



Sharing Cyber Security Information

Good Practice Stemming from the Dutch Public-Private-
Participation Approach

March 2015

Eric Luijff and Allard Kernkamp



The preparation and publication of this document has been funded with the support of the Dutch Ministry of Security and Justice as part of their Vraaggestuurd Programma Maatschappelijke Veiligheid (Demand-driven Public Security and Safety Research & Development Program), theme Cyber Security. This publication reflects the views only of the authors; the Ministry cannot be held responsible for any use which may be made of the information contained therein.



Foreword



When discussing cyber security in an international context, information sharing is one of the most heard suggested solutions for increasing cyber resilience. However, there is a world, if not a universe, between the concept of information sharing and the practice of doing it. When partners visit the Netherlands, and specifically our National Cyber Security Centre, they are always very interested in the manner in which we have taken this subject into practical use. Because of this widespread interest we have asked TNO to write this booklet which contains the Dutch experiences, knowledge and lessons learned concerning information sharing. I am confident that the contents will provide useful building blocks bring anyone interested in setting up information sharing.

Wilma van Dijk
Director Cyber Security
Ministry of Security and Justice





Summary

The failure of a national critical infrastructure may seriously impact the health and well-being of citizens, the economy, the environment, and the functioning of the government. Moreover, critical infrastructures increasingly depend on information and communication technologies (ICT) or, in short, cyber. Cyber security and resilience are therefore seen as increasingly important governance topics and major challenges **for today's societies, as the threat landscape is continuously changing. Sharing cyber** security related information between organisations – in a critical sector, cross-sector, nationally and internationally – is widely perceived as an effective measure in support of managing the cyber security challenges of organisations. Information sharing, however, is not an easy topic. It comes with many facets. For example, information sharing spans strategic, tactical, operational and technical levels; spans all phases of the cyber incident response cycle (proactive, pre-emption, prevention, preparation, incident response, recovery, aftercare/ follow up); is highly dynamic; crosses the boundary of public and private domains; and concerns sensitive information which can be potentially harmful for one organisation on the one hand, while being very useful to others. This Good Practice on information sharing discusses many of these facets. Its aim is to assist you as public and private policy-makers, middle management, researchers, and cyber security practitioners, and to steer you away from pitfalls. Reflect on the earlier lessons identified to find your own effective and efficient arrangements for information sharing which fit your specific situation.

On behalf of the authors,

Eric Luijff



Contents

Foreword	3
Summary	5
1 Introduction	9
1.1 The Need for Sharing Cyber Security Relevant Information	9
1.2 Purpose of Information Sharing	9
1.3 The Audience	10
1.4 Purposes of these Good Practices	10
1.5 How to use this guide	11
2 Information Sharing: The Building Blocks	15
2.1  Information Sharing: Speculate to Accumulate	15
2.2  Embed at the Top	16
2.3  Building Trust Takes Time	17
2.4  Mandated Sharing: A Barrier to Reaching Heaven	19
2.5  Noblesse Oblige: No Free Ride	19
2.6  The Spiral Boost	20
2.7  Keep the Fly-Wheel in Motion	21
2.8  Fit to Your Position	21
2.9  Actionable Information for the Right Level and Responsibility	23
2.10  Scoping is Key to Success	24
2.11  Secure, Trusted and Controlled	25
2.12  Sharing is Caring, but the Devil's in the Details	26
2.13  One Size does not Fit All	27
2.14  Avoid Show Stoppers: the Legal Perspective	32



2.15	 Incentives for and Culture of Sharing	36
2.16	 Procedural and Technical Aspects of Handling Sensitive Information	37
2.17	 Information Sharing Standards	39
3	Analysis of Good Practice Use Cases	41
3.1	Approach of the Analysis	41
3.2	Dutch Information Sharing Use Cases	41
3.3	International Information Sharing Communities	43
3.4	Analysis of the Use Cases	45
4	Future Outlook and Challenges	51
4.1	And the next step is	51
4.2	What are the challenges to achieve this?	52
	References	54
	List of Abbreviations	60
	Appendix A: Definitions used in the use case studies	62
	Appendix B: Dutch national cyber security activities	64





1 Introduction

1.1 The Need for Sharing Cyber Security Relevant Information

Our society and its citizens depend on the undisturbed functioning of infrastructures, their products and services. Nations have identified critical infrastructure, which means that the failure of such an infrastructure may seriously impact the health and well-being of citizens, the economy, the environment, and the functioning of the government. Examples of critical infrastructures are energy, telecommunications/ICT, transport, drinking water, financial services, and administration. Critical infrastructures increasingly depend on information and communication technologies (ICT) or, in short, cyber. Cyber security and resilience of critical services and critical service chains are therefore seen as increasingly important governance topics¹ and **major challenges for today's societies** [26].

Timely and speedy sharing of cyber security related information between organisations – in a critical sector, cross-sector, nationally and internationally – is widely perceived as an effective measure to address the cyber security challenges of organisations. Information sharing is an effective approach in support of managing the collaborative cyber risk in a domain where the threat landscape is continuously changing.

1.2 Purpose of Information Sharing

The purpose of sharing cyber security related information is, in the end, to reduce uncertainty with regards to the performance and business continuity of an individual organisation, a whole critical sector, and/or service chains spanning multiple organisations. The performance includes the image and reputation. For many, (see for instance [2] and [45]), it is abundantly clear that no organisation can address the full spectrum of its cyber security and resilience on its own, as organisations are increasingly globally interconnected and exposed to the same global cyber security threats. Collaboration with partners across organisational, sectoral, and national boundaries, and from small and medium enterprises up to multinationals and governments is therefore required in order to counter cyber security threats which may negatively impact the organisation and its services.

¹ See Appendix B for a short overview of the Dutch Cyber Security and governance activities.



Information sharing may create a collaborative insight in cyber security related threats and risk, and in prospects for mitigating actions [15]. Information sharing builds on a symbiotic relationship of organisations which have developed and sustain a collaborative trusted environment to share security-relevant information.

The purpose of these Good Practices on information sharing is to assist you to choose your own approach in information sharing of cyber security-related information while steering you away from possible pitfalls. This guide provides methods, building blocks, opportunities, and threats related to the sharing of cyber security-related information. This guide does not provide you with simple solutions, but good practice building blocks and pointers to literature which enable you to operate and interact in a hyperconnected world where cyber security is one of the managed factors that you, your organisation, and society deal with every day.

“Information sharing is a mindset, not a tick box mandated by an ISO or other **standard.**”

Anonymous ISAC member

1.3 The Audience

The intended audience of this Good Practice on information sharing comprises amongst others:

- the broad spectrum of middle management of public and private critical infrastructure operators involved in cyber security and resilience,
- government policy-makers, legal advisors, and regulators,
- officials of government agencies involved in cyber security,
- tactical level cyber security practitioners, and
- scientists and consultants in the field of cyber security and resilience.

1.4 Purposes of these Good Practices

“Information sharing” is a notion which is a source of confusion. Information sharing may have quite different meanings to people and organisations. Does one look at information sharing at either the strategic/policy, tactical, operational, or deep technical level? In which phases of the cyber incident management cycle (proactive, prevention, preparation, incident response, recovery, aftercare/ follow up) is one interested? Are we looking towards fully automated information exchange 24 hours per day, seven days per week, or just a telephone call? Are we looking at the business side of multi-organisation service chains, or at the technical



domain of system and network components? This guide assists you to answer these questions and proposes the key factors in considering what kind of information sharing may be effective in the right circumstances.

This guide aims to provide an insight into what we would now do differently if we had to start information sharing all over again, while taking into account the lessons learned by many organisations who put information sharing into practice. It also describes what the authors think about how information sharing can be brought to the next level. This guide aims to assist you to avoid the pitfalls and mistakes in information sharing identified by others, and to become a valued member of the (inter)national information sharing community. The earlier you can effectively and efficiently share cyber security-related information, not only will you and your organisation benefit, everyone benefits!

1.5 How to use this guide

By means of a brainstorm, the authors have identified more than ten key topics and seventy subtopics concerning information sharing. This was certainly not complete. It will be obvious that we had to cut back on the number of subtopics when developing this guide. In the next sections, we have laid out the set of key elements which we consider to be of primary importance to you and your organisation in order to effectively and efficiently share cyber security information with other people and organisations.

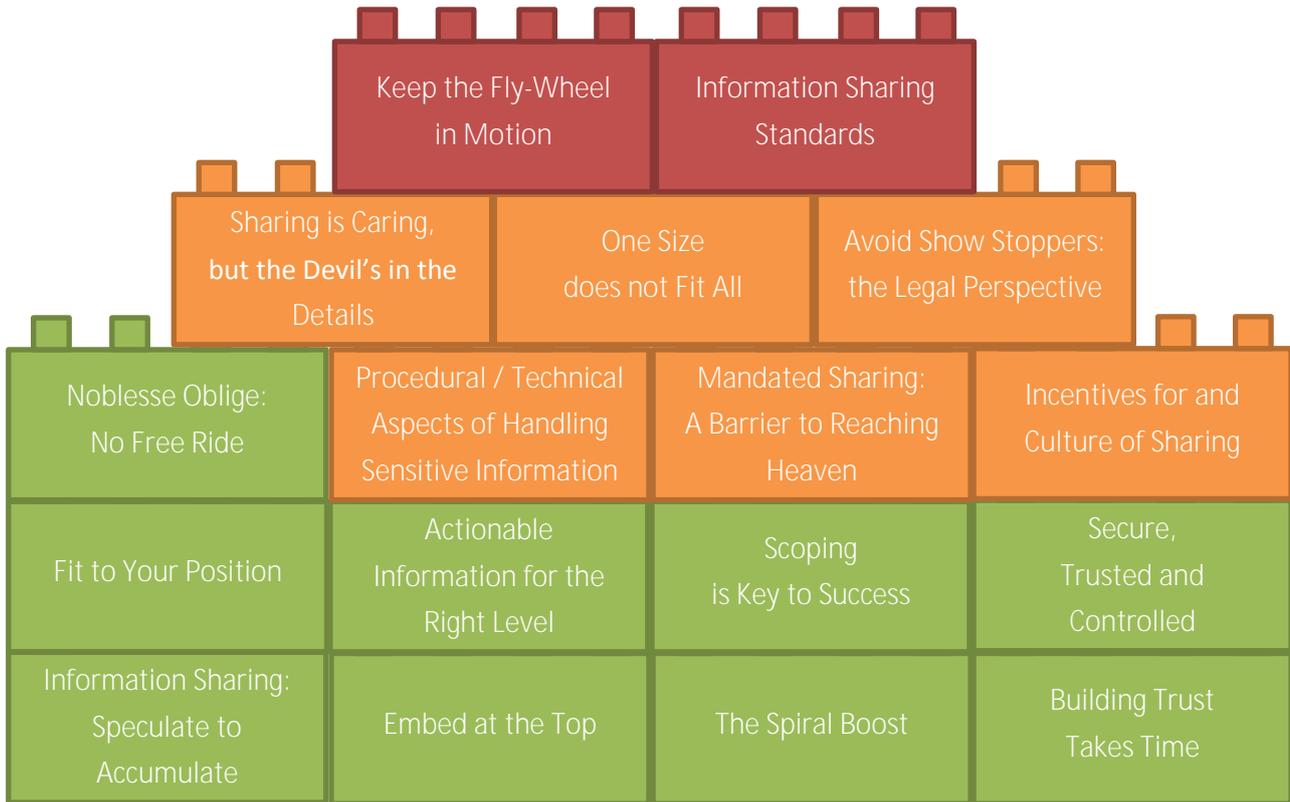
You can read this guide from start to end. Another way is to use the quick-access tables below. They provide immediate access in the right order to high-priority elements you need to understand and put into practice in order to start (**B** Beginner), improve (**A** Advanced), or excel (**E** Expert) your information sharing community. Last but not least, you can pick specific elements of interest using the list of elements with experience-level indicators which you will find in the table of contents on page 5.

Quick-access tables

Three different experience levels of users of these Good Practice are distinguished:

- **B** Beginner: I want to start an information sharing community. Where to start? Dos and don'ts?
- **A** Advanced user: I am already involved in information sharing. What can I (we) learn in order to improve?
- **E** Expert: I have been involved in information sharing for a long-time. How can I/we tweak the information sharing community to make the sharing of cyber security related information even more efficient and effective?

Beginner



Advanced user



Expert

	Keep the Fly-Wheel in Motion	Mandated Sharing: A Barrier to Reaching Heaven	Information Sharing Standards	
Secure, Trusted and Controlled	Procedural / Technical Aspects of Handling Sensitive Information	Noblesse Oblige: No Free Ride	Incentives for and Culture of Sharing	
Sharing is Caring, but the Devil's in the Details	Avoid Show Stoppers: the Legal Perspective	One Size does not Fit All	Scoping is Key to Success	
Embed at the Top	The Spiral Boost	Fit to Your Position	Actionable Information for the Right Level and Responsibility	



2 Information Sharing: The Building Blocks

Following the purpose of information sharing as stated in section 1.2, this chapter will explain some practical insights and challenges for information sharing. The good practice building blocks below stem from a decade of experience in sharing cyber security related information, both in The Netherlands and abroad. But first follow a few considerations on a selection of information sharing theories.

2.1 Information Sharing: Speculate to Accumulate

Information sharing contributes to a common understanding of threats, risk factors and measures. For most organisations, information sharing is a cost/benefit dilemma as a leakage of the often very sensitive cyber security related information may harm the organisation.

Information sharing improves the quality of risk management, incident response, and recovery management across the set of participating critical infrastructure operators, government agencies, and other organisations involved in an information sharing arrangement. Therefore, information sharing may raise the level of cyber security and resilience of critical infrastructure(s) as a whole. Sharing information with government agencies improves the interpretation of weak signals, the collaborative intelligence position, the situational awareness (see the big picture) position of crisis management, and the collaborative addressing of a clear and present cyber danger and risk.

The phrase: ‘need to know’ versus the ‘obligation to share’ embodies a paradigm shift in the last years that drives to a higher level of collaborative maturity in information sharing. Most organisations see information about incidents that have happened within their organisation as something that needs to have a tight lid kept on it. If information about a serious cyber incident hits the media, it could harm the image and reputation of the organisations involved, and be a cause for liability [16]. The result could lead to a drop in value at the stock exchange or be the start of a class action lawsuit. As cyber security has become a hot topic in the media during the last few years, this fear of exposure is understandable. However, not communicating transparently about cyber security incidents (in a timely fashion) and under control, has cost organisations in the end more than was foreseen.

The decision to share information is for an organisation almost a **prisoner's dilemma known from game theory [68]** or can **be summed up as 'speculate to accumulate'**. If information sharing is merely a one-way channel, the supplying organisation only indirectly gains as the society as a whole becomes more secure. When two organisations refrain from

Beliefs necessary for sharing cyber security information:

1. *I know that my information is important and urgent*
2. *I know that what I share will help others*
3. *I know I am trusted by my organisation*
4. *I know how to get the information to the right people*
5. *I know I can control what happens with what I share*
6. *I know they will all act with my interests at heart*
7. *I know others will reciprocate*

Mandy Messenger [67]

sharing, they are both on their own. The opportunities for receiving timely and actionable information are few, and the sector and society suffer most. However, when two organisations mutually share information, both organisations gain and may be better protected and more resilient. Organisations will have a much wider situational awareness and can see the big picture better when sharing information than when keeping the information to themselves. The total gained value exceeds the sum of the values of each individual piece of information, a win-win situation, or 1 plus 1 is 3. The more organisations share reliable and high-value information, the more value is added. Sharing one piece of information in a group with k members, one stands to receive k-1 pieces of information in return. That is a very high-yielding investment!

Received information can be put into perspective, and a common operational picture about the cyber threats, incidents and or cyber risk can be built. In the end, the sector and society gain most as the organisations involved create a synergetic relation. Scientifically, the economic gain of information sharing has been researched using a detailed mathematical model that can be found in [59]. **The "Why would I tell you?" study [67]** provides an excellent insight into the socio-psychology of information sharing between organisations.

2.2 Embed at the Top

Preceding any cyber security relevant information sharing activities, the top management of the organisation needs to have a clear view of the objectives of these activities and how it is beneficial to the business objectives of the organisation such as protecting shareholder interests ([30], [31], [41], [42]). Cyber security is not an ICT-department problem but a business issue of the board room.



The lack of earlier top management endorsement has led to the organisational halt of long-term bottom-up information sharing activities. However, if information sharing is not part of the culture of an organisation, when and how is a CEO expected to be informed in a timely way about their cyber security risk? On the other hand, when cyber security and the culture of sharing is a standard item on the boardroom agenda, the security professionals of the organisation need to provide the proper type of information that supports well-balanced decisions. Moreover, stakeholders and shareholders may ask for transparency of the organisation with respect to the number of serious cyber incidents, data protection breaches, and the overall cyber risk [66]. Just as financial and business risk audits provide assurance to the board room, cyber security related issues need to be part of the permanent risk management cycle of an organisation ([30], [31], [42]).

The motto ‘Leading by doing’ gains weight in board rooms regarding the cyber security and resilience topic. Sharing cyber security-related information at the board room level across organisations is stimulated by the World Economic Forum (WEF) [30] [31]. Likewise, the European NIS Platform [21] promotes collaborative leadership and coordination of multiple stakeholder interests across value-chains [16]. Organisations can obtain an accurate information position by enriching their intelligence with what is provided by peer organisations on cyber security issues, un-commercialised and even verified by public security sector bodies if possible.

However, in their drive to create sharing communities, public authorities sometimes make the mistake of thinking that private companies are anxiously waiting for them. Just sending a letter to the CEO or a director may then land on stony ground. Figuring out first who is the right person at the right intended level of authority (see section 2.8 “Fit to Your Position”) **in an organisation being responsible for cyber security helps** to find a trusted intermediary who can introduce you. That opens doors and is the right way to establish trust and to start an effective collaboration.

2.3 Building Trust Takes Time

Trust is naturally attributable to relationships between social actors, both individuals and groups (social systems). **Trust between individuals and within groups can’t be established instantly; it needs to grow over time.** Currently, there is an increasing number of ways to establish trust, for example: the classic person to person building trust over time, through introduction by a trusted third party, or, the more recent networks of trust [62] and reputation-based trust anonymously established by voting (like web shop reputation) [76]. Background information on establishing trust in information exchanges can be found in Annex B of [32].



Experience has shown that it may take a few years of building trust before really valuable information is shared amongst a relatively small set of people and organisations with a similar background but who are new to each other, e.g. in a new Information Sharing and Analysis Centre (ISAC)² or Information Sharing and Analysis Organisation (ISAO). Several successful Information Exchanges, e.g. [40], stress that starting small and focussed will help to establish the required level of trust sooner. Moreover, there must be continuity in the people attending Information Exchange meetings. The participants should be appointed at a personal level with enough mandate and responsibility in their own environment. Generally, no substitutes are allowed. Reference [67] outlines these aspects in great detail.

Jointly starting a focussed project on a new area that touches all organisations (e.g. how to secure process control systems within the critical sector) reduces the time to build trust significantly. Within a social system like the Dutch ISAC structure (see section 3.2.4), trust in the other participants develops gradually by creating value through sharing of **cyber security incidents, 'war stories', good practices, threat information and the like**. Trust, in the end, correlates to the expectation that the other party acts in a consistent and repeatable way that minimises harm and maximises protection [60].

Experience has proven that the social aspect is very important to stimulate the mutual understanding and the building of trust, especially if it comes to international information sharing communities (for instance joint lunches, dinners or some drinks after the meeting). Trust cannot be commanded, it builds upon interpersonal and inter-organisational experiences. Social events are beneficial to that.

Trust is also precious. "Trust comes on foot, but leaves on horseback" is a Dutch saying. Sharing is the carrot in collaboration. However, one should establish a stick as well: serious consequences linked to acts that break established trust. An example is exclusion from future information sharing meetings.

One should not look **only to external trust building: building trust within one's own organisation and empowering people** should not be forgotten. Remove red tape and trust your professionals at the operations level to share, within pre-set boundaries, cyber security related information with public authorities and other organisations.

² The Dutch ISAC model had its origin in the UK's Information Exchange model which was derived from the original US Network Security Information Exchange (NSIE).

2.4 Mandated Sharing: A Barrier to Reaching Heaven

Most examples of successful information sharing happen on a voluntary basis built on trust. However, mandatory arrangements exist which, by law or regulation, require certain information on risk assessments and incidents to be shared with a government agency or regulator. Although authorities often call such an arrangement ‘information sharing’, it is in fact one-way reporting. Examples are the obligatory data breach notification reporting regarding large disturbances to public communications networks, and risk to personal data, based on the national implementation of the EU telecommunications package Article 13a of [22] and the European Directive on privacy and electronic communications Article 4 [24].

The hierarchical difference of the organisations in such a mandated arrangement and the one-directional approach does not generate two-way trust [60]. Therefore, it is often hard to guarantee the quality of the exchanged information and the promptness of the information provision. The focus in a mandated arrangement may then shift to minimum compliance with the regulatory requirements. Or at the one end of the spectrum, be over-compliant by ‘spamming’ the recipient with many megabytes of low or no-value incident information. The common goals of information sharing on a voluntary basis may be far away.

“Trust comes on foot, but leaves on horseback”

Johan Thorbecke, the Dutch politician who wrote the first Netherlands Constitution in 1848

Successful mandatory approaches therefore emphasise that a key to the success of their scheme is still to build trust that proper security measures have been taken (e.g. with respect to privacy protection (see for example [36])), or that a spirit of voluntary co-operation exists [20]. Moreover, even when the mandated information flow is predominantly one-way (e.g. the mandated sharing of information about unusual electronic transactions), the recipient should do their utmost to create a feedback loop that makes clear the importance of the (mandatory) shared information for follow-up activities. The perception that information is ending in a bit-bucket is de-motivating for promptness and the quality of the mandatory shared information.

2.5 Noblesse Oblige: No Free Ride

To build trust in the group and with the individual professionals, you need to keep investing in the creation of value for others by sharing good information. This can be done by regular encounters, be it virtual or physical meetings. Experience has shown that trust is best built-up in small sized face-to-face meetings.



Of course what is considered as good information can only be judged by the others in the group. This is also a process that will take time to get used to the way of working in a collaborative environment. What is expected from my organisation and what do I expect from others? [67]

Information sharing is a two-way, reciprocal process. If you do not contribute something of equal value to the information you receive, the others will stop sharing their information in your presence and you will be required to leave the group. There is no free ride!

Moreover, in any information **sharing community one has to ‘practice what you preach’**. You need to find the right information in your organisation to assess what information is valuable for both your own organisation and for others. Last, but not least, in an information sharing community common actions may be identified that need to be followed up or investigated. Such burden-sharing requires spending time on actions that will benefit your organisation in the long term. Therefore, a formal or informal management buy-in on time spent in information sharing communities is usually a good thing to arrange. You also are expected to implement collaboratively identified measures that need to be taken to protect the information sharing community as a whole.

2.6 The Spiral Boost

Putting some **information of value on the sharing table will increase the other recipients’ level of trust in your organisation**. The increased trust allows the other organisations to put some valuable information for you on the sharing table increasing their trustworthiness to you. You will reach a point where you will feel comfortable enough to put more and more sensitive information on the table, again and again. Slowly, but gradually, the level of mutual trust and the value of the shared information spirals to increasingly higher levels. Note, however, that actions that introduce some form of distrust in each other (e.g. real or perceived breach of confidentiality) cause a fast spiralling movement in the opposite direction.

To start the spiral, the common objectives of the information sharing community need to be clear. Spending too much time on formal agreements is not recommended, unless the community is large in size. Just some agreement on how to handle sensitive information, e.g., by using the Traffic Light Protocol (2.16.1) or Chatham House rule (2.16.2), may be sufficient to start the flywheel. Later, when the community is extended and need arises, the rules can be codified. A (Cyber) Information Sharing Agreement ((C)ISA) can be formed, for example. Before doing so, note the general perception that when lawyers arrive, trust is gone. Legal agreements will focus on the risk and penalties, not on the positive gains of trust-based sharing.



2.7 Keep the Fly-Wheel in Motion

Starting collaboration and information sharing requires energy. Collaboration does not come for free. A good practice is to make use of existing initiatives, and energy which is already moving in the right direction [2]. Continuous attention is required as cyberspace and its use continuously change. Is the right type and level of sharing of cyber security related information addressed? Are weak signals and new threats properly covered? How could it be even more effective and efficient? Is it time to collaboratively start a new project on cyber security sharing experiences, possible solutions and a common (cross)-sector approach, for instance on a new challenge such as cloud computing? Energetic engagement by each of the participating organisations in sharing the right type and level of information will keep the fly-wheel in motion with continuously increasing added-value.

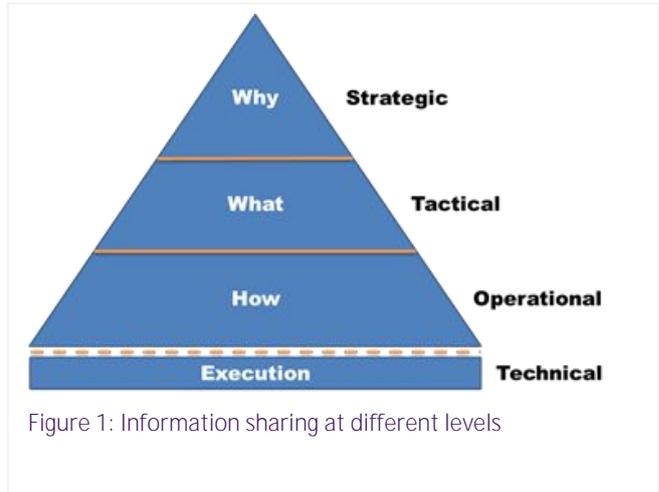
However, staffing of cyber security functions in private organisations is often at the bare minimum level. Experience and knowledge may be concentrated in a single or limited number of people. The pressure of work is high, certainly in crisis situations. Sharing cyber security related information under such circumstances may not be top-priority (e.g., [25], [27]) and largely depends on the experience of the crisis team and the understanding of the needs of the information sharing community [70]. Only when an established collaboration has real added-value does the effectiveness of the scarce staff improve considerably; that is when sharing information by them results in a prompt return of relevant information collected by their information sharing peers and of expert support by their information sharing network.

2.8 Fit to Your Position

2.8.1 Strategic, Tactical, Operational & Technical

Information sharing takes place at three different levels: the strategic long-term policy-making level, the tactical steering level, and the operational - technical level as is shown in Figure 1. The level you act on depends a lot on the relative job position and responsibilities you have in the organisation, and on the type of information that you have and are able to share or receive. Information sharing usually takes place within the same level (horizontally) when it goes cross-organisation or cross-sector. It can also travel vertically, but then it is usually within the organisation. Diagonal information sharing is not favoured as that may cause organisational confusion [51].

One should not underestimate the need to bridge the communication gap between the operational and strategic levels. The strategic level is at the core of the business, the existence of the organisation now and in the long-term. The perception of the risk to the business at the strategic level is expressed in other terminology than is used in the cyber security domain. Moreover, the technical-oriented slang interwoven with marketing terms ('a zero-day Trojan in our cloud') used at the tactical and operational levels may not adequately convey the risk to the business and to the continuity of the organisation. This is an internal information-sharing pitfall that has been noticed in many organisations. Investing in improving cross-level communication pays off. Major improvements of organisational effectiveness were made by organisations that invested in training of their middle management on how to convey cyber risk to their board level.



As a general rule of thumb, information shared from a lower to a higher level should not be too detailed and too specific as the recipient needs to understand the relevance of the shared information first. If more details are considered necessary, the recipient may specifically ask the provider for more detailed information.

Moreover, one should make full use of the shared information by conducting analysis, e.g. by an ISAC, for instance, root cause analysis of specific attack paths [60]. Such analyses provide insight in long-term trends and risk factors that an organisation may face. As a benefit of information sharing, such information is very worthwhile at the tactical and strategic decision-making levels of an organisation, or for a set of collaborating organisations.

2.8.2 Your Focus in the Incident Management Cycle

Information sharing is a cross-mandate spanning various public and private mandates as is outlined in The National Cyber Security Framework Manual [27], pages 120-121. Based upon that framework, Figure 2 shows that information sharing spans one or more phases of the expanded incident response cycle. This cycle comprises pro-action³, via prevention, preparation, incident response, recovery, and aftercare/ (legal) follow-up activities. Some examples: organisations may decide to concentrate on sharing information on proactive and prevention activities given the mandates of the participants; other sharing communities, e.g., Computer

³ Pro-action = anticipatory phase



Emergency Response Teams (CERT), focus on sharing incident response and recovery information; and lastly, law enforcement may concentrate on either collecting shared intelligence to disrupt and prevent an incident from occurring, or to derive from an incident specific evidence and situational information which helps them in the investigation and the prosecution of the culprit [61].

2.9 Actionable Information for the Right Level and Responsibility

The most valuable information received by organisations is information that can be used directly to reduce risk or improve resilience. Such information is of importance to the right cyber responsibilities of an organisation, both vertically (strategic, tactical, operational and technical) and horizontally (incident response phase) as depicted in Figure 2 [65]. For instance, a board member may be able to act on strategic threat information but not on a trace from an intrusion detection device denoting a possible cyber reconnaissance activity by an unknown actor; the latter information may be of great interest to a national intelligence organisation.

However, before sharing, the originators of the information should question themselves on how and on what level of detail they would like to receive themselves. Is the information fit for purpose and does it potentially add value for the recipient? Does the information have relevance? Is it shared in a timely manner? Is it accurate? Is it complete? Is it digestible? [13]

Moreover, there are many types of information to share. Earlier work [27] distinguishes a set of various types and subtypes of information on: actor intelligence and law enforcement information, background and reference information, compliance status, detection and mitigation, (analysed) incident information, (situational) metrics, good practices, threat information, and vulnerability information (Figure 2). For the exchange of some of these information exchange (sub)types, international standards and protocols exist, a number of them is outlined in [14]. Other types of elements are transferred as plain text documents, by simple email or SMS exchanges, or by voice communication.

Do not be too careful in exchanging vague information with peers. Information on some ill-defined abnormality, which on its own is too weak to raise a major alarm, may collaboratively turn into a weak signal which in the end may unearth an Advanced Persistent Threat (APT).

2.11 Secure, Trusted and Controlled

Before valuable information is shared, a set of mutually agreed clear rules is required to ensure the control over, and confidentiality of, shared information. Such an agreement helps to build trust as the expectations about how each organisation transports, processes and stores shared cyber security related information are laid down. A principle is that the originator as owner of the shared information determines the rules and conditions on its use by the recipient(s) and whether, and how widely, the shared information may be disseminated. The recipient needs to adhere to this principle and, on a case by case basis, may ask the originator and owner of the information for guidance in cases where there are urgent reasons for extending the original controlled dissemination. The best information for the recipient is actionable information [13]; the originator of shared information may overlook this **aspect in the heat of a crisis and only report ‘the story’**, not the solution. The various methods to exchange sensitive information, including electronic means, are explained in sections 2.16.3 and 2.17.

Moreover, one has to understand the difference between dissemination controls and security classification controls. Dissemination controls (section 2.16: Traffic Light Protocol, Chatham House rule) simply control how far information could be disseminated, not how it should be protected, etc. Security classification systems focus on the potential harm from disclosure; therefore confidentiality and a wide set of protection measures are paramount. These two systems of controls are orthogonal and can be used in combination where necessary.

“You’re not talking about companies sharing their advertising and marketing material, you’re taking about sharing their deepest, darkest secrets.”

Harris Miller (ITAA) [72]

Sharing national, EU or NATO classified information is based upon formal regulations, accreditations, and clearances (vetting of staff) which relate to the protection of information at the specific security classification level. Two approaches by public authorities to the formal process of vetting exist. The first approach is one where nations vet and provide a clearance for a *specific person* in a *specific function*. The second approach is one where nations vet a person for a *specific information security level independent of the person’s current* (or future) function and responsibilities. The latter approach makes information sharing more flexible as one may not know beforehand what type of cyber threat or vulnerability information may urgently need to be shared with private organisations on a need-to-know basis.

When disclosing sensitive operational information about a vulnerability for which no mitigation exists yet, the originator, especially if it is a manufacturer, has to consider the trade-offs of sharing the knowledge with a wider community against the risk of it becoming known to the public too early. Sharing within a trusted community should never enhance the potential success of the threat or its exploitation. If the discovery stems from the hacker community, for instance through responsible disclosure (see also section 2.14.7), the clock is ticking. A decision to share needs to take into account the risk that the vulnerability becomes known in cybercriminal communities or to the public, before the system or network owners can take mitigating actions.

2.12 **Sharing is Caring, but the Devil's in the Details**

Experiences have shown that inter-person and inter-organisational trust are the key success factors for information sharing. In general, there are some basic dos and don'ts:

- The information provider should ensure that the information provided is of the right level of content and background. Based upon the information, the recipients of the information should be able to take appropriate actions in their respective organisations or need to be alerted about new threats. Above all, the information provider remains the owner of the shared information and dictates its dissemination conditions.
- In case of doubt whether you can share valuable information, it is good practice to check the source, e.g., with the original information provider, not with a trusted intermediary (see section 2.13.5). As in the intelligence business, sharing sensitive information without taking precautions might hurt the source of the information which will really damage the trust relationship(s) that has been established and will cause disruption to the sharing community, sometimes leading to a set-back of years.
- **Sharing the fact that you don't have any new or additional information than already shared is also an enrichment of the joint situational awareness.** Often, not all of the dots can be connected. However, for **everybody's information position in the information sharing community it is important to know that no relevant information is held back.**
- Prepare basic and explicit rules or guidelines for the information sharing community to work with. **Complicated models won't work; people need to intuitively understand the rules and guidelines.** Let newcomers in your trust circle be part of a democratic process, so it will not become a cartel-like structure. The purpose of information sharing is to reduce a common risk, not to gain a competitive advantage.
- **Keeping each other's contact information updated is elementary to enable a collaborative well-oiled action and response machine.** CERT-communities under TF-CSIRT [54] use the Trusted Introducer (TI) model [35] to ensure that the trust you have in a specific person is trustfully delegated to another

colleague. This model can be useful if it is not possible to get through directly to the trusted peer. The underlying TI maturity model measures 44 parameters [1], some of which may be of interest to be discussed in other information sharing communities as well.

- **Sometimes an organisation's representative in an information sharing community does not share the same goals or understandings as the remainder of the group.** If this undermines the trustworthiness that has been built, it is wise to discuss this issue openly between the subject and a representative from the group. If no common ground can be found to continue a sharing relationship, the group can decide to exclude the subject from further involvement in order to preserve the information sharing community. Although this is not an action to be taken lightly, it will preserve the core trust in the remaining group and even strengthen it further, as it has been tested.
- A successful Information Sharing model has a generic weakness. If it is successful and effective it will be inclined to grow in size, and that growth will undermine the collaborative trust and make it harder to function. Splitting a successful group is not a satisfactory solution as many will prefer to be in the other group or miss out on key players' **inputs**. A common broker (e.g., NISCC/ Centre for the Protection of National Infrastructure (CPNI) in the UK Information Exchange model; see paragraph 3.3.1) can mitigate this to some extent, but the effectiveness of each group will inevitably be diminished.

2.13 One Size does not Fit All

Starting an information sharing community is not just copying a standard format for success. The success largely depends upon the experience of participants, their background, culture, nationality and ethics. Moreover, the difference between success and failure may depend on: the structure of the community as a whole, the method of information sharing, equality of capabilities, and the level of experience of the **organisations ('maturity'), and common or similar interests. All these aspects are explained further below.**

2.13.1 Peering or Public-Private Partnership/Participation?

In most nations, more than eighty percent of the critical infrastructures (CI) are owned and operated by private companies. In order to achieve community resilience, public and private CI owners need to work together in a co-ordinated way with the public authorities and agencies in protecting the CI before, during, and after a major incident. National and local first-responders, emergency managers and others may frequently interact in an established public-private partnership (PPP) or – more actively – public-private participation, with CI owners and operators to plan for, and respond to, attacks and natural hazards. PPPs are found in many different forms, varying from very informal types of co-operation to more formal or even mandated partnerships ([12], [33]). The degree of formality or obligation is often associated with the amount of control the governmental bodies aim to exert over each CI sector [73].

The sharing of cyber security related information between public authorities and agencies and CI operators often takes place in a PPP setting. Therefore, a number of key success factors for PPP [8] are of importance for cyber security related information sharing arrangements:

- Trust: as PPP in CIP often concern touchy topics (commercially and security wise, or in terms of established structures), it is essential to create an atmosphere of trust in which both public and private **parties show awareness of each other’s need for discretion, and consistently act accordingly; see section 2.10.**
- Respect: both public and private parties have to recognise and respect the added value another party **brings to the information sharing community. This can be reached by ‘selling’ your own added value (in your partner’s terminology) while actively** looking for the added value of each of the other partners.
- Transparency: the openness on procurement policies and practices is an important factor and should not conflict with the information sharing of cyber security-related information as that could cause conflict with antitrust laws. See section 2.14.2 as well.
- Clear legislative and regulatory framework: a clear framework of legislation and regulation sets out the PPP framework. It is recommended to have fewer and simpler laws (avoid duplication).
- Do not re-invent wheels: **learn from existing ‘information sharing wheels in motion’ and improve them.**
- Neutrality: it is necessary to have clear, specific and predictable rules for sharing cyber security related information. The rules should prevent any conflict of interest and reduce ambiguity.
- Common interest: a public-private information sharing collaboration should be based on a common interest in order to establish a basis for co-operation and create a win-win situation for all participants. An example of common interest is a thematic information sharing community such as a cross-sector operating SCADA/Industrial Control Systems ISAC.
Note that there is also no need to be in every loop, as long as you are informed through the right channels about the information that is important to you. This however, requires professional judgement by the information provider or broker.
- **Agree to disagree: awareness of each other’s opportunities and restrictions is necessary. This prevents conflict through misjudgement of the cause of a negative response and allows for an optimum return on the efforts of the PPP. In many countries, there may also be real concerns in the private sector that potentially heavy-handed ministerial or government involvement might result in requirements or regulation that reflect government priorities but do not make sense from a business standpoint [76]. This implies that both public and private parties should know each other’s (business) drivers.**

“Voluntary, but not without engagement”

- Realistic expectations: both public and private parties have to take into consideration affordability of information sharing resources to ensure realistic expectations of the PPP.
- Regular evaluations: PPP regularly need to evaluate whether the objectives are still clear and information sharing activities align with these objectives.
- Avoid hierarchic relationships: hierarchic relationships, like those often present in mandatory information sharing schemes, are a barrier for an open and transparent information sharing culture (see section 2.4). In a truly equal networked information sharing environment, there is no hierarchy between partners.
- Public authorities have to consider taking a back seat: public authorities should ask themselves the **question each time ‘Do I need to take part in this information sharing community?’ Authorities do not always need to be ‘in the loop’.** They need to trust private communities. Only if they can provide real added value should they suggest being part of an information sharing community, either directly in the main loop, or as a called upon.
- Different models: An information sharing arrangement in one community may require a different model in another community. Learn from other communities, but make the right fit of arrangements with the partners in your own sharing community. Nevertheless, keep an open mind to new developments and other information sharing communities; changes over time may be beneficial.

“You throw out what goes wrong and keep the success: Learning by Doing.” [2]

2.13.2 Meet in Person or Automate by Proxy

Meeting in person has proved to be the most important way of building trust and a relationship for information sharing. It requires time to meet on a regular basis, but it has advantages in building personal trust with other people and their organisations. Therefore, meeting in person acts as a cornerstone for establishing trust and further automation of the information exchange underlying to the sharing of cyber security-related information. Moreover, it may help people to improve their work as a professional in their organisation as one becomes part of a group that has a common goal to raise the bar in cyber security. Meeting in person gives the opportunity to discuss various issues in a group during a meeting or via a bilateral talk during lunch or a coffee-break as well as to sharing RED-type information (see 2.16.1 “Traffic Light Protocol”).

Depending on how widely the geographical locations of the member organisations are apart - it needs to be practical to meet - one can select the frequency of the meetings in person. Depending on the experience and



relationships the information sharing community has with each other, they may try to find other ways of communication and exchanging information, for instance via a telephone or video conference, chat session, or similar. For each of these forms of communication they need to develop guidelines and etiquette to meet in a structured and useful way. When starting sharing information, people are often not aware of the knowledge they carry in their mind and which is valuable to others. Such tacit knowledge can come to the fore as a result of a weak cue by other participants in a face to face meeting. When meeting in a telephone conference or when exchanging emails, such cues may be missed and tacit knowledge is not unlocked [56]. Therefore, information sharing by meeting each other in person is, again, the best start.

Looking at the other side of the coin, when it comes to sharing operational or technical information, automation is key. This electronic information exchange is explained further in section 2.16.3. It will reduce communication mistakes you would get when verbally exchanging information, but needs the trust backing of **regular meetings with the people 'behind the buttons' of electronic information exchange. As a general rule you can take away that you can automate at the operational/technical level, but this becomes more difficult at the tactical and strategic levels of sharing.**

2.13.3 Near Equal Maturity of the Sharing Partners

Information sharing works best when the collaborating organisations operate at much the same cyber security maturity level. In such a case, the information being shared by an originator is quantitatively and qualitatively comparable with information that is received in return from partners. The maturity of the organisation is displayed by its willingness to share sensitive cyber security-related information, the professionalism and experience of its cyber security staff and organisation, and the ability to professionally and securely handle sensitive information received from other organisations. A good match of organisations creates added value for all. Moreover, experiences have shown that sharing partners may not always accept top-down coordination by one of the partners if they only want to collaborate equally [1].

In contrast to the preference for organisations of **comparable capabilities or equal 'cyber maturity', in some communities not all organisations are equally capable or as 'mature' as others. In that case it is commonly understood that the organisations with fewer capabilities that perhaps cannot bring information to the table at every meeting, are not regarded as free riders. Larger organisations still may benefit from investing in sharing with and taking care of 'younger siblings', as it positively contributes to the sector's image [13].**

2.13.4 Culture and Ethics

Organisations have different backgrounds and ways of operating, especially if it concerns organisations in an international context. The differences stem from a mixture of perspectives such as: public or private, more or

less cooperatively minded (in Dutch: “polder model”), culture, national history, organisation’s history, language, judicial system, political and ethical differences, as well as experience, norms, procedures, processes and practices, etc. [70]. Language differences stem both from translation between, for example, **English and German, and from different vocabulary such as technical terms (“sector-specific slang”)**. Insufficient attention to such differences on the edges of interaction between people, technology and processes may hamper collaboration and information sharing; a phenomenon learned by defence organisations during international coalition operations [63]. **Involving individuals who can cross cultural barriers as linking pins (and not their ‘bosses’ who might not be able to do so), may help to stimulate the information flow between diverse communities [74].**

Examples show that organisations should not be pressed to share information against their will. They will sabotage the obligation, for instance by overloading the recipient with low value information. Such organisations should be left out of the sharing community as early as possible as they drain energy. In contrast, the creation of a joint, open and transparent culture of information sharing creates a win-win for all partners in an information sharing arrangement.

2.13.5 Push, Pull, or a Trusted Intermediary

Sharing information between organisations can be arranged in various ways:

1. The originator actively supplies the recipient(s) with cyber security-relevant information (push). Various means can be used: telephone, SMS, direct email, an email to a list of recipients via an email list-server.
2. The originator places the information on a secure server where it can be accessed by trusted recipient(s), e.g. forums, updates for anti-malware packages, and ISAC repositories. An intermediate form is sending a short email to the recipient(s) providing a link to the full set of data.
3. A trusted intermediary, also known as clearing house, fusion cell or centre, information broker, or ISAC or ISAO centre, may provide a central repository service to its constituency or customers, both for uploading incident data as well as for retrieving shared information, good practices, and security solutions such as patches. Examples are the Malware Information Sharing Platform (MISP) as outlined in [14] and [29] and the Cyber Security Information Sharing Partnership (CISP) [45]. Where a community consists of a heterogeneous set of organisations, the intermediary may customise information to make it fit for purpose for different communities; for example a small and medium enterprise requires different information to act upon compared with a large organisation that provides a multitude of cyber services ([45], [74]).



2.13.6 Cross-Border Sharing

International communities may share information based upon trust and a protocol, as explained in sections 2.11 and 2.16. Sharing of national, NATO and EU *classified* information across (inter)national borders is based upon formal regulations, accreditations, clearances (vetting of staff), and formal international agreements on equivalency schemes. An example of such rules and regulations can be found in [11] regarding the handling, transport, and storing of EU classified information (EUCI). Due to the formalities and regulations involved, it is often less easy to share such classified information with private parties.

In an international environment, it can also prove to be more difficult to build the trust needed for effective information sharing. Again, there are some examples of cross-border information sharing in relatively small communities on a regional basis (e.g., the Visegrád Group), information sharing for a specific topic (e.g., the European Information Exchange on security for SCADA and control systems EuroSCSIE [48]), and European-wide information sharing in the financial sector (EU FI-ISAC). CERT community examples are FIRST [50] and the European Government CERTs Group (EGC) [47].

2.14 Avoid Show Stoppers: the Legal Perspective

2.14.1 Freedom of Information Act (FOIA)

Sharing sensitive confidential information with public authorities can lead to an unwanted disclosure of such information to the public if an appeal is made for public release under a Freedom of Information Act (FOIA). A FOIA causes private parties to be concerned and reluctant to share cyber security-related incident information with public authorities as it may damage their reputation, may disadvantage their market positions, their intellectual property rights (IPR), and may reduce the stock value ([17], [71]). For those reasons, a number of nations have exempted voluntarily supplied critical infrastructure and private sensitive cyber security information from disclosure by their FOIA if the shared information concerns the safeguarding of their national security. For instance, voluntarily shared critical information infrastructure information is exempted from FOIA disclosure in the USA [43]. A wider reaching cyber information sharing act, however, is under in debate.

Other nations circumvent the FOIA by exchanging private sensitive information through their security services which may be ex officio exempted from the FOIA. Even then the exemption might not be an absolute exemption and may be subject to a public interest test in court. Nevertheless, private industry may be reluctant to share information with their government as they lose control over their shared information which



often is subject to wide distribution to cleared personnel within the government, its agencies and their international counterparts [72].

In nations where voluntarily supplied sensitive information may be subject to the FOIA, private organisations need to be very careful when sharing information with public authorities, especially when it is in the form of electronic or written communication. It needs to be crystal clear for both public and private organisations how the information exchange is organised, how each party handles the provided information, and what the remaining risk and benefits are when sharing sensitive information. For instance, the risk is that threats to, and vulnerabilities in, their critical infrastructure are not mitigated as fast as would have been possible.

“You don’t exchange business cards in the middle of a crisis. You have to build the social network before.” [2]

There may exist some practical solutions. One solution is to provide a trusted employee of a public authority access to the information within the compound of the private organisation or another private organisation which acts as an escrow organisation. He/she is able to verify that the information is deposited and may read it. However, no information or notes are allowed to be brought to the outside. A second solution is only sharing such sensitive information between the private parties. The representatives of the public authorities would need to wait outside the meeting room.

2.14.2 Antitrust Law

In some legal frameworks, sharing certain information between competitors in the same critical infrastructure sector may be seen as a violation of the competition laws, also known as antitrust laws. Sharing some types of cyber security related information may therefore cause a legal risk to the organisations that share such information. In support of their national security, some nations have exempted the sharing of cyber security related information from antitrust laws. If in doubt about what is allowed and what is not allowed according to the antitrust laws in force, organisations should clarify with the sector-specific regulator, the type of information, the intended organisational level, and for which phases of the incident management cycle one plans to share, and formally ask permission. Figure 2 may be of help. Note that contrary to antitrust laws, **some governments even act as a “safe harbour” for public and private organisations to share cyber security related data.** More information on this legal dilemma, specifically for the USA and Canada, can be found in [17], [55], [70] and [71].

2.14.3 Privacy Protection Concerns All Information Sharing

Sharing cyber security related information on incidents with other organisations, and even in some nations between governmental organisations, may violate stringent privacy also known as (personal) data protection laws and regulations. An internet protocol (IP) address may be seen as a personal identifying piece of information (see, for example, the Article 29 WP opinion 4/2007 [23] and the discussion in [17]).

If a legal system is less forgiving, even when the recipient protects the information according to high standards, information can be shared only after sanitisation of the information. One can use masks to create partial-anonymity or use pseudo-anonymity transformations (Annex B of [32]) on the privacy sensitive fields of the shared data. It will, however, be much harder to reach a full situational awareness across organisations [64]. An early discussion with the Privacy Regulator on how to acquire threat intelligence and acquiring situational awareness, while preserving privacy rights, may help to find a workable and accepted solution. It should be noted that when information sharing partners oblige themselves to the same (inter)national legal framework with regard to protecting personal data, it is seen as an incentive for sharing information [17].

Therefore, proactively sharing one's legal framework and understanding may smooth the way. Another option is to agree to an Information Sharing Agreement (ISA) which provides cross-organisational formal, legally binding arrangements for sharing cyber security-related information [64].

2.14.4 Different Legal Frameworks

In case of cross-border sharing of cyber security related information, the partners are subject to different frameworks. This may affect what type of information they are allowed to share and with whom ([15], [17]). Some of the legal aspects to consider have been outlined in the previous section. However, there are other laws which may be applicable, for instance a national security act. Proactively discuss with authorities which laws apply, which one takes precedence, how to interpret the law, and or how to prepare for the right set of measures in the context of the information sharing objectives. This may keep the lawyers away if the need for sharing information is high. In the context of a wider (international) community, openly publishing policies and some relevant procedures may increase transparency and be an incentive for other parties to participate [57].

2.14.5 Friend or Foe: Law Enforcement has Multiple Hats

Information sharing by private companies of corporate sensitive cyber security related data with law enforcement or any other public authority requires the building of trust. Unfortunately, law enforcement and other public officials may have multiple conflicting tasks and role ambiguity [70]. While sharing detailed threat information as part of, e.g. an ISAC or ISAO, to enhance the common situational awareness may, under certain legal frameworks, oblige a law enforcement official to change hats and use that information for



investigation purposes. As a result, the source of the information may be leaked to court and or may damage the reputation of the affected organisation(s). **Pre-arranged protocols such as ‘Chinese walls’ between the different ‘hat-wearers’ may guarantee that sensitive information provided for one purpose is not used for another conflicting purpose** by a public authority. However, it comes down to the individual official who continuously needs to be aware of under what conditions such information was provided by the information owner. Any intended use outside the trusted community in which the information was shared always requires consultation and agreement in advance. In some nations, Law Enforcement Agencies have initiated a confidentiality charter which allows intelligence-only reporting.

2.14.6 Friend or Foe: The Regulator

Depending on the national legal framework, it can either be beneficial or counter-productive to involve the sector-specific regulator in the sharing arrangement. The regulator, like Law Enforcement before, may switch hats when information about cyber security incidents is shared. Collaboration is only feasible if both sides **perfectly understand each other’s objectives, their mandate and way of working** [19]. In some nations, the **regulator takes part in an ISAC as a full member by using a ‘Chinese wall’ construct within the regulatory organisation**, whereas in other nations the participation of the regulator would inhibit the sharing community.

2.14.7 Mutual Foes: Public versus Private

According to Rosenberg [73], certain legal restrictions weaken the ability of governments and their agencies to adequately share (cyber security) threat information with the private sector, whilst – as discussed above – privacy regulations restrict the reverse flow. Our collective response to new (cyber) threats is therefore **limited by law. Rosenberg: ‘what really restricts cooperation is the inherent caution of lawyers who do not wish to push the envelope of legal authority and/or policy and economic factors such as proprietary self-interest that limit the desire to cooperate.’** **The good practice to beat this mutual state of blockade is obvious:** leadership at both sides which puts the objectives of information sharing on top. The lawyers then need to find a workable solution. A reverse approach will find even more reasons to not allow information sharing.

2.14.8 A Hacker Wants to Share Information: Responsible Disclosure

Responsible disclosure is a slightly different approach to sharing than mentioned in the previous sections. **Sharing information between the hackers’ community** or a security researcher and a responsible acting organisation in case of vulnerabilities in their systems and software has often created serious misunderstandings. A hacker or security researcher in question who has unearthed a cyber vulnerability may fear that the vulnerable organisation reports a cybercrime or starts a legal procedure claiming damages. On the other hand, the organisation that receives information from a hacker about an identified vulnerability may fear that for instance an entire database has been stolen. Also in this case, information sharing is a trade-off



between the risk of unwanted information disclosure versus the extra information that can be gained by sharing [60].

Fruitful information sharing between these two communities therefore needs a different approach. In 2013, the Dutch National Cyber Security Centre (NCSC) published a framework for responsible disclosure. This framework helps organisations to create and publish their own responsible disclosure policy. The framework also provides guidelines for hackers on how to act in finding and reporting a vulnerability [7]. It helps to set policy guidelines and rules for both parties in disclosing cyber security vulnerabilities in a responsible and cooperative way [6]. During 2013 and 2014, a significant number of organisations adopted this type of policy and related guidelines. This approach helped to ease the growing tensions between the hacker community and the private and public (critical infrastructure) organisations while simultaneously improving their cyber security.

2.15 Incentives for and Culture of Sharing

Both incentives, and a culture of sharing, may boost the sharing of information by an organisation, a set of organisations, or an information sharing community. This helps to keep the fly-wheel turning.

2.15.1 Enabling incentives for information sharing

The lack of incentives for sharing cyber security related information will become a show stopper in the end [70]. Incentives can be of economic, legal, technological and image nature:

- Shared information which has a clear content and is actionable, is of immediate use to the recipient and saves costs ([13], [18]). Information sharing even may lead to economic advantages [59].
- Being publicly known as a responsible organisation with regard to cyber security by taking part in an information sharing community may boost the image of the organisation.
- An information sharing community has an exclusive membership. Being a member, an insider, and one of the first to receive valuable information is an incentive on its own.
- Regarding public-private partnerships/participations, an incentive for the information sharing community will be when private organisations spend their precious time and the public side provides the out-of-pocket costs such as lunch, logistical organisation, and the meeting place. Providing the secretariat for the community is another incentive.
- An incentive for taking part in an information sharing community may be a reduced premium for cyber insurance [18].



2.15.2 Joint Objectives without Hidden Agenda

Public authorities are often the initiator of an information sharing community. From that perspective, they may fall into the trap that they take the chair and try to steer the private sector organisations.

Misunderstanding the culture and different objectives of the private sector, their steering may pursue the wrong interests. Invest in establishing the joint objectives and agenda. Select amongst the information sharing collaborators a person from private industry with a high personal drive as chairperson. Moreover, the public sector organisation(s) must also contribute information of equal value as private sector organisations. That will make the collaboration more likely to succeed as the public sector representation is seen as equal amongst peers.

2.16 Procedural and Technical Aspects of Handling Sensitive Information

Sharing valuable cyber security related information touches the issue of sensitivities of public and private information. Therefore, mutually agreed procedures and guarantees are required on how to handle and use sensitive information. Three methods stand out: the Traffic Light Protocol, the Chatham House Rule, and electronic exchange of information.

2.16.1 Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) provides a very easy method for labelling and handling shared sensitive information. TLP was developed by the National Infrastructure Security Co-ordination Centre (NISCC), an inter-departmental centre of the UK government (now CPNI), in support of their Information Exchange **information sharing model in the early 2000's. The TLP model has been adopted by a number of nations, ISACs, and other national and international communities for sharing information.** One of the key principles of the TLP is that whoever contributes sensitive information also establishes if and how widely the information **can be circulated ('originator control'). The originator** of the information can label the information with one of four colours [34]:

- **RED** – non-disclosable information and restricted to representatives present at the meeting only.
- **AMBER** - limited disclosure and restricted to the members of the community who have a need to know in order to take action.
- **GREEN** - community wide. Information in this category can be circulated widely within a particular community and the organisations which take part in that community. However, the information may not be published or posted publicly on the Internet, nor released outside of the community of participating organisations.
- **WHITE** – unlimited; public information. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.



The strength of TLP is that it is very easy to use and that the responsibility of both the originator and receiver of the information are very clear. The challenge is for those who provide RED labelled information to consider on how to provide related actionable Amber labelled information.

2.16.2 Chatham House Rule

Another protocol that can be used to protect the anonymity of *orally* shared sensitive information is the Chatham House Rule. Under the Chatham House Rule, participants are free to use the received information, but neither the identity, nor the affiliation of the originator(s), nor that of any other participant(s), may be revealed [37].

2.16.3 ISO/IEC 27010:2012

As part of the ISO/IEC-27000 series of good practices, the ISO/IEC 27010:2012 - information security management for inter-sector and inter-organisational communications document [32] outlines guidance on information security interworking and communications between industries in the same sectors, across different sectors and with public authorities. With respect to the topic information sharing, the ISO/IEC 27010:2012 annexes A through D discuss Sharing sensitive information, Establishing trust in information exchanges, the Traffic Light Protocol (see section 2.16.1), and Models for organising an information sharing community. The latter includes the description of Trusted Information Communication Entities (TICE) and of Warning, Advice and Reporting Points (WARP) [44]. **In combination with ENISA's Good Practice Guide Network Security Exchanges** [19], the TICE guidance provides guidance on the possible organisational structure, operating model, and services of an intermediary organisation of a formalised information exchange.

2.16.4 Electronic Sharing of Information

Sharing cyber security related information electronically or even machine to machine (M2M) [60] requires trusted environments at the premises of all partners. Several initiatives have tried to create a secure and trusted electronic platform for information sharing, e.g., by using a protected extranet for storing minutes of meetings and interesting documents. Key to fruitful electronic exchange is a mutual trust in the communication channels and server that are used to share the sensitive information [64].

The most successful electronic exchange initiatives support communities that also have face-to-face meetings. If no level of trust exists, then it is very hard to create a high level of federated trust in the electronic environment. Apart from CIWIN [46], a CI warning network by the EU, and the research project result NEISAS ([69], [75]), an increasing set of commercial tools for information sharing is being offered. Moreover, private industry in the UK has established an extranet portal (National Resilience Extranet (NRE)) to share trusted information with the civil resilience constituency of category 1 and 2 responders [52].



The need for electronic sharing, especially at the operational/technical level, increases for the following reasons [26]:

1. Human resistance to sharing.
If humans have to decide whether or not to share information with others, and, if so, when, it might result in subjective actions and resistance to information sharing. This means that important information may not be shared, or there may be delays in information dissemination, impacting its usefulness. The resistance to share might be based on humans being too busy, lack of the perceived benefit of sharing, lack of trust in partners, unclear policy on when to share, or sharing being a lower priority task. Establishing automated sharing mechanisms by the organisation forces a clear articulation of the information sharing criteria at the tactical level in advance. This creates a form of objective decision-making, rather than leaving it to the judgement of individuals.
2. Rapid event time scales.
Cyber vulnerabilities and incidents appear out of the blue and the risk propagates extremely fast. For example, malware propagation can occur with such great speed that automated detection and information sharing becomes the only effective way to deal with these events. The 2003 Slammer worm is a well-known example of the speed of propagation and the resulting havoc. It reached its full scanning rate of more than 55 million scans per second in roughly three minutes and compromised over 90% of vulnerable hosts worldwide in less than ten minutes [58].
3. Information exchange volume and complexity.
The exchange of raw or partially processed network sensor information can constitute huge volumes of security-related data, e.g., from a wide variety of systems in different time zones. This volume may exceed the capacity of manual methods for exchanging and processing the cyber–security data.

2.17 Information Sharing Standards

Sharing cyber–security related information can be very simple by means of voice communication or by using simple unstructured email. For 24/7, high-speed and high-volume type of information (data), information exchange standards may be of help. Confidentiality and privacy play a role in what information can be shared and under what conditions and agreements. In a number of cases, de facto or international standards help to exchange information between different types of systems of different owners ([14],[51]). As Figure 3 shows, most information exchange standards cover the sharing of threat, vulnerability and incident information. A number of standards, depicted by red circles, are clearly missing. Even worse, a number of the information sharing standards are developed by diverse communities without taking interoperability into account.

Moreover, there are not many standards available for sharing information between the operational, tactical and strategic levels. Nevertheless, there are standards; use them as best as you can.

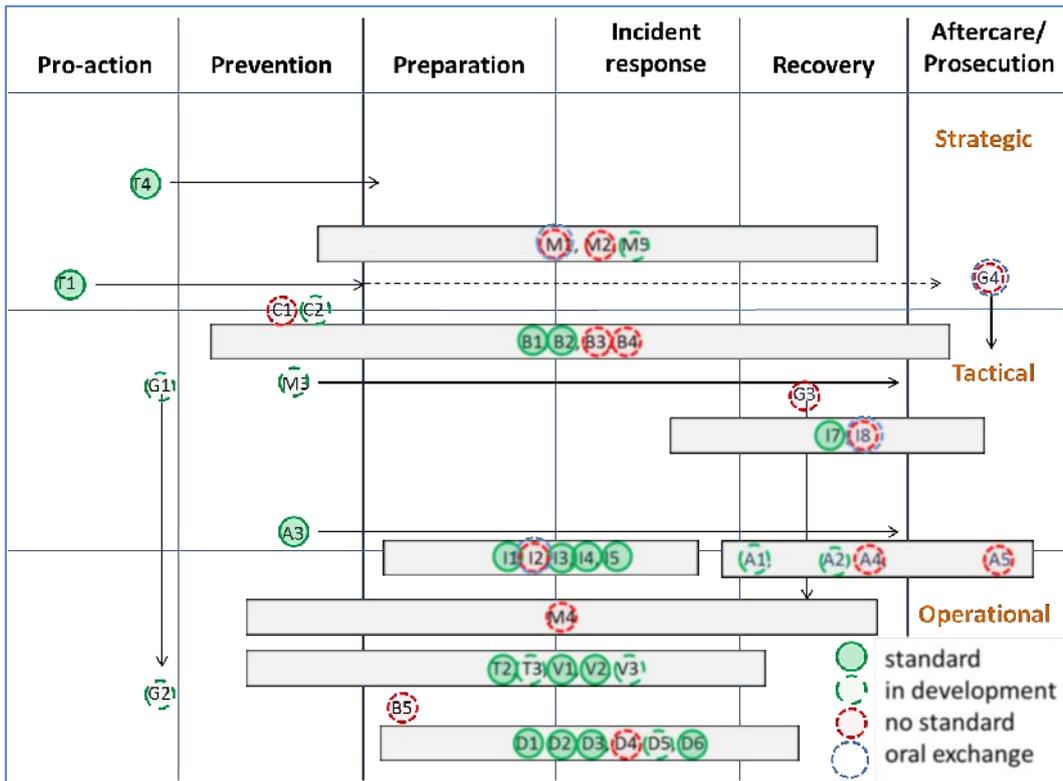


Figure 3: Mapping of information exchange standards onto elements identified in Figure 2 (from: [65]).

3 Analysis of Good Practice Use Cases

In this chapter we will briefly describe some security information sharing platforms that are considered to be good practice use cases to learn from, both from a national and an international perspective. Distinguishing characteristics of these use cases, in terms of general benefits and challenges, have been analysed in section 3.4. When developing a new cyber security information sharing community, these characteristics may help to set the stage.

3.1 Approach of the Analysis

In the next two subsections, several information sharing arrangements are compared along various axes. Most examples are not cyber-related and therefore show a spectrum of diversity in information sharing arrangements. These use cases are analysed along the set of features that are explained more elaborately in Appendix A. Based on these features, you will be able to construct or improve your own information sharing community. For each use-case we assess dimensions and characteristics. In the end, these features enable us to make an adequate comparison of the various information sharing platforms.

The dimensions are constructed to map the selected use cases on numerous, more abstract features. Within the information sharing use cases, all these features form the basis for the collaboration, in terms of partnership and operational characteristics. Before we visually map out these dimensions, we will – briefly – introduce you to the selected use cases.

3.2 Dutch Information Sharing Use Cases

3.2.1 Electronic Crimes Task Force (ECTF)

The Electronic Crimes Taskforce (ECTF) is a public-private initiative of the Netherlands National Police, ABN AMRO, ING, Rabobank, Dutch Banking Association, the Public Prosecution Service, and the Centre for Protection of the National Infrastructure (CPNI.NL). The ECTF became operational as of 2011. The ECTF focuses on information sharing at the tactical level, specifically regarding (financial) cybercrime. Aiming at strengthening the intelligence position of all partners, it produces innovative intervention strategies. The ECTF is housed at the Dutch National Police and therefore uses its organisational capabilities, technical features, and communication plans. The ECTF is collaboratively funded by all the partners.



3.2.2 Financial Intelligence Unit Netherlands

The Financial Intelligence Unit Netherlands (FIU-Netherlands) was created in 2006. It is an independent and autonomous entity within the Department of International Police Information of the Netherlands National Police. The mission of the FIU is to contribute to strengthening the quality of investigation and prosecution as well as the prevention of and fight against crime; in particular money laundering and the financing of terrorism. Forced by law, banks, casinos, art dealers, real estate agents, etc. are obliged to share operational data regarding money laundering and the funding of terrorism. The FIU is an independent body within the Dutch National Police, and uses their organisational capabilities, technical features, and communication plans. The FIU is funded by the ministries of Finance and Security & Justice.

3.2.3 Beveiliging en Publieke Veiligheid Schiphol (BPVS)

After research done by the Schiphol Access Management Commission there was an apparent need to provide additional control and guidance regarding a structural risk management process with regards to aviation security and the fight against crime. For this purpose a control entity called Schiphol Security and Public Safety (or *Beveiliging en Publieke Veiligheid Schiphol*, BPVS in Dutch) was founded in 2005. Both public and private stakeholders work together to improve the effectiveness and efficiency of aviation security and the fight against crime at Schiphol Airport.

BPVS has a coordinating and controlling function, and funding for those professionals involved is provided by each of their stakeholder representatives. BPVS is active on all levels (strategic, tactical and operational), but has different forms at each level; the BPVS platform, the BPVS governance board and multiple working and project groups.

3.2.4 Information Sharing and Analysis Centres

The Dutch Information Sharing and Analysis Centres (ISAC) are usually CI-sector specific (drinking water, financial, energy, etc.) cyber security oriented public-private platforms. Organisations can exchange their cyber security problems in confidence and anonymously. Following an analysis, a warning can be issued to all participating organisations about a threat, vulnerability or incident, or about a good practice that can be applied to mitigate a risk. Most ISACs organise tactical level professionals from public or private CI operators. Public representatives from the General Intelligence and Security Service, the national High Tech Crime Unit, and the Dutch National Cyber Security Centre (NCSC-NL) are part of each ISAC. The NCSC-NL hosts the ISAC platforms. Moreover, the NCSC provides cyber security expertise to the ISAC.



In 2003, the financial ISAC (FI-ISAC) was formed as a private sector initiative. In 2006, it became a public-private ISAC under the Dutch National Infrastructure against Cybercrime (NICC) programme which established other ISACs as well. That initiative has grown to twelve ISACs in 2014 with in total over 150 stakeholder organisations and about 250 tactical level contacts. Using the TLP protocol (section 2.16.1), the ISACs share information about new threats, modus operandi of cyber criminals, trends, good practices, and (most importantly) incident information. ISAC members learn from each other and create better situational awareness and understand the big picture. The sector is in the lead, which means that the CI operators control the ISAC agenda. Some ISACs have developed some analysis capability by topic-related working groups, where this is deemed appropriate. The level of detail of the shared information varies per ISAC but is mostly at the tactical level. The technical and ISAC secretariat support is funded by the NCSC-NL. ISAC communication runs via closed mailing lists, tele-conferences, and physical meetings which are held on a regular basis.

“It’s not public private, but private public participation, as the CI sector is in the lead.” [2]

3.2.5 National Detection Network (NDN)

The Dutch National Detection Network (NDN) is a platform for both public and private stakeholders in the critical infrastructure and includes the ministry of Security & Justice, the National Coordinator for Security and Counterterrorism, the General Intelligence and Security Service, and the Defence Intelligence and Security Service. As of 2014, the NDN has started as a collaboration aiming at sharpening the insights in specific cyber security risk and trends. By sharing threat information between all stakeholders, they can – each stakeholder by their own responsibility – act accordingly with intelligence-led countermeasures and or interventions. The NDN is an integral part of the NCSC-NL primary CERT process and uses its organisational capabilities, technical features and communication plans. The NDN is jointly funded by the ministries of the Interior and Security & Justice.

3.3 International Information Sharing Communities

3.3.1 CPNI UK and the Information Exchanges

The Centre for the Protection of National Infrastructure (CPNI) is the United Kingdom government authority which provides protective security advice to businesses and organisations that are part of their national infrastructure. The UK national infrastructure is categorised by nine critical sectors and covers a number of cross-sector themes [38]. CPNI is responsible for several security strategies, cyber security being one of the topics. CPNI facilitates Information Exchanges (IEs) that allow information to be shared amongst trusted contacts in public and private CI sectors [39]. Currently, fourteen Information Exchanges are operational.



Information about threats, vulnerabilities and effective mitigation measures is shared, allowing businesses and organisations in the national infrastructure to protect their assets better. Similar to the Dutch ISAC model (which is derived from the IE model), Information Exchanges are free to join. Membership is determined by the existing members. CPNI typically provides a co-chair and a co-ordinator for the Information Exchange. CPNI acts as host for the meetings. The large difference from the Dutch model is that CPNI is part of the UK Security Service, therefore information sharing is exempt from the FOIA, although the exemption is not absolute and may be subject to a public interest test (section 2.14.1).

3.3.2 Financial Services ISAC

Launched in 1999, the US-based FS-ISAC was established as a private initiative by the financial services sector as a resource for cyber and physical threat intelligence analysis and sharing response to the national Policy on Critical Infrastructure Protection (Presidential Decision Directive 63 of May 22, 1998). The FS-ISAC model, which was derived from the earlier US Network Security Information Exchange (NSIE) model, was created by and for its members. The FS-ISAC operates as a member-owned non-profit entity. Aiming at gathering reliable and timely information from financial service providers, commercial security firms, government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts as well as other critical information to its members. The FS-ISAC is an independent private entity using its own organisational capabilities, technical features, and communication plans. The FS-ISAC is funded by collecting membership fees [49].

3.3.3 Project Griffin

Project Griffin is an effective police initiative in the physical security domain to protect UK cities and communities from the threat of terrorism [53]. It was developed by the City of London Police. Project Griffin started in 2004 as a joint venture between the City and Metropolitan police forces. It brings together and coordinates the resources of the police, emergency services, local authorities, businesses and the private security industry, both at the tactical and operational levels.

Project Griffin relies on building relationships and sharing security and other information through a system of bridge calls. These regular contacts can be via conference calls, SMS, pager, or email. They provide information updates and intelligence on terrorism/extremism and other crime-related issues. The exchange is also used for specific local situations, such as measures to be employed in times of an emergency. During the bridge calls, actionable information is shared amongst the participants, with no use of TLP or similar classification protocols. Because the shared information is made actionable, both public and private organisations can directly use it in their daily work, for example when patrolling the streets.



Project Griffin has been recognised as a UK best practice and is being implemented by police forces, cities, and other communities throughout the UK. It has also generated interest and acclaim in the United States, Canada and Australia.

3.3.4 Network and Information Security Platform

The Network and Information Security Platform (NIS-P) followed out of the Cybersecurity Strategy of the European Union [9]. Its objective is to foster the resilience of the European networks and information systems that underpin the services provided by market operators and public administrations in Europe. The collective knowledge of the NIS-P may be of use for the implementation of the measures set out in the NIS directive [10] and provide input to realise convergent and harmonised application across the EU. In order to do so, a community of members have formed from European public and private organisations across multiple sectors. The work of the NIS-P will draw from international standards, and cross cutting / horizontal good practices. NIS-P has set up three working groups covering:

- risk management, including information assurance, risk metrics and awareness raising;
- information exchange and incident coordination, including incident reporting and risk metrics for the purpose of information exchange;
- research and innovation in secure ICT.

The findings of the NIS-P may be of use for the implementation of the measures set out in the NIS Directive [10] and provide input to realise a convergent and harmonised application of such measures across the EU.

3.4 Analysis of the Use Cases

The abovementioned dimensions and characteristics are used to analyse the use cases briefly introduced above. Next to this brief description, these use cases will be analysed in some more detail by comparing them along the lines of several axes. Starting with the dimensions (Table 1, Figure 4, and Figure 5), we will examine the extent to which the use cases overlap or differ in aspects such as maturity level and archetype of the case. A first visual representation (Table 1) is accompanied by a descriptive and comparative analysis of the national and international use cases. This should shed some light on the different types of distinctive elements between the various arrangements and communities. Finally, this analysis will form the basis for the Good Practice of information sharing.

3.4.1 Dimensions

When plotting the specific use cases on the dimensions outlined in Appendix A, tables 1 and 2 below emerge. We see a dispersion of the use cases along the lines of all dimensions. When looking at the type of collaboration, both public-private, private and public initiatives are amongst the use cases. The use cases also comprise operational, tactical and strategic level activities. Regarding the target sectors of the arrangement, different approaches appear. Where the FS-ISAC is limited to the financial sector, the ECTF includes both the financial and the law-enforcement sectors. The FIU adds more sectors to both of these use cases. The NDN case, on the contrary, shows that its operational focus is on the government sector, but it aims at including the CI-sectors in the next coming years. A long life-time of an information sharing arrangement may provide an indication of its success and value to the constituency. The opposite is not true; one cannot judge a recently started information sharing arrangement on the basis of its life-time. The FS-ISAC, for example, is operating for more than ten years giving an indication of its usefulness. At the other end of the spectrum, the NDN recently started with phase 1.

All of the information sharing arrangements show that they share data and or trend information. None just shares ‘stories’ or ‘impressions’. If they do, they combine those ‘stories’ with either data or trends. Finally, looking at the number of partners involved, there is a vast difference between the information sharing arrangements. The ECTF has a small number of partners, compared to, for instance, the FS-ISAC and FIU, who have more than hundred partners each.

Table 1: Individual use cases across the different dimensions (Dutch communities)

<i>Dimensions</i> <i>Use case</i>	Type of collaboration	Level of participants	Sector(s)	Life-time	Archetype level	# partner organisations
ECTF	Public-private	Tactical	Finance, Law Enforcement	> 5 years	Incident examples	<10
FIU	Public	Tactical	Law Enforcement, 10+ sectors	> 5 years	Data	100+
BPVS	Public-private	Strategic / Tactical / Operational	Airport	> 5 years	Trends	<10
Dutch ISAC	Public-private	Tactical	12 ISAC in various sectors, Law Enforcement, Intelligence and security services	1-10 years	Trends, incident examples	150+
NDN	Public-private	Tactical / Operational	Government, CI sectors	< 1 year	Trends, data	<20

Comparative

When analysing the use cases above along the lines of the selected dimensions, numerous correlations stand out. First, we see that all Dutch use cases are still private initiatives or have started as private initiatives. Noticeable is that the two operational level use cases are bottom-up initiatives. They are not examples of government initiated programs, later reformed into a private body. These initiatives started consciously without any government involvement and government partners. Both the initiatives are working with data, not with aggregated level information at the level of incidents. Obviously, the threshold for sharing detailed information (i.e., data) is lower. Second, nearly all the public-private collaborations are at the tactical level of collaboration. This level of collaboration fits both public and private organisations as it creates value in both worlds. Third, all the collaborations at the tactical level consist of both public and private organisations from multiple sectors. Fourth, the initiatives wherein (raw) data is being exchanged exceed the amount of hundred or more partners. It can be argued that before the amount of data reaches a critical mass above which data gives new insights, a correlation exists with the number of partners. More partners may mean more shared data. And more shared data increases the potential for new insights. Fifth, we see that all the strategic level collaborations involve one or more government partners. One may deduce that a strategic level collaboration is more beneficial to the public partners than to private partners. Sixth and last, all the international use cases comprise more than a hundred partners.

For a visual representation, leaving out the dimension of the type of collaboration which is too descriptive, the different dimensions of information exchange for a set of use cases can be mapped in a single figure. Figure 4 visualises the Dutch national use cases. Figure 5 visualises the international use cases.

Table 2: Individual use cases across the different dimensions (international communities)

<i>Dimensions Use case</i>	<i>Type of collaboration</i>	<i>Level of participants</i>	<i>Sector(s)</i>	<i>Life-time</i>	<i>Archetype level</i>	<i># partner organisations</i>
CPNI.UK and the Information Exchanges	Public-private	Tactical	Government, 9 CI sectors	1-10 years	Trends, incident examples	100+
FS-ISAC	Private	Tactical / Operational	Finance	> 10 years	Incident examples, data	300+
Project Griffin	Public-private	Operational	Security, counter-terrorism	< 10 years	Data	50+
NIS-P	Public-private	Operational	Government, CI representative from various nations	< 2 years	Good Practices, needs	50+

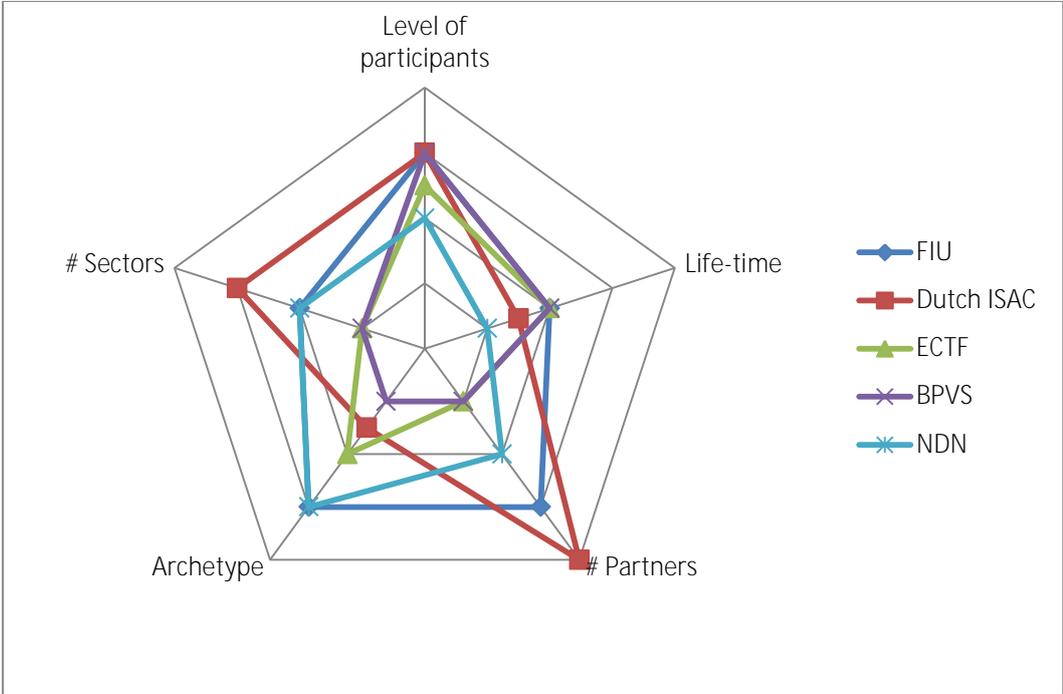


Figure 4: Radar chart of the Dutch use cases

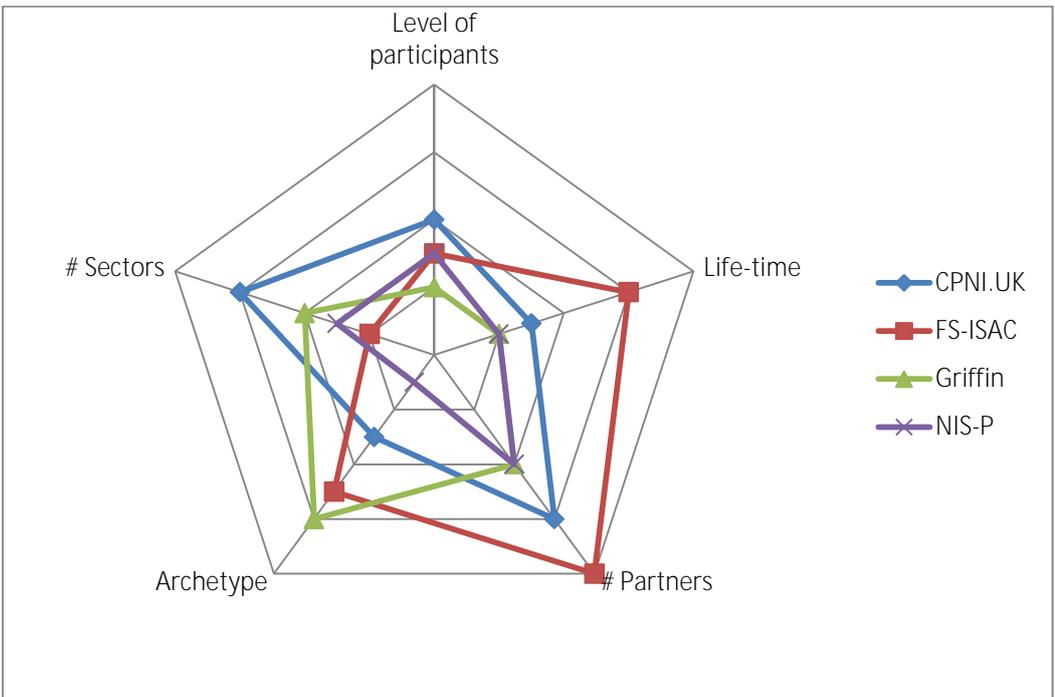


Figure 5: Radar chart of international sharing communities



Figure 4 represents the differences in the dimension as shown before in table 1 and elaborated on in the section above. Taking the Dutch ISAC use case as example, we start at the top of the figure. While going round clockwise, we see that the ISACs operate at the tactical level, have a medium life-time (one to ten years), have many partners (150+ in total for all ISACs), operate at a low/medium level of detail (sharing incident examples and trends) and operate in various (CI-) sectors.

Taking the FS-ISAC use case as example, we start at the top of Figure 5 going round clockwise. The FS-ISAC operates at the operational/tactical level, is already in existence for a long time (10+ years), has many partners (300+), operates in medium/high level of detail (sharing of data and incident examples) but operates only in the financial and insurance sector.

3.4.2 Comparison: Benefits & Challenges

Benefits

Bottom-up approach: Most information sharing initiatives were created using a bottom-up approach. They started with a small group and a small scope and built on the good practices the stakeholders created.

All archetype information is useful: Stakeholders usually begin with sharing of incident information, so they can learn from each other and from good practice mitigation measures. Based on enough incident information, organisations start (collaboratively) analyse these incidents and assess trend information. If an initiative grows in number of participants and the amount of shared information, the need for efficiency through automated exchange of information and analysis grows along with it. Information from all archetypes is useful. However, the real usefulness depends on the expected level and objective of the information sharing arrangement. Raw data will be used more at the operational level. Incident information and trends will be used mainly at the tactical level. Trend information will provide input to the strategic level of an organisation.

Timeliness of success: Most of the initiatives discussed above have been gradually expanded and existed for a decade or more. This means that the need for information sharing is permanent and brings value. Most of the initiatives concern PPP. This indicates the need to collaborate, as organisations realise that they cannot solve the security challenges all by themselves.



Challenges

Trust does not grow fast: **Larger collaborations have a greater potential for ‘valuable’ information for all, but** have a challenge in a trusted governance structure.

Information overload and underload: information brings risk for decision-makers of on the one hand overload, and on the other hand indecision as decision-makers may keep waiting for information which is not coming.

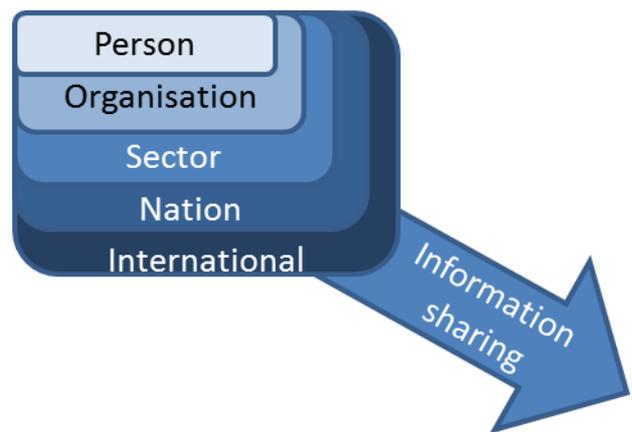
Understand information needs: A good stakeholder management in the community keeps track of the information needs of the partners in the community, so it will pay off in abundance.

Top down legal implementations: creating ad-hoc collaborations, such as FIU, creates a sense of urgency with the partners involved. On the other hand, when the private sector sees FOIA (see 2.14.1) as a barrier, this will hamper the flow of information sharing.

4 Future Outlook and Challenges

4.1 And the next step is ...

... a layered approach. By sharing various types of cyber security-related information at different levels, people, organisations, critical infrastructure and other sectors, as well as nations, will benefit. In order to share information within a nation's critical infrastructure, public and private partnerships/participation (see 2.13.1) need to be created first. With the right level of commitment and energy, PPP will develop over time. Relevant information will be shared, combined and enriched [1]. The next step will be a real public-private collaboration and participation: acting on the shared, combined and enriched information.



To provide an overview of each layer in perspective:

- Personal perspective: As mentioned before, sharing is caring. People need to be intrinsically motivated to really share sensitive information with trusted peers, assuming they have the right prerequisites to do so. It will take time to get used to such sharing in a comfortable manner, but this granular level is the most important one, preceding the other layers.
- Organisational perspective: Your organisation needs to be ready and willing to trust some of their professionals to share and receive information with external peers and stakeholders under the right conditions to create better situational cyber awareness. The benefits of an approach where you gather information in your environment by interacting with your peers on the cyber security topic will ultimately outweigh the risk of uncontrolled data disclosure that is involved with sharing. By implementing the right systems and procedures (see sections 2.9 and 2.13) without being too strict and legally restricted (see section 2.14), organisations can manage this risk to acceptable levels. This will also mean that cyber security will become a regular topic in the board room of organisations (section 2.2). Therefore, relevant information in the right context is needed and the (Chief) Information Security Officers ((C)ISO) need to learn to address issues in the boardroom at the right level (see section 2.22.9). This requires actionable and reliable information [13].
- Sector perspective: Only by combining the information from multiple sources (bought, shared, or otherwise), will organisations in a specific sector be able to create a trusted common picture, be it threats, trends, or good practices. If information is processed through analysis centres, working groups

or the like, organisations will be able to really form actionable information and knowledge. This information might be on the strategic, tactical, or operational/technical level. Some issues (like forming a responsible disclosure policy) require a united action in order to raise the cyber security bar. If organisations in a specific (critical) sector do not compete with each other on the subject of cyber security, the professionals involved will have lots of experience in common to not only make their own organisation more resilient, but also their entire sector.

- National perspective: At the national level, information sharing needs to be stimulated in the right way. This can be done by providing the right conditions and incentives. For example, by public support by offering a meeting place and enough manpower to information sharing platforms such as ISAC, or by providing the right balance between sharing incentives and law and regulations (see section 2.14). By assessing and stimulating the right cross-sector information sharing initiatives, the greatest effect on a national level can be achieved. This will result in an improved level of cyber resilience throughout the nation, starting with the resilience of the national critical infrastructure.
- International perspective: Many private organisations and also some public agencies operate internationally. As information sharing can only be done properly under the right conditions and with the right mind-set, other nations would need to foster the approach and culture of information sharing. Bilateral or multilateral agreements, covenants and international regulations need to form a comfortable habitat for an information sharing community to flourish.

4.2 What are the challenges to achieve this?

Some challenges have been experienced during information sharing in the past:

- The flow of the shared information.
Cyber security information sharing is performed with trusted stakeholders in trust circles, but each stakeholder is part of multiple supply chains in their environment in which organisations are dependent **on each other's information. For instance, a managed security service provider (MSSP) who manages a security service for your organisation.** If your organisation is able to receive sensitive information that is also of value to your supply chain, would it be possible to share this information with other parties although they are not formally a trusted party (yet)? Would the MSSP approve if you shared the information with others, but only you have paid for it? And if the source of the information is a public entity, would the security service provider not be given information superiority over other competitors? Other organisations **may be 'multiply included'** [74], i.e. being part of multiple information sharing communities. This will make it a challenge to decide which type of information can be shared with another community or not.

A set of basic rules will need to be developed for handling this multi-layered issue, whether they are made formally or just used in an informal way between the different trust circles. These rules will become part of the information sharing protocols that are in use. In this case, the public entity would take the improvement of the cyber security situation in the nation as a whole into account and share anyway. Separate Non-Disclosure Agreements (NDA) need to be prepared in order to not promulgate the information beyond those that need it to improve the cyber security of their respective supply chain.

- Granularity in a hyperconnected world.

With almost every ICT-enabled device becoming part of a hyperconnected world, society has also **opened a Pandora's cyber security box**. Information about vulnerabilities, cyber intrusions, attacks, patches, et cetera, will become an integral part of that hyperconnected world. Moreover, outsourcing, offshoring and new collaboration and business models with third parties complicate the cyber security landscape even more [42]. Due to the sheer amount of (big) data, granular levels of shared information need to be distinguished. Bulk data analysis is and will be largely automated. But at what level of abstraction are trends extrapolated? And how is this shared meta-data analysed and enriched? The other side of the coin is that if there is a real need to act upon the information, what are the viable alternatives and actionable measures that would reduce the risk that accompanied the realisation of a hyperconnected world in the first place?

- The role of the new cyber security insurance incentives is unclear.

Insurance companies are developing insurance products for individuals and organisations to manage their cyber risk. Will this risk management measure hamper information sharing as organisations alter their cyber risk strategy from risk reduction to an external transfer of the cyber risk? It seems to be a paradox of choice. This might be a beneficial choice for one organisation in the short-term to achieve internal or external compliance, but other organisations in their sector and society as a whole will not benefit from this strategy.

- Victim of success.

A more mature cyber security information sharing community may come at a cost. A future challenge might be when cyber security professionals do their work successfully; cyber security will become an integrated part of the core of the organisation and its products and services. This will spark the commercial department to market the cyber security features of the products and services in a competitive mode [64]. At this point, it will become very difficult to maintain the trust basis of information sharing with other organisations. Alternatively, to end with a positive note: it might be just a phenomenon of the maturing information sharing community and the start of a new and improved information sharing era.



References

Netherlands Government and Agencies

- [1] K. Clark, D. Stikvoort, E. Stofbergen, E. van den Heuvel (2014), "The Dutch Approach to Cybersecurity", in: *IEEE Computer and Reliability Societies*, Sept/Oct 2014, pp. 27-33.
- [2] CPNI.NL (2013), "From learning by doing to leading by doing," The Hague, The Netherlands. Online: <http://www.cpni.nl/files/8513/7171/9356/CPNI-slotbericht.pdf>
- [3] Ministry of Security and Justice. (2014), "National Cyber Security Assessment 4", Ministry of Security and Justice/NCTV/NCSC, The Hague, The Netherlands. Online: <https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/cyber-security-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat/1/CSAN%2B4.pdf>
- [4] Ministry of Security and Justice (2013), "National Cyber Security Strategy 2.0", The Hague, The Netherlands. Online: http://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf
- [5] Ministry of Security and Justice (2013), "Beschrijving producten en diensten NCSC" (products and services catalogue NCSC), The Hague, the Netherlands. Online: <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/dienstverlening/producten--en-dienstencatalogus-pdc-2013/1/NCSC%2BProducten%2Ben%2BDiensten.pdf>
- [6] NCSC (2013), "Leidraad om te komen tot een praktijk van Responsible Disclosure", Ministry of Security and Justice, The Hague, The Netherlands. Online: <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/richtlijnen/2013/01/03/leidraad-om-te-komen-tot-een-praktijk-van-responsible-disclosure/pers-5766b-document-responsible-disclosur-1.pdf>
- [7] NCSC (2013), "Guideline for responsible disclosure of IT vulnerabilities", Ministry of Security and Justice, The Hague, The Netherlands. Online: <http://www.government.nl/news/2013/01/03/guideline-for-responsible-disclosure-of-it-vulnerabilities.html>
- [8] NICC (2008), "Public Private Partnership in the Cybercrime Information Exchange", NICC brochure, The Hague, the Netherlands. Online: http://www.samentagencybercrime.nl/UserFiles/File/NICC%20brochure_uk.pdf

Europe (European Commission, European Union, and ENISA)

- [9] European Commission (2013), "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace", Brussels, Belgium. Online: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

- [10] European Commission (2013), “Proposal for a directive of the European Parliament and Council concerning measures to ensure a high common level of network and information security across the Union”, COM(2013)48 final, Brussels, Belgium. Online: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666
- [11] European Commission (2013), Council Decision of 23 September 2013 on “the security rules for protecting EU classified information” (2013/488/EU), Brussels, Belgium. Online: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN>
- [12] M. Klaver, H. Luijff, A. Nieuwenhuijs, et al. (2011), “RECIPE Good Practices Manual for CIP Policies”, The Hague, 92 pages. Online: <http://www.tno.nl/recipereport>
- [13] ENISA (2014), “Actionable Information for Security Incident Response”, ENISA, Heraklion, Greece. Online: http://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security/at_download/fullReport
- [14] ENISA (2014), “Standards and tools for exchange and processing of actionable Information”, ENISA, Heraklion, Greece. Online: http://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport
- [15] ENISA (2013), “Detect, SHARE, Protect: Solutions for Improving Threat Data Exchange among CERTs”, ENISA, Heraklion, Greece. Online: http://www.enisa.europa.eu/activities/cert/support/information-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/at_download/fullReport
- [16] ENISA (2013), “NIS Public-Private Platform: WG2 Outcome draft”, ENISA, Heraklion, Greece. Online: <https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg2-documents/wg2-outcome-draft/view>
- [17] ENISA (2011), “A flair for sharing – encouraging information exchange between CERTs; A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe”, ENISA, Heraklion, Greece. Online: <https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing>
- [18] ENISA (2010), “Incentives and Challenges for Information Sharing in the Context of Network and Information Security”, ENISA, Heraklion, Greece. Online: http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport
- [19] ENISA (2009), “Good Practice Guide Network Security Information Exchanges”, ENISA, Heraklion, Greece. Online: <http://www.enisa.europa.eu/media/press-releases/guide-to-mitigate-vulnerabilities-threats-cyber-attacks>
- [20] ENISA (2009), “Good Practices on Reporting Security Incidents”, ENISA, Greece. Online: <http://www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms/reporting-security-incidents-good-practices>

- [21] ENISA, “NIS Public-Private Platform”. Online: <https://resilience.enisa.europa.eu/nis-platform>
- [22] EU Telecommunications Package (2009), “Regulatory framework for electronic communications”, EU, Brussels, Belgium. Online: http://ec.europa.eu/information_society/policy/ecomms/doc/library/regframeforec_dec2009.pdf
- [23] EU’s Article 29 Working Party. Online: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
- [24] European Parliament and Council (2002), “Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)”, Brussels, Belgium. Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>

International Organisations (NATO, OECD, World Bank, World Economic Forum)

- [25] L. Beaudoin, M. Grégoire, B. Heinbockel, Ph. Lagadec, J. Lefebvre, E. Luijff, R. Mc Quaid, J. Tölle, “Coalition Network Defence -- **Common Operational Picture**”, in: Proceedings Symposium on Information Assurance and Cyber Defence, Tallinn, Estonia, 22-23 November 2010, NATO RTA: Paris, France. RTO-MP-IST-091.
- [26] R. Bruce, S. Dynes, H. Brechbuhl, et al., (2005), “International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues”, TNO report 33680, TNO, The Netherlands & Tuck School of Business/Center for Digital Strategies at Dartmouth, USA. Online: <http://www.ists.dartmouth.edu/library/158.pdf>
- [27] J. Lefebvre, M. Grégoire, L. Beaudoin, J. Tölle, P. Lagadec, L. Dandurand, H. Luijff, T. Parisi, G. Heaton, J. Sidoran, R. Hall, J. Caplan, R. McQuaid, W. Heinbockel (2013), “Coalition Network Defence Common Operational Picture (CNetD-COP)”, unpublished draft report NATO IST-081/RTG-039.
- [28] E. Luijff and J. Healey (2012), “Organisational Structures & Considerations”, in: A. Klimburg, *National Cyber Security Framework Manual*, NATO CCD-COE Publications. Online: <http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf>
- [29] NATO NCI Agency (2013), “Malware Information Sharing Platform”, Mons, Belgium. Online: <http://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20%28MISP%29.pdf>
- [30] World Economic Forum (2014), “Risk and Responsibility in a Hyperconnected World (WEF principles)”, Geneva, Switzerland. Online: <http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience>
- [31] World Economic Forum (2012), “Partnering for Cyber Resilience. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience”, Geneva, Switzerland. Online: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf



Standards (ISO, NIST, de facto)

- [32] **ISO/IEC 27010 (2012)**, “ISO/IEC 27010:2012: Information technology — Security techniques — Information security management for inter-sector and inter-organisational communications”, ISO, Geneva, Switzerland.
- [33] **C. Johnson, L. Badger, D. Waltermire (2014)**, “NIST SP 800-150 (draft): Guide to Cyber Threat Information Sharing”, NIST, Washington DC, USA.
- [34] Traffic Light Protocol. Online: http://en.wikipedia.org/wiki/Traffic_Light_Protocol
- [35] Trusted Introducer (TI). Online: <https://www.trusted-introducer.org>

National Resources

- [36] **Bundesregierung (2014)**, “Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)”, Berlin, Germany. Online: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile
- [37] Chatham House. Online: <http://www.chathamhouse.org.uk/about/chathamhouserule/>
- [38] Centre for the Protection of National Infrastructure (CPNI), United Kingdom. Online: <http://www.cpni.gov.uk/about/cni/>
- [39] **CPNI (2010)**, “CPNI information exchange membership guidelines”, London, United Kingdom. Online: <http://www.cpni.gov.uk>
- [40] **CPNI**, “Who we work with – Information Exchanges”, London, United Kingdom. Online: <http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/>
- [41] **GOV.UK**, 10 Steps: A Board Level Responsibility, CESG/CPNI, London, United Kingdom, 16 January 2015. Online: <https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-a-board-level-responsibility>
- [42] **N.N. (2014)**, “Belgian Cyber Security Guide: Protect Your Information”, Belgium. Online: <https://www.b-ccentre.be/wp-content/uploads/2014/04/B-CCENTRE-BCSG-EN.pdf>
- [43] **USA DHS (2002)**, “Critical Infrastructure Information Act”, Washington DC. Online: http://www.dhs.gov/sites/default/files/publications/CII-Act_508.pdf
- [44] Warning Advice and Reporting Point (WARP) – United Kingdom. Online: <http://www.warp.gov.uk/index.html>

Information Sharing Communities

- [45] Cyber security Information Sharing Partnership (CiSP). Online: <https://www.cert.gov.uk/cisp/>
- [46] Critical Infrastructure Warning Information Network (CIWIN). Online: <https://ciwin.europa.eu/Pages/Home.aspx>
- [47] European Government CERTs (EGC) group. Online: <http://www.egc-group.org/>



- [48] EuroSCSIE. Online: <https://espace.cern.ch/EuroSCSIE/default.aspx>
- [49] Financial Services ISAC website. Online: <https://www.fsisac.com>
- [50] FIRST. Online: <http://www.first.org/>
- [51] **MACCSA (2013), "Information Sharing Framework (ISF) Released 20 Nov 2013 (Version 2.4)",** United Kingdom. Online: <https://www.terena.org/mail-archives/refeds/pdfjJz1CRtYC4.pdf>
- [52] National Resilience Extranet (NRE). Online: <http://www.resilience-extranet.co.uk>
- [53] Project Griffin, London, United Kingdom. Online: <http://www.projectgriffin.org.uk/>
- [54] TF-CISRT. Online: <http://www.terena.org/activities/tf-csirt/>

Academic References and Research Organisations

- [55] **A. Brantz (2014), "Critical Infrastructure Protection and Antitrust Law",** in: *Infrastructure Resilience Risk Reporter*, Vol. 1, Issue 2 (December, 2014), Ottawa, Canada, pp. 16-19. Online: <http://carleton.ca/irrg/journal/>
- [56] **G. Bridgeman, R. Hulten, B. Danielsson, S. Nousula (2007), "European Risk Assessment Methodology – Good Practices in Information Sharing",** EURAM, Brussels, Belgium.
- [57] N. Brownlee, and E. Guttman (1998), "Expectations for Computer Security Incident Response", BCP 21, RFC 2350. Online: <http://www.rfc-editor.org/rfc/rfc2350.txt>
- [58] **CAIDA (2003), "Slammer worm propagation".** Online: <http://www.caida.org/publications/papers/2003/sapphire/sapphire.html>
- [59] E. Gall-Or, A. Ghose (2005), "The Economic Incentives for Sharing Security Information", in: *Inform* Vol. 16, No.2., pp. 186-208. Online: <http://pages.stern.nyu.edu/~aghose/ISR.pdf>
- [60] **C. Goodwin, J.P. Nicholas (2015), "A framework for cybersecurity information sharing and risk reduction",** Microsoft Corporation, USA. Online: <http://www.microsoft.com/en-us/download/confirmation.aspx?id=45516>
- [61] **W.H.M. Hafkamp (2008), "Proefschrift: Als alle informatie telt: een onderzoek naar kwetsbaarheden en incidentenresponse bij ICT-organisaties",** University of Amsterdam, The Netherlands. Online: <http://dare.uva.nl/>
- [62] **B. Hämmerli, N. Raaum, G. Franceschetti (2013), "Trust Networks among Human Beings: Analysis, Modeling, and Recommendations",** in: *F. Flammini, R. Setola, and G. Franceschetti (eds.), Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*, Taylor & Francis.
- [63] **N. Houston and C. Haynes (2011), "Cultural Aspects of Information Sharing and Collaboration",** in: *Militaire Spectator*, The Hague, The Netherlands, pp. 480-486.
- [64] **R. Lewis, P. Louvieris, P. Abbott, N. Clewley, K. Jones (2014), "CyberSecurity Information Sharing: A Framework for Information Security Management in UK SME Supply Chains",** in: proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv. Online: <http://ecis2014.eu/E-poster/files/0413-file1.pdf>

- [65] H.A.M. Luijff, M.H.A. Klaver, R. Wolthuis, et al. (2014), “Cross-sector Information Sharing”, TNO report 2014 R10945 (in Dutch), TNO, The Hague, The Netherlands.
- [66] P. Massart, A. Ghianda, S. Smith (2013), “Where Cyber Security is Heading”, Security & Defence Agenda (SDA), Brussels, Belgium. Online: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=159402>
- [67] M. Messenger (2008), “Why would I tell you? Perceived Influences for Disclosure Decisions by Senior Professionals in Inter Organisation Sharing Forums”, London, UK. Online: <http://collection.europarchive.org/tna/20141002130836/http://warp.gov.uk/downloads/Why-would-I-tell-you.pdf>
- [68] Roger B. Myerson (1991), “Game Theory: Analysis of Conflict”, Harvard University Press, USA.
- [69] NEISAS. Online: <http://www.neisas.eu>
- [70] B. Petrenj, E. Lettieri, and P. Trucco (2013), “Information sharing and collaboration for critical infrastructure resilience – a comprehensive review resilience on barriers and emerging capabilities”, in: *Int. J. Critical Infrastructures*, Vol. 9, No. 4, pp. 304-329.
- [71] Stewart D. Personick and Cynthia A. Patterson (2003), “Critical Information Infrastructure Protection and the Law: An Overview of Key Issues”, The National Academies Press, USA. Online: https://download.nap.edu/login.php?record_id=10685&page=http%3A%2F%2Fwww.nap.edu%2Fdownload.php%3Frecord_id%3D10685
- [72] K. Poulsen (2005), “U.S. Info-sharing Called a Flop”, in: Security Focus, 11 February 2005. Online: <http://www.securityfocus.com/news/10481>
- [73] Paul Rosenberg (2012), “Cybersecurity and Public Goods: The Public Private-Partnership”, Hoover Institution, Stanford University, USA. Online: http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf
- [74] L.L.J. Spijkervet, “Less is more. A theory driven research project to determine what collaboration design best supports the sharing of pragmatic cyber security related information between organisations.”, Thesis, TBM, Technical University of Delft, The Netherlands, February 2014. Online: http://www.tbm.tudelft.nl/fileadmin/Faculteit/TBM/Over_de_Faculteit/Afdelingen/Afdeling_Infrastructure_Systems_and_Services/Sectie_Informatie_en_Communicatie_Technologie/medewerkers/jan_van_den_berg/news/doc/Final-Msc-thesis-Bart-Spijkervet.pdf
- [75] D. Sutton, J. Harrison, S. Bologna, V. Rosato (2013), “The Contribution of NEISAS to EP3R” in: S. Bologna et al. (eds.): CRITIS 2011, LNCS 6983, Springer, Heidelberg, pp. 175–186, 2013. Online: http://link.springer.com/chapter/10.1007%2F978-3-642-41476-3_15
- [76] C. Tomkins (2001), “Interdependencies, trust and information in relationships, alliances and networks”, in: Accounting, Organizations and Society, pp. 161-191. Online: <http://www.sciencedirect.com/science/article/pii/S0361368200000180>



List of Abbreviations

BPVS	Beveiliging en Publieke Veiligheid Schiphol
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cyber Information Sharing Agreement
CISP	Cyber security Information Sharing Partnership
CISO	Chief Information Security Officer
CIWIN	Critical Infrastructure Warning Information Network
CPNI	Centre for the Protection of National Infrastructure (UK)
CSIRT	Computer Security Incident Response Team
EC	European Commission
EGC	European Government CERTs
EUCI	EU Classified Information
ECTF	Electronic Crimes Task Force
ENISA	European Union Agency for Network and Information Security
EuroSCSIE	European SCADA and Control Systems Information Exchange
FIU-Netherlands	Financial Intelligence Unit Netherlands
FoI(A)	Freedom of Information (Act)
FS-ISAC	Financial Services ISAC
ICT	Information and Communication Technologies
IP	Internet Protocol (suite)
IPR	Intellectual Property Rights
ISA	Information Sharing Agreement
ISAC	Information Sharing and Analysis Centre
ISAO	Information Sharing and Analysis Organisation
ISO	International Organization for Standardization ⁴
ICT	Information and Communication Technology
IT	Information Technology

⁴ note: ISO is not an abbreviation



MISP	Malware Information Sharing Platform
MSSP	Managed Security Service Provider
NATO	North Atlantic Treaty Organization
NDA	Non-Disclosure Agreements
NDN	National Detection Network (Netherlands)
NEISAS	National & European Information Sharing & Alerting System
NICC	National Infrastructure against Cybercrime
NIS	Network and Information Security
NISCC	(former) National Infrastructure Security Co-ordination Centre (UK)
NRE	National Resilience Extranet (UK)
NSIE	Network Security Information Exchange
PPP	Public-Private Partnership
SCADA	Supervisory Control And Data Acquisition
TICE	Trusted Information Communication Entity
TLP	Traffic Light Protocol
WARP	Warning, Advice and Reporting Point



Appendix A: Definitions used in the use case studies

Dimensions

Type of collaboration

The type of collaboration is a first denominator in describing the use cases in the terms of the overall idea of the collaboration. In this way there are three categories; a) the collaboration is a public initiative consisting of only public partners, b) the collaboration is a private initiative consisting of only private partners, or c) the initiative is a form of public-private cooperation and the partners in the collaboration consist of both public and private partners.

Level of participation

The average level of participation in a sharing community can be a person from a strategic, tactical or operational level in a stakeholder organisation.

Sector / cross-sector

This indicator shows whether the collaboration is constricted to one sector, is active in more than one sector or acts cross-sector.

Life-time

The duration of the collaboration is based on the life-time of the initiative measured in years.

Archetype level

A collaboration can be one of three kinds of archetypes in sharing information. In increasing levels of detail, archetypes are: sharing of trends (i.e., I have seen an increase in threat X), sharing of incident examples (i.e., I have experienced an incident considering threat X) and the sharing of data (i.e. see for you self).

Partner organisations involved

The number of partner organisations which is involved in the collaboration. Each partner organisation can have one or more persons involved in the sharing platform(s).



Characteristics

Organisational aspects

These aspects describe the organisational implementation of the initiative in terms of legal status and governance structure.

Technical aspects

Describing the (owners of) technical enablers which make information sharing between the partners within the collaboration technically possible.

Communication aspects

Aspects of the communication plans that the collaboration uses and the ownership of these plans. Who is the main communicator and originator of the collaboration?

Finance plan / funding

What is the finance plan behind the collaboration? How much financing is necessary, and if this is the case, who finances the collaboration?



Appendix B: Dutch national cyber security activities

A short overview on the governance of cyber security in the Netherlands [1]:

- The Cyber Security Council (Cyber Security Raad), established on July 9, 2012 acts as an independent public-private non-binding strategic advisory council to the Dutch Cabinet on the implementation and effect of the Dutch National Cyber Security Strategy (NCSS) [4].
- The Dutch Ministry of Security and Justice (V&J) is the coordinating ministry for cyber security. It is responsible for the development and maintenance of the NCSS [1].
- The Dutch National Cyber Security Centre (NCSC-NL) is part of the same ministry. Its tactical and operational tasks and services comprise [5]:
 - 24/7 response to cyber threats and incidents,
 - providing insight in cyber threats, trends and countering options at the strategic and tactical level,
 - cyber crisis management which falls apart in the operational coordination during the ICT-crisis for the nation and the NCSC-NL constituency, and an advisory role to the national crisis management structure. The public-private Incident Response Board (IRB) provides advice both to government and critical infrastructure operators during the crisis.
- The public-private collaboration platform function. In this platform, the own NCSC-NL assets and its liaisons with governmental agencies such as Team High-Tech Crime of the Dutch Police, the Intelligence and Security Service AIVD, and DefCERT, are linked to Information Sharing and Analysis Centres (ISAC) of the Dutch critical infrastructure sectors and other ICT-communities.

Next to the governance of cyber security, there is an active policy-cycle on cyber security in the Netherlands. This cycle is based on the following components:

- The NCSS [4] is a government-wide vision on cyber security and its governmental responsibilities and concrete actions.
- The Cyber Security Assessment Netherlands (CSBN) is a yearly update on trends and threats related to cyber security as well as an overview of the implementation of the vision laid down in the NCSS and evaluation of the responsibilities and concrete actions [3].
- Secondary in the cycle are documents aiming at shaping society based, scientific research needs. Documents such as the National Cyber Security Research Agenda II (NCSRA). This is a strategic document identifying the challenges in the cyber security domain. The NCSRA is a co-production by various scientific disciplines (computer science, law, criminology, psychology etc.) and knowledge institutes (TNO, NCSC-NL, WODC, NSCR, NFI) and experts in critical infrastructures.

Key to all of these activities and the underlying exchange of cyber security related information is collaboration through (public-private) partnerships.



Colophon



Oude Waalsdorperweg 63
2597 AK The Hague
Netherlands
<http://www.tno.nl>

Authors

Eric Luijff
Allard Kernkamp

eric.luijff@tno.nl
allard.kernkamp@tno.nl

With contributions by

- Rolf van Wegberg, TNO
- Meridian CIIP Community
(Meridian Coordinator – Peter Burnett)
www.meridianprocess.org

Contact information

National Cyber Security Centre
Dutch Ministry of Security and Justice

info@ncsc.nl

An electronic version of this document is available at <http://www.tno.nl/infosharing>



TNO

©TNO 2015

This document is generated for informational purpose only. The user is allowed to freely copy and/or distribute this document within the aforementioned purposes and provided the document and its contents remain in full and unchanged. Without TNO prior written consent it is prohibited to submit this document for any registration or legal purposes, advertising or negative publicity. Users are welcome to translate this document into a different language, provided they notify TNO beforehand and have received an explicit written consent. Unauthorised or improper use of this document or its content may breach intellectual property rights of TNO, for which you are responsible. Although TNO has exercised due care to ensure the correctness of the information as stated in the document, TNO expressly **disclaims any warranties on the contents. All content is provided "as is" and "as available".** Decisions which you take on the basis of this information will be at your own expense and risk.