Cooperative Models for Effective Public Private Partnerships
Desktop Research Report

About ENISA

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency which acts as a centre of expertise for the EU Member States and European institutions. It gives advice and recommendations on good practice, and acts as a "switchboard" for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the Member States, and private business and industry.

Contact details:

Editors: Lionel Dupré, Nicole Falessi and Dimitra Liveri.

Resilience and CIIP Program
Technical Department
Email: resilience@enisa.europa.eu

Acknowledgments

This report was prepared by Landitd Ltd. on behalf of ENISA.

It is part of ENISA's Work Program on Resilience of Public e-communication Networks. Under this Work Program, the Agency, among others, takes stock and analyses of Member States (MSs) regulatory and policy environments related to resilience of public communication networks.

ENISA would also like to thank Landitd Ltd. for their professionalism and dedication that resulted in this great report.

Legal notice

Table of contents

Executive summary

Executive Summary

Critical Information Infrastructure Protection (CIIP) is seen as a vital part of national security. At the same time, a large part of the critical infrastructure of Member States is managed by industry. Industry and government must, therefore, work together to ensure that critical infrastructure is secure and resilient.

In many Member States public and private organisations co-operate through Public Private Partnerships (PPPs) in order to address CIIP. There is no common definition of what constitutes a PPP. Diversity is valuable yet there also exists a need for interworking and a common understanding, especially when taking a European.

Some of the PPPs have developed effective processes and co-operative models. Sharing their experiences will enable others to address the barriers and issues involved in initiating and sustaining partnerships and thus increase the likelihood of success.

In light of this ENISA has conducted a study looking at Public Private Partnerships, in order to collate information from the learning and experiences of existing PPPs. This report is for:

- Those national authorities and private industries who are establishing a well-formed partnership for the first time. Here the value might encompass recommendations and ideas for providing membership incentives.
- Those in existing partnerships who are experiencing barriers who can draw from advice.

This is the first report of this study, which sets out findings from the initial phase of a research project to study 'Cooperative Models for Effective Public Private Partnerships'. This report summarises the desktop research.

Key findings

Despite the diverse variety of PPPs studied, a taxonomy with seven components has been identified. Each component includes characteristics needed to describe the range of options for establishing a PPP.

The components of the taxonomy cover:

- How the PPP is organised,
- What aspects of security and resilience the PPP addresses
- What types of services the PPP offers in addressing its scope
- What types of security threats the PPP considers within its scope
- What defines the scope of the community in the PPP
- What links the PPP has with others and
- How the PPP started and evolved

Several interesting points were noted when analysing the example PPPs.

- As many threats are international, some Member States' PPPs see the value of international co-operation and partake in bilateral, or even multilateral agreements.
- Sometimes the PPP is a sub part of a larger organisation and cannot be easily distinguished from the parent organisation.
- There are different governance models used by PPPs and their correlation with other aspects such as services and/or their scope should be explored further.
- Many PPPs focus on either Protection or Response/Recovery, while some appear to do both.
- Both Mandatory and Voluntary membership have been identified as different characteristics of a PPP. However, on closer examination, the differences are more subtle. For example, membership subscription may be mandatory but taking part in Information Sharing could be voluntary.

The next stage in the project will draw from direct input from PPP participants and/or academic literature, to refine this early taxonomy.

Introduction

1. Introduction

1.1 Background, Policy Context

The importance of public-private partnerships has been widely recognised by both public sector policy-makers and industry alike. Recent European Commission's Communications[1] have highlighted the importance of Network and Information Security (NIS), and resilience for the creation of a single European Information Space. They stress the importance of dialogue, partnership, and empowerment of all stakeholders to properly address these threats. The reviewed eCommunications Regulatory Framework as well as the Commission's Communication on Critical Information Infrastructure Protection (CIIP) propose concrete policy and regulatory provisions for the improvement of security and resiliency[2] of public telecommunications including the establishment of a European Public-Private Partnership for Resilience (EP3R). Moreover, the Council Resolution on "A collaborative European Approach to Network and Information Security" recognises "the importance of multi-stakeholder models such as Public-Private Partnerships (PPPs)" in addressing current and emerging threats in an effective way.

A number of EU Member States have gained substantial experience with Public-Private Partnerships, where they have brought together key stakeholders, including government departments, national agencies, regulators, and industry. The incentives for a co-operative partnership between public and private sector are evident, such as economic and qualitative incentives deriving from information sharing. However the barriers and challenges throughout the establishment and progress of this partnership remain and must be eliminated or at least handled with care to avoid jeopardising the level of trust between the involved parties[3].

Analysis of governance models can help identify how and which co-operative frameworks are best suited to address the issues at stake. As in all partnership cases, especially those who involve information sharing, a clear framework is needed which will include:

- specific definition of the **roles** in the public and private stakeholders involved,
- their **relationships** and
- the **areas** for co-operation.

If organisations are to face effective regulatory and/or non-regulatory requirements, public-private co-ordination needs to be optimised.

ENISA's scope on this particular stage of the project is to engage with national and international stakeholders in order to understand their current use of co-operative models for effective Public-Private Partnerships.

1 "i2010 – A European Information Society for growth and employment" and "A strategy for a Secure Information Society".
2 The ability of a network to provide and maintain an acceptable level of service in the face of various challenges to normal operation, ENISA, 'Stock Taking of Policies and Regulations - Resilience of Communications Networks', 2008 http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/?searchterm=stock taking
3 ENISA Study on 'Incentives and Challenges for Information Sharing in the context of network and information security', 2010 http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing

1.2 Research Aims

Thus there is a need to understand and analyse these experiences and finally to reach stakeholder consensus on:

"How and which pan-European co-operative frameworks are best suited to address the issues at stake"

The final report on Cooperative Models for PPPs, will provide recommendations and options on the effective inauguration of a partnership and on any reformulation that can be used to get over challenges in an already existing partnership.

This desktop research forms an initial step in understanding these co-operative frameworks (or models) for PPPs. The desktop research aim was to:

"Define a common mechanism to describe the rich variety of ways PPPs are implemented".

Published information about PPPs was analysed and the output from this research formed a structure or taxonomy for characterising PPPs. Once validated by key stakeholders, this could be used as part of a Good Practice Guide (GPG) assisting stakeholders to select which characteristics are likely to be the most effective, given their particular environment and issues.

All those who influence or lead national or international PPPs will gain insights into the range of PPP co-operative models found at this early research stage and the implementation options for PPPs. Reflecting on the implementation decisions of others can offer valuable inspiration.

1.3 Clarity of Terms

During the research it became clear that we needed to understand what the term 'Stakeholder' means in the context of various documents. In our study, stakeholders can refer to either PPP organisations or participants and their representatives within a PPP.

We therefore propose to replace the use of stakeholders with the following:

- **PPPs** - These are the partnership organisations that are the focus of this study. The co-operative models they employ will be analysed in order to understand good practice.
- **Participants** - These are the organisations who are members of the PPP. They may be public or private organisations and have a variety of classifications: Government, ISP, Telcos, Content providers, Research organisations, Regulatory bodies etc.
- **Representatives** - These are people who may be representing both their participating organisation (such as a Telco) as well as the PPP that they are active within.

Scope and criteria

2. Scope and Criteria

For the purposes of this study we define a PPP as:

An organised relationship between public and private organisations which establishes common scope and objectives, and uses defined roles and work methodology to achieve shared goals.

Therefore PPPs were selected which:

- Included national, international and pan European partnerships;
- address threats to enhance security and resilience of e-Communication networks including all hazards threats;
- address the ever growing number and complexity of threats to the availability and integrity of networks and services. (This focus was weighted towards those PPPs which address high impact consequences such as risks to critical national infrastructure and Cybercrime).

2.1 Criteria for selecting PPPs to approach for desk-top research:

In order to ensure the quality of this initial study, a spread of PPPs was selected so that the following criteria were met:

- They have a specific clear focus that aligns to our interests (CIIP, Cybercrime)
- They contribute to agreed geographical spread requirements addressing maturity and cultural spread
- They contribute to agreed spread of activities, e.g,. Information Sharing, Resilience Exercises etc
- They contribute to the agreed spread of organisational roles within PPP membership e.g. regulator, service provider.
- There is sufficient quality and quantity of published material.

In total 20 PPPs and other organisations were researched during this desk-top study and they covered 12 Member States, 2 other nations, 1 international organisation. In some cases, a PPP is a clearly defined, stand-alone, organisation. In other cases, published details do not make clear the relationship between the PPP and an overarching, larger organisation.

Research Methodology

3. Research Methodology

3.1 Profiling PPPs

The desktop research focused on collating and analysing information from public sources such as websites and conference presentations.

Methods and approach

The information in this report is drawn from three sources:

- A desktop review of internet based resources on twenty PPPs
- A review of academic publications.
- Contact with a small number of subject experts

A sample of twenty PPPs, which work to address threats to the security and resilience of e-communication networks, was identified against specific criteria. The sample spanned twelve Member States and three other countries.

Australia	TISN (Trusted information sharing network)
Austria	Cert-AT A-Sit (Austrian centre for secure information technology)
Belgium	BELNIS (Belgian network of information security)
Estonia	Look@world and Computer Protection 2009
Finland	NESO (National emergency supply organisation) which hosts clusters and pools of PPPs UISA (Ubiquitous information society advisory board)
France	ANSSI (Agence nationale de la securite des systems d'information) hosting the Operations centre of the security of information systems (COSS)
Germany	BSI (Federal office for information security) which has the Umsetzungsplan KRITIS (UP KRITIS)
Italy	AIIC (Italian association of critical infrastructure experts)
Netherlands	NCOT (national continuity forum telecommunication) ECP-EPN (Electronic platform Netherlands) NICC- ISACs (National Infrastructure against cybercrime – Information Sharing and analysis centres.
Spain	CNPIC (National centre for the protection of the critical infrastructure)
Sweden	PTS (Swedish post and telecom agency) NTSG (National crisis management coordination group)
Switzerland	MELANI (Reporting and analysis centre for information assurance)
United Kingdom	CPNI IEs (Centre for the protection of the national infrastructure Information exchanges in a variety of sectors) EC-RRG (Electronic communications resilience and response group)
United States	NCC-ISAC (National coordinating centre for telecommunication Information sharing and analysis centre.) NSIE (Network security information exchange)
CCD COE	Cooperative cyber defence centre of excellence (Germany, Italy, Latvia, Lithuania, Estonia, Spain, Slovakia)

Table 1. Studied PPPs

A significant number of sources were obtained and these can be found in Appendix A. The search for PPPs utilised ENISA resources such as the Stock take documents[4] and other research findings such as the work on incentives and barriers[5]. This provided a starting point for a deeper internet search. Each researcher provided an identifier for the source of evidence, which was peer reviewed for accuracy and relevance.

The taxonomy emerged from the initial study of these partnerships using a framework which was common. They derived, for each PPP selected for inclusion in the study, from information which was collated and profiled using the following framework:

- Size and composition of partnerships
- National or Pan-European or international
- Profile and role of participants
- Sectors addressed
- Topics covered
- Legal issues
- Incentives provided
- Services offered
- Establishment and management of trust
- International links.

In some cases, documents were translated from their original language. The subsequent stages of the research, which include a questionnaire, interviews and a validation workshop will enable the findings to be enriched and validated.

3.2 Analysis of PPP Profiles

The 20 profiles of the co-operative models and their environments were then analysed. Initially a brainstorm created a candidate list of characteristics about PPPs which was then tested and adapted by reviewing each of the 20 profiles in turn. Each profile was analysed using the taxonomy which indicated how the taxonomy should evolve. Characteristics were recognised as describing common aspects and these were clustered and reorganised into a hierarchy. This method of analysis ensured the taxonomy could be used to represent the co-operative model used by all 20 of the example PPPs.

In order to analyse each PPP, definitions for each element in the taxonomy hierarchy needed to be agreed. The resulting taxonomy and definitions can be found in section 4, 'A Preliminary Taxonomy for PPPs'.

Thus the analysis session commenced with an initial list of characteristics and finished with an early taxonomy for describing PPPs which can be validated with direct input from Member State representatives. While moving forward with this study and analysing the components of more PPPs, the taxonomy will be refined to create an easily adapted framework for private and public stakeholders, regardless of the stage they are at in the partnership process.

The observations from the desktop research and analysis are detailed in section 5 'Conclusions and Outlook'.

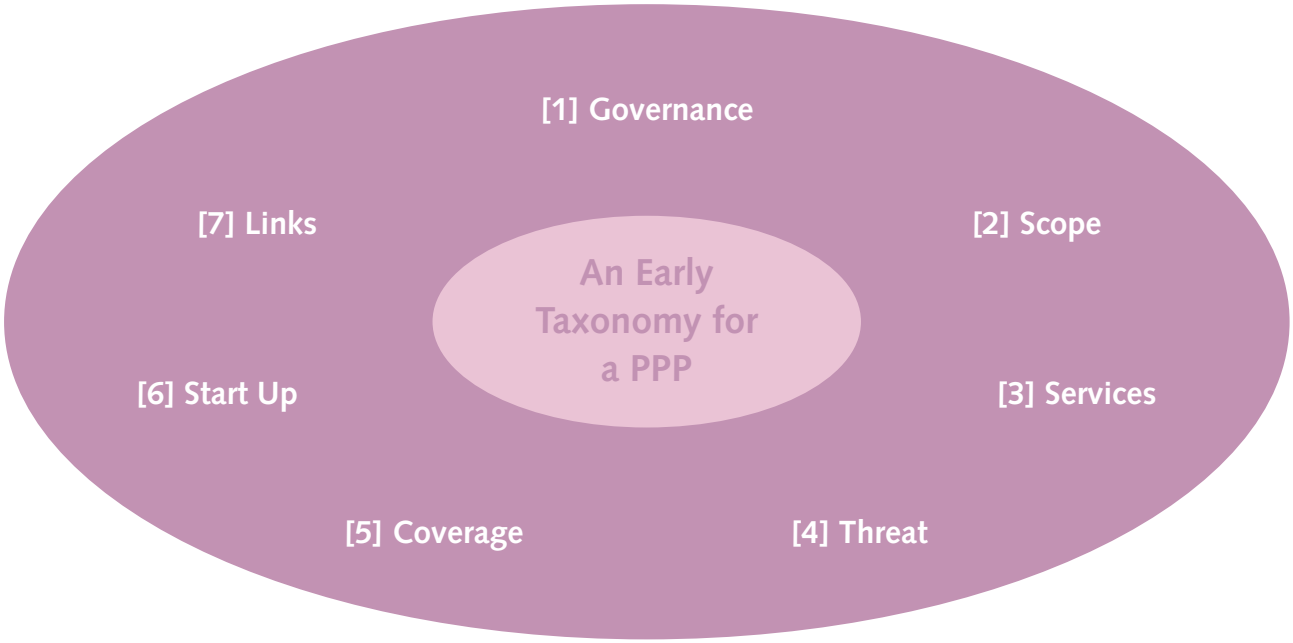
4 http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies
5 http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing

A Preliminary Taxonomy for PPPs

4. A Preliminary Taxonomy for PPPs

After analysing all the information on the profiled PPPs, the outcome was a taxonomy with components and characteristics for describing the co-operative models used by PPPs.

The top level of the taxonomy of a PPP covers 7 components:



[1] Governance Structure: This component covers how the PPP is organised, how partners work together, its rules and financing.

[2] Scope: This component covers what aspects of security and resilience the PPP addresses. A life-cycle model of security is used as it covers the range of activities involved, such as protection and response.

[3] Services: This component lists the types of services that the PPP offers in addressing its scope, which includes, for example, information sharing and running exercises.

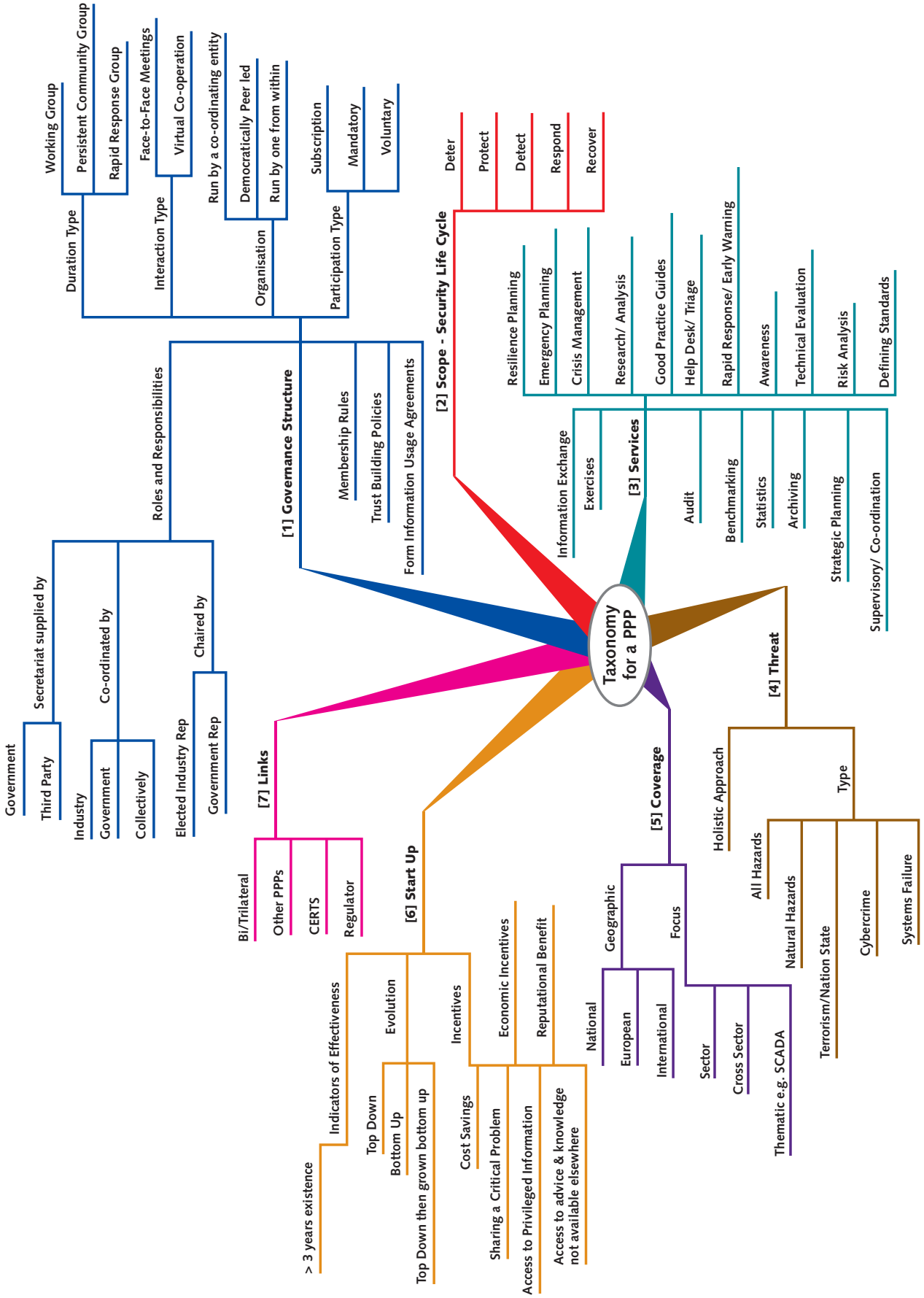
[4] Threat: This component covers the types of security threats that the PPP considers within its scope and which helps define the detail in the services provided. In addition, this notes if the PPP addresses threats using a holistic approach.

[5] Coverage: This component specifies whether the PPP involves partners at a national, pan- European or International level, as well as whether its focus is thematic, sectoral or cross-sectoral.

[6] Start Up: This component describes how the PPP started up; how it evolved and grew as well as incentives used to encourage participation. Finally, we note if the PPP is older than 3 years, in order to identify PPPs in their early stages.

[7] Links: The final component describes what links the PPP has with other PPPs and organisations outside its immediate membership.

This taxonomy is the result of a desktop study and is an early and evolving hierarchy that will be strengthened and validated by a questionnaire survey, interviews with PPP participants and a validation workshop involving PPP participants. The full hierarchy for this early taxonomy for describing PPPs is depicted in the following diagram:


Taxonomy for a PPP
[1] Governance Structure
Duration Type
Working Group
Persistent Community Group
Rapid Response Group
Interaction Type
Face-to-Face Meetings
Virtual Co-operation
Organisation
Run by a co-ordinating entity
Democratically Peer led
Run by one from within
Participation Type
Subscription
Mandatory
Voluntary
Roles and Responsibilities
Secretariat supplied by
Government
Third Party
Co-ordinated by
Industry
Government
Collectively
Chaired by
Elected Industry Rep
Government Rep
Membership Rules
Trust Building Policies
Form Information Usage Agreements
[2] Scope - Security Life Cycle
Deter
Protect
Detect
Respond
Recover
[3] Services
Resilience Planning
Emergency Planning
Crisis Management
Research/ Analysis
Good Practice Guides
Help Desk/ Triage
Rapid Response/ Early Warning
Awareness
Technical Evaluation
Risk Analysis
Defining Standards
Information Exchange
Exercises
Audit
Benchmarking
Statistics
Archiving
Strategic Planning
Supervisory/ Co-ordination
[4] Threat
Holistic Approach
Type
All Hazards
Natural Hazards
Terrorism/Nation State
Cybercrime
Systems Failure
[5] Coverage
Geographic
National
European
International
Focus
Sector
Cross Sector
Thematic e.g. SCADA
[6] Start Up
Indicators of Effectiveness
> 3 years existence
Evolution
Top Down
Bottom Up
Top Down then grown bottom up
Incentives
Cost Savings
Economic Incentives
Sharing a Critical Problem
Reputational Benefit
Access to Privileged Information
Access to advice & knowledge not available elsewhere
[7] Links
Bi/Trilateral
Other PPPs
CERTS
Regulator

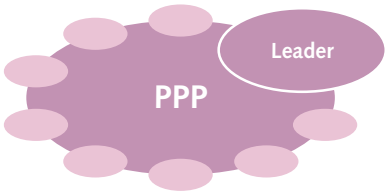
Each of these components and the characteristics of the taxonomy are now described. There is no significance to the order in which they are presented.

[1] Governance Structures

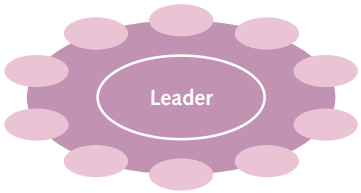
From this desktop research, governance structure was the most complex part of the taxonomy. More detailed information on PPPs and how they relate to the governance models will be gained in the later stages of the study.

[1.1] Organisation - This described how the PPP was led, co-ordinated and organised. These categories were inspired by the work of Milward and Provan on collaborative networks[6].

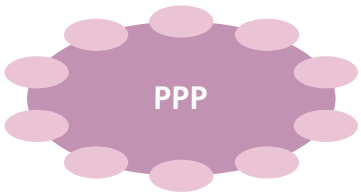
- **Run by one from within** -
  Having one of the members of the partnership being responsible for the leadership of the PPP was by far the most frequently found organisational structure.



- **Run by a coordinating entity** -
  A less frequent option is to have a body specifically created that is responsible for the leadership and co-ordination of the partnership.



- **Democratically Peer led** -
  True peer or democratic collaboration was seen infrequently in this desktop study. Sometimes PPPs use a rotating chair in order to approach achieving this type.



[1.2] Roles and Responsibilities - In describing or designing a PPP the roles can be a key decision. Defining who provides secretariat services, who co-ordinates the activities as well as who leads the PPP, are important characteristics. A variety of choices were discovered during the desktop study. The following taxonomy categories define these options:

- **Chaired by**
  - **elected representatives from Industry**
  - **representative from Government**
- **Secretariat supplied by**
  - **third party (non government)**
  - **national government**
- **Co-ordinated by**
  - **government**
  - **industry**
  - **collectively**

6 http://www.businessofgovernment.org/sites/default/files/CollaborativeNetworks.pdf

[1.3] Duration Type - The purpose and duration of activity for a PPP, combined and fell into three distinct types which have a close maping, but not perfect map, to the work of Milward and Provan on collaborative networks[7]:

- **Persistent Community Groups** - These are set up to persist for a long time and to develop a community for a specific purpose. There is unlikely to be a clear end point to the usefulness of the PPP. These most closely match a combination of Milward and Provan's Information Diffusion Network but also Community Capacity Networks. Information Exchanges typify this category.

- **Working Groups** - These are set up for a specific, discrete, purpose and often belong to a parent organisation, which may or may not be a PPP. There is a problem to solve or a plan to implement and the partnership works together to make this happen. There is an expectation that once the purpose has been achieved that the PPP might dissolve. These most closely match Milward and Provan's Service Implementation Networks.

- **Rapid Response Groups** - Here the PPP could exist for a short number of days or even hours, the PPP has a very specific purpose in order to address an urgent issue. This issue is often an incident or newly discovered vulnerability. The same PPP may re-occur at different moments in time, each time with a different membership dependant on the urgent issue. These most closely match Milward and Provan's Problem Solving Network. Some PPPs combine persistent and rapid response. They meet and plan and practise strategies, then if there is an emergency they use rapid response.

[1.4] Participation Type - How the partners participate within the PPP is an important characteristic that complements the characteristics about roles and responsibilities in [1.2].

- **Subscription** - The requirement to pay a subscription is a key consideration and the PPPs studied included both those with subscriptions and without. Research recognised that subscriptions might link with the decision to make membership mandatory or voluntary.
- **Mandatory** - Some PPPs require all members of a sector to be members. This may be regulated. We recognised that this might be linked to the scope and services offered by the PPP. From desktop sources this appears to be an unusual option.
- **Voluntary** - Other PPPs recognise that they can be effective with partial coverage of their target members or believe that mandating membership would be counter-productive and utilise other incentives in order to gain appropriate coverage in their membership.

[1.5] Interaction Type - The interaction type for a PPP is believed to be linked to the nature of the relationships necessary between participants and the complexity of the information and activities. Some PPPs use a combination of both interaction types for different services.

- **Face-to-Face Meetings** - Regular physical meetings are a strong characteristic of this type of PPP. Co-ordination and secretariat information may well be transferred virtually but the core purposes of the partnership are achieved face to face. There is believed to be a strong requirement for this type of interaction for effective information exchange.
- **Virtual Co-operation** - This is where the core purpose of the PPP is to work together using virtual means such as conference calls, emails and shared work spaces. There may be periodic face to face meetings in to co-ordinate activities or provide updates on progress but the main purpose of the PPP is achieved virtually.

[1.6] Membership Rules - Some PPPs have a formal set of membership rules. These can include requirements for entering membership, details of the rights and responsibilities of membership and some define what would cause a member to be excluded from membership.

7 http://www.businessofgovernment.org/sites/default/files/CollaborativeNetworks.pdf

[1.7] Formal Information Usage Agreements - Some PPPs involve the exchange of information. For example, this can relate to incidents and vulnerabilities. In order to enable participants to share information, a formal agreement between participants is used. This may assign grading to information that defines how and when information can be used. Examples include:

- **Non Disclosure Agreements (NDAs),**
- **The Traffic Light Protocol (TLP) ,**
- **Deed of confidentiality.**

[1.8] Trust Building Policies - Depending on the services offered, participants in a PPP may need to develop a trusting relationship with their fellow participants. This is widely reported to be necessary in Information Exchanges. Often PPPs that require trust have carefully designed their policies, membership rules, requirement for security clearance, and interaction type. They have limited substitution for attending meetings, and use formal information usage agreements in order to enable trusted information sharing.

[2] Scope

Scope is mapped to the security life cycle. Some PPPs have a scope that covers all aspects of the life cycle while others focus on part of the life cycle. From this research it is likely that some types of service (as categorised in [3] - see below) can support all parts of the life cycle while other services might focus on delivering specific parts of the life cycle.

- **Deter** - A PPP with this scope will focus on trying to deter attackers and an example service might be public awareness raising of security and consequences, or law enforcement actions.
- **Protect** - A PPP with this scope uses research into new security threats as well as protection mechanisms, and focuses on developing industry standards as well as information sharing communities.
- **Detect** - A PPP with this scope often uses Information Sharing and Early Warning systems to understand and address new threats.
- **Respond** - A PPP with this scope will develop and deliver capability to cope with the initial impact of an incident or emergency. This might include services such as Computer Security Incident Response support, Mutual aid, Exercises, Emergency Planning and Crisis Management.
- **Recover** - A PPP with this scope would develop and deliver capability to repair the final impact of an incident. Whereas responding might involve using back up equipment, recover involves returning systems to business as usual. Again this might include services such as Exercises, Emergency Planning and Crisis Management.

[3] PPP Services

Through the desktop research a rich set of services was identified. These may evolve into clusters of similar or related services as the study progresses. Some services will generate outputs that feed other services. For example an exercise might feed insights into Resilience Planning. More detailed analysis and categorizing of these services will be conducted if it is recognised that the resulting taxonomy will be important in increasing knowledge of effective co-operating models.

- Research/Analysis
- Good Practice Guides
- Information Exchange
- Rapid Response/ Early Warning
- Exercises
- Awareness Raising
- Technical Evaluation
- Defining Standards
- Help Desk/ Triage
- Risk Analysis
- Crisis Management
- Resilience Planning
- Emergency Planning
- Security Audit
- Benchmarking
- Supervisory/ Co-ordination
- Statistics
- Archiving
- Strategic Planning

[4] Threat types

PPPs can be characterised by the nature of the security threats that they aim to address. It is recognised that this list is not exhaustive, for example some may say the 'Insider threat' should be included. However at this stage of the research the following have been chosen as key threat types:

- **All Hazards** - Here PPPs are aiming to address threats of all types.
- **Natural Hazards** - Natural hazards would include floods, hurricanes etc. Natural Hazards are unintentional.
- **Systems Failure** - This type of threat covers both hardware and software failure. This might include a software upgrade that causes an unintended side effect or a failure in a hardware component. System Failure in this context is taken as an unintentional act.
- **Cyber-crime**- These are threats resulting from malicious acts associated with illegal activities. Examples might be fraud, cyber theft and denial-of-service attacks.
- **Terrorism/Nation State** - This covers malicious acts which compromise confidentially or integrity by cyber means and deliberate, disruption of computer networks (often large scale) and typically with the purpose of creating alarm and panic. In Cyber-crime the objective is for criminal gain; here the purpose is disruption or espionage.

[4.2] Holistic Approach - An emerging trend is for security to address threats by considering issues from a range of viewpoints. For example Natural Hazards such as flooding can be addressed not only from ensuring electronic services are maintained but also addressing problems in physical security such as looting and well as training personnel through exercises.

[5] Community coverage

A PPP is also defined by the community that is involved in, and is served by, the PPP. This is characterised by both its geographical level and the sector and thematic focus.

[5.1] Geographic -

- **National** - The PPP participants are from within the national boundary
- **European** - The PPP participants are from several European nations.
- **International** - The PPP community is from international countries.

[5.2] Focus - This characteristic details the community that is involved in and is served by the PPP.

- **Sector** - The PPP serves particular sectors such as Finance, Transport, Power etc
- **Cross Sector** - Here the PPP is focused on serving the security community across a range of sectors, for example, addressing all sectors involved in Critical Infrastructure.
- **Thematic** - PPPs can also be brought together to address a particular issue or common area of interest e.g. Supervisory Control and Data Acquisition (SCADA).

[6] Start Up

The information about how the PPP started and how it evolved is valuable in understanding how to develop new partnerships. This covers how they grew and evolved, how participants were attracted to become members and what indicators there are that the PPP is effective.

[6.1] Evolution - This category describes how the PPP started and then grew.

- **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. It started top down with a strategic requirement but then the membership and leadership developed bottom up.

[6.2] Incentives - Many of the PPPs studied listed the advantages of membership and these were categorised in relation to the incentives documented in ENISAs work on Incentives and Barriers[8]. This resulted in following characteristics:

- **Cost Savings**
- **Sharing a Critical Problem**
- **Access to Privileged Information from government**
- **Economic Incentives above cost savings**
- **Reputational Benefits, both from a personal and organisational viewpoint**
- **Access to advice & Knowledge not available elsewhere**

[6.3] Indicators of Effectiveness - Some Characteristics of a PPP indicate that the PPP has been effective. The analysis highlighted that more information is needed to represent this component.

[7] Links

PPPs also link with other organisations. These are links with external organisations that are not members of the PPP.

- **Bi/Trilateral** - Some PPPs have special trusting relationships with mirror organisations in other nations.
- **Other PPPs** - PPPs have links with other PPPs within the same nation.
- **CERTS** - PPPs link with Emergency Response teams.
- **Regulator** - PPPs have links with their regulatory body.

8 http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing

Conclusions and Outlook

5. Conclusions and Outlook

This research provided the foundations of the later stages of the wider study. The following points summarise this learning.

- As many threats are international, some Member States' PPPs see the value of international co-operation and partake in bilateral or even multilateral agreements.
- Sometimes the PPP is a sub part of a larger organisation and cannot be easily distinguished from the parent organisation.
- There are different governance models used by PPPs and their correlation with other aspects such as services and/or their scope should be explored further.
- Many PPPs focus on either Protection or Response/Recovery, while some appear to do both.
- Both Mandatory and Voluntary membership have been identified as different characteristics of a PPP. However, on closer examination, the differences are more subtle. For example, membership subscription may be mandatory but taking part in Information Sharing could be voluntary.
- This study enabled the definition of a taxonomy with 7 components, each with a set of characteristics that could guide the implementation choices for a PPP. From desktop research little is available about the incentives for each of those choices. This will be addressed in the later stages of this study.
- Little published information is available on the barriers faced by PPPs or their problem areas with related solutions. These are unlikely to be openly published because of concerns about damage to reputation or in case weaknesses would be exploited. Later stages in this study plan to provide a mechanism that will enable PPPs to share this information confidentially, in a manner that addresses these concerns.
- The desktop study highlighted that a body of information issuing from academic research, pertaining to PPPs, their function, structure and governance exists. Carefully selected academic literature will be used to complement learning from later stages of this study.
- The analysis workshop that finalised the desktop stage identified some interesting possible correlations between some of the taxonomy components, for example between the scope and the services supplied by the PPP. These correlations will be investigated further in the later stages of this study.
- Valuable insights can be gained by drawing from other ENISA documents, such as the recently published 'Incentives and Challenges to Information Sharing in the context of Network and Information Security' which influenced the [6.2] Incentives section of the taxonomy.
- A challenge for the interviews and questionnaire in the later stages of this study will be to determine what constitutes good practice. A PPP might contain partial elements of Good Practice and/or good practice might change depending on the maturity of the partnership, the political context, the purpose etc. What does become clear, however, is that practices evolve over time, and that flexibility is required.

Lessons Learnt

6. Lessons Learnt

Despite the variety of PPPs studied and limitations of desktop research, it has been possible to identify an early taxonomy with seven components, each with characteristics describing the range of options for implementing a PPP to address security and resilience for e-communication.

This preliminary taxonomy can be used as a common framework for understanding PPPs. In addition, future studies could use other sources, such as direct input from PPP participants and/or academic literature, to refine this taxonomy.

In the progress of this study on Cooperative Models for Effective PPPs, the taxonomy will be refined according to the information shared by the stakeholders. The model in the final report will aim to be sufficiently flexible to be relevant to partnerships at both early and later stages of development. It will aim to inspire approaches to increase effectiveness and propose solutions to address issues.

Appendix A

Appendix A: List of Desktop Research Sources

International and European Sources

www.enisa.europa.eu/act/sr/files/deliverables/who-is-who-directory-on-nis.-2009

www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide

www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing

www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies?searchterm=stock

www.nis-summer-school.eu/nis09/presentations/ouzounis_thorbruegge.pdf

www.enisa.europa.eu/act/it/inf/tech/ws2008/ws1/ws1-report/view

kms2.isn.ethz.ch/serviceengine/Files/CRN/90663/ipublicationdocument_singledocument/C264D47C-0AB6-45FD-9869-2A24380F8A38/en/CIIP_HB_08.pdf or

www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663

www.thebci.org/ContSeptOct10_full%20issue.pdf

ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf

www.ictsb.org/Working_Groups/NISSG/NISSG_introduction.htm

Austria

www.a-sit.at/

translate.google.co.uk/translate?hl=en&sl=de&tl=en&u=http%3A%2F%2Fwww.a-sit.at%2F

www.enisa.europa.eu/act/sr/files/country-reports/Austria.pdf

www.cert.at/

www.first.org/members/teams/aconet-cert/

www.first.org/members/teams/cert_at/

Australia

www.tisn.gov.au/

www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29~TISN+Deed+of+Confidentiality+-+Fact+Sheet.PDF/$file/TISN+Deed+of+Confidentiality+-+Fact+Sheet.PDF

www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF

www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/%289A5D88DBA63D32A661E6369859739356%29~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy+Supplement.PDF

Belgium

www.enisa.europa.eu/act/sr/files/country-reports/Belgium.pdf

www.fedict.belgium.be/nl/binaries/Fedict_rapport_ENG_v01_HR_tcm167-60449.pdf

www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf

Switzerland

www.melani.admin.ch/index.html?lang=en

www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/melani/view

www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en

Germany

www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/uwe

www.bsi.bund.de/cln_156/EN/Home/home_node.html

www.bsi.bund.de/cln_156/ContentBSI/Themen/CERT_Bund/AufgabeZiele/aufgaben.html

www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/cip_stategy.pdf?__blob=publicationFile

www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

www.enisa.europa.eu/act/sr/files/country-reports/Germany.pdf

Spain

www.aetic.es/CLI_AETIC/ftpportalweb/documentos/AETIC_INGL%C3%89S.pdf

www.enisa.europa.eu/act/sr/files/country-reports/Spain.pdf

www.utpl.edu.ec/gcblog/

www.cnpic-es.es/cnpic/index.php?option=com_content&view=article&id=38&Itemid=56&lang=en

www.cnpic-es.es/cnpic/images/ponencias/forociip/panel2/cnpic_foro_ciip.pdf

Finland

www.enisa.europa.eu/act/sr/files/country-reports/Finland.pdf

www.nesa.fi/security-of-supply/public-private-partnership/

www.nesa.fi/security-of-supply/public-private-partnership/

www.arjentietoyhteiskunta.fi/inenglish

www.arjentietoyhteiskunta.fi/files/73/Esite_englanniksi.pdf

www.arjentietoyhteiskunta.fi/files/39/members_of_the_information_society_council.pdf

Estonia

www.riso.ee/en/node/80

www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdfstonia

www.ccdcoe.org/37.html

docs.google.com/viewer?a=v&q=cache:_EF82nicx8IJ:www3.lrs.lt/owa-bin/owarepl/inter/owa/U0037979.pdf+Look%40world+estonia&hl=en&gl=fr&pid=bl&srcid=ADGEESgX904cRq6_FBkBfYZfrFqXllrVIuL3PLOKhhYOf95XqZVWGef1nmVfPV5-w6hmuca6rAbfWMI4iEFtyYiK3d3w0RmeH0ntDoma9HPb8UQ6HZcSPCNMk3QXxOj1WoKFBEMF1Zqh&sig=AHIEtbSMFvnKwP851hA9WgAEUbJ0-02Dmw

www.ebaltics.com/00705650?PHPSESSID=c6b15e9cafef1a23f94512dff948263e

www.ebaltics.com

France

www.enisa.europa.eu/act/sr/files/country-reports/France.pdf
www.ssi.gouv.fr
www.eurosafe-forum.org/userfiles/4_1_French%20approach%20protection%20crit%20services_Dodeman.pdf
www.sgdsn.gouv.fr/

Italy

www.enisa.europa.eu/act/sr/files/country-reports/Italy.pdf/view

Netherlands

www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf
www.enisa.europa.eu/act/sr/files/country-reports/Netherlands.pdf
www.nis-summer-school.eu/nis09/presentations/11B-%20Hafkamp.pdf
www.samentegencybercrime.nl/UserFiles/File/NICC%20brochure_uk.pdf
www.nis-summer-school.eu/nis09/cvs/simon_van_merkom.html
www.govcert.nl/render.html?it=41
www.intgovforum.org
www.ecp.nl
www.vde.de/de/technik/aal/steckbriefe/seiten/ecp-epn.aspx
www.ddsi.org/htdocs/DDSI/RandD/De%20Bruin.pps
www.nis-summer-school.eu/nis09/presentations/11a-Merkom.pdf
www.rijksoverheid.nl/documenten-en-publicaties/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi.html
www.samentegencybercrime.nl/UserFiles/File/NEW-lentebericht_2010-UK%20DEFINITIEF.pdf
www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/wim
ec.europa.eu/information_society/policy/nis/docs/ep3r_workshops/1st_june2009/04_merkom_moea_nl.pdf

Sweden

www.enisa.europa.eu/act/sr/files/country-reports/Sweden.pdf
www.pts.se/en-gb/
www.pts.se/en-gb/About-PTS/Information-materials/
ec.europa.eu/information_society/policy/nis/docs/ep3r_workshops/1st_june2009/02_engvall_pts_se.pdf
www.pts.se/upload/Faktablad/En/facts-about-ntsg.pdf
www.pts.se/upload/Faktablad/En/facts-about-glu.pdf

UK

www.cpni.gov.uk/Docs/re-20040601-00395.pdf

www.cpni.gov.uk/Docs/ie-membership-guidelines.pdf

www.cpni.gov.uk

eu2009.pts.se/Documents/PTS%20Resilience%20Conference%20-%20Keith%20Wallis.pdf?epslanguage=en-GB

www.cabinetoffice.gov.uk/media/131474/telecoms_ec-rrg_tor_101108.pdf

www.enisa.europa.eu/act/res/workshops-1/2010/information-sharing-workshop/presentations/uk-information-sharing

www.enisa.europa.eu/act/sr/files/country-reports/UK.pdf/view

US

www.ncs.gov/nstac/reports/2000/NCC_NSIE.pdf

www.ncs.gov/tpos/esf/mclean/Tab%2010%20-%20NCC%20Watch.ppt

www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf

European Network and Information Security Agency

Desktop Research Report– Cooperative Models for Effective Public Private Partnerships

Luxembourg: Publications Office of the European Union, 2011

ISBN: 978-92-9204-055-0

doi:10.2824/21793

Catalogue Number: TP-32-11-860-EN-N

TP-32-11-860-EN-N

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu

ISBN 978-92-9204-055-0