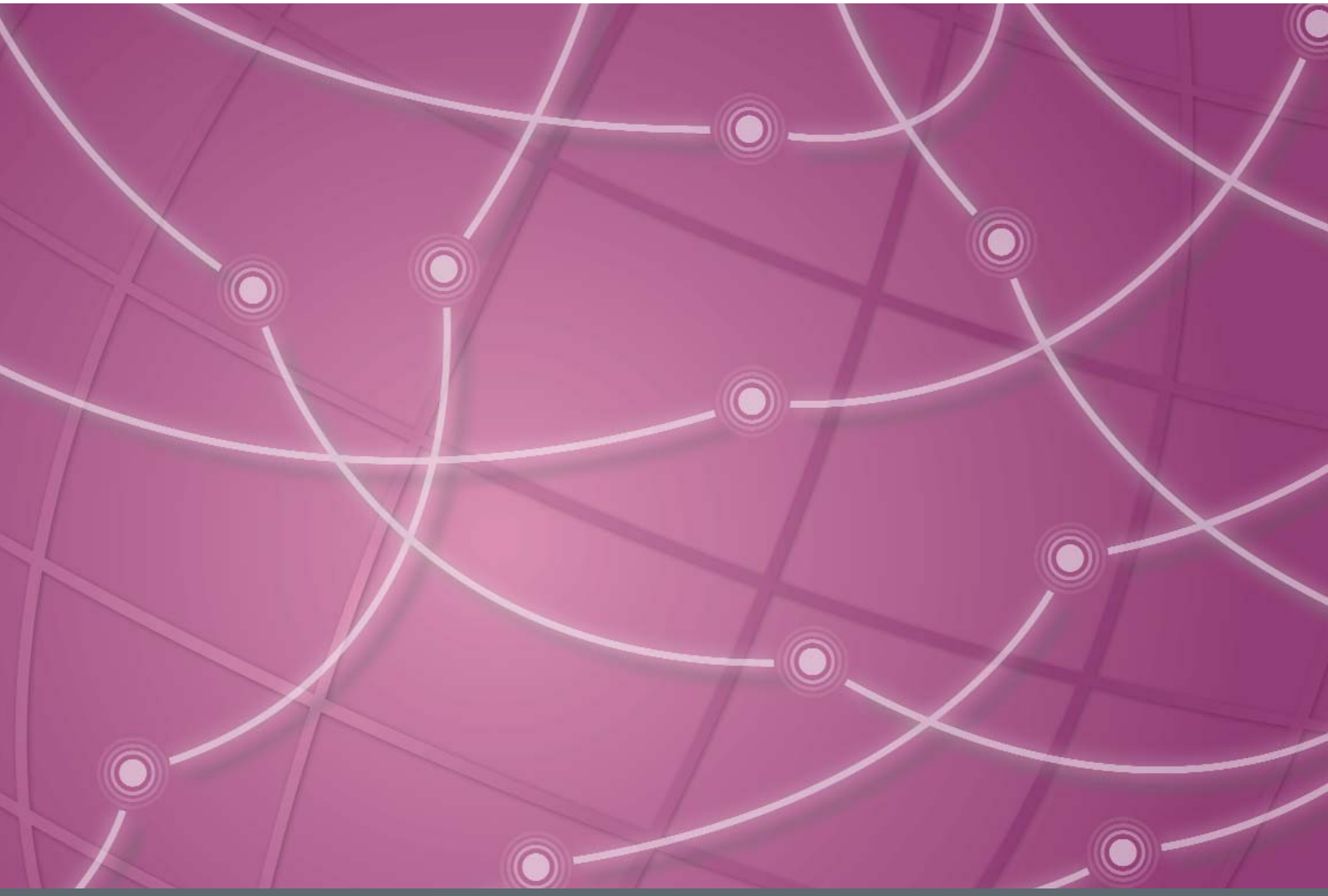

Cooperative Models for Effective Public Private Partnerships
Good Practice Guide

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.

The Authors wish to record their sincere gratitude to the many people working in, or with Public Private Partnerships, who willingly gave up their time to complete the questionnaire survey and to participate in the telephone interviews. Their contributions have been invaluable and mean that this Good Practice Guide is based on the opinions of those who have been actively involved in the setting up and running of successful Public Private Partnerships.

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

With much of a Member State's critical infrastructure in the hands of the private sector, it seems a natural solution for industry and government to work together in ensuring it is both secure and resilient. This cooperation in the form of Public Private Partnerships (PPPs) has evolved in many Member States and at different times, depending on the environment, culture and legal framework. It is therefore not surprising that there is no common definition of what constitutes a PPP addressing this area. Diversity is a strength when making networks and systems resilient, yet there also exists a need for interworking and a common understanding, especially when taking a European view. The need for a European view is demonstrated by the emergence of the European Public Private Partnership for Resilience (EP3R) that is engaging with national PPPs to address Critical Information Infrastructure Protection (CIIP) issues at a European level. There is also a need for an international view as there is a growing awareness for a truly global approach to Cyber Security and Critical Infrastructure Protection. No country can create a CIIP strategy in isolation, as there are no national boundaries in cyber-space. At the European level this is being addressed by the EU/US working group where an item on the agenda are PPPs.

This Good Practice Guide (GPG) on Cooperative Models for Effective Public Private Partnerships builds on the desktop research, which revealed a set of characteristics that can be used to describe these PPPs in a common form despite their diversity. The results from 30 questionnaires and 15 interviews consolidated and validated a taxonomy, presented in the desk-top research as a supporting document, and revealed five main components addressing the **Why**, **Who**, **How**, **What** and **When** questions associated with creating and maintaining PPPs. This data was collected from both public and private sector stakeholders across 20 countries.

This is not a prescriptive guide, but has a focus on clarity of purpose and approach so that stakeholders can easily choose those aspects that will add value to their endeavours in setting up and running PPPs.

The Guide starts with a section on understanding the problems, which the PPP aims to address. To help the reader, a list of problems which existing PPPs have addressed is provided when answering the 'why' question. This then leads onto the identified Good Practice observed in addressing these problems. The Guide highlights recommendations, observations and, where appropriate, includes interview quotes.

Our analysis shows that despite the large number and apparent diversity, there are three main approaches taken by PPPs in addressing the problems of security and resilience of e-communication networks and systems. These have been termed Prevention Focused PPPs, Response Focused PPPs and Umbrella PPPs and their characteristics are discussed in Section 3 of the Guide.

The in-depth analysis resulting from interviews has shown some interesting and helpful consistencies in approach. For example it was previously believed that many countries supported by law the scheme of trusted information sharing because membership of PPPs was mandated. In reality, even though membership is mandated, taking part in trusted information sharing is voluntary as it is acknowledged that you cannot force members to reveal sensitive information if they see a reputational risk and see no value in doing so. The Guide clearly identifies 'Observations' such as this and any associated 'Recommendation' for good practice.

An example recommendation for good practice in this context is to provide anonymity for trusted sharing. In at least one instance a PPP has cited non-attribution as the main reason for the PPP being successful.

A second example of consistencies that were not immediately obvious relates to PPPs whose focus is cross-sector. An example of good practice from many other PPPs suggests that the communities should be homogeneous for optimum value to members, which is not consistent with cross-sector membership. In reality these cross-sector PPPs have sub-groups whose makeup is homogeneous. This realisation increases the importance of the homogeneity recommendation made in this Guide.

A third example relates to the involvement of the Regulator which in many countries is seen as a barrier to trusted information sharing because of potential conflicts of interest. In some countries the Regulator is seen as a key member and does indeed add value to the activities of the PPP. However, those PPPs who involve the Regulator do in fact recognise there is a time and place for their involvement and that they can be a barrier to trusted information sharing. Those PPPs who manage this complex relationship successfully are seen as demonstrating a notable example of good practice and again demonstrates an important consistency.

These examples show how the guide will help both existing and emerging PPPs to share a common understanding of the characteristics for an effective PPP which can be used to refine and build effective co-operation at the National and European level.

This guide provides a complement to the European good practice by introducing PPPs from the USA, Canada and Australia (detailed in Section 4). Each international PPP is briefly described and mapped to the three generic types identified from the European research. This section concludes with: seven key points detailing advice extracted from the publications of these PPPs, as well as listing their critical success factors for information sharing and finally, describes a possible way forward for international collaboration.

This Guide contains 36 recommendations described in Section 2, which are listed for easy reference in the Section 5. The overall conclusions reached are that the diversity in approach of PPPs is supported by a core set of principles, and it is recognition of these common principles, which opens the door to greater co-operation between PPPs in the future.

List of Figures

List of Figures

Introduction

1. Introduction

1.1 Background

Reliable communications networks and services are critical to both public welfare and economic stability in Europe. Today's society relies increasingly on these networks and related services. With infrastructures operated by the private sector and governments remaining responsible for the overall policy setting, a high level of network and information security can only be attained if public and private sector co-operate closely to address the ever growing number and complexity of threats. The importance of Public Private Partnerships in this field has been widely recognised by both policy-makers and industry alike.

Recent European Commission (EC) 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[2] 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[3] 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.

The European Network and Information Security Agency (ENISA), as part of its Multi-annual Thematic Programme (MTP), conducted a study, related to the overall topic of governance models for effective co-operation between public and private sector stakeholders. This Good Practice Guide is the final deliverable of the study.

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. Incentives for a co-operative partnership between public and private sector have been recognised by many stakeholders, 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[4].

Partnerships require a clear framework specifying the roles of the public and private sectors, their relationships and the areas for co-operation. If organisations are to face coherent, straightforward and effective regulatory and/or non-regulatory requirements, public-private co-ordination needs to be optimised.

This Good Practice Guide (GPG) will feed back some of the experiences of those already involved with PPPs and provide advice to those setting up new PPPs or evolving/improving an existing one.

The Guide recognises the global nature of the problem and consequently PPPs have been studied in the US, Canada and Australia as well as Europe.

1 "i2010 – A European Information Society for growth and employment" and "A strategy for a Secure Information Society".
2 http://ec.europa.eu/information_society/policy/ecomm/library/legislation/index_en.htm
3 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
4 ENISA Study on 'Incentives and Challenges for Information Sharing in the context of network and information security', 2010

1.2 Scope

For the purposes of this Guide 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.

Given the large variety of PPPs in existence, the scope of the study, which delivered the GPG was focused using the following criteria:

- To include national, international and pan European partnerships;
- To include PPPs which addressed threats and hazards in order to enhanced security and resilience of e-Communication networks including using the all-hazards approach;
- To weight the focus towards those PPPs which address high impact consequences such as risks to critical national infrastructure and cybercrime.

1.3 Target Audience

The main audience for this Guide is both private and public stakeholders with a policy and/or an operational role, for security and/or resilience of communication networks and information systems. For example, it can help those who are:

- Establishing a partnership for the first time. Here the value might encompass recommendations and ideas for providing membership incentives;
- In existing partnerships, who can learn from the evolution of other partnerships;
- In existing partnerships who are experiencing barriers, who can draw from the experience of others.

1.4 How to use the Guide

This guide has 6 sections.

Section 1 introduces the Guide and covers the background, the sources and approach.

Section 2 describes a framework for designing or describing PPPs using the questions why, who, how, what and when. The options for answering each question are described and the experience of existing PPPs detailed through observations, recommendations and quotes. This section starts with the observed list of problems which PPPs addressed when the interviewees considered 'why' their respective PPPs were created.

Section 3 proposes and describes three generic types of PPP and provides observations and recommendations.

Sections 2 and 3 highlight these observations, recommendations and quotes as shown below. Each observation and recommendation has a unique reference number.

[Observation x]

Observations are in blue boxes

[Recommendation y]

Recommendations are in green boxes

"Quotes obtained during the study are shown indented and in bold italics"

The quotes are all anonymous however authorisation was sought from contributors.

Section 4 provides information about International PPPs within the US, Canada and Australia. Firstly, a mapping is provided for the PPPs of these nations to the generic types, and then key lessons that can be learned from their experiences are listed.

Section 5 summarises the recommendations in a single list as a quick reference.

Section 6 provides final high level conclusions.

1.5 Sources

This guide was produced using the results of a research that had three phases;

- A comprehensive desktop survey of PPPs
- A questionnaire sent to PPP stakeholders across Europe
- Telephone interviews with a sample of questionnaire respondents

In total, 20 nations, including 16 EU members, contributed to the research. In alphabetical order they are:

Australia
Austria
Czech Rep.
Denmark
Estonia
Finland
France
Germany
Ireland
Italy
Lithuania
Netherlands
Norway
Poland
Portugal
Slovenia
Sweden
Switzerland
UK
USA
International Organisations

More information can be found in Appendix C.

General Advice for PPPs – Why, who, how, what & when

2.0 General Advice for PPPs - Why, who, how, what & when

"The measure of success for a PPP is the right people coming together to do the right things in the right way."

Despite the variety of PPPs present across the EU and internationally, a common framework has been developed which describes how these partnerships operate. The Guide uses this framework to provide a structure for understanding a range of diverse implementation approaches both for new PPPs and for evolving PPPs.

This 5 part framework will be described in detail through the rest of this section. The following diagram summarises the underlying taxonomy for this framework and provides an indication of the rich diversity of existing PPPs as well as the range of options available to those starting up a PPP.

In the Figure I overleaf:

Why

Scope

- Deter
- Protect
- Detect
- Respond
- Recover

Threat

- All Hazards
- Natural Hazards
- System Failure
- Cyber-crime
- Terrorism

Who

Coverage

Geographical
- National
- European
- International
- Protect

Focus
- Geographical
- Sector
- Cross Sector
- Thematic

Links

- Across National Boundaries
- Within national boundary
- CERTS or CSIRTS
- Regulator
- Government Bodies
- Law Enforcement Bodies

How

Governance

Activity type
- Long term community
- Working group
- Rapid response
- Combined activity
- Overarching strategy or advisory group

Leadership
- Run by one from within
- Run by a coordinating entity
- Democratically Peer led

Funding
- Mandatory Membership
- Charging for value
- Public pays all or some
- Members own time and travel

Communication Style
- Face-to-face
- Virtual but personal
- Computer based distribution
- Computer based collaboration

Rules
- Formal membership rules
- Formal information usage agreements
- Trust building policies
- Membership requires security clearance

What

Services

- Research/Analysis
- Good practice guides
- Early warnings
- Exercises
- Awareness raising
- Etc.

Incentives

- Reduced exposure
- Cost Savings
- Access to valuable knowledge
- Influence regulation or national policies
- Etc.

When

Start up/ Sustainability

- Top down
- Bottom up
- Top down then grown bottom up
- Bottom up then grown top down
- Fire and forget
- Split or merge

To implement a new PPP, 5 key questions need to be considered: Why is it needed, who will it involve, how will it be governed, what services and incentives will be offered and when will action be taken to start it and make it sustainable? Evolving PPPs may choose to consider all questions or focus on specific questions.

Figure II: Chart showing the structure of the Good Practice Guide

In answering each of these 5 key questions much can be learned from the endeavours of other PPPs. The knowledge gain by these PPPs can be crystallised into a framework for PPPs where each element of the framework can be addressed by selecting from a range of implementation options and considering the accompanying advice.

This Good Practice Guide will cover each of these areas in turn.

"Identify the real problem. Try to solve it by covering all possible aspects."

2.1 Why is a PPP needed?

"Defining the scope is key. Once you identify what the problem set is that you are going to address, issues such as deciding what services will be provided to help address that problem will come naturally"

This quote stresses the need to identify the problem set at the very early stages in creating a PPP. Many successful PPPs were created as a result of a specific problem being identified by many private sector stakeholders. The public sector stakeholder then facilitated and encouraged the creation of the PPP.
In other cases, the political situation of the Member State led to the formation of PPPs. As the political situation has evolved, so has the focus of the PPP.

Other successful PPPs recognised the wider problem of terrorism with events such as 9/11 or the growing threat from Cybercrime where the public sector took the lead at the strategic level and engaged with the private sector. These examples answer the 'why' a PPP was created, but members will have their own reasons. A list of observed reasons (problems needed to be addressed) is described in the next section 2.1.1.

[Observation 1]

The reasons why a PPP is needed can be different if the initiative is being led by the public sector than if it is being driven from the private sector.

It is important for potential members to clearly understand the relevance of the PPP to their own organisation. This will help support them in justifying their involvement to their own management. This is also true where membership is mandated, as it will determine the level of involvement.

[Recommendation 1]

Membership of a PPP should offer a clear value proposition for both public and private sector stakeholders.

2.1.1 Example reasons why a PPP might be created

This set of reasons is from those PPPs researched. There may be many other reasons beyond these examples:

Public Sector led reasons

- There is a national strategy but there is a limited means to deliver it so a PPP is needed to provide this mechanism.
- Government recognized the need for a mechanism to get industry to help respond to a crisis.
- National security strategy requires a capability to share with industry representatives.
- The government has a responsibility to protect the CIIP and does not have a mechanism to involve industry.
- There is not enough money for the public sector to engage all small stakeholders in CIIP/ Crisis (for example SME etc.).

Private Sector led reasons

- An industry organisation has a problem and recognizes that the solution or impact is wider than their own organisational boundaries.
- There is a lack of Senior Management buy-in to the actions to address security issues.
- National Security Strategy/policy is not realistic or fit for purpose.
- Industry wants to be able to influence future National Security Strategy, policy and/or regulation.
- Conforming to regulation requires an industry organisation to be a member of a PPP.
- A desire for a mechanism to feedback on inappropriate elements of regulation or the threat of regulation.

Relevant to both Public and Private Sector

- The organisations have had experience of being a target and now wish to address vulnerabilities.
- Organisations recognized that there is duplication of effort.
- Organisations recognized that there is insufficient co-ordination and/or sharing of information between areas of specialism or sectors.
- Organisations recognized a gap in coverage across the security life cycle.
- Organisations recognized threats are evolving as communications and information technology merge and so the need to be considered together rather than as separate industry sectors.
- Organisations recognized a merging threat from terrorism and cyber-attack.
- Organisations recognized that the threat was evolving and moving from the national/sector level to international.
- There is a lack of trust between competitors within a geography, sector or theme area so a trusted broker is needed.

[Observation 2]

The problem set will be a defining factor in determining which parts of the security life cycle the PPP should focus on.

2.1.2 What aspects of security and resilience to address

This Good Practice Guide covers PPPs focusing on security and resilience. So defining which aspects of security and resilience is naturally an important step. Using a life cycle model the aspects can be defined as:

Deter - A PPP with this scope will focus on trying to deter attackers and an example service might be raising public awareness of security and consequences, or law enforcement actions.

Protect - With this focus a PPP 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 - The focus is to 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.

"Respond and Recover is already being done elsewhere so it is not in our scope"

This quote shows the advantage in understanding the scope and nature of existing PPPs. This understanding is normally the responsibility of the public sector alongside the co-ordination between these PPPs. In some countries this coordination is very tightly controlled by a central agency while in other countries there is more autonomy in the relationship.

[Observation 3]

PPPs focus within the life cycle in three ways. They either focus on the whole life cycle (umbrella approach), the early stages (prevention approach) or the later stages (response approach).

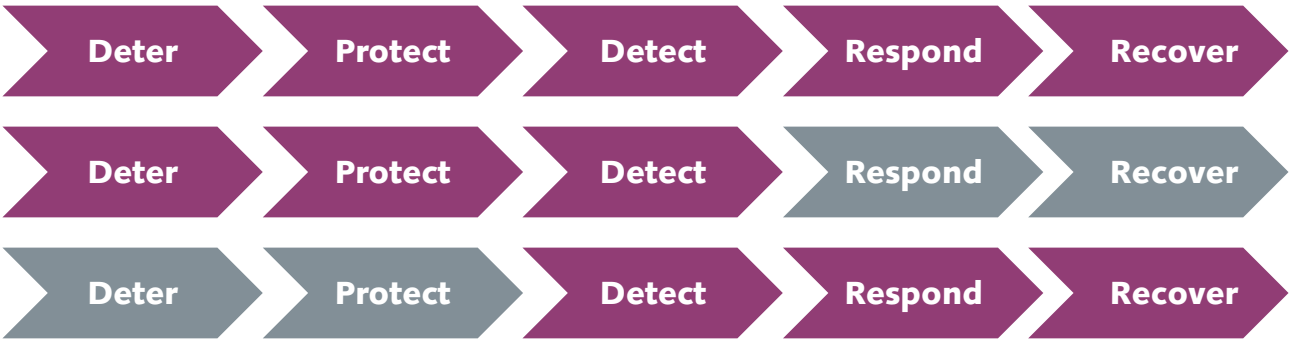

Figure III: Chart showing the three types of focus used by PPPs

[Recommendation 2]

PPPs should consider the focus of other organisations to ensure that duplication is avoided and that all areas of the life cycle are covered with appropriate co-ordination and information sharing links.

When an umbrella approach is adopted the PPP is often broken down into topic specific working groups to ensure that the membership has the right skills. This problem was observed to be less if the PPP adopted either a prevention or response approach.

[Observation 4]

Deciding where to focus within the life cycle will influence which members will take part in the PPP.

The scope and threat change with time with many successful PPPs responding to this by changing the answer to the 'why' question over time. One PPP started by addressing vulnerabilities until the membership adopted standards, which made the issue part of business as usual. The PPP then changed its focus to look at incident reporting.

There are observed examples of PPPs failing because they have not kept up to date with the most important problems or the latest threats and members have reduced their involvement because they see no value in taking part.

[Recommendation 3]

PPPs should constantly ask themselves why they exist. If a problem has been resolved then they should identify the next priority issue to address.

2.1.3 Which type of threats to address

The categories of security threats that the PPP considers within its scope and which helps define the detail in the services provided for this GPG are listed below:

All Hazards – 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.

Cybercrime - These are threats resulting from malicious acts associated with illegal activities, external or internal (insider threats). 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 cybercrime the objective is for criminal gain; here the purpose is disruption or espionage.

Many of the PPPs studied addressed a subset of these threats, especially in the early stages of their maturity. It was observed that some PPPs moved towards an all hazards threat approach as their environment changed.

[Recommendation 4]

PPP should consider the type of threat addressed as this will be a defining factor in shaping the membership and determining which external links are to be forged.

Links with law enforcement will be needed if cybercrime is within scope and Intelligence agencies may well be involved in order to address terrorist threats.
The type of threat considered in focus varied between PPPs. All Hazards, Cybercrime and Terrorism/National State all were included by 48% of PPPs, while Systems Failure was included by 38% and Natural Hazards by 21%.

[Observation 5]

PPPs members will focus on what is relevant for them so the threat type for a PPP may evolve over time.

The Threat component was noted as being a difficult aspect to address and one where the public sector could add real value with the involvement of law enforcement and the Intelligence agencies. It was also noted that some PPPs felt that some public sector members were holding back on threat information.

[Observation 6]

Some PPPs remove barriers to sharing sensitive information between Public and Private sector members, for example, by mandating a security clearance for membership. Of those surveyed 21% currently used Security Clearance and another 24% planned to use them.

[Recommendation 5]

Public sector members should find ways to share sensitive information on threats with their private sector members. If the public sector is the first mover, the private sector stakeholders may be incentivised to participate

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. This is referred to as a holistic approach.

> ***"There is a convergence of technology and the exploitation of technology by people wishing to exploit. An example is using mobile phones to detonate. There was a compelling convergence of need to understand physical, personnel and technology. It was a natural step to bring the 3 together."***

Over half the PPPs studied used a holistic approach. Many started out by addressing the electronic threat and evolved into addressing the physical and personnel threats. However, there are some issues with this approach, mainly associated with the balance in addressing the threat and the skills needed.

[Recommendation 6]

PPPs should study carefully the implications of adopting a holistic approach to ensure they have the right skills and resources to achieve an optimum balance between the electronic, physical and personnel areas.

Who **Coverage & Links**

"Have people who are passionate about what they are doing."

2.2 Who should it involve?

2.2.1 Which community to serve

A PPP can involve partners at a national, pan- European or International level and its focus may be thematic, sectorial or cross-sectorial.

Geographic - The geographic focus of a PPP can be:
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.

"We need close contact with international operators so that if there is an incident we can act quickly to respond to the situation. Cyber is the stimulus for much international linking"

Focus – The defining characteristic for the community that is involved in, and is served by, the PPP can be mainly:

Geographical - The PPP services a specific area of the nation.
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).

[Observation 7]

Many countries have found that creating homogeneous, single-sector or theme organisations adds value for members, enabling them to focus on topics of specific relevance to their industry or role.

"Also, the trust within the sector is much greater than that between sectors. A company will share within its sector rather than with all members. Members are more comfortable within their sector than cross- sector"

Despite the apparent advantages of single sector PPP's, there exist a number of cross sector PPPs which are developing and growing. As these PPPs develop it was noted that subgroups are often created to promote homogeneity and to help ensure members see value by working with their peers.

[Observation 8]

Often, these cross sector groups have an overall central organisation, which coordinates activities and facilitates cross-sector sharing.

[Recommendation 7]

The central co-ordinating body should look for and promote groups with strong homogeneity. This also applies to cross sector PPPs.

2.2.2 What links to establish with others

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

Other PPPs across national boundaries - Some PPPs have special trusting relationships with mirror organisations in other nations.

Other PPPs within the national boundary - PPPs have links with other PPPs within the same nation.

CERTS or CSIRTs - Emergency Response teams.

Regulator - PPPs have links with their regulatory body.

Government Bodies – Government may have specific bodies responsible for civil contingence and resilience.

Law Enforcement Bodies – Both operational and intelligence agencies.

Links with other organisations are normally created as a result of identifying the scope and threat which the PPP is addressing. The links then become self-evident. In some countries there is a high level body, sometimes a PPP in its own right, whose job it is to coordinate the activities and provide links to the relevant organisations.

[Recommendation 8]

PPPs should plan how they will link with other organisations, to share information and expertise and to avoid duplication. This plan may form part of a National Strategy to coordinate the protection of the Critical Information Infrastructure.

2.2.3 Involving the regulator

Many PPPs invite representatives from other organisations, as the need arises, to address an area of common interest. These organisations are not full members as their regular involvement is not consistent with the aims of the group. In fact, regular involvement by some organisations such as the Regulator or Law Enforcement is seen by some as a barrier to effective PPPs due to the potential conflict of interest.

[Observation 9]

Several organisations who share sensitive information do not include the Regulator, as their presence is seen to inhibit information sharing.

"If the regulator was there, providers would not discuss certain issues, in case he were to decide that they were not fulfilling requirements. When a new member joins, they often ask why the regulator is not there. This gives us the chance to explain that we can talk more openly and share information more readily"

In contrast, some PPPs see the involvement of the Regulator as important for a number of reasons, including providing evidence that the PPP is not taking part in anti-competitive behaviour by creating a closed membership organisation. The risk of breaching competition law is seen as very important as described later in section 2.3.5.

[Observation 10]

There are organisations where the Regulator may have initiated the PPP, or is seen as a partner, and as 'positively helpful.' If the Regulator is able to participate in a way that is not looking to be punitive, there can be a useful, 2-way relationship.

"The regulator needs to be able to understand his sector and this understanding might even prevent regulation, as the regulators can ask questions and explore things. This free flow of information can help to work through misunderstandings and can get rid of the need for regulation"

"The regulator attends, but generally the fields of regulation and the voluntary activities are separated. Some Telecom laws involve regulation, but these are topics we do not discuss in the PPP. We are discussing how to operate in a crisis"

If information sharing forms a major part of the PPP, having the regulator as a member may stifle sharing. Achieving the right balance in this complex relationship is a key.

Some PPPs appear to manage the complexity of involving the Regulator very well. Previously the involvement of the Regulator by some PPPs was not considered achievable. However, it would appear that, with the right legal, cultural and historical environment, this is possible.

[Recommendation 9]

The relationship with the Regulator must be considered carefully to take account of the legal environment, national culture and the needs of the membership

2.2.4 International Links

International links and cross border co-operation are seen as a positive with many organisations enthusiastic to create more relationships. In some countries this international involvement is through existing international organisations addressing cyber security such as the FIRST[5] community. In other countries relationships were built on a bilateral basis which grew into multilateral links. Of the 30 PPPs studied, about 34% had regular international links with PPPs in other countries with another 45% linking infrequently.

"Yes, there is the normal international exchange with CERTS, and also, as we are part of the Intelligence Service, they also have international exchange of information. We have contact with our neighbouring countries and are keen to join international initiatives"

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

[Observation 11]

There are well developed links between many nations both within the EU and wider afield. For example the tri-lateral relationships on Information Exchanges in UK, US, Canada.

[Recommendation 10]

National PPPs should look for opportunities to create international links with other PPPs for cross border sharing and collaboration. This could be facilitated by organisations with existing international contacts.

"To me, it boils down to this:
– The infrastructure is interconnected, so our security is interconnected
– The bad guys are well organized and are not confining attacks to specific countries or regions
– No one organization has the capability to build all the needed relationships with various country CERTS and CIIP related PPPs
– Therefore, we need a capability to share information with critical sectors across national boundaries in a "one stop" fashion."

[Recommendation 11]

National PPPs should look closely at the benefits of becoming members of an organisation, which represents their wider geographic/economic interests in relation to CIIP and who could facilitate the creation of an interface with other parts of the world. For example in Europe this could be the European Public Private Partnership for Resilience (EP3R).

2.2.5 High-level Strategic Partnerships

In some countries, there is a high level strategic group, which involves CEO's of the major critical infrastructure industries. This allows 2-way communication between senior industrialists and government. It also means that CEO support for their company's involvement in CIP projects is more forthcoming. Examples include The President's National Security Telecommunications Advisory Committee (NSTAC) in the US and the Telecommunications Industry Security Advisory Council (TISAC) in the UK. This approach was not universal and may be influenced by cultural factors as many of the countries who adopted this approach have close cultural ties.

"We have a Business Government Advisory Group, where our Minister meets the CEO's of the 20 largest companies in XXX every 12 months for a frank discussion of national Security issues. This receives very good feedback from industry as the CEO's appreciate having the ear of the Minister. If there is support from the CEO, funding is more forthcoming. Having this senior forum has definitely helped"

[Observation 12]

The presence of high-level strategic partnerships between industry and government with a remit to oversee more tactical PPPs was not universal. However, in those countries, which had adopted this approach, they appeared to work well.

[Recommendation 12]

PPPs should consider the use of a high level strategic partnership at the CEO level in order to support senior level understanding and awareness.

2.2.6 Getting the right people

Many PPPs highlighted the importance of getting the right 'informed' people from both the public and private sectors. There is also a downside to getting the wrong people as outlined in the following quote.

> ***"Problems can be caused by 'lurkers', people who do not attend, churn (caused by changes in job roles, which leads to erosion of trust). Membership can be terminated for the individual, or for the company. In one PPP, 6 non-contributors were expelled. This was a motivating factor for those who remained. The important thing here is to listen to your membership."***

Members need to be empowered to share information as well as to take action on the information that they received.

[Recommendation 13]

In creating the membership of PPPs great care should be taken to recruit people who are empowered and informed, from the organisations chosen.

How **Governance**

"The secret of Public Private Partnership is in the organisation of the process"

2.3 How should it be governed?

How to organise and run a PPP requires careful consideration. How a PPP is organised, how partners work together, and its rules and financing can have a key impact on the success of a partnership. The governance of a PPP was defined as critical by all the PPPs surveyed.

2.3.1 What is the general type of activity for this PPP?

The purpose and duration of activity for a PPP can be one of several distinct types. These types have a close but not perfect map, to the research of Milward and Provan on collaborative networks[6]. The general types for PPPs are:

A long term community - 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 Networks** 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. Usually these groups are established because 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, and 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 Networks**.

Combined Activity Group - Some PPPs elect to have a long term community that may meet and plan and practise strategies and then if there is an emergency a sub set of the group forms a rapid response group or task force

Over arching Strategic or Advisory Group - This is a high level organisation that links to a number of other partnerships may be to direct activity or to act as a high level advisory service to government etc.

[Observation 13]

PPPs select the general type that matches their purpose but as they evolve they may need to create other partnerships or change their type. For example a working group for a specific purpose might decide to become a long term community as they recognise the value of the informal information sharing that they have naturally evolved.

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

"Yes. We have seen the problem that one person cannot deal with all things. We may start sub-groups and look for new experts from organisations"

2.3.2 Who is going to do what?

Deciding how a partnership should be led, co-ordinated and organised requires careful consideration. Leading an organisation is a visible position of power and many PPPs desire equality between Public and Private Partnerships.

The options used by PPPs relate well to the work of Milward and Provan[7] on collaborative networks:

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.

"When 3 or 4 sat down to write the rules and define the structure, we borrowed from another PPP. The key thing that we did was to define terms of tenure for the industry chair. We wanted to make it as inclusive as possible. No individual could be chair for ever. There is a permanent government chair, but the industry chair is appointed for a year with a deputy industry chair who shadows him, then steps up the following year. This way the PPP can never be dominated by one particular company. Everyone qualified gets a chance."

[Observation 14]

As the nature of a PPP is a partnership between public and private organisations, the leadership structure often includes both, and some organisations have joint industry and government chairs with agreed rules of tenure.

In order for a PPP to succeed, there must be a clear governance structure, and practical strategies and funding for administration and venue. As the nature of a PPP is a partnership between public and private organisations, the structure often reflects this, and some organisations have joint industry and government chairs. It is more common for government to provide administrative support and venue.

"Yes, the joint chairmanship was part of the "raison d'être" (worth being)– a true partnership. For the rest, as the company provides their time and the government provides the venue and secretariat, each can see that the other is providing something"

[Recommendation 14]

The role of the industry chair is very important and the PPP should ensure it has a clear mandate with agreed rules for selection and tenure.

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

2.3.3 How the costs get paid

Funding the work of a PPP can be a challenge. A number of different approaches are.

- Making Membership Mandatory - This may mean a regulator or other government body requires it and either funds it or requires a membership fee.
- Charging for Value - Setting up incentives and valuable services and then charging a membership fee or fee for services.
- A public body pays for all or some of the costs
- Participating members pay for their own time and expense and a central body pays for centralised costs such as venue, co-ordination etc.

Costs are often split into two main categories:

- Administration cost such as secretarial support and venue etc. and
- Members' time.

[Observation 15]

Defining who provides secretariat services, who co-ordinates the activities as well as who chairs the PPP are visible roles of authority as well as being a cost consideration. It is more common for government to provide administrative support and venue.

[Recommendation 15]

Government can add value and reduce economic barriers to PPP participation by covering the costs of administration. Public sector partners should look seriously at covering these costs as it could be a significant incentive to the Private sector members to actively participate in those countries that do not mandate membership.

Some countries mandate membership of a PPP which addresses CIIP and some also levy a charge to cover costs. Of the 30 PPPs studied 14% mandated membership and 24% charged for membership.

"Mandatory membership is an advantage. We have agreed by the rules of procedure that decisions are taken by majority voting. If a company is not at the meeting, it has to abide by the decision made by the others. That's an incentive to attend. Also, I bring interesting opportunities to them. Because we involve them in policy, it is possible to discuss with other critical sectors, and they are the first to hear from Intelligence"

[Observation 16]

Membership of a PPP may be mandatory or voluntary. In some countries it is seen as a privilege to be a member; in others there is awareness that to fail to participate might place a company at a disadvantage.

[Observation 17]

Even though in some countries membership of a PPP is mandatory, taking part in activities such as trusted information sharing is voluntary. This recognises that you cannot force members to share information if they see risks and no value in doing so. PPPs should remain focused on their core objectives and avoid evolving in market-based (for profit) service providers to their members or to third parties, as this could undermine the trusted relationship among public and private partners alike.

Funding the activities of a PPP is a challenge for both the Public and Private sector. Funding is normally more forthcoming if membership can see a clear value proposition. The following quotes show the variety of funding approaches.

"It can no longer be that 'if the government wants it then it can fund it' it has to be 'find a way to do it yourself"

"Growth was complex. When a PPP is not mandatory and fees are charged you need to ensure members recognise the value for money. We offer response teams, sensors, alarms and monthly reports"

"Resources are always an issue and we must plan to combine events to save travelling"

[Recommendation 16]

Adequate funding for the PPP is vital and this is more likely if membership provides a clear value proposition by, for example, providing information which is not available anywhere else.

[Recommendation 17]

The PPP must also look for effective ways to keep down costs, such as combining events with other meetings.

2.3.4 How to communicate within the PPP

Reducing travel costs yet establishing trust and managing the information involved is an important consideration. How people interact is 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 situations where trust between partners is important. 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 but personal interaction (email and audios etc.) - Here face to face meetings are replaced with person to person interactions. This could be a working group team conference call or a private distribution list.

"It is a network of peers and we exchange information in many ways... internal mailing lists and particularly by personal links with the small group of people who are our closest partners"

Computer Enabled (Distribution only) - Here a system broadcasts information. PPPs use a range from simple website to a sophisticated set of network sensors monitoring and then broadcasting alarms.

Computer Enabled (Collaborative) - Here there is a system that allows information to be shared in both directions and may involve sophisticated categorising and distribution rules as well as anonymisation.

Formal 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.

[Observation 18]

In the creation of some PPPs they did not have any formal membership rules initially as they were often addressing the immediate problem at hand. However, over time membership rules were developed to suit the needs of the community.

[Recommendation 18]

There should be clear and agreed rules and guidelines for the organisation and structure of the PPP.

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)**[8], Also known as confidentiality agreement, confidential disclosure agreement (CDA), proprietary information agreement (PIA), or secrecy agreements.
- **The Traffic Light Protocol (TLP)**[9]**.**

There are different types of NDAs and CDAs as shown by the following quote.

"Our NDA is corporate, and it's the companies which sign the NDA, then they assign people. In another programme that we are involved in, they insist that the individuals sign the NDA, and we don't want that"

[Recommendation 19]

PPPs should consider the use of an NDA and/or a system like the TLP in the formal rules. This consideration should include whether to have a personal or corporate focus.

8 http://en.wikipedia.org/wiki/Non-disclosure_agreement
9 http://en.wikipedia.org/wiki/Traffic_Light_Protocol

Trust Building Policies – It is recognised that in any PPP the creation of trust is vital for its success. The level of trust varies over time and can depend on the services offered, For example, a high level of trust is widely reported to be necessary in Information Exchanges where information sharing is the core service provided. Often PPPs have carefully designed their policies, membership rules, requirement for security clearance, and interaction type to support trust. They have limited substitution for attending meetings, and use formal information usage agreements in order to enable trusted information sharing.

[Observation 19]

Most of these policies address trust in the context that the recipient will not abuse the information nor cause harm to the source. However, there is also a need for trust in the source so that the recipient can be confident that the information is accurate and not misleading. This second aspect of two way trust was seen by many PPPs as very important but more difficult to address with a policy solution.

[Recommendation 20]

PPPs should consider the building of two way trust as a priority.

"The key to success is the development of trust".

Membership Requiring Security Clearance - Because of the nature of the privileged information involved when a PPP is working closely with national intelligence services membership might need to be restricted to individuals who have, or are able to gain, clearance to classified information.

[Observation 20]

Many PPPs have membership rules which differ according to the nature of the PPP. Many include Non-Disclosure Agreements, and arrangements for sharing sensitive information. Details of membership rules for Information exchanges can be found in ENISA publication GPG NSIE[10].

2.3.5 Considering the legal environment

"There is legislation behind all this. This organisation is defined by law."

Some countries have a legal mandate to create a PPP as part of a national strategy to address security and resilience of critical infrastructures. In these cases the legal implications for PPP members will have been considered within this mandate.

In other countries, the legal implications have been addressed at the time of creating the PPP, taking account of services it provides and environment in which it will operate. Some of the legal issues addressed when creating a PPP relating to forced disclosure include:

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

- Where receiving organisations are public bodies, information may be required to be disclosed for Freedom of Information reasons
- Where legally compelled to do so for Law Enforcement reasons
- Where legislation is so enacted:
  - Encryption keys may be required to be disclosed, or encrypted data may be required to be decrypted
  - Information may be required to be disclosed for Environmental Law reasons
  - Information may be required to be disclosed for Competition Law reasons

It was noted that the fear of breaching competition law, in being seen to create a cartel was a major legal barrier in creating a PPP where membership is not 'open to all'

Information shared in good faith could possibly lead to anti-trust accusations for sharing infrastructure information with other industry partners, or to contract liability.

"In some cases at meetings, we have serious rivals in the same room. Advice received from the competition regulator assisted us to create a legal framework, for the conduct of meetings and information sharing"

[Recommendation 21]

PPPs should seek legal advice to ensure that they use a legal framework suitable for the jurisdiction in which they operate.

2.3.6 Developing personal trust

When the partnership involves members contributing for the greater good, possibly at their own risk, the community needs to develop a sense of trust that the others will act in such a way as to ensure any such risk is minimised. In addition, when a member receives information, they need to trust that the information is both accurate and of value.

"You need stability and continuity of people to establish the necessary trust base."

[Recommendation 22]

PPPs should implement policies which maintain continuity of membership such as clear membership rules on participation, backed up by incentives.

Incentives include ensuring that meetings add value to both public and private members; responding to members requirements; considering streamlining travel arrangements; regular contact via electronic means.

"We see 'adding value' as a root to growing trust. We recognised that it is easier to build trust if you are bringing stuff they can't get elsewhere"

Having the 'right people' in the partnership is key to developing trust. Members that are empowered to bring value that cannot be gained elsewhere will increase the motivation to build trusted relationships.

How interactions are held between PPP members is an important factor in building personal trust.

"Face to face is considered vital"

"The Telco group is about 10 while Finance is about 45 which is too big and it is impersonal"

"All of our members would be over 200, too big for trust development. Sector based meetings keeps the size down."

Having a small group of people working together and meeting regularly enables them to get to know each other and build up an understanding of how reliable and trust worthy they each are. Understanding the best size for a PPP depends on the degree of trust required as a result of the expected risk of active involvement.

"Any growing trust is boosted if you have a prior relationship"

[Recommendation 23]

PPPs should look for opportunities for members to meet face to face in order to increase trust.

[Recommendation 24]

PPPs should strive to keep the number of members who meet at any face to face meetings small, to allow personal relationships to be built and maintained.

Personal trust is more difficult to build between PPPs unless it is done by individuals such as the industry chairs. Controlling how the information will be distributed is one way to help build trust when sharing beyond the immediate PPP as well as within.

"We use open and closed sessions. The Traffic Light Protocol is used to define the type of information discussed. Closed sessions are for Red and Amber info"

[Recommendation 25]

PPPs should adopt information distribution policies such as the Traffic Light Protocol to give the source confidence that the information will only be used as agreed.

"Need to have values or lock-gates to share between sectors and internationally so you control information."

Where personal trust cannot be built successfully or where the level of trust is not high enough to allow the sharing of more sensitive information, then techniques such as anonymisation should be considered. Often it is the identity of the source which is more sensitive to a private sector member than the information itself. This can be implemented through a trusted third party, sometimes called a Trustmaster, who hides the identity of the source.

[Recommendation 26]

PPPs should implement processes that allow the anonymisation of the source to facilitate the sharing of information with other PPPs.

What **Services & Incentives**

"Have something concrete to offer. Lots of talk and no action will not succeed."

2.4 What services and incentives should be offered?

What a PPP does includes more than just the products and services that are offered; it encompasses all incentives.

"You must listen to your membership and deliver what they ask for"

2.4.1 Evolving a set of services to meet the needs of members

This component lists the types of services that the PPPs commonly offer in addressing its scope for example:

Research/Analysis:
Good Practice Guides:
Information Exchange:
Early Warnings:
Exercises:
Awareness Raising:
Technical Evaluation:
Defining Standards:
Help Desk/ Triage:
Crisis Management:
Resilience Planning:
Emergency Planning:
Security Audit:
Benchmarking:
Statistics:
Archiving:
Strategic Planning:
Risk Analysis:

The 4 most frequently offered services were Information Exchange (83%), Research/Analysis (62%), Awareness Raising (62%) and Early Warnings (59%).

"The value of good practice guides was seen early on and they are produced when relevant."

[Observation 21]

The range of services changes and grows over time, led by the needs of the membership and the lessons learned. For example Good Practice Guides are often produced after the PPP has addressed the corresponding problem.

[Recommendation 27]

PPPs should create a mechanism for members to influence the services provided which meets their needs. This could be a well-defined and focused agenda item as well as agreeing in advance a yearly work programme.

As mentioned before in section 2.1 with the quote below, the choice of service provided is linked to the problem being addressed and the scope focus in the security lifecycle. This natural order ensures that the services are more likely to add value to members.

"Defining the scope is key. Once you identify what the problem set is that you are going to address, issues such as deciding what services will be provided to help address that problem will come naturally"

[Recommendation 28]

To deliver value added activities, PPPs should ensure that the services provided address the problems identified and align with the agreed scope focus.

Many services offered align with the prevention or response scope focus. For example, a Response Focused PPP is more likely to be offering a Crisis Management and Resiliency Planning service whereas a Protection Focused PPP may be more likely to be investing in Research/Analysis of vulnerabilities and Awareness raising activities. Services common to both included Information Exchange and Good Practice Guides.

2.4.2 What types of incentives should be offered and promoted?

"It is important to recognise that, for many, this is not their day job"

Unless membership of the partnership is mandatory then the PPPs will need to be able to attract and retain members. In order to do so they need to provide and clearly articulate and promote a valuable set of incentives that matches the needs of the potential members.

ENISA has published a work on Incentives and Barriers[11] which includes the following incentives:

- Reduced risk exposure by better security and resilience
- Cost Savings from sharing the work to solve a critical problem
- Access to privileged Information from government
- Access to knowledge not available elsewhere (peers in other organisations)
- Opportunity to avoid inappropriate regulation
- Opportunities to contribute to strategic direction and national policies

"I would add "Industry is able to speak as one voice" and "Co-operative support during a crisis"

[Recommendation 29]

It is important for a PPP to define the benefits to members, both services and incentives, explicitly. This will not only sustain the interest of members but also support them in securing the support of their management.

"Incentives can be more than money. Participation reduces risks so an incentive could be part of liability protection or to reduce premiums in cyber-risk insurance"

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

[Observation 22]

Creative approaches have utilized services to gain membership interest, for example offering cheap or free training to candidate members. The training was of genuine value but also enabled the attendees to understand the importance and value of membership.

" Bring something of value to the table"

[Observation 23]

Not all members need to contribute the same types of value. Some may offer technical knowledge while others offer funding. Some may offer intelligence while others offer research and analysis.

The incentives are directly linked to the value provided by being a member of the PPP. This value is increased by the quality of the membership and how much they trust each other as described in section 2.3.6 Developing Personal Trust. The largest asset a PPP has is in its membership. The relationships and links with other PPPs is also an important asset, such as the ability for the PPP to influence the Regulator to reduce the risk of inappropriate regulation.

[Recommendation 30]

PPPs should clearly leverage the skills, experience and organisational positions of the existing members to provide an incentive for new members.

"There is a balance between what they are expected to do, and what they get out of it. "

When members are not actively contributing relevant value, over time this will erode the value of the whole partnership as other members will perceive an imbalance in their contribution when compared with others. They will be increasingly likely either to withdraw from the partnership or reduce their contributions.

[Recommendation 31]

All members of the partnership, including the public sector members, need to actively contribute information, services or support that is of relevant value to the membership. Where members fail to make a positive contribution action should be taken by the membership to resolve the situation.

The type of action taken will depend on individual circumstances but some PPPs anticipate these types of problem in their membership rules where they say that failure to attend more than 3 consecutive meetings will result in their membership being revoked. In other situations, in a different PPP, where the member was important enough, more time was given for them to actively contribute. It is worth noting that this can sometimes take years not months for the trust to grow to a level where real value is seen by some members.

When **Start up/Sustainability**

"We started very small with just a few sectors – Finance, Telcos, Energy and Government. I think it's important to stress not to try to do all sectors at the same time. We tended to be incident driven as it is easier to start with an incident."

2.5 When should action be taken to start it and maintain sustainability?

2.5.1 How do PPPs grow and evolve

The information about how the PPP started and how it evolved is valuable in understanding how to develop new partnerships. This covers 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.

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

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

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

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

[Recommendation 32]

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

2.5.2 Action to start a PPP

There are many different reasons why a PPP is needed, as described in section 2.1.1. This variety is complemented by an array of advice on how to take the first steps, which has been provided by interviewed members of PPPs, based on their own experience:

"You can plan but it will never happen that way. 'A plan is worth nothing - but planning is invaluable' quote from Eisenhower"

"When creating a PPP you need to deal with the question, 'What's in it for the private sector?' who will ask,' why should I participate?"

"We started with strong champion of First Minister who then engaged each of the heads of the main departments."

"Get the major ones to buy in and the rest will follow."

"Being too informal early on can lead to a lack of commitment which is addressed through formalization that helps"

"As it evolved it spawned working groups and inter-group sharing was established"

"Start with sectors that are most aware - ISP, Finance, proves value and grow into others."

There are several key elements to this advice which include:

- Champions who are prepared to make it happen are very important
- Pragmatic and flexible planning is important
- Start small and think big is evident - quote from ENISA EISAS report[12]
- Some sectors may be more receptive than others so a market analysis is useful
- Incentives for the Private sector are key enablers
- Formal relationships between public and private sector stakeholders are important.

It is worth noting that these key elements all relate to good management practice, which may be an obvious conclusion but worth stating as sometimes the obvious is overlooked.

[Recommendation 33]

PPPs should recognise the importance of good management practices when creating and operating partnerships.

2.5.3 Action to sustain a PPP

"Initially we tried to set up an informal forum of ISPs to start to deal with spam. We quickly realized that because it was informal, there was not the commitment on behalf of the organisations to allow the appropriate people to put in the effort. So after a year or so we realized we had to change. We thought that if it we had a formal agreement, then management would allow the technicians to participate, so in 1998 we signed bilateral agreements with the ISP providers."

12 http://www.enisa.europa.eu/act/cert/other work/eisas_folder/EISAS_finalreport.pdf

The sustainability of a PPP is often more challenging than its creation, taking account of exceptions such as PPPs which have been created with the expectation of a limited life.

Many of the key elements in starting up a PPP, as described in section 2.5.2 also apply to sustaining a PPP. The main addition is one of expectations and benefit of the doubt. Where membership of a PPP is voluntary, members will take part in the first few meetings to assess its relevance and value. If the PPP fails to deliver on these two aspects then it makes sustainability difficult. This is a recognised problem in management and emphasises the need for a strategy to provide clear short term successes - 'quick wins'.

[Recommendation 34]

For sustainability, it is important for non-mandatory PPPs to continually demonstrate added value, especially in the early stages to prove the need for the PPP.

[Observation 24]

PPPs that continually add value are likely to have private sector membership at the operational technical and policy level.

"They were interested from the beginning, but the reasons for their participation changed over time. First they had an interest because they knew if they didn't cooperate there could be regulation, so it was better to cooperate willingly. In addition there was the possibility to get advantages by having access to more (cross-sector) and governmental information. Later they acknowledged the benefit of the cooperation, especially the cross sector information exchange (including personal and reliable contacts to crisis managers of other sectors) and the participation in the national IT crisis management. After five years of cooperation there is still an intensive motivation to take part at the PPP"

The threat of inappropriate regulation at both the National and European level is sometimes seen by private sector organisations as an on-going reason to take part in a PPP. However, experience shows that over time, with the right management, a proactive value added posture can evolve from this defensive position.

[Observation 25]

Where PPPs operate mainly in the defensive mode, private sector membership is more likely to be from a legal or regulatory background.

[Recommendation 35]

Some may initially join PPPs in order to mitigate undesirable changes, (e.g. the threat of regulation), but for real long term sustainability this should be evolved into a true partnership where all members (public and private) get real value.

Metrics for the success of a PPP are hard to identify, with the length of time in existence being often quoted. There is another metric however which PPPs can use to assess the true value add of its activities.

[Recommendation 36]

PPPs can assess the value of their activities by analysing the background of its private sector membership. If they are predominantly from an operational technical and/or policy background then the PPP is more likely to be adding real value.

Three generic types of PPP

3.0 Three generic types of PPP

This section expands on observation 3, made in section '2.1.2, what aspects of security and resilience to address' which states:

[Observation 3]

PPPs focus within the life cycle in three ways. They either focus on the whole life cycle (umbrella approach), the early stages (prevention approach) or the later stages (response approach).

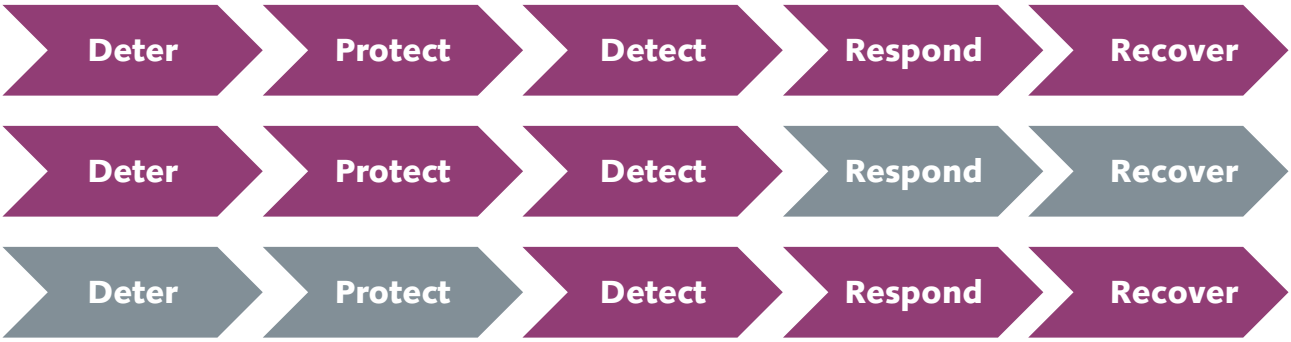

Figure IV: Chart showing the three types of focus used by PPPs (reminder of Figure III)

All 30 of the PPPs studied fall into one of these three generic types which shows that despite the diversity in environments, legal jurisdictions, cultures and organisations there is an underlying simplicity of approach.

It has also been observed that where separate prevention and response PPPs exist in a single country, over time these can combine together within a single umbrella PPP. This may not always be from an organisational perspective but can be simply from a policy perspective. This rationalisation and coordination is often driven by a national Cyber Security and Resilience Strategy.

These national strategies are in effect collapsing the three generic types of PPP into a single type, addressing the whole lifecycle and at the same time moving towards an all hazards threat approach.

It is hoped that this understanding in itself will lead to opportunities for increased cooperation between PPPs. The rest of this section describes these three generic types in more detail.

3.1 Response Focused PPPs

PPPs with a **Response Focus** i.e. those covering mainly the respond and recover elements of the life cycle, tend to operate either in real time or have a community that exists in order to sustain and improve the mechanism for responding to events. These partnerships deliver a value that is immediate and clear to private organisations and thus might be initiated by a small group of industry representatives with an understanding of the interconnected nature of CIIP and resilience as well as the benefits of mutual support for recovery. Alternatively they may have started top down with government responding to an event such as 9/11. These PPPs have a clear tactical and operational focus and tend to contain members with a professional technical skill base. These Response Focused PPPs tend to have a specific sector or thematic focus.

Examples of Response Focused PPPs are the UK EC RRG[13], NCO-T[14] in the Netherlands and the Polish CERT Polska[15].

Note that the Early Warnings in the Prevention and Response Focused type PPPs may be different types: for example, early warning of a problem happening now compared to early warning of a vulnerability.

3.2 Prevention Focused PPPs

In contrast, PPPs with a **Prevention Focus**, such as those covering principally the prevention and protection end of the security life cycle, tend not to deliver their capability in real time. They tend to have a long-term community that co-operates, learning from each other and implementing this learning over time. The capability of these PPPs tends to have a strategic and/or tactical focus. Membership may be more senior in nature and the benefits of involvement may be deferred in delivery. Because of the deferred nature of the benefits of involvement, private organisations need to be mature and able to take a longer-term view when investing in these activities. Public organisations may initiate these PPPs as they are responsible for the wider national and longer-term interests. As with Response Focus PPPs, these Prevention Focused PPPs tend to have a specific sector or thematic focus.

Examples of Prevention Focused PPPs include: VARNI NA INTERNETU[16] Slovenia, UK NSIE and IT-ISAC[17] in the US.

Given the focus of the Prevention Focused PPPs they are most likely to have offered the following services: Good Practice Guides, Information Exchange, Early Warnings, Exercises, Awareness Raising, Technical Evaluation, Defining Standards. Correspondingly they are very unlikely to offer services like Help Desk/ Triage, Crisis Management, Resilience Planning, Emergency Planning.

3.3 Umbrella PPPs

Finally, there are a number of organisations that have the ability to deliver capability across the full security life cycle. These are **Umbrella PPPs**. These types may have different forms:

- The PPP may be very large in order to contain members with the required roles, skills and responsibilities to address the full life cycle requirements (for example NESA in Finland). When the Umbrella PPP is a large organisation sub-divisions, either around sector or theme, are used to manage the interaction.

- The PPP may be a small over-arching organisation whose membership is senior representatives from numerous Response and Prevention Focus type PPPs.

Either of these types of Umbrella PPPs may have a strategic feed into the highest level of senior government both to inform and to influence such as the US NSTAC[18] or to implement a national strategy such as the German UP-KRITS[19].

These Umbrella types are not to be confused with a PPP of the Response or Prevention Focus types that for pragmatic reasons have, on occasion, stretched to address a need out of their core focus.

13 http://www.cabinetoffice.gov.uk/ukresilience
14 http://www.ncot.nl
15 http://www.cert.pl
16 http://www.varninainternetu.si
17 http://www.it-isac.org
18 http://www.ncs.gov/nstac/index.html
19 https://www.bsi.bund.de/ContentBSI/Themen/Kritis/Aktivitaeten/UmsetzungsplanKritis/umsetzungsplankritis.html
Paper by Larry Clinton given as testimony to White House Cyberspace policy review 2009

Introducing an International Viewpoint

4.0 Introducing an International Viewpoint

This section introduces the key PPPs from the USA, Canada and Australia in order to provide a complementary view of international activity.

4.1 Introducing PPPs in the US

The Office of Infrastructure Protection (IP)

IP is part of the government **Department of Homeland Security Office (DHS)** and IP works in close coordination with public- and private-sector critical infrastructure partners, leading the coordinated national effort to mitigate risk to the nation's critical infrastructure through the development and implementation of an effective critical infrastructure protection program.
(www.dhs.gov/xabout/structure/gc_1185203138955.shtm)

National Cyber-security and Communications Integration Center (NCCIC)

The NCCIC, is an umbrella organisation set up in 2009 to coordinate national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure. NCCIC integrates the efforts of:

- **the U.S. Computer Emergency Readiness Team (US-CERT),**
- **National Coordinating Center for Telecommunications (NCC)**
- **the National Cyber-security Center (NCSC)** –an office within the DHS.
- DHS Office of Intelligence.
- Private sector partners from **IT-ISAC** and **MS-ISAC.**

(http://www.dhs.gov/)

National Security Telecommunications Advisory Committee (NSTAC)

NSTAC National Security Telecommunications Advisory Committee comprising 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies, provides the President with collaborative advice and expertise, as well as robust reviews and recommendations.
(www.ncs.gov/nstac/nstac.html)

Network Security Information Exchanges (NSIE)

Industry and Government coordinate through NSIE to voluntarily share sensitive information on threats to operations, administration, maintenance, and provisioning systems supporting the telecommunications infrastructure. The NSIE does not have an operational role. There are 2 NSIE's, one a government one and one industry one; they are separate but closely coordinated.
(www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf)

Information Technology - Information Sharing and Analysis Centre (IT-ISAC)

The IT-ISAC is a community of security specialists from companies across the IT industry dedicated to protecting the IT infrastructure that propels today's global economy. They identify threats and vulnerabilities to the infrastructure, and share best practices on how to quickly and properly address them.
(http://www.isaccouncil.org/ and https://www.it-isac.org/)

Cross Sector Cyber Security Working Group (CSCSWG)

These working groups serve as a forum to bring government and the private sector together to address common cyber security elements across the 17 critical infrastructure and key resource sectors.

Institute for Information Infrastructure Protection (I3P)

The I3P is a national consortium of leading academic institutions, national laboratories and non-profit research organizations. It is described as a non-governmental organisation, but receives government funding from various sources, including the DHS, the **National Institute of Standards and Technology (NIST)** and the **National Science Foundation (NSF)**.
(www.thei3p.org)

National Infrastructure Advisory Council (NIAC)

The NIAC was formed to advise the President on issues related to the security and resiliency of the Nation's critical infrastructures in key sectors of the economy. The council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and state and local government.
(www.dhs.gov/xlibrary/assets/niac/niac_brochure.pdf)

US Computer Emergency Response Team (US-CERT)

Department of Homeland Security (DHS) cyber security division created the US-CERT, as a partnership between public and private sections, to protect the Nation's Internet infrastructure by coordinating defence against and response to cyber-attacks. US-CERT is responsible for analysing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities (now located within the NCCIC).

InfraGard

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. The primary focus of InfraGard is to share actionable intelligence information for investigative purposes. (www.infragard.net)

Sector Coordinating Councils (SCC)

The USA operates a sector partnership model which encourages critical infrastructure owners and operators to create or identify SCCs as the principal entity for coordinating with the government on a wide range of critical infrastructure protection activities and issues. There are specific SCCs for the **Information Technology sector (IT SCC) and the communications sector (C SCC)** which covers cable, broadcasters and wireless operators, as well as their respective trade associations. In addition the **Government Coordinating Council** enables interagency and cross-jurisdictional coordination.
(http://www.it-scc.org/, http://www.commscc.org.)

Armed Forces Communications and Electronics Association (AFCEA)

AFCEA is an international, non-profit membership association serving the military, government, industry, and academia as a forum for advancing professional knowledge and relationships in the fields of communications, IT, intelligence, and global security
(www.afcea.org)

Overseas Security Advisory Council (OSAC)

OSAC is a Federal Advisory Committee with a USG Charter to promote security cooperation between American business and private sector interests worldwide. (https://www.osac.gov/Pages/AboutUs.aspx)

Domestic Security Alliance Council (DSAC)

DSAC is a strategic partnership between the FBI and the private sector, which enhances communications and promotes the exchange of information. The DSAC works with the FBI in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce.
(http://www.fbi.gov/stats-services/publications/facts-and-figures-2010-2011/working-with-the-private-sector)

CERT Coordination Center (CERT CC)

CERT CC coordinates communication among experts during security emergencies, respond to major security incidents, and analyse product vulnerabilities. Develops and promotes use of appropriate technology and systems management practices
(www.cert.org/certcc.html)

4.2 Introducing PPPs in Canada

Public Safety Canada

This organisation has overall responsibility for the National Strategy and Action Plan for Critical Infrastructure and for All- hazards management in Canada. They are developing sector networks, building where possible on existing mechanisms, so that each of the critical infrastructure sectors has a forum for discussion and information exchange.
(www.publicsafety.gc.ca)

Industry Canada

This is the lead agency for the Communications and Information Technology Sector and is responsible for the CIP and emergency management.
(http://www.ic.gc.ca)

Canadian Telecommunications Cyber Protection Working Group (CTCP)

Industry Canada has established the sector network -the Canadian Telecommunications Cyber Protection Working Group (CTCP) to promote industry-to-industry, government-to-industry and industry-to-government co-operation in protecting Canadian networks.
(www.ic.gc.ca/eic/site/et-tdu.nsf/vwapj/...CTCP-e.../Fact-CTCP-e.pdf)

Network for Security Information Exchange (CNSIE)

Industry Canada and the CTCP Working Group have established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration between a larger community of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and other government departments.

CanCERT™

This is Canada's first national Computer Emergency Response Team which is operated since 1998 by Electronic Warfare Associates - Canada, Ltd., It is a trusted centre for the collection, analysis and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident response for Canadian governments, businesses and academic organizations.
(http://www.ewa-canada.com/cancert/index.php)

Canadian Telecommunications Emergency Preparedness Association (CTEPA)

This is an industry association for emergency planners representing wire line, wireless and satellite facility-based telecommunications companies in Canada.
(http://www.ctepa.ca/)

4.3 Introducing PPPs from Australia

The Trusted Information Sharing Network (TISN)

The TISN is a forum in which the owners and operators of critical infrastructure work together, an all hazards basis, and share information on threats and vulnerabilities and develop strategies and solutions to mitigate risk. It comprises seven critical infrastructure Sector Groups and two Expert Advisory Groups, Communities of Interest (CoI) and a Critical Infrastructure Advisory Council (CIAC).
(http://www.tisn.gov.au/)

Sector Groups (including the communications sector group)

These groups form the bridge between government and the individual owners and operators of Australia's critical infrastructure. They assist owners and operators to share information on issues relating to generic threats, vulnerabilities and to identify appropriate measures and strategies to mitigate risk. The Communications sector group comprises representatives from the telecommunications, broadcasting, international submarine cable and postal sectors.

4.4 Mapping of PPPs in the US, Canada and Australia to the Three Generic Types

Additional research (involving desktop, questionnaires and interviews) has allowed a mapping of the three generic types utilised in Europe to similar organisations in the US, Canada and Australia. The following table summarises these findings.

	Protect	Respond	Umbrella
The US			
NCCIC			●
NSTAC	●		
NSIE	●		
ISAC	●		
CSCSWG	●		
I3P	●		
NIAC	●		
US-CERT		●	
INFRAGARD	●		
IT SCC		●	
CSCC		●	
AFCEA	●		
OSAC	●		
DSAC	●		
CERT-CC		●	
Canada			
Public Safety			●
Industry Canada			●
CTCP			●
CNSIE	●		
Can-CERT		●	
CTEPA		●	
Australia			
TISN			●
Comms Sector Group	●		

Figure V: Chart showing how US, Canadian and Australian PPPs map to the generic types

4.5 Advice from International sources

This section contains seven key points made by PPPs in the US, Canada and Australia. Each key point is supported by a quote.

1. Use existing organisations where possible.

"Rather than setting up their own parallel universe of private sector organisations with which to partner, thus competing with industry associations, government would more efficiently leverage the existing organisations which industry has established firm commitment to and recognizes as the appropriate industry representatives". (USA L. Clinton[20])

2. Allow each sector to develop appropriate mechanisms.

"The Australian Government recognises that the TISN Sector Groups have matured over the years and the differences between the Sector Groups in terms of composition of membership, sectorial operating environments, and the nature and extent of their relationship with the Australian Government, is very apparent. Accordingly, it is acknowledged that there are practical limitations in regarding the TISN as a homogenous collective. In fact, the TISN comprises seven unique Sector Groups each with their own culture, people and approach. In recognition of these differences, the Australian Government, through the CIR Strategy is taking a more tailored approach to each Sector Group." (Australia)

3. Information shared must be protected.

"As lead Australian Government agency for CIR, the Attorney-General's Department (AGD) is responsible for management and coordination of the mechanisms that facilitate the free exchange of information within the TISN framework (including Deeds of Confidentiality, the Government Representative Confidentiality Acknowledgement, and access and security arrangements for the upgraded TISN public and TISN secure websites)" (Australia)

4. Government must be prepared to share valuable information.

"Consistent with the principles of the Emergency Management Framework for Canada, federal, provincial and territorial governments will aim to be as open as possible about the work each level of government does in emergency management, security and business continuity planning." (Canada)

20 http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Hathaway%20public%20private%20partnerships.pdf

5. Action plans must be jointly developed.

"Even though industry has the greater resources and responsibility to addressing cyber security, government still sees itself as the "senior partner" in its relationship".

"This means that too often when current public private partnerships engage in projects they are typically initiated by the government partners to address government interests. As good partners industry will attempt to assist government in these projects, but the effectiveness of the projects is sometimes compromised from the start due to government's "senior partner" role".

"Rather than government approaching its industry partners with a pre-determined organisational structure and pre-set goals and plans government ought to approach industry with a "blank page" and work on developing action plans in true partnership". (USA L. Clinton)

6. Government must fully appreciate the value proposition required by industry.

"The value of cyber security for the government is the common defence. While individuals and companies benefit from a strong national defence, the national interest is not, and ought not be, the value proposition for private interests. For the private sector the value proposition for investments in cyber security are what is justified by their individualized business plans ... government must hold out business sensitive, not simply public interest benefits." (USA L. Clinton)

7. Partnerships must be equal – co-operate not regulate.

"Be cooperative in nature, lacking punitive overtones characterized by regulatory models, so that trust and affirmative proactive steps are taken by both partners.
Have a recognized joint leadership structure in which both partners believe they have equivalent investment in and control over the workings of the partnership"(USA L.Clinton)

4.6 Critical Success Factors for Information Sharing

The information sharing practices of leading organisations and the factors they deemed critical to their successful information sharing relationships where identified.

In a review in the USA, looking at best practice, they identified a number of critical success factors. Of these, many organisations identified **trust** as the essential underlying element to successful relationships and said that trust could be built only over time and, primarily, through personal relationships:

"Other critical success factors identified included:
- ***Establishing effective and appropriately secure communication mechanisms, such as regular meetings and secure Web sites;***
- ***Obtaining the support of senior managers at member organisations regarding the sharing of potentially sensitive member information and the commitment of resources;***
- ***Ensuring organisational leadership continuity.***
- ***Providing identifiable membership benefits, such as current information about threats, vulnerabilities, and incidents. Without such benefits, according to the representatives we met with, members would not continue participating."***

(United States Government Accountability Office[21])

21 GAO, Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24 (Washington D.C: Oct. 15, 2001).

4.7. Possible way forward for collaboration

Scott C. Algeier, Executive Director of the US IT-ISAC spoke in England on 25/03/2011 at the NEISAS[22] workshop, to identify opportunities to improve international operational capabilities, and to propose areas for collaboration.

He pointed out that national economies are interdependent, often facing common threats and targeted by the same actors. Most nations depend on a functioning and reliable global information infrastructure, but working together, can enhance risk management through information sharing and collaborative analysis.

The IT-ISAC is keen to connect its capabilities to similar capabilities within the European framework, and elsewhere, in order to securely share information and trends among trusted partners.

In order to do this, the following need to be considered:

- Legal and confidentiality frameworks
- Complex and competing privacy laws
- Common understanding as to what to share
- Information based on analysed data is easier to share
- Sensitive private information should be able to be anonymised
- The ability to tailor information for specific communities of interest

22 https://www.neisas.eu/

Summary of the recommendations

5.0 Summary of the recommendations

To provide a quick reference for this Guide, this section summarises all the recommendations from Section 2 in a list. This list is divided into parts relating to the sub-sections in Section 2 so that the context to a particular recommendation can be located.

5.1 Recommendations from 2.1 'Why is a PPP needed?'

[Recommendation 1]

Membership of a PPP should offer a clear value proposition for both public and private sector stakeholders.

[Recommendation 2]

PPPs should consider the focus of other organisations to ensure that duplication is avoided and that all areas of the life cycle are covered with appropriate co-ordination and information sharing links.

[Recommendation 3]

PPPs should constantly ask themselves why they exist. If a problem has been resolved then they should identify the next priority issue to address.

[Recommendation 4]

PPP should consider the type of threat addressed as this will be a defining factor in shaping the membership and determining which external links are to be forged.

[Recommendation 5]

Public sector members should find ways to share sensitive information on threats with their private sector members.

[Recommendation 6]

PPPs should study carefully the implications of adopting a holistic approach to ensure they have the right skills and resources to achieve an optimum balance between the electronic, physical and personnel areas.

5.2 Recommendations from 2.2 'Who should it involve?'

[Recommendation 7]

The central co-ordinating body should look for and promote groups with strong homogeneity. This also applies to cross sector PPPs.

[Recommendation 8]

PPPs should plan how they will link with other organisations, to share information and expertise and to avoid duplication. This plan may form part of a National Strategy to coordinate the protection of the Critical Information Infrastructure.

[Recommendation 9]

The relationship with the Regulator must be considered carefully to take account of the legal environment, national culture and the needs of the membership.

[Recommendation 10]

National PPPs should look for opportunities to create international links with other PPPs for cross border sharing and collaboration. This could be facilitated by organisations with existing international contacts.

[Recommendation 11]

National PPPs should look closely at the benefits of becoming members of an organisation which represent their wider geographic/economic interests in relation to CIIP and who could facilitate the creation of an interface with other parts of the world. For example in Europe this could be the European Public Private Partnership for Resilience (EP3R).

[Recommendation 12]

PPPs should consider the use of a high level strategic partnership at the CEO level in order to support senior level understanding and awareness.

[Recommendation 13]

In creating the membership of PPPs great care should be taken to recruit people who are empowered and informed, from the organisations chosen.

5.3 Recommendations from 2.3 'How should it be governed?'

[Recommendation 14]

The role of the industry chair is very important and the PPP should ensure it has a clear mandate with agreed rules for selection and tenure.

[Recommendation 15]

Government can add value and reduce economic barriers to PPP participation by covering the costs of administration. Public sector partners should look seriously at covering these costs as it could be a significant incentive to the Private sector members to actively participate in those countries who that do not mandate membership.

[Recommendation 16]

Adequate funding for the PPP is vital and this is more likely if membership provides a clear value proposition by, for example, providing information which is not available anywhere else.

[Recommendation 17]

The PPP must also look for innovative ways to keep down costs, such as combining events with other meetings.

[Recommendation 18]

There should be clear and agreed rules and guidelines for the organisation and structure of the PPP.

[Recommendation 19]

PPPs should consider the use of an NDA and/or a system like the TLP in the formal rules. This consideration should include whether to have one at all or to have a personal or corporate focus.

[Recommendation 20]

PPPs should consider the building of two way trust as a priority.

[Recommendation 21]

PPPs should seek legal advice to ensure that they use a legal framework suitable for the jurisdiction in which they operate.

[Recommendation 22]

PPPs should implement policies which maintain continuity of membership such as clear membership rules on participation, backed up by incentives.

[Recommendation 23]

PPPs should look for opportunities for members to meet face to face in order to increase trust.

[Recommendation 24]

PPPs should strive to keep the number of members who meet at any face to face meetings small, to allow personal relationships to be built and maintained.

[Recommendation 25]

PPPs should adopt information distribution policies such as the Traffic Light Protocol to give the source confidence that the information will only be used as agreed.

[Recommendation 26]

PPPs should implement processes that allow the anonymisation of the source to facilitate the sharing of information with other PPPs.

5.4 Recommendations from 2.4 'What services and incentives should be offered?'

[Recommendation 27]

PPPs should create a mechanism for members to influence the services provided which meets their needs. This could be a regular agenda item as well as agreeing in advance a yearly work programme.

[Recommendation 28]

To deliver value added activities, PPPs should ensure that the services provided address the problems identified and align with the agreed scope focus.

[Recommendation 29]

It is important for a PPP to define the benefits to members, both services and incentives, explicitly. This will not only sustain the interest of members but also support them in securing the support of their management.

[Recommendation 30]

PPPs should clearly leverage the skills, experience and organisational positions of the existing members to provide an incentive for new members.

[Recommendation 31]

All members of the partnership, including the public sector members, need to actively contribute information, services or support that is of relevant value to the membership. Where members fail to make a positive contribution action should be taken by the membership to resolve the situation.

5.5 Recommendations from 2.5 'When action should be taken to start it and maintain sustainability?'

[Recommendation 32]

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

[Recommendation 33]

PPPs should recognise the importance of good management practices when creating and operating partnerships.

[Recommendation 34]

For sustainability, it is important for non-mandatory PPPs to continually demonstrate added value, especially in the early stages to prove the need for the PPP.

[Recommendation 35]

Some members may initially join PPPs in order to mitigate undesirable changes (e.g. the threat of regulation), but for real long term sustainability this should be evolved into a true partnership where all members (public and private) get real value.

[Recommendation 36]

PPPs can assess the value of their activities by analysing the background of its private sector membership. If they are predominantly from an operational technical and/or policy background then the PPP is adding real value.

Conclusions

6.0 Conclusions

Public Private Partnerships which address security and resilience have evolved in many countries as an efficient means of protecting their Critical Infrastructures. Each sector, public and private, brings its own, complementary strengths to the table, but such structures come with challenges in their formation, management, and effectiveness.

This Guide has been the result of a comprehensive survey of many of those PPPs throughout Europe, the USA, Canada and Australia. Through the administration of questionnaires and interviews of those involved in such PPPs, as members or organisers, best practice has been identified and a set of guidelines been compiled.

This Guide sets out the principles, which underpin Public Private Partnerships and considers the range of partnership options available. It also describes some of the ways in which they can be used, and advises on the issues, which need to be addressed when implementing them.

These should be of assistance to those setting up or evolving similar partnership arrangements and help optimise the chances of success. In addition, the common understanding portrayed in this Guide will lead to further opportunities for inter-working and collaboration.

Appendices

Appendix A: Summary List of Observations

To provide a quick reference for this Guide, this section summarises all the observations from Section 2 in a list. This list is divided into parts relating to the sub-sections in Section 2 so that the context to a particular observation can be located.

A.1 Observations from 2.1 'Why is a PPP needed?'

[Observation 1]

The reasons why a PPP is needed can be different if the initiative is being led by the public sector than if it is being driven from the private sector.

[Observation 2]

The problem set will be a defining factor in which parts of the security life cycle the PPP should focus on.

[Observation 3]

PPPs focus within the life cycle in three ways. They either focus on the whole life cycle (umbrella approach), the early stages (prevention approach) or the later stages (response approach).

[Observation 4]

Deciding where to focus within the life cycle will influence which members will take part in the PPP.

[Observation 5]

PPPs members will focus on what is relevant for them so the threat type for a PPP may evolve over time.

[Observation 6]

Successful PPPs find ways to share sensitive information between Public and Private sector members, for example by mandating a security clearance for membership. Of those surveyed 21% currently used Security Clearance and another 24% planned to used them

A.2 Observations from 2.2 'Who should it involve?'

[Observation 7]

Many countries have found that to create homogeneous, single-sector or theme organisations adds value for members, enabling them to focus on topics of specific relevance to their industry or role.

[Observation 8]

Often, these sector-specific groups have an overall central organisation, which coordinates activities and facilitates cross-sector sharing.

[Observation 9]

Several organisations who share sensitive information do not include the Regulator, as his presence is seen to inhibit information sharing.

[Observation 10]

There are other organisations where the Regulator may have initiated the PPP, or is seen as a partner, and as 'positively helpful.' If the Regulator is able to participate in a way that is not looking to be punitive, there can be a useful, 2-way relationship.

[Observation 11]

There are well developed links between many nations both within the EU and wider afield. For example the tri-lateral relationships on the Information Exchanges in the UK, US and Canada.

[Observation 12]

The presence of high-level strategic partnerships between industry and government with a remit to oversee more tactical PPPs was not universal. However, in those countries, which had adopted this approach, they appeared to work well.

A.3 Observations from 2.3 'How should it be governed?'

[Observation 13]

PPPs select the general type that matches their purpose but as they evolve they may need to create other partnerships or change their type. For example a working group for a specific purpose might decide to become a long term community as they recognise .the value of the informal information sharing that they have naturally evolved.

[Observation 14]

As the nature of a PPP is a partnership between public and private organisations, the leadership structure often includes both, and some organisations have joint industry and government chairs with agreed rules of tenure.

[Observation 15]

Defining who provides secretariat services, who co-ordinates the activities as well as who chairs the PPP are visible roles of authority as well as being a cost consideration. It is more common for government to provide administrative support and venue.

[Observation 16]

Membership in a PPP may be mandatory or voluntary. In some countries it is seen as a privilege to be a member; in others there is awareness that to fail to participate might place a company at a disadvantage.

[Observation 17]

Even though in some countries membership of a PPP is mandatory, taking part in activities such as trusted information sharing is voluntary. This recognises that you cannot force members to share information if they see risks and no value in doing so.

[Observation 18]

In the creation of some PPPs they did not have any formal membership rules initially as they were often addressing the immediate problem at hand. However, over time membership rules were developed to suit the needs of the community.

[Observation 19]

Most of these policies address trust in the context that the recipient will not abuse the information nor cause harm to the source. However, there is also a need for trust in the source so that the recipient can be confident that the information is accurate and not misleading. This second aspect of two way trust was seen by many PPPs as very important but more difficult to address with a policy solution.

[Observation 20]

Many PPPs have membership rules which differ according to the nature of the PPP. Many include Non-Disclosure Agreements, and arrangements for sharing sensitive information. Details of membership rules for Information exchanges can be found in ENISA publication GPG NSIE[23].

A.4 Observations from 2.4 'What services and incentives should be offered?'

[Observation 21]

The range of services changes and grows over time, led by the needs of the membership and the lessons learned. For example Good Practice Guides are often produced after the PPP has addressed the corresponding problem.

[Observation 22]

Creative approaches have utilized services to gain membership interest, for example offering cheap or free training to candidate members. The training was of genuine value but also enabled the attendees to understand the importance and value of membership.

[Observation 23]

Not all members need to contribute the same types of value. Some may offer technical knowledge while others funding. Some may offer intelligence while others research and analysis.

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

A.5 Observations from 2.5 'When action should be taken to start it and maintain sustainability?'

[Observation 24]

PPPs that continually add value are likely to have private sector membership at the operational technical and policy level.

[Observation 25]

Where PPPs operate mainly in the defensive mode, private sector membership is more likely to be from a legal or regulatory background.

Appendix B: Abbreviations and Definitions

B.1 Definitions

For the purposes of this document, the following terms and definitions apply:

Critical Information Infrastructure
Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. [Source: OECD 2008]

Electronic communications (e-Communications) Networks
Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. [Source: EU Directive 2002/21/EC].

Homogeneity
Homogeneity is the state of being homogeneous. This is a situation where all the members of a PPP are of the same nature. For example all being from the same sector, or security professionals focused on addressing malware issues. This common nature enables the partnership to focus on topics that are of common interest to all.

Central Co-ordinating Body
An organisation that relates with other organisations or partnerships with a specific role to oversee, steer and/or organise the focus of those other partnerships.

Network and Information Security (NIS)
The ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems. [Source: ENISA]

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

Resilience
The ability of a system to provide & maintain an acceptable level of service, in face of faults (unintentional, intentional, or naturally caused) affecting normal operation. [Source: ENISA]

B.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIR	Australian Critical Infrastructure Resilience Strategy
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure (UK)
CSIRT	Computer Security and Incident Response Team
DPA	Data Protection Act
EC-RRG	Electronic Communication – Resilience and Response Group (UK)
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
GPG	Good Practice Guide
IT-ISAC US	Information Technology Information Sharing and Analysis Centre
ISP	Internet Service Provider
MELANI	Swiss Reporting and Analysis Centre for Information Assurance
MTP	Multi-annual Thematic Programme
NCO-T	National Continuity Forum Telecommunications (NL)
NDA	Non-Disclosure Agreement
NESA	Finnish National Emergency Supply Agency
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee (US)
OCS	Office of Cyber Security, (UK)
OFCOM	UK Telecommunications regulator
PPP	Public Private Partnership
SCADA	Supervisory Control and Data Acquisition
SME	Small and Medium Enterprises
TISN	Australian Trusted Information Sharing Network
TLP	Traffic Light Protocol
UP- KRITS	Germany's CIP Implementation Plan (Umsetzungsplan KRITIS)
USA	United States of America

Appendix C: The Source used in creating this guide

This guide was produced using the results of a research that had three phases;

- A comprehensive desktop survey of PPPs
- A questionnaire sent to PPP stakeholders across Europe
- Telephone interviews with a sample of questionnaire respondents

This three-phase process was, used in parallel, to produce two sets of knowledge: firstly to produce data on the European PPP activity (Sections 2 and 3) and secondly data on the international viewpoint (Section 4).

C.1 Desktop Study

The first stage of the study, desktop research, formed an initial step in understanding 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.

For each PPP selected, information 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.

The researched information, gathered before March 2011 was analysed and yielded an initial taxonomy for describing PPPs. The output from the desktop research and the initial analysis workshop formed the basis for the structure and taxonomy for classifying PPPs as shown in the mind map in Section 2.0.

Information gained from desktop research was also used to steer and focus the survey and subsequent interviews, which validated the taxonomy.

C.2 Questionnaire Survey

Potential respondents were identified through ENISA, through contacts known to the project team members and from contacts provided on publicly accessible websites.

30 key stakeholders, involved with European and international PPPs, completed the questionnaire which helped to validate and enhance the information found in initial research. The questionnaire consisted of multi choice questions with comment boxes to allow clarification or amplification where necessary.

The structure of the questionnaire used in the survey was based on the taxonomy derived from the desktop research. See Section 2.0

In total, 20 nations, including 16 EU members, contributed to the research. In alphabetical order they are:

Australia
Austria
Czech Rep.
Denmark
Estonia
Finland
France
Germany
Ireland
Italy
Lithuania
Netherlands
Norway
Poland
Portugal
Slovenia
Sweden
Switzerland
UK
USA
International Organisations

The following chart highlights the 18 European Nations who actively contributed to this study. Green shows those that completed both the questionnaire and an interview while pink those who completed just the questionnaire.

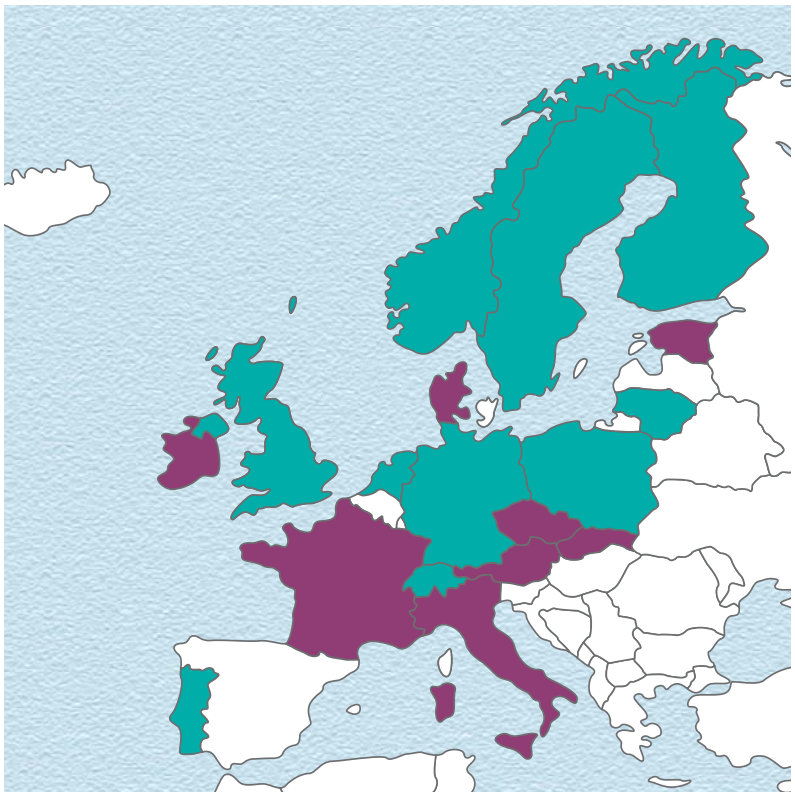

Figure C.I: European Nations who actively contributed to the research

C.3 Interviews

The final stage was to arrange interviews (in the form of conference calls) with a cross section of PPP members encompassing a wide range of PPP types and from both the private and public sector. All interviewees would have previously filled in a questionnaire survey.

All interviews were fully documented but all participants were assured that the notes would not be published and only used to help the team with their analysis. They were free format with interesting issues followed up when appropriate. Where the analysis identified succinct and highly relevant quotes, these are used to make the point but without attribution. All interviewees were given the opportunity for their quote to be removed from the final published document.

PPP members from 15 private and public sectors were interviewed to further clarify their questionnaire responses. The information obtained was then analysed and categorized, so it 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.

C.4 Example Desktop research sources

The following section lists some examples of organisations which were initially studied as part of the desktop research.

Austria

CERT-AT. In the case of significant online attacks against Austrian infrastructure, CERT- AT will coordinate the response by the targeted operators and local security teams. CERT- AT is the primary contact point for IT-security for Austria at the national level.
http://www.first.org/members/teams/cert_at/

A-SIT The Secure Technology Information Centre. Its mission is to provide concentrated support of IT security issues for public institutions and the economy.
http://www.a-sit.at

Belgium

BENIS* The Belgian Network of Information Security. This platform brings together the federal institutions involved in making policy on the security of information. It also supervises three working groups: "Classification of Information", "Critical Information Infrastructures" and "Harmonisation of the Functions Linked to the Security of Information".
(Web page not located)

Estonia

Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Look@World Foundation was established in 2001 by ten leading companies in Estonia with the goal of fostering the development of the IT society in Estonia. The Computer Protection 2009 project (also called Look@World 2) aims to foster the security of the Estonian information society.
http://www.riso.ee/en/node/80

Cooperative Cyber Defence Centre of Excellence (CCD COE)

Located in Tallinn, Estonia, the Centre is an international organisation that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain as Sponsoring Nations. It is open to all NATO nations. Its mission is to enhance the capability, cooperation and information sharing among NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.
http://www.ccdcoe.org/37.html.

Finland

NESO* The National Emergency Supply Organisation includes a planning committee network of clusters and pools that are Public Private Partnerships. The clusters, which focus on priority areas for Finland's security of supply, are broad-based, sector-specific collaborating organisations consisting of experts representing the authorities, relevant bodies and the main parties involved.
http://www.nesa.fi/security-of-supply/public-private-partnership/

Ubiquitous Information Society Advisory Board
The Ubiquitous Information Society Advisory Board is a body with members from ministries, public administration, NGOs, and business life. Its task is to ensure that the National Information Society Strategy will be put into practice.
http://www.arjentietoyhteiskunta.fi/inenglish

France

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) created in 2009. The agency will operate a centralised capability to detect and defend against cyber-attacks. It will have the resources to sponsor the development of, and acquire, the security products essential to protect the Government's most sensitive networks. The agency will also take on an advisory role to the private sector, particularly in areas of critical strategic importance, and will participate actively in the development of security for the information society.
http://www.ssi.gouv.fr

Germany

Both private and public worked together to develop the CIP Implementation Plan - Umsetzungsplan KRITIS (UP KRITIS) that was adopted in 2007. It is the foundation for a long-term partnership between the public and private sectors. Its three strategic objectives are "Prevention, Preparedness, Sustainability".
http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/cip_stategy.pdf?__blob=publicationFile

Italy

Italy has a working group on critical information infrastructure protection, established in 2003 as part of the Prime Minister's Office that composed of representatives from Government departments and agencies, and private sector operators.
http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&Itemid=99

Netherlands

ECP-EPN, the Electronic Commerce Platform and the Platform for e- Netherlands, is a non-profit platform, working with member organisations from government, industry and science on all aspects of e-Netherlands.
www.ecp.nl

The NICC, (National Infrastructure against Cybercrime), is an organisation at the heart of the Dutch National Infrastructure, which brings together a select group of government services and representatives of critical industry sectors to collaborate in the fight against cybercrime. The model comprises various consultation groups in which representatives of companies exchange confidential information with each other on a per-sector basis.
www.samentegencybercrime.nl

NCO-T* The National Continuity Forum Telecommunications (NCO-T) has the objective to develop a way to implement the obligations put down on telecom operators in the Netherlands. It addresses the preparations to be made by an operator to be able to operate critical telecommunications services during a situation of Exceptional Circumstances.
www.nis-summer-school.eu/nis09/presentations/11a-Merkom.pdf

Norway

NorCERT (Norwegian Computer Emergency Response Team) coordinates preventative work and responses against IT security breaches aimed at vital infrastructure in Norway. They alert of serious attacks, threats and other vulnerabilities related to serious IT security.
https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/

Poland

ARAKIS-GOV is an early warning system reporting threats arising on the Internet. The system has been developed by the IT Security Department of the Polish Internal Security Agency in cooperation with the CERT Polska team operating within the NASK organization.
http://www.cert.gov.pl/portal/cee/39/78/ARAKISGOV_system.html

Spain

The National Centre for the Protection of Critical Infrastructure (CNPIC) is the leading and coordinating office for every activity related to the protection of critical infrastructure.

CNPIC has aimed its efforts clearly towards critical infrastructure protection from a holistic point of view, by integration of physical and cyber security in a single scope.
http://www.cnpic-es.es/

Sweden

PTS is the Swedish Post and Telecom Agency, which monitors the electronic communications and postal sectors in Sweden. The Agency works with consumer and competition issues, efficient utilisation of resources and secure communications. One PPP within the PTS is the National Crisis Management Co-ordination group (NTGC) that has been trained to be able to function in a national emergency, to test and develop the forum, to update documentation, to develop contacts and to coordinate exercises.
http://www.pts.se/en-gb
http://www.pts.se/en-gb/About-PTS/Information-materials/

Switzerland

Within MELANI, the Reporting and Analysis Centre for Information Assurance, partners work together who are active in the area of security of computer systems and the Internet and protection of critical national infrastructures. It plays a role in all four pillars of the Swiss information assurance policy (prevention, early warning, crisis management, and technical problem solution) and is the central office for CIIP in Switzerland.

The "closed constituency" of MELANI can be described as a dedicated Public private partnership for CIIP.
http://www.isb.admin.ch/themen/sicherheit/00152/00175/index.html?lang=en

UK

CPNI Centre for the Protection of National Infrastructure. Government authority that provides protective security advice to businesses and organisations across the national infrastructure.
http://www.cpni.gov.uk/

The UK Network Security Information Exchange (UK-NSIE) formed in April 2003 to share sensitive information in the information and communications technologies sector. It currently includes IP providers, core mobile operators, and traditional telecommunications providers, as well as CPNI. Participating companies now cover over 80% of the telecommunications market in the UK. It is linked to NSIE in USA, of which BT is a member. BT acts as the channel for information between the two Exchanges. Under the aegis of the NSIE, a number of working groups have been established, and several guidance documents and technical papers have been produced. These include a guide to the procurement of resilient telecoms and best practice guidance on the secure implementation of BGP.
nsie@cpni.gsi.gov.uk

EC-RRG Electronic communications resilience and response group aims to ensure the availability of Electronic Communications infrastructure for the UK and provide an industry emergency response capability through the ownership and maintenance of the National Emergency Plan for Telecoms. They take the lead in developing and maintaining cooperation between the telecommunication industry and govt. organisations.
http://umbr4.cabinetoffice.gov.uk/media/200048/ec-rrg_tor.pdf

WARPS, Warning, Advice and Reporting Point
A WARP is a cost-effective, community-based service where members can receive and share up-to-date advice on security threats, incidents and solutions. This community is supported by a WARP operator. A WARP provides a trusted reporting point mechanism for sharing security incidents and other sensitive information without fear that the information will be used against them. Pooling and sharing this information with other members of the WARP, and possibly other WARPs as well, leads to more robust and secure systems.
www.warp.gov.uk.

International

ARECI workgroups
The Study on Availability and Robustness of Electronic Communications Infrastructures (ARECI) was conducted for the European Commission. The Final Report of the ARECI Study presented ten Recommendations to European Institutions, Member States and Private Sector stakeholders. In order to carry out some of the recommendations, workgroups were set up combining public and private stakeholders, who worked together to enhance the availability and robustness of Europe's communications networks.
http://www.epractice.eu/en/library/281377

ETSI is recognised as an official European Standards Organisation by the European Union, enabling valuable access to European markets. They produce globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical and other areas.
http://www.etsi.org/WebSite/homepage.aspx

European Network and Information Security Agency

Good Practice Guide – Cooperative Models for Effective Public Private Partnerships

Luxembourg: Publications Office of the European Union, 2011

ISBN: 978-92-9204-054-3

doi:10.2824/21641

Catalogue Number: TP-30-11-236-EN-N

TP-30-11-236-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 978-92-9204-054-3