JRC Scientific and Technical Reports

Reflections on Networking & Information Exchange

Dealing with Sensitive Data amongst Public and Private Actors

Gustav Soderlind

EUR 23693 EN - 2008

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

The Institute for the Protection and Security of the Citizen provides research-based, systems-oriented support to EU policies so as to protect the citizen against economic and technological risk. The Institute maintains and develops its expertise and networks in information, communication, space and engineering technologies in support of its mission. The strong cross-fertilisation between its nuclear and non-nuclear activities strengthens the expertise it can bring to the benefit of customers in both domains.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: TP210. Via E. Fermi 1, 21020, Ispra (VA) Italy
E-mail: gustav.soderlind@jrc.it
Tel.: +39 0332 78 95 62
Fax: +39 0332 78 95 76

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 49481

EUR 23693 EN
ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

ABSTRACT

In this report we reflect upon possible issues that need to be considered before embarking on creating a partnership or network where a main objective is the exchange of sensitive information.

To this end, we try to provide a brief overview of types of information exchange partnerships, and suggest various aspects that those embarking on a partnership should first review.

The second part of this report is devoted to highlighting operational ("soft") issues that need to be kept in mind, such as national legal and regulatory frameworks and trust issues. In the third part we sketch some technical aspects that may have an impact.

Table of Contents

1 What are Information Exchange Partnerships 6
1.1 Partnership Categories 6
1.1.1 Why Partnerships and What is shared 6
1.1.1 Stakeholders (Who) 9
1.1.2 Organizational examples 10
1.2 Degrees of Interaction (How) 11
1.3 Implementation (How) 12
1.4 An operational view of information sharing 13
2 Soft Aspects 15
2.1 Legal Commercial and Regulatory Issues 15
2.2 Handling of Sensitive Information 17
2.3 Quality 19
2.4 Analysis and Processing 19
2.5 Trust 20
2.5.1 What is trust 20
2.5.2 Concerns 22
3 Technical Aspects 23
3.1 Interoperability 23
3.2 Security 25
3.3 Applications and Mobility 26
4 Conclusions 27

Introduction

In this paper we reflect upon some issues of networking and information exchange where a primary goal is the exchange of security related information. Some of the possible areas that may need to be considered are related to the notion of Private Public Partnerships (PPP), which make take different forms and shapes.

The report is structured in three parts.

- *What are Information Exchange Partnerships*: here we provide various views on the topic.
- *Soft aspects*: this part covers issues such as legal and regulatory aspects.
- *Technical aspects*; this part covers possible issues related to the supporting technologies, such as the security of ICT systems.

In the first chapter we begin by providing some examples of the various types of networking and partnerships that may result form the interaction of public and private actors, and later point the reader to the issues, soft and technical, that we believe are most relevant. These issues can then hopefully be used to support the decision process when selecting the best shape for a given network or PPP implementation.

The importance of establishing and strengthening collaborative networks and to facilitate information sharing in the European security domain between the private and public sectors has already been identified by the European Commission; see for example the following extracts from a communication on Public-Private Dialogue in Security Research and Innovation.

> *Developing and implementing an effective security research strategy therefore requires the participation of all relevant stakeholders in the private and the public sectors, both at national and European levels.*
> *In this context, the specific policy objectives of the Private-Public Dialogue in Security Research and Innovation are:*
>
> - *to bring together all the relevant stakeholders in order to discuss issues of cross-cutting, common concern, facilitate the assessment of their differentiated strengths and resources, identify areas for potential synergies; or joint programming;*
> - *to identify proposals for forming a strategic security research and innovation agenda, involving national and European stakeholders, laying out a shared and clear view of European security research needs and priorities;*
> - *to share ideas, views and best practices in order to make better use of existing capabilities and to enhance the use of technology in security-related domains, e.g. by inter alia making the best possible use of the various funding instruments in the present financial programming period*.[1]

It is hoped that this paper will help those contemplating a partnership for sensitive issues (e.g. information exchange) to prepare themselves, not necessarily by providing answers but rather by highlighting possible pitfalls. Before embarking on the creation of a multi-party and perhaps cross-border collaboration for matters such as information exchange and its supporting systems – structure, process, equipment – there is a sequence of questions that should be examined. For instance, for an information exchange venture, the following points will be relevant:

[1] Communication from the Commission to the European Parliament and the Council on Public-Private Dialogue in Security Research and Innovation http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0511:EN:HTML

- **Why**: what is the purpose.
- **What**: what information is to be shared, what type of information, how sensitive it is, is it time critical?
- **Who**: who are the actors that will be sharing information, will it be government – industry, across industry sectors, across government departments; is it on local, regional, national or international level?
- **Where & When**: where will it be placed, when should it be active. Will the information sharing take place across legal and regulatory borders?

It is only when the preceding questions have been satisfactorily answered that work can proceed on the last question:

- **How**; how can the partnership best be structured, what supporting tools will it need and which issues need special attention.

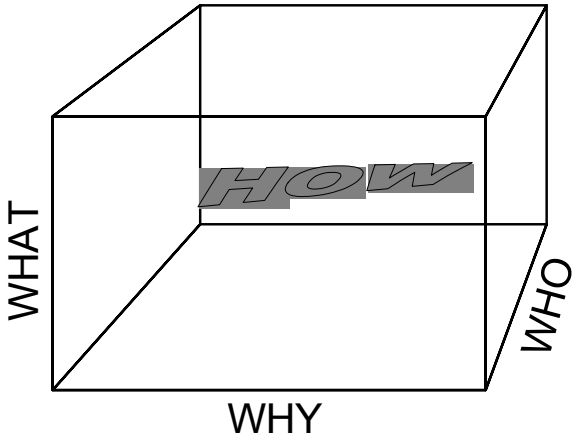

Figure 1. Implementation space.

1 What are Information Exchange Partnerships

1.1 Partnership Categories

1.1.1 Why Partnerships and What is shared

In this chapter we review various categories of partnerships that may be related to information exchange, and suggest possible ways to view the factors influencing the chosen implementation.

Depending on the role, main purpose or general mission, the best way to organise a partnership in order to facilitate information exchange - and the tools to use for it - may differ significantly. In this chapter we provide a rough sketch of some possible interaction categories and try to place information exchange in a basic context.

Information sharing should start with a purpose, a mission. Knowing this "why", it becomes possible to identify what type of information categories need to be shared, and amongst which actors. Knowing this, it becomes possible to start exploring exactly how the information sharing should proceed, both technically and methodologically.[2]

[2] Richard Wilhelm summarised the context aspects for information sharing in a speech at the 2004 RSA Conference held in San Francisco, California. *Information Sharing*: http://www.boozallen.com/publications/article/659327

The meaning of the term "Public Private Partnership" can vary significantly depending on context, and both its usage and general scope has expanded over the years. For an overview of PPP's and their applicability to security issues see the JRC technical report "*Is Public Private Partnership a suitable way to cope with security*".

For the sake of identifying similarities in operation and style between partnerships Michael Geddes[3] proposes the following rough categorisation - based on whether the output is executive or advisory, and on the reasons behind the partnership:

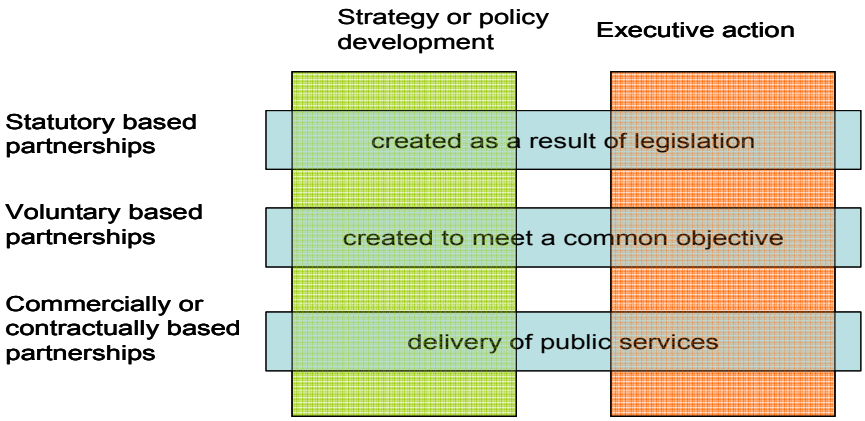

Figure 2. PPP categories based on motive and output

Depending on the motive for the partnership there will usually be very varying legal, financial and regulatory aspects to consider, there may also be differences in the degree of trust and cooperation between the partners, while depending on the type of output there will usually also be large differences in their internal structure/organisation.

Possibly the most common PPP category identifiable from the image above is the "commercially or contractually based partnership" which produces an "executive action", e.g. in this category one public authority enters into a close partnership with one or more private industries for the sake of transferring to private industry the responsibility for construction and or maintenance of an infrastructure that provides a public service. This type of partnership often entails complex legal and financial arrangements, and the European Commission has been working on facilitating this process through a number of initiatives and guidebooks.[4]

A recent notable example of EC support is the European PPP Expertise Centre (EPEC), an initiative launched in collaboration with the European Investment Bank. Its purpose is to help public institutions become more effective in their PPP participation, and one means to this end is the facilitation of information sharing regarding experiences and best practises between the member institutions. A motive given for this initiative is that "*experience is not systematically shared, resulting in a failure to learn lessons and effectively disseminate best practice. This applies both within and between countries.*"[5]

---

[3] Geddes, Michael. *Making Public Private Partnerships Work: Building Relationships and Understanding Cultures*, Gower Publishing, Ltd., 2005

[4] See for example*: Initiative on Public Private Partnerships and Community Law on Public Procurement and Concessions* http://ec.europa.eu/internal_market/publicprocurement/ppp_en.htm
Guidelines for Successful Public – Private Partnerships http://ec.europa.eu/regional_policy/sources/docgener/guides/ppp/ppp_en.pdf
Green Paper on public-private partnerships and on Community law on public contracts and concessions, COM(2004) 327, 30.4.2004 http://europa.eu/scadplus/leg/en/lvb/l22012.htm

[5] European Investment Bank press release, 16 September 2008, *European institutions take lead on PPP expertise* http://www.eib.org/attachments/press/2008-005-fact_sheet_epec_en.pdf

This leads to the objective of this paper: information sharing, i.e. partnerships where information exchange either is by itself the main objective of the partnership, or where the main objective heavily depends on information exchange. Below follows a non exhaustive list of possible motives behind information exchange partnerships, i.e. reflecting on **What** is to be shared:

- Crisis Management – such as emergency information distribution to the public – or for the sake of decision making and situational awareness information sharing – might be conducted between police, rescue services, military, medical authorities, meteorological agencies etc.
- Data clearinghouses – they collect, store and disseminate scientific, technical, environmental, legal, etc information, sometimes in processed form. An example is satellite photographs collected from various space operators.
- Incident reporting – such as virus info sharing
- Warnings and Alerts networks – such as critical infrastructure warning networks
- Educational and Awareness raising – can be used both as preparatory and for crisis management
- Expert networks – which can be used for policy support
- Law enforcement – e.g. sharing databases
- Technology Watch – which could: 1. identify, keep track & analyze positive/negative trends in security, 2. identify & analyze disruptive technologies; 3. share roadmaps/strategies[6], Experimental Labs for testing current and proposed technical systems, verify vulnerabilities, simulate attacks, verify standards
- Vulnerability data bases and disclosure: constitution by shared contributions
- Security data bases: Archives of attacks, security events
- Incident response and emergency management [7]

For the examples above it is possible to isolate some distinct differences, for instance with respect to the information they handle:

- Crisis Management information:
  - Often Time-critical
  - Can require high bandwidth
  - Sources and Recipients can change dynamically
  - Stringent interoperability issues between actors
  - Information security subject to medium-level requirements (i.e. ideally it should be as secure as possible, but security must not interfere with operational objectives)
- Data Clearinghouses:
  - Information is in long-term storage
  - Information needs maintenance, either by up-loader or by the clearinghouse
- Incident Reporting:
  - Rapid response often needed
  - Low bandwidth (e.g. e-mail)
- Warnings and Alerts:
  - Data is subject to hard time constraints
  - Data is highly sensitive
  - Authentication of sources and receivers should be strict
- Educational and Awareness raising:
  - The focus is on the contents, and their legibility and understandability.
  - There are defined roles for the actors, with different activities

[6] See for example Roadmap to Secure Control Systems in the Energy Sector http://energetics.com/csroadmap/
[7] See for instance the reports discussed in: Information Sharing and Analysis Centers Council http://www.isaccouncil.org/pub/index.php

- Expert Networks:
    - Authorship and recognition of sources are fundamental, with possible explicit requirements about confidentiality and intellectual property
    - Final output could be open to all users or dedicated to a limited set (e.g. policy makers)
    - End users might only access the final expert advice or have the possibility of browse through the discussions preceding the final results
- Law enforcement:
    - Information is highly sensitive
    - There are severe legal constraints on how information can be processed.
    - Depending on the status of the data (e.g. related to criminal investigations), the tracking of all access and actions is mandatory.
    - There are strict rules on the sequence of the actions that could be exercise onto the information (e.g. approval by hierarchy).

1.1.1 Stakeholders (Who)

Which stakeholders are involved in a partnership will influence the form and workings of the partnership, some examples of configurations are given below:

- Private – Private: this usually involves voluntary partnerships from Figure 2. e.g. for the purpose of influencing government policy.
- Public – Private: this usually involves commercially or contractually based partnerships, but could also relate to actions requiring some legal setting that otherwise would not be reached (e.g. information sharing)
- Public – Public: this usually involves voluntary or statutory partnerships, e.g. the EU may mandate that governments collaborate in certain areas, or various national government authorities may collaborate voluntarily.

The category of participants will affect the workings of the partnership, in particular if the partnership involves cross-border information sharing, even crossing regional borders may cause unexpected legal or regulatory difficulties. Other issues to consider are antitrust legislations that may make private partners reluctant to share information, competitive considerations, and trust issues. Trust and legal issues are further reviewed in a succeeding section.

The involvement of public authorities in a partnership can range from passive roles (e.g. sponsor, guarantor, mentor, proponent, etc.), to other more active ones (e.g. command and control, chairing, etc.). When a public authority chooses an active role in the partnership, it usually has two main responsibilities:

1. Coordination or secretariat (which result in the definition of the agenda, on the distribution of responsibilities and resources, in the acceptance of the results, etc.);
2. Leading by example, i.e. to be an active participant and a good user of the forums/support-tools provided.

1.1.2 Organizational examples

In this chapter we provide a short description of some partnerships based on information sharing, in order to show the wide the range of organisation forms.

Data Clearinghouse:

The Biosafety Clearing-House[8] is an information exchange mechanism established under the Cartagena Protocol on Biosafety. This protocol governs a wide range of issues related to genetically modified organisms (GMO), such as export procedures, human health etc. The Clearinghouse has two missions; serve as a platform for sharing experience and information on GMO, and to help government authorities to implement the protocol regulations. Its stakeholders include not only government but also industry and academia, which use it to share information and shape regulations.

Interesting aspects of this organisation are that it implements a common terminology on the documents and that information is owned by the government that uploaded it — i.e. that the uploading government authority is responsible for the maintenance and update of the information, as well as for ensuring its accuracy.

Crisis Management

During emergency situations such as natural disasters or terrorist attacks it is important to for decision makers, both at tactical and operational levels, to quickly obtain a cross-sector situation picture. This requires the sharing of both information and services between civilian - and also military – actors on both national and international levels. Technical experiments demonstrating the feasibility of this in Europe are ongoing.[9]

In the information and communication technologies domain, we can single out the US-CERT:[10] The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. It coordinates defense against and response to cyber attacks, getting connected to many parties in private and public organizations. US-CERT is responsible for

- analyzing and reducing cyber threats and vulnerabilities
- disseminating cyber threat warning information
- coordinating incident response activities

Expert Network, Social clubs and Network of peers

AVIEN, the Anti-Virus Information Exchange Network[11] had its informal inception amongst some of the participants to an Anti-Virus conference in late 2000. They shared the desire to learn from each other without constraints. This led to the ad-hoc creation of a closed, private network of specialists that help each other with news and advice daily. It also later led to the creation of the Anti-Virus Information & Early Warning System (AVIEWS), which expanded the scope to encompass not only people in large organizations, but vendors and smaller organizations as well.

---

[8] Kirsty GALLOWAY MCLEAN, *Bridging the gap between researchers and policy-makers: International collaboration through the Biosafety Clearing-House*. http://dx.doi.org/10.1051/ebr:2005017, See also http://en.wikipedia.org/wiki/Biosafety_Clearing-House

[9] For example: *Sweden and NATO Joint Live Experiment NEC Network Enabled Capability*. September 24-25, 2008 http://sweden-nato-nec.nc3a.nato.int

[10] For more information see United States Computer Emergency Readiness Team http://www.us-cert.gov

[11] Anti Virus Information Exchange Network. http://www.avien.net

A network with more formal origins and structure is "The Cyber Security Knowledge Transfer Network"[12] which sees itself and its mission as "*the single focal point for UK Cyber Security expertise, to collaboratively identify universal challenges and develop effective response, influence UK investment strategy and government policy, accelerate innovation and education, harness and promote UK capability internationally and help improve the UK security baseline.*"

Cavnet[13] is an example of a network evolved out of a pressing need and access to social networking tools. During the 2003 Iraq war junior U.S. officers on their own developed and deployed a private network to quickly exchange combat information such as reports about enemy troop movements amongst themselves. Although initially concerned about information security issues and loss of control, the Department of Defence (DoD) took on the idea and formally developed Cavnet for this purpose.

1.2 Degrees of Interaction (How)

In partnerships engaged in information exchange you can achieve varying "degrees" of interaction and sharing depending on the structure and purpose of the partnership. The table below lists some examples.[14]

Category	**Purpose**	**Methods**	**Uses**
Information sharing	Data exchange, networking	VoIP, e-mail, file-sharing	Sharing of best practices
Coordination	Regulated interaction	Project management, decision support	Responsibilities allocation
Cooperation	Working together, often towards a common goal	Wikipedia, discussion forums	Generation of trust
Collaboration	Genuine cooperative problem solving, working jointly with others on a common goal that is beyond what any one partner can accomplish alone	Brainstorming	Political decision making, Policy making

Table 1. Example of levels of interaction[15]

The stronger the common goal(s) is, the deeper the degree and complexity of interaction and mutual trust.

Whatever the definitions of collaboration, coordination etc, a fundamental part of them is the exchange of information; depending on the type and degree of interaction the methods for information exchange, as well as the type of information exchanged, will vary. Various degrees of collaboration can be associated with specific tools and methods[16], and each increase in the level of interaction adds a layer of complexity and requires additional support from tools and structures (organisation / process / methodology) to aid the interaction.

---

[12] The Cyber Security Knowledge Transfer Network. http://www.ktn.qinetiq-tim.net

[13] Congressional Research Service (CSR) Report for Congress *Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues*
http://www.fas.org/sgp/crs/natsec/RS22857.pdf

[14] Note, there are differences in literature on which of Coordination or Cooperation signify a deeper interaction.

[15] The table is an adaptation from Peter J. Denning and Peter Yaholkovsky, *The Profession of IT"; Getting to "We": Solidarity, not software, generates collaboration*, Communications of the ACM, April 2008/Vol. 51, No. 4

[16] E.g. the "Delphi method" if the purpose is Technology Foresight.

At the deepest levels of interaction, where it is not only information but also knowledge (see chapter 1.4) that is being shared, a good understanding of the partner's way of working (their organisational culture) is needed. Some aspects touching on the latter are presented in chapter 3.1 which examines interoperability.

1.3 Implementation (How)

There are various ways to structure a partnership or network; in this chapter we briefly list some aspects impacting on structure.

Financing and legal issues;

- The network or partnership will likely be a legal entity, the structure of which can take various forms, e.g. limited liability partnership.
- The partnership or network will need funding, at a minimum to pay for communication equipment/software and administration. In some cases the partnership or network can generate its own revenues. How income/funding are to be acquired, used and accounted for must be defined.
- Laws and regulations, on partnerships and on information exchange (such as privacy laws) will affect the structure and processes.

Admission and Membership

In some cases it will be self evident who the members will be, or at least which key members must participate for the information sharing to be meaningful. In other cases, depending on its goals, this may not be as clear cut.

- What are the criteria that members must fulfil to be eligible to participate?
- Inclusiveness is usually a good thing, but too many members may lead to unwieldiness and lack of trust.
- Should the partnership strive for a numerical balance between interest groups, e.g. public and private partners?
- What will the power structure be, e.g. if the partnership is steered by votes then private partners may be reluctant to participate if they can be outvoted by NGO's.

Roles and responsibilities

- If the partnership is expected to produce anything beyond a "social club" then there will have to be roles, responsibilities, and enforcement mechanisms, all geared to the purposes of the partnership.
- Regardless of the type of organisation there will have to be at least a minimum level of coordination and administration.

Supporting technologies and methodologies/processes

- The network/partnership will have to operate under a number of legal and regulatory frameworks (administrative/financial/information exchange specific). Work processes and other business practises will have to be set up to ensure that the applicable laws are followed.

- The equipment in support of information exchange, and other associated tasks, will have to be selected and maintained. The technical requirements on this equipment will vary depending on objective, but may include aspects such as security, bandwidth, and storage space.
- Work processes and methodologies will need to be selected and adapted.
- Security and other processes will need to be adapted to the information security concerns of all members.
- In some cases it might be foreseeable that the mission or size of the partnership will change over time, in which case adaptable or easily replaceable processes and technologies should be selected from the start with this in mind.

1.4 An operational view of information sharing

In this chapter we use some terms commonly used in the military and business sector in order to identify some noteworthy aspects of information sharing.

When discussing information exchange it should be kept in mind that there is a hierarchy of at least 4 classes of "information".

- Data; the bits and bytes
- Information; processed, structured, and or summarised data. E.g. an incident report.
- Knowledge; correlated, analysed information.
- Understanding; knowledge is integrated with previous experience. We become aware of the issues and what is going on, and can extrapolate. We can visualise the situation.

In particular the difference between data and information is of interest, since to be useful the latter requires that the user understand how it is structured and other implicit information such as semantics and terminology. These issues are further explored in the chapter on interoperability.

In order to understand the purpose of various partnerships designed for information change, especially those dealing with real-time or close to real time information it is worthwhile to examine some ways that information may be used. The OODA loop, commonly used in military and business strategy, can be used for context.

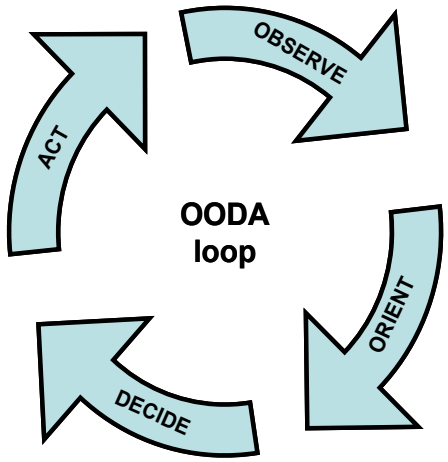

Figure 3. The OODA-loop. Decision making occurs in a recurring cycle of observe-orient-decide-act.

- **OBSERVE**, collect the needed information.
- **ORIENT**, organise, interpret or process the new information. E.g. create a model of the situation based on the collected information. The processing will be affected by previously collected information, your education, culture, previous experience etc.

- **DECIDE**, based on the new understanding, e.g. similarity with previous experiences, evaluate options and make a choice.
- **ACT**, implement the decisions, i.e. give orders, propose legislation etc.

New observations, possibly as a result of the chosen actions, will result in new decisions and so forth in a continuous loop.

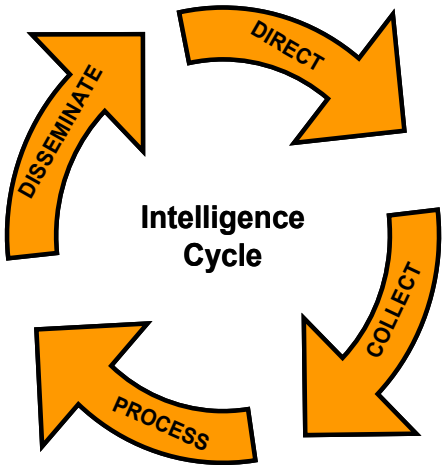

Figure 4 . The Intelligence Cycle.

The Intelligence cycle is in some respects analogous to the OODA loop, and is for the information exchange purpose more pertinent.

- **DIRECT**, decide what category of information that is needed, and on which topics.
- **COLLECT**, using available sources - Internet, partnerships, etc – gather the required information.
- **PROCESS**, structure and evaluate the collected information, e.g. its reliability and relevance. Can you trust the source, is it conflicting with other information? Interpret the information.
- **DISSEMINATE**, provide the information or knowledge (conclusions) to those in need using pertinent means – e-mail, PPPs etc, e.g. warnings of Internet attacks to CERTS, proposals for research policy directions to politicians etc.

The cycles above are applicable for placing information exchange partnerships in context, in particular when the exchange of information has a specific goal, when something it to be produced or achieved, and particularly when time is short, such as in the case of partnerships for crisis management.

One aspect that can be highlighted from the above images is the issue of dissemination. In order for decision makers - whatever their level - to be able to orient themselves about any given situation or topic area, they need to be provided with the appropriate information. Thus partnerships should not only be seen as a means for accessing information, they are also a means for distributing and in some cases also processing information. In order to connect the above 2 cycles to the realities of PPP the following, slightly forced, example is given:

> The first Computer Emergency Response Team (CERT) at Carnegie Mellon University was formed under U.S. Government contract in response to the increase in Internet viruses and worms. Today there are many national CERT/CSIRTs[17] who collaborate by exchanging information on best practises and new threats.

[17] CERT: Resource for National CSIRTs
http://www.cert.org/csirts/national/

When identifying a new threat a CERT is dependent on reports and warnings to reach them, for example from the network of IDS sensors across Europe set up by The European CSIRT Network.[18]

When a new threat or warning has been received by a CERT it must be integrated with other warnings and reports for the purpose of creating an understanding of the nature of the threat, the possible consequences, and which counter measures that may be applicable. Partnerships of relevance to the creation of such a situational awareness are for example:

- Collaboration through information exchange with other national CERT;
- Partnerships for the training of the operators who have to draw the conclusions;
- The use of Data repositories, for example clearing houses, to access supporting information.

2 Soft Aspects

By "soft" aspects we in principle refer to the context the information exchange partnership/network is working within, but excluding the technical aspects such as technical platforms – topics dealt with in the section on "technical aspects". The issues in this section include laws and regulations, trust, and information focused aspects such as quality. Topics not explored here include financing and fund management, since there is no apparent difference between information sharing and other generic partnerships in this respect.

2.1 Legal Commercial and Regulatory Issues

Some semi-recent studies highlight the impact that legal issues may have on partnerships.[19][20] Before initiating a partnership it is important to investigate the legal and regulatory implications. Aside from laws and regulations that affect the choice of financing and organisational form of the partnership, e.g. limited liability corporation or public company, there will also be a host of issues to consider regarding the information exchange itself.

Note that when the information crosses legal jurisdictions, such as European national – and possibly also regional[21] – borders, the number of laws and regulations that need to be investigated by the partnership are multiplied. The legal domiciles of the organisations involved will also be a factor that has to be considered. Some examples of the legal areas that can be involved are given below.

- Administrative law: this will affect which partnerships the public partner can engage in, and how.

[18] The European CSIRT Network. http://www.ecsirt.net/
[19] In 2002, Two workshops were held by a project investigating European "Information Infrastructure Dependability"
DSI Public-Private Cooperation Workshop Report: *Warning and Information Sharing: Technical, Legal and commercial Issues*. http://www.ddsi.org/htdocs/DDSI/Events/Bxl/DDSI_D8A_WIS_WS_Report_WP.pdf
DSI Public-Private Cooperation Workshop Report: *the Public-Private Cooperation approach to Information Infrastructure Dependability*. http://www.ddsi.org/htdocs/DDSI/Stockholm/DDSI_D9A_PPC_WS_Report_WP.pdf
[20] S. D. Personick, C.A. Patterson, Eds. "*Critical Information Infrastructure Protection and the Law*", The National Academies Press. 2003. http://www.nap.edu
[21] E.g. the Flemish parliament has the power to regulate partnerships, see Flemish Public Private Partnership (PPP) Knowledge Centre: Legislative framework. http://www2.vlaanderen.be/pps/english/legislative_eng.html

- Commercial (antitrust law): private companies exchanging information risk violating competition laws, e.g. restraint of trade.
- Data protection laws: e.g. in Sweden there are strict limits on what information that may be shared even within departments of a government authority, let alone between separate Swedish authorities.[22]
- Privacy laws:[23] e.g. partnerships involving the exchange of medical records face strict legal limits.
- Liability laws: e.g. might be relevant if some harm is caused to a 3rd party due to inaccuracies in the information shared by a partner or in the information produced by the partnership, or if a partner shares information about a product or service weakness that if exposed may be used in lawsuits or criminal proceedings against the partner.
- Intellectual property laws: who owns the potentially valuable shared information, and who owns the end-product if the shared information is further processed?
- Criminal law: Some information may be prohibited to transfer across national boundaries, i.e. information classified as "sensitive information" or "restricted technology", e.g. bio-safety information or crypto algorithms.[24] There are may also be legal requirements regarding logging of information exchange and the storage of such logs for access by law enforcement agencies. In some jurisdictions the possession of certain categories of information may itself be a punishable offence, e.g. virus source code.
- Public procurement law: i.e. if the partnership provides a government authority with information, and the government in some way compensates the partnership for this then public procurement laws may become applicable.
- Lawful interception: while this does not seem to be an issue for private networks, the laws differ between countries, are evolving, and could affect the choice of communications equipment.[25]

What laws and regulations that affect the partnership will depend on the partners involved, which political borders the information crosses, and the type of information that is being shared between the partners. After investigating these factors, and if the partnership is still considered to be possible, business practises and processes need to be established to ensure conformity with all applicable laws and regulations. These processes also need to take account any privacy concerns the partners may have as a result of their business practises, i.e. in order to maintain their trust in the partnership.

Of particular interest for the issue of trust are the various national equivalents to the U.S. "Freedom of Information Act", whereby the public is given the legal right to access information held by their government unless the information has been explicitly exempted through security classification or other means. In Sweden the closest equivalent is the Swedish Freedom of the Press Act, where it is stated that "every Swedish subject shall have free access to official documents." What is deemed an official document extends for example also to the correspondence of the Prime Minister.[26]

---

[22] In Sweden the secrecy laws give a government authority the right to deny a request for information from other Swedish government authorities.

[23] The EU Data Protection Directive 95/46/EC establishes a regulatory framework that tries to balance between the protection for the privacy of individuals and the free movement of personal data within the European Union, while the ePrivacy Directive 2002/58/EC provides complementary regulations.

[24] Council Regulation 1334/2000 covers dual-use technology and "intangible transfers of technology" that can take place for example over e-mail or telephone.

[25] Duffy, Jim. *Higher ed fears wiretapping law* Network World , 05/01/2006 http://www.networkworld.com/news/2006/050106-calea.html

[26] Banisar, David. *Freedominfo.org Global Survey of Freedom of Information and Access to Government Record Laws around the world*. May 2004. http://www.freedominfo.org/documents/global_survey2004.pdf

This type of legislation may cause apprehension amongst partners that information shared by them in confidence may be released due to the laws and regulations that other partners are obliged to operate under. In a 2003 report the GAO revealed that:

> *"For example, neither the IT nor the energy or the water ISACs share their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns."*[27]

In short, an important obstacle to overcome when dealing with information exchange is the task of understanding the sometimes multiple and possibly conflicting legal and regulatory frameworks that the partnership will be obliged to operate under. If there is confusion regarding the interpretation of the laws, or contradictions between national laws and jurisdictions this may not only slow down the formation of a partnership, it may also cause reluctance amongst partners to release relevant information.

2.2 Handling of Sensitive Information

When handling sensitive information there are usually at least the following three aspects to consider.

- Information designation
- Processes for safeguarding the information
- Processes for dissemination of information

By designation we mean the process whereby the information is assigned a value on the "sensitivity" scale. A designation usually has a name, e.g. "CONFIDENTIAL", "SECRET" or "For Internal Use Only", and a definition explaining what the designation actually means, e.g. that if leaked the information can lead to significant costs for a company, or endanger international relations.

Processes for safeguarding information can comprise the training and assignment of staff responsible for carrying out designation or re-designation and the processes to be followed for protecting the information, e.g. a very simplified fictitious example of the rules that may apply:

- "COMPANY CONFIDENTIAL" information must not be sent by unencrypted e-mail, copied on photocopiers with an internal hard-disk, and must be kept in a locked drawer when not in use if stored on a portable format;
- "SECRET" information may require that both the company and those employees with access to the information have received a security clearance by the appropriate national police authorities, that printouts be kept in safe-boxes and audited, and that any electronic copies be kept on computer systems or other media galvanically separated from computer systems connected to the Internet.

Processes for dissemination of information include the rules to be followed when a government authority receives a request for information from another government authority or the equivalent of a "Freedom of Information Act" request from a member of the public. The workflow may include examining the risk-factors involved in releasing the information, evaluating the legal grounds for releasing the information versus the legal grounds for protecting the information.

"Facility Security Clearance (FSC)": For information classified as CONFIDENTIAL and above the United Kingdom maintains a "List X" company list of those organisations, mostly from the defence

---

[27] *HOMELAND SECURITY: Information Sharing Responsibilities, Challenges, and Key Management Issues*, May 2003. GAO-03-715T. http://www.gao.gov/new.items/d03715t.pdf

industry, that are authorised to receive information of importance to national security. This may involve amongst other things periodically certified compliance with rules and procedures regarding perimeter protection, computer security, and procedures for the secure handling of classified information.

Each organisation that intends to participate in a partnership where it will be expected to release potentially sensitive information with others will face a problem similar to that faced by governments who have to create and maintain the equivalents of a "List X"; how to ensure that the recipients of the information will handle it at least as securely as the originator. This may involve costly and time consuming investigations of the security arrangements of all the partners, provided that the partners are at all willing to allow such outside investigation of their internal operating procedures.

One issue that was discovered in a 2006 U.S. survey of federal government agencies was that 56 separate designations were being used for sensitive but unclassified information:

> "*For example, one agency uses the Protected Critical Infrastructure Information designation, which has statutorily prescribed criteria for applying, sharing and protecting the information, whereas 13 agencies designate information For Official Use Only, which does not have similarly proscribed criteria. Sometimes agencies used different labels and handling requirements for similar information and, conversely, similar label and handling requirements for very different kinds of information*"[28]

A large part of the surveyed agencies reported difficulties sharing information, and the Department of Homeland Defence reported that on occasion shared sensitive information had been posted on the Internet or in other ways compromised by its partners "*potentially revealing possible vulnerabilities to business competitors*".

Partly as a consequence of this the U.S. is currently implementing the Information Sharing Environment (ISE) which includes:

> "*steps towards standardizing procedures for managing, handling, and disseminating sensitive but unclassified information – information that is generally restricted from public disclosure but not designated as classified national security information – as well as protecting information privacy*."[29]

In May 2008 the "Controlled Unclassified Information Office" (CUIO) within the U.S. National Archives and Records Administration was created, its main responsibilities lies in developing and enforcing the procedures for common designations.[30]

It seems not wholly unreasonable to assume that a similar lack of standardisation in designation and handling of unclassified but sensitive information exists across European national agencies and authorities, as well as a similar lack of standardisation in in-house designations and handling procedures within the private sectors.

---

[28] GAO report. *Information Sharing*, March 2006. GAO-06-385. http://www.gao.gov/new.items/d06385.pdf
[29] GAO report. *Information Sharing Environment*, June 2008. GAO-08-492 http://www.gao.gov/new.items/d08492.pdf
[30] Press Release *Archivist of the United States Establishes "Controlled Unclassified Information Office*, May 22, 2008 http://www.archives.gov/press/press-releases/2008/nr08-107.html

2.3 Quality

"Information sharing is only as valuable as the information shared."[31]

The factors determining the "Quality" or "Validity" of information can amongst other variables for example depend on the category of information, and to which purpose it is to be used. It can typically be affected by the following attributes:

- Timeliness; The value of a discrete information item usually decreases over time, how rapidly this happens depends on the context, e.g. for crisis management or alert networks the time-span can be very short. Being able to receive information while it is still possible to act upon it is thus an important aspect. Conversely, being able to trust the recipient system or recipient partner to receive and act upon the information in time can be of importance to the sender.
- Accuracy; The accuracy of information can be decreased by factors such as, misinterpretation, unreliable sources, obsolescence and deliberate misinformation.
- Relevancy: If the shared information is not of relevance to the receiver, or if it is redundant, i.e. the recipient is already receiving the same or similar information from other sources. This type of lack of coordination can lead to inefficiency and risk overwhelming the recipient.
- Provenance: Where did the information originate, how was it collected/created (using which methodology), how was it verified?

One aspect of quality management is the ownership of data, i.e. with whom the responsibility for quality control and possibly also for updating the data lies. The problems with keeping the information up-to-date increases with distributed systems where information is stored and replicated in multiple locales.

Poor quality Information can lead to loss of trust and to inefficiencies, and may also lead to legal consequences if it directly or indirectly causes harm to a 3rd party. Before putting received information to use it is therefore important to have an estimate of its quality.

2.4 Analysis and Processing

In some cases it is just as important to analyse and process the information as it is to share it. There are two separate aspects to this, one at the sending and one at the receiving end.

1. The organisation sharing the information may, depending on the type of partnership(s) it is involved in, need to perform any one of a number of operations on the information it has available. For example:

- Determining if an information item is of relevance for sharing and if so with which partners.
- If the potential sharing is in response to an external information request, legal and policy issues will need to be examined, e.g. possible negative consequences from sharing the information.
- Legal and policy issues: Are there legal grounds for withholding a specific information item, are there legal grounds mandating the release of the information? Are there internal policies to be followed when deciding whether to release the information?
- Depending on the topic competencies of the recipient organisation(s) and the level of hierarchy at which it wilt be dealt with at the receiving end, the information may need pre-processing/tailoring for it to be useful to the recipient. This is separate from the more generic

[31] *Good Practices: Information Sharing in Complex Emergencies.* United States Institute of Peace. http://www.usip.org/virtualdiplomacy/publications/reports/11.html

issue of interoperability regarding communications equipment, data formats, semantic definitions, terminologies and languages.
- Updating already shared information may be of importance, e.g. if it is provided to a data clearing house, then any changes may need to be monitored to ensure the quality of the data that is provided by the clearing house.

2. The receiving organisation may typically either be an end-user (information consumer), or a way-station on the path to the end-users; such as a data clearing house (information maintainer and provider), or a fusion node or analysis centre (information processing). Some of the issues related to the latter two (clearing house or fusion nodes) are:

- Quality control, e.g. based on reliability of the source and the consistency of the information with related information from other sources.
- Maintenance, i.e. ensure that the information is up to date.
- Standardising, i.e. modifying the information so that it conforms to a common format, be it with regards to terminology, semantics, data format, presentation format.
- Indexing, e.g. applying meta-data for enabling searches.
- Analysis, e.g. data fusion, pattern extraction, data mining.

In some cases analysis may be costly, requiring dedicated visualisation systems and operator training, e.g. for SAR imagery analysis.

The quality of an analysis can be affected by its perceived trustworthiness. Factors that may influence this include potential conflicts of interest, i.e. that the output is biased by the interests of the organisations conducting the analysis. Possible remedies include transparency in the process, use of standardized methodologies, standard terminologies, and standardised sets of evaluation factors.

2.5 Trust

Trust influences information sharing in various manners, means different things depending on context and is correspondingly affected by a number of variables.

2.5.1 What is trust

What do we mean by trust? Here we limit ourselves to three simple and partly interdependent domains; trust in the "system", trust in the partners, and trust in the information.

- **System:** the word "system" is here intended to denote the context surrounding the information exchange. It includes issues such as:
    - Laws and regulations, how they are interpreted and the perceptions they generate, e.g. uncertainties or misinterpretations.
    - Agreements, on confidentiality or equitable sharing, and perceptions of how reliable and long-term they are.
    - The structure of the organisation, e.g. network of peers or hierarchical with roles responsibilities and enforcement; distribution of power amongst the participants.
    - The information sharing technical platform, this includes the perceived information protection offered by the ICT equipment, its reliability and ease of use (e.g. "single sign-on").

- **Partners:** where partners denote both the organisation with which information is being shared, and the individuals representing those organisations. Trust in the latter case is of particular importance in close collaborative partnerships.
    - Partners perceived ability to protect sensitive or confidential information
    - Perception that partners will not use the shared information in ways contrary to the interests of the originator.
    - Conflicts of interests within the partnership
    - Perception that partners will keep confidentiality promises.
    - Perception that partners will reciprocate with information of equal value.

- **Information:** Trust in the information is closely coupled both to partners and system, but some aspects may merit highlight nevertheless.
    - The Quality and Accuracy of the information will influence the degree to which it is possible to act upon the information or use it for further processing.
    - The Methodology used to derive the information will influence the degree to which the quality can be assessed.
    - The original source and, in the case of processed or amalgamated information, chain of sources will influence the degree of trust, e.g. the likelihood that relevant information is accidentally misinterpreted or has been intentionally withheld, that information has been selectively shared in order to produce a false impression, that bias (commercial/political) amongst those performing information processing has led to a skewed information product.

Is trust needed?

This would tend to depend on the type of information exchange that is involved, i.e. how sensitive the information is, and for what purpose the information is being shared. A network where merely best practises are shared may not even require encrypted communications, while collaborative projects using classified information or where partners need to be explicit about their needs and motivations will require a high degree of trust to be effective as they otherwise may hold a mutual fear of exploitation by the other part. Generally speaking, the closer the partnership has to be, i.e. the further down a partnership can be placed in the list provided in "Table 1. *Example of levels of interaction*" the greater the importance of trust will be.

What are the effects of trust on information sharing?

Low or absent trust will impede not only the sharing of sensitive information, but also the use to which any shared information can be put to by the recipient.

How is trust to be established?

Trust often takes time to develop and is then the result of a history of successful interactions between individuals or organisations. The generation of trust can involve tools such as contracts, reputation models, regular – preferably face-to-face – interactions between individuals and so forth.

Note that trust is only a part of the issue; the partners also need to have an incentive for participating and contributing e.g. visible benefits such as something to be gained, be it in terms of reputation, ideological or financial gain.

2.5.2 Concerns

We provide below a listing of trust related concerns amongst the public and private sectors found during the literature review.

- Inadvertent exposure:
  - Exposure of corporate secrets
  - Weaknesses and vulnerabilities known to the general public can lead to consumer confidence being eroded
  - Loss of control over the information, over how it is used and with whom it may be further shared.
- Use of shared information
  - Revealing weaknesses and vulnerabilities to a public partner may lead to additional regulations
  - Revealing weaknesses and vulnerabilities to a private partner may lead to commercial exploitation
- Unknowns
  - Could lead to unexpected legal consequences, e.g. from liability or anti-trust laws.
  - Recipients of the information may lack the required expertise to properly understand the information and draw the "right" conclusions.
- Fairness
  - In some cases creation of information involves a direct cost, or the information has an inherent value for other reasons. If there is a perception that the partners do not reciprocate with information of equal value, i.e. if there are "free loaders", there might be decreased incentive to participate.
- Confidence
  - Public partners might not be seen as reliable on promises of long term confidentiality. E.g. events such as 9/11 may cause policy changes.
  - Lack of confidence in the security aspects of equipment used by the network to store and transmit the sensitive information.
- Control
  - By sharing information with certain partners, other partners may in turn stop sharing with you due to concerns about the further spread of their data. (this is of particular concern when dealing with international sharing of classified information, but is to varying degrees relevant in other cases too).
  - In some cases the issue of government inter agency competition has been raised, especially where the missions of the agencies overlap there may be a perceived loss of prestige and control from sharing information.
  - Information superiority is one of the tools needed for gaining influence, thus sharing information may lead to decreased leverage.

3 Technical Aspects

The issues that receive a cursory investigation in this chapter range from infrastructure issues to the role of semantics. The purpose is not to do an in-depth investigation of how to build secure and interoperable communications systems, but rather to highlight some issues relevant to secure information exchange partnerships.

3.1 Interoperability

Interoperability means the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge.[32]

Definitions of interoperability vary, the example given above was chosen as most appropriate since it is used by Interoperable Delivery of European eGovernment Services (IDABC).

When organisations with different backgrounds, such as business areas or cultures, wish to interact then the question of interoperability comes into play. It is necessary that the technical equipment possessed by the two organisations is made compatible enough to share information, or that they acquire common equipment. It is also a precondition that the information itself can fit in the recipient's business processes.

In this chapter we try to provide a sample of possible interoperability issues related to information exchange.

Semantics

When exchanging information much of the exchange is implicit, i.e. it is useful only if the recipient possesses the necessary background information necessary to interpret it. In a very simplified form, this is what communication standards are all about.

To exemplify with a fictitious message:

"*COM/2005/0597*[33] *requires that you use SQL*". *Date: 2007:03:03:12:00 Name: Mihai Simon*

The first standard that is obvious here is the spoken language, i.e. "U.S. English". The second notable aspect is the use of acronyms and designations. The reader is expected to know that it is a specific Communication from the European Commission, and it is also expected that "SQL" be interpreted as "Structured Query Language" and that it refers to a database computer language designed for the retrieval and management of data in relational database management systems. Other notable aspects are the inclusion of "Date" and "Name". Unless we know the semantic significance of "Date" and "Name" in this context then that particular information becomes useless. Is it the "date" the information was first created, date it was sent, or date it was received? Is the "name" the name of the sender or recipient? Does the family name come first or last?

Sometimes organisations, even departments within the same government authority, will tend to develop their own nomenclature, possibly using similar designations but assigning differing meaning to them.

---

[32] Definition used by the European Interoperability Framework and IDABC. http://ec.europa.eu/idabc/en/chapter/5883

[33] Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs

At the highest levels we have languages, terminologies and semantics that need to be common for both sender and receiver (or clearly translated) for the information exchange to be meaningful. We also have the issue of interoperable business practises and formats. If two organisations wish to collaborate on measuring economic progress in a country, but one bases its statistics on GDP, while the other works on GNP, then simply pooling the databases of the two organisations will do neither any good, i.e. the information must first be adapted to the recipients' ways of working, or the ways of working need to be streamlined.

Standards

Closer to the application layer, the hardware-boxes that perform the actual information sharing, we have a separate set of interoperability issues. The layers in the partly obsolete OSI model are presented in Table 2 below to show the various layers where common standards may be needed for an information exchange to be possible.

OSI Model			
	Data Unit	**Layer**	**Function**
Host Layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment/Datagram	4. Transport	End to end connections and reliability
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

Table 2. Open Systems Interconnection Basic Reference Model (OSI Model)[34]

There are a number of issues that may come into play here. Looking at an area revolving around the physical layer we for example find the issue of radio spectrum allocation and waveforms. Rescue services seeking interoperability, i.e. if police and fire-fighters at an accident scene wish to communicate they may, depending on communications equipment procurement policies, be forced to resort to using their personal cellular phones, this since the two organisations may be using different radio communication technologies.[35]

Another issue that may come into play is "proprietary systems", i.e. if a vendor has supplied a full system (including databases, presentation and communications equipment) then it is unlikely that it will be compatible with the systems of competitors unless it specifically was designed to follow open standards. Sharing information in such cases will involve the possibly costly design and incorporation of "bridges" that translate the information between the systems. Proprietary systems might have some security advantages thanks to this though.

Government departments – and others – wishing to easily be able to share their data with other authorities need to consider which standards they implement, from the lowest to the highest levels,

[34] *Open Systems Interconnection Basic Reference Model*. http://en.wikipedia.org/wiki/OSI_Model
[35] One attempt to alleviate such issues is the research into Software Defined Radio

from how they store their data to how it is presented to how it is transmitted. Unfortunately there are many standards out there, and choosing the right ones when building the system can be difficult without an overarching policy that points all interested in sharing to a single set of architectural components, standards and protocols.

3.2 Security

In this chapter we describe some of the technical aspects related to the security of transmitted information, i.e. as it relates to the technical platform. It should be noted that technology is only part of the issue, physical security such as perimeter guards and employee background investigations, training, and security-policies and guidelines play an equally important and complementary role.

What level of information assurance that will be needed will depend on the type of partnership, the threat to the information and naturally also economic considerations.

What platforms will security considerations be applied to?

This will depend on the needed level of information assurance, and which platforms the network needs. A rough example of which categories of platforms that may be used is given by the U.S. Information Sharing and Analysis Centers (ISACS):

> *"a secure database, analytic tools, and information gathering and distribution facilities designed to allow authorized participants to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions."*[36]

Thus we need

- Information storage. (Servers and Databases)
- Analysis tools (Often ordinary computers running specialised software)
- Communications (e.g. VPN over the Internet)

When discussing security in connection to computer system the following aspects are usually mentioned:

- Confidentiality
  Keeping information secret. Avoiding unauthorised disclosure of information.
- Integrity
  No unauthorised alteration of the information, e.g. it should not be possible to insert a false message.
- Authentication
  Verification that a user or system is who they claim to be, e.g. by password.
- Availability
  That the information can be accessed by authorised actors when needed Denial of Service attacks impact on availability
- Non-repudiation.
  Activities can not falsely be denied afterwards, e.g. the transmission or reception of a message.
- Access Control
  There is usually a complicated situation regarding which user has access to what information. Access control ensures that users only access information they are authorised to access.
- Accountability

[36] WW-ISAC Frequently Asked Questions http://www.wwisac.com/faqs/

System audits with regards to actions affecting security should be possible

When building a system from scratch for a private or public actor for its internal needs it is not too difficult to ensure that all the parts are compliant with the aspects listed above, there are numerous standards[37] and policies to use, e.g. to avoid using wireless communications. The basic building blocks such as PKI and Certificates are widely available. For extra sensitive information standards such as Emissions Security regulations (Tempest) may come into play, where it has to be ensured that spurious electromagnetic emissions can not be detected from a distance e.g. be used to reconstruct the information being presented on a computer screen.

The issue becomes somewhat more difficult when the time comes to connect separate organisations in an information exchange network. To seamlessly, and more importantly securely, connect the systems of separate organisations is often not possible as it likely would require a common security infrastructure.[38] The solution will often be to on top of existing equipment add a completely new system what will be common to all partners. In some cases where the information sharing does not consist of too sensitive information and is simple in form or shape it will often suffice to simply add a new software system on top of existing applications.[39] For more sensitive information there may be a need also for new hardware shared between all the partners and running in parallel to the systems used for the partners' normal business practises.

3.3 Applications and Mobility

In this last chapter we briefly mention some mixed issues relating to information exchange, topics perhaps not that important but nevertheless included here to try to provide a fuller picture.

Depending on context the image that is conjured up when talking about "information exchange" will vary significantly.

If it is the government that needs access to information, e.g. about a public infrastructure, that is stored in a database owned by a private company that manages the infrastructure then we might see a deep technical integration between the two organisations and large amounts of data being transferred, possibly without any manual intervention at the private part.

If it instead is a question of a network such as a CERT then there will be a wide variety of ad-hoc information exchanges taking place, using phone, video-conferences, e-mails and file-sharing. There will also be both secured and open web-portals used for distribution of alerts and also for general public awareness raising.

A close knit security expert network, with no particular task other than to provide each other with instant support and advice might rely exclusively on encrypted e-mail and encrypted cellular-phone[40] conversations (and file sharing over the same). This leads to an emerging topic, mobile collaboration[41], where those sharing information are not locked to a specific workplace for doing their job.

---

[37] See for example ISO/IEC 17799:2005 *Information technology - Security techniques - Code of practice for information security management*

[38] Although some proof of concept experiments that might help public partners interconnect are ongoing using Service Oriented Architecture, see for example http://sweden-nato-nec.nc3a.nato.int/

[39] See for example PGP for secure e-mail or Microsoft Groove for more advanced file sharing.

[40] The Sectra Tiger system is for example approved for use with the NATO SECRET and the European Union SECRET UE classifications.

[41] See for example Lyn Bartram, Michael Blackstock *Designing Portable Collaborative Networks* ACM Queue vol. 1, no. 3 - May 2003. http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=35

This type of collaboration, flexible instead of centralised, presents interesting technical challenges, security and otherwise.

When working outside the premises of the home organisation connectivity will be variable both in bandwidth and in its presence and will of course risk being compromised security wise, presenting a threat not only to the exchanged information but to the terminal itself.

This will also in the cases where the collaboration involves more than simple message exchanges necessitate local data replication of sensitive information, with associated security and consistency issues. Other possible issues are the remote authentication both of user and terminal, the need for dynamic presentation adaption (adapted to variable bandwidth and changes in presentation equipment, e.g. switching from notebook to cellular phone), and dynamic session maintenance when switching access networks, e.g. from a WLAN to UMTS.

We can end this report with one last reflection: “technical” and “soft” issues are in reality inseparable, we may have separated them in this report for convenience but in reality they continuously impact on and drive the evolution of each other. New tools, such as those tools that support the interconnection of cross sector and cross-nation organisations, the sharing and processing of vast amounts of data, and those tools now enabling individuals to collaborate also when on the move will impact on business models, processes, legal and regulatory frameworks, and the ways partnerships such as those we’ve been reflecting on in this paper are organised, and all of these factors will in turn help drive the technical development further. In short; new opportunities will continuously appear, as will new obstacles to be overcome.

4 Conclusions

When planning a partnership or network there will be a series of context dependent questions that need to be answered. These questions may include; goals, projected membership, information categories.

Of particular interest for information exchange is to be completely clear on legal issues and the issues of trust. If a partnership/network is not carefully engineered to foster trust amongst the participants (and in its output), then whatever information that is shared will, just as the partnership itself, be of limited value.

To ensure a workable partnership, and also to promote trust, there are a number of obstacles to overcome. Some of these obstacles are technical in nature, such as ensuring that the security of the chosen technical platforms is adequate for its needs, and that common terminologies are applied to the shared information. Other obstacles are less tangible but just as important and include topics such as reciprocity and each partner’s internal procedures for handling sensitive information.

European Commission

EUR 23693 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Reflections on Networking & Information Exchange: Dealing with Sensitive Data amongst Public and Private Actors
Author(s): SODERLIND Gustav
Luxembourg: Office for Official Publications of the European Communities
2008 – 30 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593

Abstract
In this report we reflect upon possible issues that need to be considered before embarking on creating a partnership or network where a main objective is the exchange of sensitive information.

To this end, we try to provide a brief overview of types of information exchange partnerships, and suggest various aspects that those embarking on a partnership should first review.

The second part of this report is devoted to highlighting operational ("soft") issues that need to be kept in mind, such as national legal and regulatory frameworks and trust issues. In the third part we sketch some technical aspects that may have an impact.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

Publications Office
Publications.eu.int