to the selected leaders |

| | | |
|---|---|---|
| **6. Action sharing is preferable to information sharing under certain circumstances** | Where objectives and purposes are clearly set up, action sharing may be preferable to information sharing. This approach could be considered of high value for security and resilience issues related recovery and crisis management. | **Advantages**<br>Lower risk of sensible information loss perceived by participants<br>Concrete result achievement<br>**Pitfalls**<br>Immediate response instead of consolidated interactions<br>Mainly based on bilateral agreements |
| **7. Regulatory provisions should be established at regional level** | The lack of regulatory homogeneity among the EU28 Member States is a systemic weakness and a cost for private actors in terms of adaptive efforts. The standardization of regulatory requirements related to Network and Information security and resilience would enhance regional interactions. | **Advantages**<br>Regional security and resilience enhancement<br>**Pitfalls**<br>Initial relevant adaptive costs for a regulatory framework different from the national one |
| **8. Addressed topics should be selected among those related to protection of Critical Information Infrastructures** | The major issue at stake is Critical Information Infrastructures Protection. After the identification about potential risks affecting CIIs, a coordination strategy among the public and private players seems to be the most appropriate approach also to raise awareness on the topics of interest. | **Advantages**<br>Improvement of protection of infrastructural assets and services provided through CIIs<br>**Pitfalls**<br>Objective achievable only on long term perspective and active involvement of many actors managing/ owning CIIs |
| **9. Geographical scope should reach regional coverage involving all the EU28 Member States** | The interdependent framework of reference for the Network and Information security and resilience needs a more integrated and regional approach in order to effectively address emerging challenges. The regional scope is considered the most appropriate one even though important difficultness should be faced to translate national experiences in a European initiative. | **Advantages**<br>European preparedness enhancement<br>More effective response to security threats and to resilience challenges<br>**Pitfalls**<br>Additional management effort<br>Issues in facing heterogeneity in the national contexts |

| | | |
|---|---|---|
| **10. Interaction model should necessarily include regular meetings in presence** | Meetings in presence are the best option to improve trust and to consolidate commitment among participants. | **Advantages**<br>Trust improvement<br>Commitment consolidation<br>**Pitfalls**<br>High direct costs for participants |
| **11. Leadership approach should be based on coordination among public and private stakeholders** | Within coordination among public and private stakeholders, leadership of public actors would be preferable. Management roles covered by professionals with recognised reputation may improve participants' commitment and responsibility. | **Advantages**<br>Improvement of commitment and responsibility<br>Effective impact of the cooperation initiative on policy/regulatory decision makers<br>**Pitfalls**<br>Potential misalignment of the public actors requirements with the private actors needs |
| **12. Funding strategy should provision for participants' time and effort investment** | Participants' time and effort seem to be the most pragmatic solution also by maintaining low the cost of interaction and by guaranteeing participation of stakeholders really interested in the foreseen cooperation activities. | **Advantages**<br>Low cost PPP initiatives<br>**Pitfalls**<br>Dependency of the cooperation effort from commitment of the involved stakeholders and their possibility to sustain direct and indirect costs |
| **13. The most desirable outcome would be the delivery of technical/ organizational solutions** | Among the most desirable concrete outcomes technical or organisational solutions in terms of security and resilience were identified. Action sharing can be a preferable option especially when sensible information sharing is needed. A specific operative outcome is preferred to a general theoretical one. | **Advantages**<br>Tangible operative outcomes and solutions<br>**Pitfalls**<br>Difficulties to achieve general objectives |
| **14. Participants' profile should include both public sector decision makers and private sector high level security managers** | High-profile professionals in the security and resilience domain should be involved. Their decision making position in the organisation to which they belong to allow them to take pro-active behaviours in the PPP. | **Advantages**<br>High probability to obtain concrete outcomes and strong commitment of the stakeholders<br>**Pitfalls**<br>Limited availability of effort out of the organisation to which they belong to |

| | | |
|---|---|---|
| **15. Involved stakeholders should be organizations with specific predefined characteristics and approved by a relevant part of the PPP participants** | Inclusion should be based on participants' approval and should be open strictly to the stakeholders of the identified sectors. Homogeneity of stakeholders' profiles helps to focus on common issues in which all participants have high interest to face. | **Advantages**<br>Focus on common issues of interest<br>**Pitfalls**<br>Limited number of participants |
| **16. Participation rule should be based on formal membership and subordinate to active involvement in the working groups** | Participation based on a formal membership and on proof of active contribution help to avoid to involve participant not interested to contribute but mainly to benefit from the activities in the PPP (i.e. information sharing). | **Advantages**<br>Improvement of the commitment of participants<br>Perception of the possibility to achieve concrete outcomes<br>**Pitfalls**<br>Higher management effort |

**Figure 13 - Observations and lessons learnt for future initiatives**

# 5 Recommendations for future initiatives

The key recommendations for the future pertain for four main areas:

- Implement agile PPPs which can adapt to new needs and topics;
- Incentivise Industry initiatives;
- Define simple but formal rules and governance;
- Publish and advertise successful results.

### *Use Agile PPPs*

While the global constituency of the EP3R was large (more than 250 registered participants), the most attractive aspect rapidly became the constitution of smaller groups of active participants (i.e. the Working Groups). For this reason, while keeping bi-annual plenary meetings (mostly for the review and acceptance of the produced work), experts participated to the actual works of the Working Groups and then Task Forces on a more regular basis creating a trusted relationships among the group participants.

The US and UK examples also support this model: such a PPP is most likely successful when it is composed of several hives which can host and bear several different topics, but with similar methods. Only then the cost effectiveness reaches its optimum.

| |
|---|
| The successors of EP3R in the security and resilience domain should take the form of a platform where ISACs, Working Groups and Task Forces can be created very rapidly when the need arises and have a short lifespan. Their scope should be focused and limited, and they should be assigned one clear objective to reach. Such a platform could be co-chaired by European Officials and by major industry players. |

### *Incentivise participation in PPPs at industry level*

While the bottom-up approach should be used to trigger activities in a PPP platform, the lack of support of industry players could be a major barrier to a generalisation of this practice.

The engagement must be twofold:

- Initiatives can arise bottom-up, or top-down, or both;
- Financial and Human Resources support needs to be approved and engaged.

| |
|---|
| A formal partnership needs to be agreed and established by relevant European Officials and major industry players on the base of a future commitment and a concrete activity plan. |

### *Adopt formal PPPs rules and governance*

A proper leadership team should be appointed to manage the PPP and to set-up basic rules that will allow participants to understand the objective, the expected outcomes and how contribute to them.

Participants themselves need to understand the key features of the PPP[16]. In addition, the empirical observation of the governance model of successful PPPs in the world allowed to design a typical PPP skeleton.

| |
|---|
| Future PPP platform should adopt and document its governance model based on a structure similar to the proposed one based on PPP key features. |

[16]. This approach was already published in December 2011 on the ENISA Good Practice Guide on Cooperative Models for Effective PPPs (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps)

### *Advertise successful initiatives*

Larger geographical coverage, engagement of the right participants to take part in such a future platform would require the increase of the attractiveness of its results. This means that the initiative and the impact achieved should be properly advertised and publicised.

This requires the implementation of two preliminary activities:

- An Impact Assessment of any activity carried out within the Platform, i.e. the assurance that the recommendations or reports issued were followed by effects and real-life implementations;
- A surveying mechanism evaluating trend of satisfaction of participants and reputation out of the platform.

| |
|---|
| Initiatives conducted within such platforms need to be properly evaluated, and the effects should be assessed on a yearly basis to ensure that the time invested by participants achieved a positive impact. |

# Annex A: An insight on overseas CIIP approach: the National Council of ISACs and the Framework to Reduce Cyber Risks to Critical Infrastructure.

Security of critical infrastructures has traditionally be an issue of main concern not only for the US government but also for national private operators.

The National Council of ISACs (*Information Sharing and Analysis Centres*) is a volunteer group of ISACs representatives who meet monthly since 2003. Their objective is to develop trusted relationships among sectors and address common issues and concerns. The ISACs are trusted entities established by Critical Infrastructure owners and operators, whose original primary business was to provide comprehensive sector analysis to be shared among relevant stakeholders, including government. Services provided by ISACs include risk mitigation, incident response, alert and information sharing. The mission of the National Council of ISACs, "*is to advance physical and cyber security of critical infrastructures of North America by establishing and maintaining a framework for valuable interaction*".

In light of this purposes, the National Council of ISACs works for the realization of drills and exercises, real-time sector threat level reporting and emergency classified briefing. Furthermore, during incidents of national significance, the Council hosts a private sector liaison at the Department of Homeland Security (DHS) in the National Infrastructure Coordinating Centre (NICC).

Among the initiatives sponsored by the National Council of ISACs it is worth to point out the case of NICCIC (*National Cyber security and Communication Integration Centre*) whose mission is to address threats and incidents affecting the Nation's critical information technology and cyber infrastructures. The initiative concerns the *Level-Top Secret/Sensitive Compartmented Information* (TS/SCI). NICCIC operates at steady state (by promoting information sharing and data and situational awareness of its participants), during incident response phase (e.g. joint incident management) and in de-escalation phase (decision-makers support).

Furthermore, in July 2013 the U.S. Commerce Department's National Institute of Standards and Technology (NIST) released its draft outline on *Preliminary Framework to Reduce Cyber Risks to Critical Infrastructures*. The objective addressed is to kick-off the establishment process of a voluntarily-based Cyber Security Public-Private Framework which will involve "*a broad mix of companies, not-for-profit organizations, and government agencies across different sectors*". As stated in the document, the Partnership, besides being lead and coordinated by the NIST department, will rely on "*private sector inputs*". Issues have been identified as of primary concern for the Framework attention, i.e. the "*lack of standards, guidelines, and practices to address privacy and civil liberties issues, as well as the scarcity of helpful metrics for an organization's cyber security effectiveness*". The general aim is to set up an adaptable, complete and consistent interaction scheme able to deal with cyber security risks, innovation, emerging challenging and awareness raising. Finally, the interaction strategy will be based on participants' "*response to public notices, discussion at workshops […] direct communication and comments on […] documents*".

# Annex B: List of Figures

# Annex C: Consolidation of the relationships and guarantee system

*Consolidation of the relationships*

- Consolidation of existing relations among participants (created inside or outside the PPP) helps in the establishment of a trusted environment.
- Reduction of the frequent turnover of participants, involvement of experts with a high-level experience and attitude in working on collective decision-making procedures helps to create interest in other stakeholders out of the PPP.
- Set-up of regular meetings in presence helps to foster mutual trust, to share information, knowledge and experience and to stimulate new solutions for common objectives.

*Guarantee system*

- A guarantee system setting up basic rules of unishment of passive and unfair behaviours of participants is essential to set-up a collaborative interaction. All participants to the cooperation activities should subscribe it.
- An *ex novo* gurantee system should be set-up accordingly to the main features of the collaborative mechanism. A guarantee system can help to overpass initial mistrust among participants improving mutual agreement and commitment.
- Application methods of basic rules of the guarantee system should be defined and integrated in the governance of cooperation initiative. Management should be in charge of applying punischments.

TP-06-14-225-EN-N

**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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN: 978-92-9204-119-9
DOI: 10.2824/565581

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