

# Information nodes in the Dutch security sector

*Finding problems and opportunities when facilitating inter-organizational information exchange*

## Thesis

version 1.1 – November 16, 2012

Bas Diender (3171779)  
b.b.diender@students.uu.nl

Master Content and Knowledge Engineering  
Department of Information and Computing Sciences

Utrecht University

Supervisors:  
Robbert-Jan Beun (1<sup>st</sup> supervisor)  
Marijn Plomp (2<sup>nd</sup> supervisor)  
Tjitske Visser (supervisor PwC)



Universiteit Utrecht

# ***Table of Contents***

Summary .....	4
Acknowledgements.....	6
1 Introduction.....	7
1.1 Research Questions.....	8
1.2 Scope.....	9
1.3 Research setup .....	9
1.4 Relevance.....	10
1.4.1 Scientific relevance .....	10
1.4.2 Social relevance.....	11
2 What is an information node? .....	12
2.1 Context .....	13
2.1.1 Chain-computerization.....	13
2.1.2 Inter-Organizational Systems .....	14
2.1.3 Trust in inter-organizational relationships .....	15
2.1.4 Administration Theory .....	16
2.2 Characteristics of an information node .....	16
2.3 Other forms of inter-organizational collaboration .....	17
2.3.1 Comparison with joint chain body.....	17
2.3.2 Comparison with consortium.....	18
2.3.3 Comparison with Strategic Alliance.....	20
2.3.4 Comparison with shared service center.....	21
2.3.5 Comparison with extended enterprise .....	22
2.3.6 Comparison with Inter-Organizational Systems .....	22
2.3.7 Summary/conclusion .....	24
3 A model for analyzing information nodes.....	25
4 Research Approach.....	30
4.1 Selected cases .....	30
4.2 Analysis of the information nodes .....	32
4.2.1 Interviews.....	32
5 Comparison of the information nodes .....	35
5.1 Comparison .....	35
5.2 Relation to the chain-computerization theory .....	42
6 Lessons Learned .....	44
7 Conclusion / Discussion.....	54
7.1 Limitations and future research.....	56
8 References.....	57
Appendix 1 – Models for information sharing.....	60
Appendix 2 – The mission profile.....	62
Appendix 3 – interview questions .....	63
Appendix 4 – Factsheets .....	64

A4.1	CT Infobox .....	64
A4.1.1	General description of the information node.....	64
A4.1.2	Context of the information node.....	65
A4.1.3	Information node in context .....	65
A4.1.4	Lessons learned .....	68
A4.2	Financial Expertise Center (FEC) .....	70
A4.2.1	General description of the information node.....	70
A4.2.2	Context of the information node.....	71
A4.2.3	Information node in context .....	71
A4.2.4	Lessons learned: .....	74
A4.3	InformatieKnooppunt Cybercrime (IKC) .....	76
A4.3.1	General description of the information node.....	76
A4.3.2	Context of the information node.....	77
A4.3.3	Information node in context .....	78
A4.3.4	Lessons learned .....	80
A4.4	Maritiem Informatie Knooppunt (MIK).....	82
A4.4.1	General description of the information node.....	82
A4.4.2	Context of the information node.....	83
A4.4.3	Information node in context .....	84
A4.4.4	Lessons learned: .....	86
A4.5	Regionaal Informatie en Expertise Centrum (RIEC).....	88
A4.5.1	General description of the information node.....	88
A4.5.2	Context of the information node.....	90
A4.5.3	Information node in context .....	90
A4.5.4	Lessons learned: .....	94
A4.6	Centraal Informatiepunt Voetbalvandalisme (CIV) .....	96
A4.6.1	General description of the information node.....	96
A4.6.2	Context of the information node.....	96
A4.6.3	Information node in context .....	97
Appendix 5 – Abbreviations.....		101

# Summary

A seemingly new form of inter-organizational collaboration exists in the Dutch security sector, which we call an information node. This form of collaboration takes place in a complex environment and attempt to combat a unique problem. Because of this, there are differences in the way each information node operates. Because of this, each information node is created nearly from scratch and time and resources are lost reinventing the wheel. Knowledge from other information node could prove valuable to existing and new information nodes and can prevent them from making mistakes other information nodes have already found solutions for.

Based on literature on chain-computerization, Inter-Organizational Systems (IOS), Trust in inter-organizational relationships, and Administration theory as well as through discussions with experts in the field, a definition of an information node has been created:

*‘A formal, structured collaboration between a number of organizations within a **social chain**, which includes some form of **interpersonal contact**, that is focused on combating the **dominant chain problem** and that resolves around, but is not limited to, the **sharing of critical information**.’*

A social chain (Grijpink, 2010b) is a chain creating an immaterial social product, such as safety or security for the information nodes in this research. It does not share the linearity of a value/supply-chain as the subject can move back and forth between partners.

‘A dominant chain problem is one that none of the chain partners can solve on its own. It is only by effectively co-operating that chain partners can prevent the systematic failure of their own organization and the entire chain’ (Grijpink, 2010b, p. 30).

Critical information is the information required to be exchanged between participants in order to be able to effectively combat the dominant chain problem.

In addition to the definition, a list of aspects on which information nodes can differ has been identified. This list can be used to compare the information nodes directly. Table 1 shows this list of aspects and their categories.

**Table 1 -aspects of information nodes**

<b>Context</b>	<p>Using criteria following from the definition and a number of practical criteria, 5 information nodes were selected for further analysis. These are: the Maritiem Informatie Knooppunt (MIK), Regionale Informatie en Expertise Centra (RIEC), Financieel Expertise Centrum (FEC), Contra Terrorisme Infobox (CT Infobox), and InformatieKnooppunt Cybercrime (IKC).</p> <p>For each of the information nodes a factsheet has been created, filling in the aspects of an information node based on available documentation, interviews with the information nodes and experts, and discussions with experts. These also include a number of lessons learned for each of the information nodes.</p> <p>A direct comparison of the information nodes shows a number of aspects on which the information nodes can differ and two which show the largest variation. First, the way of collaborating within an information node can consist of daily collaboration, periodical meeting, or a combination of both. Second, the information that is shared by information nodes differs between the nodes from direct sharing of information between the participants to a black box construct which shares no information but merely gives out an advice.</p> <p>The strongest similarities are found in the reason for the creation of the information nodes. For all information nodes this was a government issued research which found a problem, indicating that political support is of importance for the success of an information node. Also, none of the information nodes researched here consists</p>
Chain	
<b>Node in context</b>	
Level of the chain process	
Position in the chain.	
Reason	
Scale	
Product	
<b>Collaboration</b>	
Forms of collaboration.	
Participating organizations	
Entry/exit barriers	
Trust	
<b>Information Sharing</b>	
How	
What	
Who	
<b>Support</b>	
Systems	
Integration	
<b>Preconditions</b>	
Finance	
Legal	
Information security	

of more than 10 primary partners.

As the creation of a blueprint for the perfect information node is impossible (Grijpink, 2010b; regarding solutions on the chain level, to which information nodes are related), a checklist of 19 lessons has been created through comparison, combination, and generalization of the lessons learned by the information nodes based on discussions with experts. Not all lessons are of equal importance and some lessons might not be relevant for some information nodes, but considering the options each lesson provides can help prevent problems. The checklist containing the lessons can be found in Table 2.

**Table 2 - checklist of lessons for information nodes**

<b>1</b>	The information node should have a clear goal to manage expectations.
<b>2</b>	Get operational soon, sort out the details later.
<b>3</b>	Take enough time for creating the information node, decision making in organizations can be slow.
<b>4</b>	Be persistent, when an approach fails, look for other options.
<b>5</b>	Without political and/or societal support an information node has little chance of success, create publicity.
<b>6</b>	Each node is unique, you cannot use a blueprint.
<b>7</b>	Participants should have the right qualifications.
<b>8</b>	Financing can be hard, it should be considered at the start of the information node and entails more than just the setup.
<b>9</b>	It is important to consider where to physically locate the information node.
<b>10</b>	Being legally able to share information is more important than a system for sharing this information.
<b>11</b>	Resistance against the creation on a personal and organizational level should be accounted for; people might fear for losing existing work.
<b>12</b>	Joining the information node should provide an advantage both for the node and for the participant
<b>13</b>	Trust is important, the information node can help it increases over time.
<b>14</b>	Clarify the tasks of the supervisors early on.
<b>15</b>	Specify the form of collaboration
<b>16</b>	All information should be shared formally, ensuring the origin of the information is clear and the information can be used.
<b>17</b>	All important partners should be present at all meetings.
<b>18</b>	In order to keep information richer, the employees of an information node should maintain sufficient knowledge of the organization they originate from.
<b>19</b>	Physical collaboration is important, it leads to richer information exchange.

These lessons can be used by practitioners during the creation and use of an information node to have some foothold when working in the complex environment in which information nodes exist.

## ***Acknowledgements***

This research has been performed at PwC and would not have been possible without the support of PwC and the guidance and support of its employees. PwC is the brand under which member firms of PricewaterhouseCoopers International limited (PwCIL) operate and provide services. PwC is a network of firms in 158 countries with close to 169,000 people. In the Netherlands, it consists of 4.600 employees working from 12 offices. PwC consists of four entities: Assurance, Tax & HRS (Human Resource Services), Advisory, and Compliance Services. This research has been performed at the Advisory entity, at the New Technologies & Security Group.

First and foremost thanks to my supervisor at PwC, Tjitske Visser, for the daily guidance and support, countless reads and useful feedback. Special thanks go to PwC colleagues Michael van de Velde for his input and support and to Ilja van Poppel and Manou Ali for their help and expertise.

My thanks go out to those involved with the information nodes who took the time and effort to see me for an interview; Edwin van der Pol of the MIK, Lou Mennens of the RIEC, Hans de Wit of the CT Infobox, Anita Reijnders and Martijn Snijder of the FEC, and Martin Visser of the IKC.

Also, I want to thank my supervisors Robbert-Jan Beun from the University of Utrecht and Marijn Plomp from the VU University Amsterdam for their guidance and feedback during the process of writing my thesis.

Finally, I want to thank Hannemarie van Manen for providing general feedback on my writing.

# 1 Introduction

The Dutch security sector contains a large number of organizations working on subjects that closely relate or overlap. These organizations are active in a number of social chains, chains in which organizations work to create an immaterial social product (Grijpink, 2010b). Because the organizations work on the same or closely related subjects, they could benefit from a formal collaboration with other organizations.

The nature of the social chains leads to organizations being mutually dependent of each other, with information critical for achieving the goal of the chain scattered throughout different organizations. Availability of this information is important, because decisions made using incorrect or incomplete information could have a life changing effect on those involved and could negatively affect the chain as a whole (Grijpink, 2010b). However, the sharing of information is complicated because of the sensitive nature of the information; strict rules and regulations -most regarding privacy- must be adhered to (Whitman & Mattord, 2011).

A report by the 'Adviescommissie Informatiestromen Veiligheid' (2007) indicates that the number of parties in the Dutch security sector that uses the available external sources is growing, creating a chaotic network of information flows. They concluded that parties in the security sector show insufficient collaboration regarding matters involving the gathering of information, regarding the sharing of existing information, and regarding the implementation of new technologies. They state that because of this, links between cases might not be made and chances in the fight against crime and terrorism might be missed. This indicates the necessity of formal collaboration between organizations.

The construct of organizations working together and sharing information in a formal and structured way, as has been identified for this research and can be found in numerous sectors, has not yet been well defined or researched in the field of social chains as defined by Grijpink (2010b). This research refers to this form of collaboration as an '*information node*' and uses the chain-computerization doctrine (Grijpink, 1997; 1999; 2009; 2010a; 2010b) as a basis to analyze what an information node is and how it relates to other forms of inter-organizational collaboration.

Chain-computerization theory looks at social chains, which also form the context of an information node. In addition, information nodes focus on combating a chain-wide problem, much like the chain-computerization theory combats the dominant chain problem.

It is expected that the activity in the area of information nodes will increase in the coming years; a number of new information nodes are planned or are being set up at this time. The government has shown willingness to invest in security and has shown interest in structural solutions on a large scale. Finally, it is expected that more collaborations and information nodes will emerge on a European/international level.

In practice it is often the case that each of these new inter-organizational collaborations or information nodes is created without all available knowledge of how earlier projects were set up. This makes it hard for practitioners to grasp the concept of an information node and to create a form of collaboration that is optimal for the specific case.

This research attempts to assist these practitioners by on the one hand creating a definition of an information node and placing it in the context of a chain and other forms of inter-organizational collaboration. On the other hand it identifies lessons learned during the creation of earlier nodes and links these lessons to characteristics of the information nodes. These lessons can then be used as a theoretical basis from which to create new information nodes.

This basis is not a guide to the perfect information node, because each chain and dominant chain problem are unique, requiring a unique approach, which makes it impossible to find a common ground for all information nodes (Pigmans, 2009). It is a theoretical framework containing options and possible pitfalls and opportunities that can arise when creating an information node.

This research has been commissioned by PwC, which is frequently involved as an advisor with the (further) development of information nodes. Examples of recent projects are the CT-Infobox(Contra Terrorisme-Infobox)<sup>1</sup> and the IKC(InformatieKnooppunt Cybercrime). PwC wants to take the knowledge gathered from the aforementioned projects and combine it with knowledge from other information nodes in the security sector.

---

<sup>1</sup> Because of the large number of abbreviations used in this research, mainly indicating organizations, a list of these abbreviations is provided in Appendix 5.

## 1.1 Research Questions

The main research question this research answers is:

*“What aspects should be taken into account when creating an information node and can earlier experiences in this field be used to create a checklist to support both the creation of new and the functioning of existing information nodes?”*

In order to answer this question the goal is to find a number of lessons learned experienced by information nodes in the Dutch security sector, which can then be used to create a checklist covering potential problems an information node could encounter. To be able to find these, the sub-questions that will be asked can be organized into three parts. To get an understanding of what an information node is and of the relation between information nodes and their context, the first sub-question is two-fold:

### *1.1 “What is an information node?”*

How can an information node be defined? How does an information node relate to a chain? How does it relate to other forms of organizations, for example a joint chain body as described by chain-computerization theory or a consortium? These questions are addressed in chapter 3.

### *1.2 “What are aspects of an information node?”*

This question identifies the aspects on which the different information nodes can be compared and is addressed in chapters 3.3 and 4.

Second, existing information nodes are analyzed. This is done to construct an overview of each of the nodes in a uniform format and to identify any problems that arose during the creation and existence of the information nodes.

The sub-question is:

### *2. “How are these aspects, found in sub-question 1.2, realized in each node?”*

An analysis of each of the selected nodes is performed, based on the aspects identified by the previous question. This is done in Table 13 in chapter 6.

This analysis is performed using both available documents on the information nodes and through conducting interviews. The interviews are used to verify and complete the information that has been found in the documents.

Thirdly, when a clear overview of each node and its contents has been constructed, the information gathered from the different nodes will be analyzed and compared in order to find what common elements and differences exist. For example, all nodes handle sensitive information and might have found similar solutions to do this in a legal and responsible way.

The sub-questions that are answered are therefore:

### *3. “What patterns can be found in the way the different nodes have been constructed?”*

Based on the aspects identified in sub-question 2 the nodes are compared in chapter 6, looking for patterns and differences between the information nodes.

### *4. “What lessons can be learned from the creation of earlier information nodes and how are these usable for the creation of new information nodes?”*

Through the interviews, lessons learned are identified, which apply to the node in which they are found. In order to possibly generalize these to other (new) nodes, these other nodes should be similar in respect to the aspect that was affected by the problem. Ideally, a lesson learned will be found in multiple nodes that show similarities in some aspects.

Sub-question 4 considers to which extent the lessons found in the interviews can be generalized to other nodes and to new nodes that are created. These lessons learned, together with the patterns



found in sub-question 3 can be used to create a checklist based on the lessons learned that are applicable to new and existing information nodes, thereby providing an answer to the main research question. The lessons learned can be found in chapter 7.

## 1.2 Scope

The research is of an explorative nature and limits its scope to information nodes in the Dutch security sector. This sector has been chosen because of the number of contacts that already exists with information nodes in this sector and the large amount of unique nodes. Furthermore, this research focuses on the creation of the information node itself. The rest of the chain will be taken into account to provide the context. However, it is not the goal of this research to test whether or not an information node should have been created in the first place. The research focuses on the creation of the node itself, not the process preceding this (such as societal feasibility and financial possibility).

## 1.3 Research setup

This research uses the case study method (Yin, 2003), shown in Figure 1.

**Develop theory** uses literature from two main fields of research; chain-computerization and the closely related Inter-Organizational Systems (IOS). In addition, some relevant literature from the administration theory is used. Some of the IOS literature can be used to describe the systems used for sharing information between the parties in an information node, forming a practical approach. IOS literature covers a broad range of topics, including the forms of inter-organizational collaboration discussed in Chapter 3.3, potentially including chain-computerization, focusing mainly on the systems used in the collaboration. The chain-computerization theory can be used to describe and create the best way to collaborate or share information, providing a more theoretical and broader view on how the collaboration within a chain should be organized. The administration theory literature is an addition to this, looking at the information nodes from a theoretical viewpoint which differs slightly from that of chain-computerization, providing useful models of inter organizational collaboration and noting the existence of entry and exit barriers. The literature from these fields is first used to create a definition of an information node, and second to identify aspects on which information nodes can differ. From these aspects a model is created, which is validated first by consulting experts in the field of information nodes and later through conducting the case studies.

The **data collection protocol** consists of a multiple case study design. It consists of the analysis of available documents on the information nodes first. Second, when available it includes interviews with experts which have been involved with the creation of information nodes and finally, interviews with people involved with information nodes at this time. Chapter 4 contains more information on the data collection protocol and on the **selected cases**. Chapter 5 contains the results of these **case studies** and the comparison between the information nodes.

The subsequent chapters contain the **cross-case conclusions** drawn from this and the **implications** this has for the theory. More detailed reports of the different case studies can be found in the appendices.

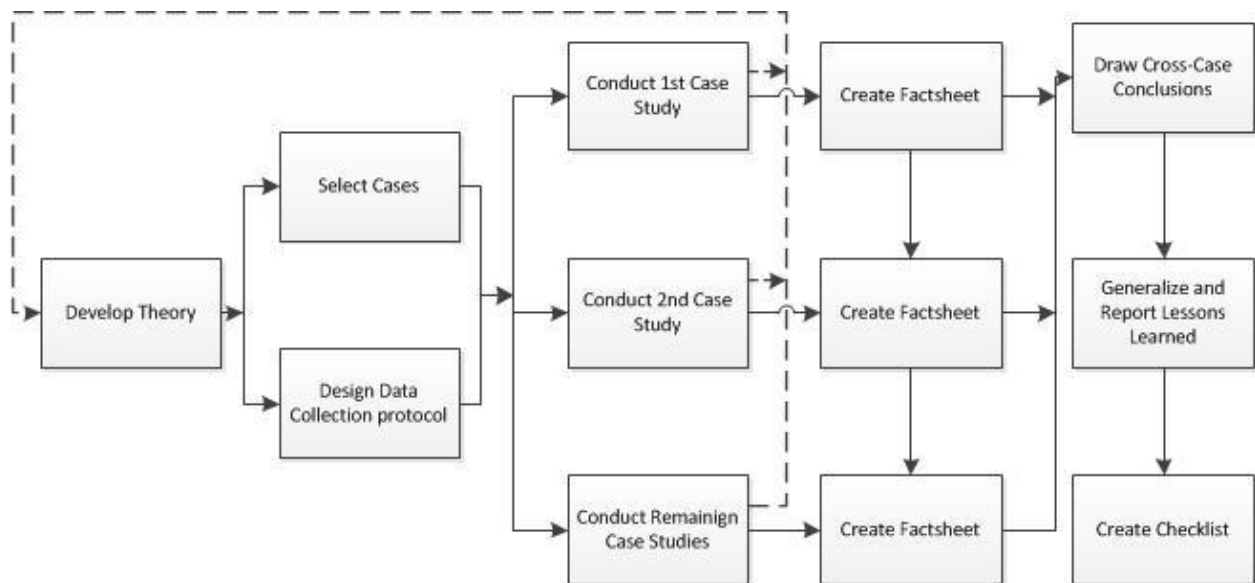


Figure 1 - Case Study Method (Adapted from Yin, 2003)

## 1.4 Relevance

### 1.4.1 Scientific relevance

This research is an addition to existing literature in two fields. On the one hand, literature exists on Inter-Organizational (Information) Systems (IOS). This literature focuses on how an organization can use information systems to improve the collaboration between it and its suppliers and its customers. The literature on IOS often looks at value/supply-chains, where it seems to be generally assumed that one organization in the supply chain is the most powerful and uses its position to force the smaller parties to adopt the system as well (for example: Barrett & Konsynski, 1982; Kumar & van Dissel, 1996; Boonstra, Boddy & Bell, 2008). In the end, the focus is often on improving the efficiency of the supply chain and, most importantly, staying competitive and increasing profits (Holland, 1995; Faerman, McCaffrey & Slyke, 2001).

Less research has been done on the use of IOS in social chains, creating immaterial, social products, and even less of this research focuses on networked IOS, which are the IOS that are active in environments similar to information nodes and social chains. This research will provide some more insight on the use of Inter-Organizational Systems in social chains, although it will not go into the technical details of these systems.

On the other hand, literature exists on chain-computerization (Grijpink, 1997; 1999; 2010a; 2010b). This research focuses on collaboration within social chains. It describes the problems with setting up such collaboration and the requirements for setting it up. This research will position an information node within a chain and therefore within the chain-computerization theory. In this respect it should be noted though that the nature of this research is not technical and the actual working of the information systems is not examined. The research considers the sharing of information and how information systems are involved on a higher level.

Besides forming an addition to these two related fields, this research examines a form of inter-organization collaboration of which no mention has been found in literature, but which does seem to relate to the IOS and chain-computerization literature. By researching information nodes, not only the position of an information node in relation to other inter organizational collaborations and theories is examined, but also the relation and applicability of the theory to information nodes. In this way, the research lays the foundation for expanding the chain-computerization theory beyond its original scope to include information nodes. Or to create a new theory derived from the chain-computerization theory which is applicable to information nodes.

### **1.4.2 Social relevance**

The creation and managing of information nodes or similar inter-organizational collaborations is currently often done largely from scratch without much reference material. Some other information nodes might be considered, but because of the unique nature of each information node, it is seldom possible to use aspects of existing information nodes directly and an analysis of multiple information nodes for each project is rarely feasible. This could lead to time and other resources being wasted on reinventing the wheel, possibly even a less effective wheel than has already been invented by other information nodes.

This research performs an analysis of a number of information nodes, extracting relevant aspects and experiences that are generalized to a checklist which can be used by other (new or existing) information nodes. This checklist enables practitioners to consider the aspects relevant for information nodes, while the research also contains information on how the aspects are realized in other existing information nodes. This leaves the required freedom to find a unique solution for each problem, but at the same time creates an overview of the points that require attention during the creation and use of an information node.

Using the checklist can save time and money which would else be used for analyzing existing nodes or wasted on avoidable mistakes. Both time and money have been found in this research to generally be in short supply when creating an information node.

## 2 What is an information node?

Although an information node is found in practice, it has not been analyzed or defined from theory. This chapter presents a definition of an information node from practice, followed by the theory from which this definition is derived.

The form and amount of inter-organizational collaboration differs for each chain, but some frequently occurring forms can be identified. Some collaboration exists of only a referral index, which indicates where information is located in the systems of the individual organizations, but does not provide this information itself. Organizations which seek this information can then approach the owner and request the information.

More involvement is required when the collaboration consists of structured and formal meetings, possibly accompanied by an information system, where on a periodical basis a number of representatives from the involved parties meet to discuss what action should be taken to face the issues at hand and what information is needed to do so. They can discuss what information should be shared and either share this information directly or use a shared system to share this information. An example of this is the 'InformatieKnooppunt Cybercrime' (IKC), which organizes formal meetings for organizations active in a specific sector to enable them to share critical information which can help protect them from cybercrime. These meetings happen structurally, not only to combat existing problems, but also to help prevent new problems. Within the IKC, information is shared between parties working together in the same chain or sector, but also between different chains (when the participants agree to this). The knowledge gathered by all chains can be used by the organizations that manage the collaboration (the AIVD, the Team High Tech Crime of the KLPD, and the National Cyber Security Centrum (NCSC)) to combat cybercrime on a higher level.

In other forms of collaboration, employees from the different organizations work together on a daily basis in a dedicated physical location. In that case each employee has access to its own systems, but they can request information from the information systems of the other participants. This collaboration happens for example at the Maritiem Informatie Knooppunt (MIK), where different organizations concerned with activity on the North Sea physically share information in a dedicated location which is then usable by the involved parties.

This research considers these last two forms to be examples of an information node, which is an existing but theoretically undefined form of inter-organizational collaboration. In this chapter the term information node is defined through literature research and by analyzing what are believed to be existing information nodes as well as by consulting experts with experience in this field. An information node is then compared to other forms of collaboration and to an organization in general. This comparison will test the definition, specifying it further by placing it in the context of other forms of (inter-organizational) collaboration. Also, it is a check to avoid redefining an existing concept. Finally, the similarities between an information node and the other forms of collaboration are used to create a theoretical framework for comparing information nodes in chapter 4.

In this research, an information node is defined as:

*'A formal, structured collaboration between a number of organizations within a **social chain**, which includes some form of **interpersonal contact**, that is focused on combating the **dominant chain problem** and that resolves around, but is not limited to, the **sharing of critical information**.'*

The interpersonal contact and sharing of information should happen on the same level as where the information is used. When the information is practical, it should be exchanged and used by practitioners. When the information is strategic, it should be shared and used by the policy makers.

This definition is derived from theories on a number of subjects; chain-computerization, Inter-organizational Systems (IOS), trust in inter-organizational relationships, and Administration Theory. The concept of a social chain and the existence of a dominant chain problem origin in the chain-computerization theory. The focus on the sharing of information follows from the chain-computerization theory and the theory on inter-organizational systems (IOS). The requirement of interpersonal contact follows partly from the literature on IOS and partly from observing existing nodes.

In addition to explaining the origins of the definition, literature is also used to identify aspects of information nodes. These aspects can differ between information nodes and form a ground on which to compare different nodes which will be elaborated on in chapter 4.

## **2.1 Context**

### **2.1.1 Chain-computerization**

A social chain is a chain in which a number of organizations work together to create an immaterial social product (Grijpink, 2010b), such as safety or social security (Venrooy & Sonnenschein, 2008). In a social chain, the information and goods don't follow a straight line through the chain. Instead the subject moves through the chain back and forth between the different parties, with some coordination through process steps that create deliverables such as reports. This is because the immaterial product the chain produces can only be created by working together and sharing information. A social chain differs from a traditional value/supply-chain where suppliers, producers and customers work together to create a physical product. This difference shows both in the way the organizations collaborate and in the way products or information move through the chain, which for a value/supply-chain is in a fairly linear fashion from raw material to final product. In such a chain, communication and collaboration focuses often on automation existing tasks. The communication happens between the customer(s) and the supplier(s), usually in a one-to-one or one-to-many relationship (Chi & Holsapple, 2009) as opposed to many-to-many relationships which are more common in a social chain. Chain-computerization can be used to analyze such a social chain and the collaborations that are used in a social chain. In this research chain-computerization theory can be used to analyze the context in which the information node exists (Grijpink, 2010b). To visualize the difference between social chains and value/supply-chains, Table 3 shows a number of interdependencies. A (standard) value-supply chain can be considered to have sequential interdependency, where parties in a social chain are (for the most part) reciprocally interdependent.

Chain-computerization theory has as its main goal to identify and combat a dominant chain problem. 'A dominant chain problem is one that none of the chain partners can solve on its own. It is only by effectively co-operating that chain partners can prevent the systematic failure of their own organization and the entire chain' (Grijpink, 2010b, p. 30). Important to note is that problems like lack of efficiency or insufficient sharing of information in itself are not dominant chain problems, they can lay at the core of a dominant chain problem and are therefore often the key to combating the dominant chain problem, but are in itself not severe enough to act upon. Over time, a dominant chain problem could change, for example because criminals use different methods when the actions performed to combat the dominant chain problem are effective. This means that the solution created to combat the dominant chain problem should adapt to this.

An example of a dominant chain problem are the avoidable mistakes made by medical practitioners leading to injury or death of patients. This potentially leads to the entire chain being discredited and could do damage to the image of all organizations involved. By improving the exchange of information, the problem might be countered.

There are three components in the way chain-computerization looks at a chain, the so-called chain perspective.

First, it assumes that there is irrationality within the chain. Even though each partner in the chain can be expected to act in a way that is rational from their point of view, it might not be the best course of action for the chain and might therefore be irrational when looking from the chain perspective.

Secondly, as mentioned before, the dominant chain problem has a major impact on the chain to the extent that it 'runs' the chain, greatly influencing the actions of the parties involved.

Finally, chain-computerization makes a distinction between the chain level and the base level of a chain. The chain level is the level where the actions of different chain partners are coordinated and where chain-wide systems are located. The base level of a chain is where the actual chain activities happen within and between organizations, activities that do not involve all parties involved with the chain (Grijpink, 2010b).

According to chain-computerization theory, a chain-wide solution can exist on one or more of three levels of the chain process; support, primary process, or policy, where activity on the higher levels also implies activity on the levels beneath it (Horstink, 2009).

A support-level solution only helps with tasks that are not part of the core activities of the chain, for example the emergency services control room which, although important, has little to do with the actual solving of crime or firefighting. Primary process solutions actually support the core processes within the chain, for example by providing a firefighter with information about potential dangers in a burning building. A solution on the policy level means that the future actions of the parties involved with the chain are coordinated through the joint chain body.

As can be imagined, a 'support' solution is easier to implement than a 'policy' solution since a solution on the policy level is often feared to "(...) *adversely affect the institutional autonomy of a participating organization*" (Grijpink, 2010b, p.20). Because an information node exists in a social chain, it should be active on one or more of these levels.

So, according to the chain-computerization theory, any collaboration within a chain can only be successful if there is sufficient need, this need comes in the form of a dominant chain problem. This means that the reason for creating an information node should be to combat the dominant chain problem. An information node is created to be a structural solution without a predefined duration. It should combat the dominant chain problem and does this by facilitating the sharing of information which often leads to more active collaboration. Although it will usually have an initial running time after which it will be evaluated, it is designed to in itself be a solution to manage the dominant chain problem and is designed to exist as long as the dominant chain problem exists, or would exist without the information node. If the dominant chain problem changes or shifts over time the information node should adapt.

Since an information node exists in the context of a social chain and chain-computerization can be used to analyze a social chain, chain-computerization can be used to describe the context of an information node. As for the definition of an information node, it means that it should exist in a social chain and should have as its goal to combat the dominant chain problem. Also, it should resolve around the sharing of information and, because it is active on the chain level, involve multiple organizations.

In addition, aspects of an information node that follow from the theory on chain-computerization are the context (the surrounding node), the level of the chain process it is active on, and the reason for starting the node (which should be the dominant chain problem).

### **2.1.2 Inter-Organizational Systems**

Besides the theory on chain-computerization, there is another field of research that is relevant for information nodes; Inter-Organizational Systems (IOS). An IOS is an information system that enables information flow between different organizations, facilitating the easy and automated sharing of information between parties (Hong, 2002; Chi & Holsapple, 2005; Kumar & Crook, 1999; Meier, 1995; Boonstra & de Vries, 2005). The usefulness or perhaps even necessity of IOS has been acknowledged by a number of researchers (Chi & Holsapple, 2005; Ahuja, 2000). For example, Ahuja found that the number of ties to other organizations that exist has a positive impact on innovation. This seems also to be true for information nodes; when more parties are involved, more information can be shared and better solutions can be created, provided that this information is shared in a proper way and that the extra parties own new information or perform critical tasks. For information nodes this would mean that it should be more effective when it includes a larger part of the chain.

Some research has been done on Networked IOS (Chi & Holsapple, 2005; Kumar & van Dissel, 1996) which are active in environments that show similarities with the social chains this research looks at. Kumar & van Dissel map the different types of IOS to the interdependency types defined by Thompson in 1967. These types can be found in Table 3. It shows that an information node seems to contain reciprocal interdependency, where a Networked IOS could be used. Information nodes could therefore use networked IOS.

Volkoff, Chan, & Newson (1999) come even closer to a type of IOS that seems to be applicable to information nodes by describing what they call collaborative IOS. This has greater similarities to the chain-computerization theory because it is a networked IOS which is built to support collaboration and cooperation with no obvious focal point for leadership. This leads them to be built cooperatively. The biggest thing keeping collaborative IOS from being directly applicable to information nodes is the lack of focus on the dominant chain problem.

More specifically aimed at chains than the model by Kumar and van Dissel are the models by van Duivenboden, Heemskerck, Luitjens & Meijer (2005), originating from administration theory. They provide five models for information exchange within a chain that show similarities with a more elaborate classification of the types of interdependency identified before. These five models are shown and explained in Appendix 1.

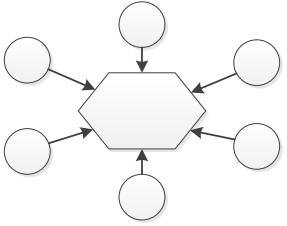
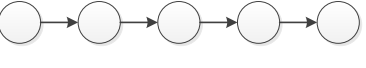
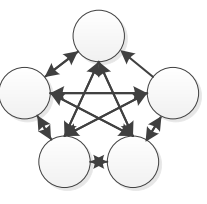
The models show that the sharing of information between partners in a chain can happen on different levels of intensity, ranging from unstructured and non-intrusive (the prosthesis approach) to integrated and potentially game-changing (the network approach).

The more integrated the information sharing is, the more it influences the organizations and the harder it is to realize. The prosthesis approach is easier to implement than the other approaches and the network approach is the hardest because it requires the biggest commitment from the involved parties.

When information is exchanged between parties, only information that is crucial for the goal of the information sharing should be shared (Grijpink, 2010b). Also, integration of the information systems of different organizations might sound like a good way to improve the sharing of information, but it encounters a lot of resistance from the organizations (Homburg & Bekkers, 2005). A less intrusive way to share the required information would be better, for example a referral index that shows where information can be found without giving direct access to this information, leaving organizations with some control over what they share. (Grijpink, 2010b)

Although some of the research on IOS is relevant for information nodes, it covers only some aspects of an information node, it should be combined with some interpersonal contact. For information nodes it is relevant to analyze how the information is shared, what systems are used to share the information, and how these systems are linked to the systems of the individual organizations. Also, it should be considered what information is shared, and if all this information is critical for combating the dominant chain problem.

**Table 3 - Interdependence, Structure, and potential for Conflict (Adapted from Kumar & van Dissel, 1996, table 1, p.287; based on Thompson, 1967)**

<b>Type of interdependence</b>	<b>Pooled Interdependency</b>	<b>Sequential Interdependency</b>	<b>Reciprocal Interdependency</b>
<u>Configuration</u>			
<u>Potential for Conflict</u>	Low	Medium	High
<u>Type of IOS</u>	Pooled Information Resource IOS	Value/Supply-Chain IOS	Networked IOS

### **2.1.3 Trust in inter-organizational relationships**

Another important area of research, closely related to IOS, regards the importance of trust when establishing inter-organizational relationships (Karahannas & Jones, 1999; Meier, 1995; Monczka, Petersen, Handfield & Ragatz, 1998; Premkumar, 2000; Chi & Holsapple, 2005; Hart & Saunders, 1997; Cousins, 2002; Homburg & Bekkers, 2005; Zaheer, McEvily, & Perrone, 1998). When organizations are comfortable with the people or organizations they do business with and they trust that they are treated fairly, they are more willing to share valuable information, thereby improving the success of the relationship. This is also true for information nodes and is explicitly named as an important factor for the success of the 'InformatieKnooppunt Cybercrime' (IKC).

Trust is not limited to the people involved. It also includes trust in the control systems that are used to share the information (Tan & Thoen, 2000). If trust between two or more parties is insufficient to establish a good relationship, this can be compensated by having a sufficiently trusted control system. If there is enough trust, however there is no need for strong control systems. Tan and Thoen refer to this as 'Party trust' and 'Control trust'. Both forms of trust have objective (such as certificates) and subjective (such as personal experience) reasons. As long as the total amount of trust –both party trust and control trust combined- for a certain relation rises above the trust threshold, there is enough trust to collaborate effectively. Unfortunately, there is no way to put a number on trust or the systems without studying the specific situation extensively. This means that it will be up to the judgment of the creator of the information node whether or not there is enough trust to function properly.

This is relevant for information nodes, because a lack of trust leads to reluctance to share information which might undermine the success of an information node.

### **2.1.4 Administration Theory**

Literature in the field of administration provides some insights that fit the chain-computerization theory and have been addressed earlier (Homburg & Bekkers, 2005; van Duivenboden et al., 2005), but also some that fit an own category. Eisenhardt and Schoonhoven (1996) name the existence of entry- and exit barriers; what rules do organizations have to adhere to in order to join the collaboration and can organizations leave the collaboration at any time, or do they have to meet certain conditions (i.e. only when the collaboration has its annual evaluation, or when certain goals have been reached). This also applies to information nodes, since they do not necessarily include all parties active in the chain.

In addition, it should be considered whether all parties have access to all shared information or if information can be shared with a select number of parties. In the definition, this leads to the emphasis on information sharing.

## **2.2 Characteristics of an information node**

In addition to the characteristics found in literature and described before, analysis of existing information nodes that have been identified by experts experienced in this field and discussions with these experts led to a number of additional characteristics. These characteristics are that not all parties that are involved in a chain have to be active in an information node and that an information node does not have to span the entire chain. For example, an information node consisting of a physical office where employees from different organizations collaborate and share information could only contain the three major parties within a chain who then share the relevant information with other organizations in the chain on the ground level of the chain when necessary. Also, such an information node could exist in one or a number of process steps, it does not necessarily span the entire chain, but the node will affect the rest of the chain as well. It was also found that, in addition to facilitating the sharing of information, it is possible that an information node performs tasks itself, for example by managing a taskforce that coordinates projects.

This has led to the following characteristics of an information node:

- It should be looked at in the context of a chain. (chain-computerization)
  - Active in social chain.
- The focus is on the dominant chain problem. (chain-computerization)
- It functions on both the chain level (chain-computerization) and on the base level of the chain (experts/existing nodes)
- Multiple organizations are involved (more than two). (chain-computerization)
- It is designed to be active for as long as necessary; the duration is indefinite. (chain-computerization, existing nodes)
- It facilitates sharing of information critical for combating the dominant chain problem and collaboration. It possibly performs actions itself. (chain-computerization; administration theory; IOS; existing nodes)
- It is functional either in the entire chain or in a number of process steps. (experts/existing nodes)



- There is some form of structural interpersonal contact. (IOS, existing nodes)

These characteristics have led to the definition shown earlier in this chapter.

## **2.3 Other forms of inter-organizational collaboration**

The characteristics of an information node will be used to compare an information node to other forms of collaboration bodies. The goal of this comparison is to further clarify the aspects that distinguish an information node from other forms of collaboration, to see on which aspects other forms of collaboration are similar (potentially providing relevant literature), and to avoid redefining an existing concept. Following from the similarities with other forms of inter-organizational collaboration, some literature on these other collaboration forms could be useful when creating a theoretical framework for information nodes. These specific forms of collaboration have been selected because they were encountered in literature (for example, Todeva & Knoke, 2005) and at first sight seem to have similarities with information nodes.

As an organization can be defined as any collaboration with some form of structure, an information node can be considered to be a form of organization. This, however, is true for all inter-organizational collaboration discussed here and because of this it is not discussed further.

The legend for the comparison can be found in Table 4. If a characteristic of an information node is considered characteristic for the form of collaboration it is compared with, this means that this characteristic is always applicable to this form of collaboration. When it is not-characteristic it differs from an information node. When it is possible it might show the characteristic of an information node, but it could also take other values.

### **2.3.1 Comparison with joint chain body**

A joint chain body is a solution on the chain level (Grijpink, 2010b). This means that it is owned by the chain as a whole, instead of by one of the involved organizations. For example by forming a third party consisting of employees from the different organizations. This differs from a solution on the base level of the chain where actual interaction between two (or more) organizations takes place directly. This is for example where the internal information systems of organizations are located, the chain level contains the chain information systems such as a referral registry.

Since, like a joint chain body, an information node is considered as a part of a social chain, it is possible that it is a form of a joint chain body. A joint chain body is a body created by partners in a chain that operates separate from the partners in the chain. It exists to support the partners in combating the dominant chain problem, for example by providing a means to share information or by providing advice.

A joint chain body is also considered in the context of a social chain, since it originates from the chain-computerization theory. It is an independent organ, controlled by all parties in the chain. Its focus is on the dominant chain problem, which it combats for an undefined duration, and it functions on the chain level. It also involves a number of organizations; according to the theory, it is only considered to be a joint chain body if a substantial part of the involved chain partners participates in the form of collaboration at this scale (Horstink, 2009). However, this is also where it differs slightly from an information node, since an information node can exist either in the entire chain, only a number of process steps, or just one process step.

If an information node exists in only part of the chain, it might be that less than a substantial part of the involved chain partners participate and it cannot be called a joint chain body. Finally, the form and functionality of a joint chain body is not clearly defined in the theory and is dependent on the level of the chain process on which it exists. Therefore, even though it is clear that a joint chain body facilitates information sharing, the literature is unclear on whether or not it can facilitate more practical collaboration.

Another point where an information node might differ from a joint chain body is in what information they share. According to chain-computerization theory, only information that is critical for combating the dominant chain problem should be shared. It is unclear if information nodes adhere to this, it is part of this research to clarify this.

**Table 4 - Legend**

✓	Characteristic
✗	Not-characteristic
-	Possible

**Table 5 - comparison joint chain body with information node**

<b>Information Node</b>	<b>Joint Chain Body</b>	
It should be looked at in the context of a chain	✓	Originating from the chain-computerization theory, it is part of a chain
The focus is on the dominant chain problem	✓	The goal of a joint chain body is to combat the dominant chain problem
It facilitates sharing of information and collaboration, possibly performs actions itself.	-	It facilitates collaboration in the form of information sharing and collaboration, but it is unclear if it can perform actions itself.
It functions on both the chain level and the base level of the chain	✗	A joint chain body is governed independent of the individual organizations
It is functional either in the entire chain or in a number of process steps.	✗	A joint chain body always covers the entire chain; it cannot be active in just a number of process steps.
Multiple organizations are involved (>2)	✓	A joint chain body covers the entire chain which consists of more than two organizations
Active in social chain	✓	Since it is part of chain-computerization theory it is active in a social chain
Designed to be active for as long as necessary	✓	It will combat the dominant chain problem for as long as it exists and can adapt if the problem changes
Structural interpersonal contact	✓	The body is characterized by being a separate organization consisting of employees working together.

As can be seen in Table 5, a joint chain body shares the majority of the characteristics of an information node that have been identified. This is not surprising because a joint chain body originates from the chain-computerization doctrine which is also the core theory used for defining an information node.

Following from the table it could be stated that an information node is a more general form of a joint chain body. An information node can focus on part of the chain instead of the chain as a whole and a joint chain body might not perform tasks itself, but it supports collaboration by facilitating sharing of information and planning on a higher level. The biggest difference, however is that an information node functions on both the chain level and the base level of the chain, where a joint chain body functions only on the chain level.

The similarities indicate that part of the chain-computerization theory, which is applicable to a joint chain body, is applicable to information nodes as well.

### **2.3.2 Comparison with consortium**

A consortium is a collaboration between a number of organizations to reach a certain goal. It can for example be set up to create a new standard (Updegrave, 1995) or to support collaboration between academic institutions (Baus & Ramsbottom, 1999). A consortium can either have a clear goal that requires a single solution, such as the creation of a new standard, or a goal that is less concrete and that requires it to be active for a undefined duration, such as a collaboration between academic institutions, where the goal is to optimally use resources and save money.

This form of inter-organizational collaboration has, at first sight, similarities with an information node mainly because there is structural contact between the participants. However, there is no

dominant chain problem and the focus is on collaboration to achieve optimal results instead of information sharing. A consortium is created to either solve a problem that is not important enough according to chain-computerization theory (such as efficiency, costs, profits, or information sharing; Grijpink, 2010b), or to take advantage of an opportunity which, according to chain-computerization theory, is not enough reason to collaborate within a chain. There is no reason to assume that consortia operate on the chain level, since the consortia are run directly by the different parties involved and not on a higher level. Even though a consortium is owned by the participating parties, the shares do not have to be equal and it is possible for one party to ‘run’ the consortium because they are the largest stakeholder.

An example of a consortium, the ‘Living Lab Veiligheid’ (LLV) has been created to be an experimental area for innovative products, services and concepts with regards to social security.<sup>2</sup>

This consortium does exist in a chain, the social security chain, and is viewed in the context of a chain to set up the LLV as a usable entity for all parties involved, but it does not combat a dominant chain problem.

Comparing the LLV to other consortia shows some differences, for example the goal of a consortium creating a standard is more clearly defined. The LLV will exist for as long as the participating parties deem necessary, while a consortium for setting a standard will be terminated after the standard has been created. So although some consortia can be of an undefined duration, it cannot be said that all consortia are, which differs from an information node.

**Table 6 - comparison consortium with information node**

<b>Information Node</b>	<b>Consortium</b>	
It should be looked at in the context of a chain	-	A consortium can consider the chain as its context, but it might only look at the problem it was created for and ignore the context.
The focus is on the dominant chain problem	✗	A consortium will focus on something that could potentially be a dominant chain problem, but just as likely a lesser problem or an opportunity.
It facilitates sharing of information and collaboration, possibly performs actions itself.	-	The focus of a consortium is on collaboration to achieve the optimal results instead of sharing information, but the sharing of information can be part of a consortium. In larger consortia it is possible for the consortium to perform tasks independent of the participants.
It functions on both the chain level and the base level of the chain	✗	It is possible for one party to control and guide the consortium.
It is functional either in the entire chain or in a number of process steps.	-	When a consortium uses a chain as its context it can span any part of that chain.
Multiple organizations are involved (>2)	✗	A consortium is a collaboration of two or more organizations.
Active in social chain	-	It is possible for a consortium to be active in a social chain, but it could also be used in a value/supply-chain, for example to create a new product or standard.
Designed to be active for as long as necessary	-	Some consortia can have a undefined duration, but others have a clear goal such as creating a standard.
Structural interpersonal contact	✓	The participants work together physically to reach the desired goal.

As can be seen in Table 6, despite the similarities at first sight, the way a consortium works differs from an information node. It should be noted that it is possible for a consortium to be considered in the context of a chain and to be designed to be permanent. Also, some consortia are active in social

<sup>2</sup> <http://www.livinglabveiligheid.nl/wat-is-het-llv/living-lab-veiligheid>

chains. However, these are not characteristics that apply to all consortia, so they are checked as possible characteristics in the table.

When the consortium creates a new legal entity to which all participants contribute, it is often referred to as a joint venture. A joint venture is generally not designed to be permanent and is created to achieve a clear, usually commercial goal. It is similar to a consortium on the other aspects that are relevant here, so it will not be discussed in greater detail.

### 2.3.3 Comparison with Strategic Alliance

According to Devlin & Bleackley (1988) strategic alliances regard the long-term strategic plans and are aimed at dramatically changing a organization’s competitive position. A strategic alliance is designed to be active for as long the involved parties see its value.

For a strategic alliance, the focus is on improving the competitive position, where for information nodes the goal is to solve the dominant chain problem (which might ultimately lead to an increase in profit, but this is not the goal). Both an information node and a strategic alliance include collaboration between organizations to achieve goals that a single organization is unable to achieve. However, a strategic alliance exists between two organizations, not between a number of organizations within a chain like an information node (Baker, Gibbons, & Murphy, 2008; Lorange, Roos & Brønn, 1992). This also means that a strategic alliance is not considered in the context of a chain, but only between the two involved organizations.

Dyer, Kale & Singh (2001) reported that the top 500 global businesses had an average of 60 major strategic alliances each. This large number of strategic alliances that one business is involved in suggests that the contact and sharing of information is less intense than in an information node.

Because of the focus on increasing the competitive position of the organization and the assumption that the partner has the same goal for its own organization there is little trust. Both parties will do what is best for their own organization. Parkhe (1993) argues that, in accordance with game theory, each party in the collaboration should perceive direct benefit from the collaboration, which is also concluded by Whipple & Frankel (2000). This also means that a strategic alliance isn’t permanent, since each organization has its own goals and will pursue them. When the alliance doesn’t give them the advantage they want, it can be terminated. The strategic alliance isn’t independent of the participants, both parties will attempt to get the maximum amount of profit from it and will try to control the alliance.

Strategic alliances are made to collaborate and share knowledge, so in this aspect they are similar to information nodes. However, because there is often a lack of trust the sharing of information happens in a less open way.

**Table 7 - comparison strategic alliance with information node**

<b>Information Node</b>	<b>Strategic Alliance</b>	
It should be looked at in the context of a chain	✘	A strategic alliance happens between two organizations and does not consider the chain.
The focus is on the dominant chain problem	✘	A strategic alliance is about improving the competitive position and increasing results.
It facilitates sharing of information and collaboration, possibly performs actions itself.	-	Knowledge is shared between partners in a strategic alliance. It could facilitate some collaboration, but since it does not exist as a separate body, it cannot perform actions itself.
It functions on both the chain level and the base level of the chain	✘	A strategic alliance happens on the ground level between two organizations.
It is functional either in the entire chain or in a number of process steps.	✘	It only happens between two organizations.
Multiple organizations are involved (>2)	✘	Two organizations are involved.
Active in social chain	✘	A strategic alliance is aimed at increasing profit and is active in a value/supply-chain.
Designed to be active for as long as necessary	✓	It exists for as long as both parties see its use and can be terminated at any time.

Structural interpersonal contact	✓	There is structural contact between the two organizations.
----------------------------------	---	--

Table 7 also shows this. Apart from the facilitation of both collaboration and information sharing (although it cannot perform tasks itself), and the undefined duration, a strategic alliance does not show similarities to an information node.

### 2.3.4 Comparison with shared service center

A shared service center (SSC) is a semi-autonomous unit within an organization or between multiple organizations that is used to bundle activities and perform services for the units involved. It performs tasks that each of the participating units would else do themselves and that are not critical for the operations of the units (Mechling, 2007). An SSC can exist either within an organization, where the different departments let some tasks be performed by the SSC, or between multiple organizations, where different organization that perform the same tasks let these tasks be performed by the SSC to increase efficiency (Janssen & Joha, 2006).

An SSC is designed to be active for an undefined duration, performing the tasks for the involved units until these tasks might become obsolete. Also, it is possible for an SSC to be active in a social chain and to include any number of organizations (even just one if it is an internal organ supporting departments).

The tasks performed by an SSC are performed on the ground level of the chain and often within one process step. The chain is not considered as a context. Also, the focus is on efficiency and while lack of efficiency can be a problem, it is not a dominant chain problem (Grijpink, 2010b). As stated before, the goal of the SSC is to perform certain tasks more efficiently; there is no sharing of information involved. The SSC is active within one process step at most and even then it does not have to cover all organizations that perform this step as it can exist within one organization.

A shared service center is often set up by one of the participants and later expanded to support the collaboration. Because of this it will start off as part of one of the participants, but it might become an independent organ over time.

**Table 8 - comparison shared service center with information node**

Information Node		Shared Service Center
It should be looked at in the context of a chain	✗	An SSC often exists within one organization and is later (possibly) expanded to facilitate multiple organizations. Also, because it only performs one action it is not relevant for all parties in a chain.
The focus is on the dominant chain problem	✗	The focus is on lowering costs by performing an action in a uniform way for all participants.
It facilitates sharing of information and collaboration, possibly performs actions itself.	✗	It only facilitates some collaboration, if any.
It functions on both the chain level and the base level of the chain	✗	It functions on the ground level, often even within one organization and is (at least at its start) controlled by this organization.
It is functional either in the entire chain or in a number of process steps.	✗	It is often not functional in a chain, since it does not use the chain perspective and can be active within an organization.
Multiple organizations are involved (>2)	-	It is possible for multiple organizations to be involved, but it can also be two or only one organization.
Active in social chain	-	An SSC could exist in both a value/supply-chain and in a social chain.
Designed to be active for as long as necessary	✓	It is designed to exist until the task it performs might become obsolete.
Structural interpersonal contact	-	The SSC can be used as a simple black box, which creates a product; no interpersonal contact is required as long as it works.

Although a shared service center could be used in a social chain and can possibly be used to support an information node when there is enough trust between participants, it differs from an information node. Table 8 shows this, with only the (potentially) permanent nature as common characteristic.

### 2.3.5 Comparison with extended enterprise

The term extended enterprise was first used at Chrysler Corporation to indicate the information exchange and cost reduction practices within the supply chain (Post, Preston & Sachs, 2002). This indicates that an extended enterprise exists in the context of a chain and that it includes either the entire chain or a number of process steps. Ideally it covers the entire chain to achieve optimal results, but this is not a requirement. Also, it includes multiple organizations and is active for as long as necessary.

However, there is no focus on the dominant chain problem and although it considers the chain, it is usually initiated from one organization in the chain, preventing it from operating on the chain level because this organization forms the basis of the extended enterprise and controls it. An extended Enterprise exists only in value/supply-chains and not in social chains (Jagdev & Browne, 1998). Structural interpersonal contact is possible, but it could also perform mainly through computer systems.

An extended enterprise facilitates both the sharing of information and collaboration, with the focus on the sharing of information for example regarding the stock of a supplier.

**Table 9 - comparison extended enterprise with information node**

<b>Information Node</b>	<b>Extended Enterprise</b>	
It should be looked at in the context of a chain	✓	An extended enterprise is active within a chain, since it is an organization that collaborates with its chain partners.
The focus is on the dominant chain problem	✗	The focus is on improving efficiency and cutting costs.
It facilitates sharing of information and collaboration, possibly performs actions itself.	-	The focus is on sharing information with suppliers and customers. Since it doesn't exist as a separate body, it cannot perform actions itself.
It functions on both the chain level and the base level of the chain	✗	It is set up by one organization and runs on the ground level between that organization and organizations that it is involved with.
It is functional either in the entire chain or in a number of process steps.	✓	It is active in all process steps the initiating organization is involved in and could extend to the rest of the chain.
Multiple organizations are involved (>2)	✓	It is a collaboration between the initiating organization and its chain partners.
Active in social chain	✗	Extended enterprises exist in value/supply-chains.
Designed to be active for as long as necessary	✓	As long as the initiating organization and its partners see value in the collaboration it will remain active.
Structural interpersonal contact	-	It can be just a linking of systems to optimize stock control, or include structural interpersonal contact to create plans for the future.

Table 9 shows that there are a number of similarities between an extended enterprise and an information node. However, the difference in the level on which it is active, the lack of focus on a dominant chain problem and its focus on value/supply-chains give it little value for this research.

### 2.3.6 Comparison with Inter-Organizational Systems

Inter-Organizational Systems (IOS) are systems mainly used in value/supply-chains to coordinate actions between the different parties in the chain, facilitating for example automatic resupply and enabling the involved parties to synchronize production, lowering inventory costs. They are active



throughout the entire chain or between a substantial number of partners and focus on sharing of information. Where the forms of collaboration discussed before consider the organizations and their actions, IOS are the practical implementation that accompany forms of collaborations. It is the actual system that facilitates information sharing. An IOS is designed to be active for an undefined duration, increasing the efficiency of the entire chain and providing some benefits for the organizations involved, even if these might not be equal.

The focus of an IOS is on increasing efficiency and thereby improving the competitive situation and profits. It does not in itself combat a dominant chain problem, but the sharing of information through an IOS could contribute to combating the dominant chain problem.

It is possible for an IOS to be active on the chain level, but because an IOS can be managed by an influential party in the chain, this is not necessarily the case.

While most IOS's are used in value/supply-chains, there has been some research on networked IOS, which are active in chains that show similarities to social chains (Chi & Holsapple, 2005; Kumar & van Dissel, 1996). **Error! Reference source not found.** shows more information on networked IOS. Because of this, the IOS used in these chains are largely applicable to social chains as well.

Where networked IOS can be independent of participants, regular value/supply-chain IOS are often initiated by a large organization in the chain with the power to force smaller parties to adopt it as well. It therefore cannot be considered to always be independent of the participants.

**Table 10 - comparison inter-organizational system with information node**

<b>Information Node</b>	<b>Inter-Organizational Systems</b>	
It should be looked at in the context of a chain	✓	It is usually a system that spans the entire value/supply-chain and coordinates actions between parties.
The focus is on the dominant chain problem	-	The focus is on sharing information, improving efficiency; it could be part of the solution to a dominant chain problem.
It facilitates sharing of information and collaboration, possibly performs actions itself.	✓	It only shares information, the system could perform automated actions.
It functions on both the chain level and the base level of the chain	✗	It is possible for one party to control and maintain the system on the ground level, but it could also function on a higher level.
It is functional either in the entire chain or in a number of process steps.	✓	The entire chain can be involved or only a number of consecutive process steps.
Multiple organizations are involved (>2)	✓	An IOS is used throughout a chain and often broadly implemented
Active in social chain	-	Most IOS's are used in value/supply-chains, but there are IOS's that are designed for networked or social chains.
Designed to be active for as long as necessary	✓	When the IOS is terminated the benefits to efficiency it provides stop as well, so it is designed to be active for an undefined duration.
Structural interpersonal contact	-	In general, contact happens through the IOS, as the IOS connects the different organizations. It is possible for some structural interpersonal contact to occur when planning for the future.

As can be seen in Table 10, IOS's show some similarities with information nodes with the major differences that they do not necessarily regard a dominant chain problem and functions on only one level of the chain process. Also, most IOS's are active in value/supply-chains instead of social chains. An IOS differs from the other forms of collaboration discussed in this chapter in that it often regards the tool for collaboration rather than a collaboration in itself. This tool is used to support a collaboration and an IOS that can be applied to a social chain is therefore relevant for information nodes.

### **2.3.7 Summary/conclusion**

The comparison of these different forms of collaboration with an information node has shown that an information node is indeed different from these other concepts. This does not mean that there are no similarities, mainly the joint chain body and inter-organizational systems are similar to information nodes in some aspects. Because of this, literature on these relevant aspects can largely be used to describe an information node and are used for further refining the definition and for creating the theoretical model in chapter 4.

The two forms of collaboration, Joint Chain Body and IOS, cover both aspects of an information node. On the one hand does the joint chain body cover the collaboration within the node, with at the basis the dominant chain problem and a strong focus on using the chain perspective. On the other hand, there is IOS theory with attention for the sharing of information between organizations and even some research on IOS in networked chains, which shows similarities with social chains and is therefore even more directly applicable.

The other collaboration forms described in this chapter are less usable in this respect. This is either because they are too different from an information node (for example the strategic alliance) or too general to apply (for example the organization). They will not be used further in this research.



### 3 A model for analyzing information nodes

When looking at the definition of an information node given before, roughly three elements can be discriminated. An information node is a form of **collaboration**, it revolves around the sharing of **information** and it is structured, so it needs to be **supported**. Also of importance is its positioning in the context of a social **chain**. In addition to these elements, there are some **preconditions** that are of importance, such as finance and security. These elements of an information node are portrayed in Figure 2. The importance of the focus on the dominant chain problem is considered to be part of the context here, because it should be the reason to create the information node.

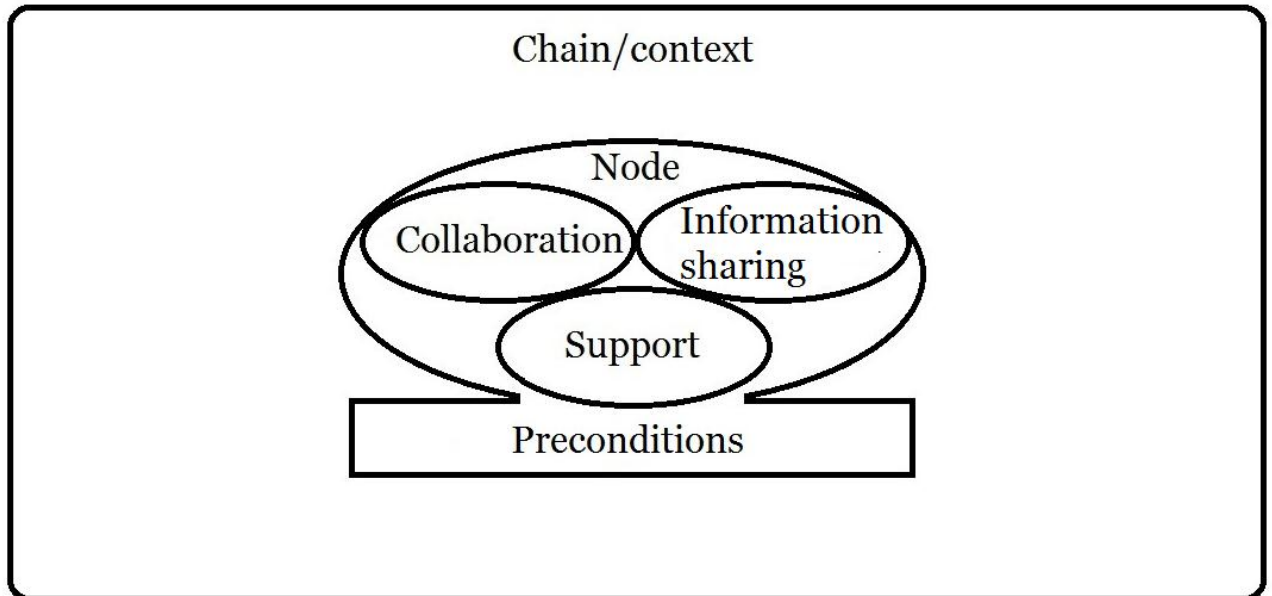


Figure 2- a model of categorizing the different aspects of an information node

Even though these three elements form the basis of the definition of an information node, the way they are filled in can differ for each information node. When the aspects on which the information nodes can differ from each other are identified for each of these elements, it is possible to compare information nodes directly. Some of these aspects have been found in the literature discussed in the previous chapter and a number have been added after examination of existing information nodes and discussions with experts in the field. This chapter describes these aspects and places them into categories which together form an information node. The aspects can be seen as a practical application of the concepts used in the definition.

In order to use the model in Figure 2 for analyzing an information node, it zooms in from the surrounding chain to the different aspects of the node itself.

First, there is the **chain** in which the node exists. To get a clear overview of this context, the mission profile as described by Grijpink (1997) will be created. This profile describes, among other aspects, the parties included in the chain, the dominant chain problem, the critical information required to combat this problem, and a specification of the subject of the chain. It is described in more detail in Appendix 2.

Next, the node will be placed within this context, looking at which process steps of the chain it covers and at what level of the chain process it influences the participating organizations (support, primary process, or policy). The scale on which it operates is also considered; local, regional, national, or international.

Then it will be regarded how the **node** was started. Possibly it was initiated by a governmental body, by one of the parties or by a number of parties together. Does this party still have a leading role, does it carry the responsibility of the node? According to the chain-computerization theory, this should provide the dominant chain problem.

Following this, the node itself is examined. First the **collaboration**; does it exist beyond merely the sharing of information? There might be a separate unit specially designed to support collaboration or

informal collaboration might sprout from the information sharing. Who are the participants and are they all equally involved, or are parties taking the lead? Are there parties who benefit more strongly from the information node? Can parties join and leave the information node easily or are there entry and/or exit barriers? Do parties trust each other enough to freely share information, or are systems in place to substitute this trust?

Then, the **information sharing** itself is considered. What information is shared? Is this only the information that is critical for performing the required actions, or more substantive information? Does it include operational information only or managerial information as well? Who has access to this information? Is the information shared with all participating parties, or a select number?

Next, looking at the **supporting** information systems it is considered what systems are used to share the information. This does not cover the technical details of the system, but merely the type of system in place and how it is used. Also, how are the systems that are used in the information node implemented within the organizations, are they linked directly to the information systems of the participating organizations, or is information transferred manually?

Finally, there are some **preconditions** that should be considered. These are issues not directly related to the collaboration and information sharing, but that do influence the working of the node. This includes the financial aspect, who pays for the information node, do all parties contribute equally, has one party taken the lead, or is there a third party (most likely the government) supporting the information node financially? How are rules and regulations, especially with regard to the sharing of information, implemented in the system? What mechanisms are in place regarding information security, identification, and other security measures?

The different categories and the aspects they contain are also shown in Table 11.

**Table 11 - The different aspects and their issues**

<b>Category/Aspect</b>	<b>Explanation</b>	<b>Operationalization</b>
<b>Context</b>		
Chain	Description of the key element of the chain that is the context of the information node.	Creation of the mission profile based on Grijpink (2010b; described in Appendix 2).
<b>Node in context</b>		
Level of the chain process	At what level of the chain process is the node active? (Grijpink, 2010b)	Is the node active on the level of support, primary process, or policy?
Position in the chain.	Does the node cover all process steps, or a number and which?	Which process steps of the chain are covered by the information node?
Reason	Why was the information node started?	Who first initiated the node, possibly a governmental body or one or more parties in the chain.
Scale	On what scale does the information node operate?	Is the node active on a local, regional, national or international level?
Product	What does the node create?	For example, an advice, strategic plan, actual projects.
<b>Collaboration</b>		
Forms of collaboration.	What forms of collaboration exist?	Is there collaboration beyond the sharing of information? Where and how does this collaboration happen? Does the information node perform tasks itself?
Participating organizations	Which organizations participate in the information node?	Which parties participate and which have chosen not to? Are all parties equally involved or do parties take the lead? How are the benefits of the information node divided?  Who has the final responsibility for the actions of the node?
Entry/exit barriers	What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)	Should organizations adhere to certain rules or standards before they can join the information node or can anyone join? And when can parties leave the information node?
Trust	How important is trust in other parties within the information node and are there systems in place to secure this trust? (Tan &	Do the parties involved in the information node trust each other? What systems exist to secure this trust? How important do

	Thoen, 2000)	participants recon trust to be?
<b>Information Sharing</b>		
How	How is the information shared between organization in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.	How is the sharing of information organized in the information node?
What	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?	What type of information is shared, only critical information for solving the problem at hand, or more general information as well? Is information shared on specific cases only, or also on the policy and strategy of the organizations?
Who	Who has access to the information?	Do all parties have access to the pool of information, or only a select number? Can organizations decide who to share their information with, or is it always shared with all participants?
<b>Support</b>		
Systems	What systems are used and what do they look like?	How do the systems supporting the sharing of information work?
Integration	How are the systems in the node linked to the organizations?	Are the information systems in the node integrated into the individual systems at the base level of the chain?
<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	Where do the financial resources to run the information node come from?	Who pays for the information node? Does this correspond to the benefits received by the organizations?
Legal (Whitman & Mattord, 2011)	The use of sensitive information requires care, how is this organized?	What rules are considered regarding the sharing of information? What measures are taken to adhere to these rules?
Information security (Whitman & Mattord, 2011)	How is unauthorized access and manipulation of information prevented?	What mechanisms are in place to secure the information? For example, how do users identify themselves?

The model is used to create a uniform overview of the aspects of each of the information nodes in order to be able to compare them directly. From this comparison, combined with the lessons learned, generalizations can be made about to what extent lessons learned from the creation of an information

node are applicable to other nodes. When multiple information nodes that are similar on an aspect experienced a certain problem during their creation, this could be considered during the creation of new information nodes. This is done in Chapter 7.

The model has been validated and complemented through interviews with experts who have been involved with the creation of information nodes or are experienced in the field of chain-computerization. The case studies itself also are considered to be a validation of the model and are used to check if the model is complete.

The questions used in the interviews follow directly from the questions asked in the 'operationalization' column in Table 11, with the addition of some questions regarding the lessons learned and experiences while creating and using the information node. The list of interview questions can be found in Appendix 3.

## **4 Research Approach**

### **4.1 Selected cases**

The nodes that are used for this research have been selected based on a number of criteria. These criteria are either theoretical or practical. Theoretical criteria have been found in the theory; the cases should fit the definition of an information node and should fit within the scope of the research. Practical criteria are chosen to select information nodes that are practically useful for this research, for example because they involve a larger number of organizations, increasing the chances to find suitable employees for interview.

The theoretical criteria are:

- The information node has to be active in the Dutch security sector.
- The information node should involve some inter-human contact between the different organizations.
- The focus should be on the sharing of information
- The information node is run by the participating parties; no 1 party has the lead

The dominant chain problem is not considered as a theoretical criterion, because it is hard or nearly impossible to see if an information node really revolves around combating the dominant chain problem without doing thorough research.

Practical criteria are:

- Five or more organizations are involved.
- The node has been active for longer than their initial (pilot) period.
- A regional or national focus

The first of these three practical criteria has been chosen to increase the chance of finding a cooperative organization within the information node.

The second criterion is chosen to select information nodes that are considered useful and that have most likely encountered some problems during their existence which are potentially useful for this research.

The third criterion is selected in an attempt to avoid differences caused by the local environment in which the nodes operate, increasing the possibility of generalizing the results. Also, it should avoid nodes that include factors such as different work ethics, which are expected to be found at nodes with an international focus. The longlist of potential information nodes was created from discussion with experts in the field, and from tips from existing information nodes during the interviews.

Initially, the following (assumed) information nodes were identified:

1. IKC (InformatieKnooppunt Cybercrime)
2. CT Infobox (Contraterrorisme Infobox)
3. FEC (Financieel Expertisecentrum)
4. RIEC's (Regionale Informatie- en Expertisecentra)
5. MIK (Maritiem Informatie Knooppunt)
  
6. CIV (Centraal Informatiepunt Voetbalvandalisme)
  
7. BPVS (Beveiliging en Publieke Veiligheid Schiphol)
8. EPICC (Euregionaal Politie Informatie en Coördinatie Centrum)
9. CIRL (Convenant Informatie en Registratie Ladingdiefstal)
10. LIV (Landelijk Informatiecentrum Voertuigcriminaliteit)
11. ANV (Analistennetwerk Nationale Veiligheid)
12. CMI (Centraal Meld- en informatiepunt Identiteitsfraude en -fouten)

13. Informatieknooppunt huiselijk geweld
14. EMM (Expertisecentrum Mensenhandel en Mensensmokkel)
15. CCV (Centrum Criminaliteitspreventie Veiligheid)
16. CoMensha (Coördinatiecentrum mensenhandel)
17. RCF - Kenniscentrum Handhaving
18. NIAG (Nationaal Informatie- en Analysecentrum Grensmanagement)

After applying the aforementioned criteria, the first 6 nodes remain. These nodes will be considered in the following chapter. Due to organizational issues, the CIV was unable to cooperate in this research and has been excluded. A longlist of the nodes can be found in Table 12.

**Table 12 - longlist of possible cases**

	Dutch security sector	Inter-human contact	Run by all parties	Sharing of information	Five or more organizations	Active longer than pilot	Regional or national focus
IKC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CT Infobox	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FEC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIEC's	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MIK	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CIV	Yes	Yes	Yes	Yes	Yes	Yes	Yes
BPVS	Yes	Yes	Yes	Yes	Yes	Yes	No
EPICC	Yes	Yes	Yes	Yes	No	Yes	No
CIRL	Yes	Yes	Yes	Yes	No	Yes	Yes
LIV	Yes	Yes	Yes	Yes	No	Yes	Yes
ANV	Yes	Yes	Yes	Yes	Yes	No	Yes
NIAG	Yes	Yes	Yes	Yes	Yes	No	yes
CMI	Yes	No	No	No	Yes	Yes	Yes
Informatieknooppunt huiselijk geweld	Yes	No	No	Yes	Yes	Yes	Yes
EMM	Yes	Yes	Yes	Yes	No	Yes	Yes
CCV	Yes	No	Yes	Yes	Yes	Yes	Yes
CoMensha	Yes	Yes	No	Yes	Yes	Yes	Yes
RCF– Kenniscentrum handhaving	Yes	Yes	No	Yes	Yes	Yes	Yes

The twelve unused (apparent) information nodes are excluded from further analysis for a number of reasons. These reasons are covered shortly for each node:

1. The BPVS is excluded because of its local focus, it only concerns the safety and security of Schiphol Airport.
2. The EPICC is not used because each only involves three organizations and the EPICC is also largely international, being a collaboration between the Dutch, Belgian, and German police forces.
3. The 'Convenant informatie en Registratie Ladingdiefstal' is not used because it only involves three organizations.
4. The LIV is not used because it only involves three organizations.
5. The ANV is not included because it has not yet finished its initial period.
6. The NIAG is not included because it has not yet finished its initial period
7. The CMI is opposed to how it appears at first sight, not an actual information node. The CMI helps people who are victim of identity fraud or mistakes to find a solution. It can coordinate actions between the parties it has contact with, governments and other organizations, but this is only done to help the victim in its specific case, not to facilitate structural information sharing. The CMI works on the base level of the chain only.

8. The Informatieknooppunt Huiselijk Geweld is a platform for showcasing projects on the subject of domestic violence and functions as a way to educate people. It stimulates such projects and indirectly supports information sharing and collaboration, however this is not done through a special system, but has to be done by parties on the base level of the chain. The actual collaboration is initiated by the municipalities. It functions as a portal, collecting initiatives from the different municipalities as examples for colleagues and it is used to direct people who are victim of domestic violence or want to report domestic violence to the right organizations.
9. The EMM consists of four organizations which perform tasks to fight human trafficking. They seem to work together in an information node, but the small number of organizations involved in this information node had led it to be excluded from this research.
10. The CCV appears to be an information node, but at close examination acts as an extension of the RIEC's and the EMM. It supports the exchange of knowledge and best practices for problems such as prostitution and human trafficking, but leaves the actual collaboration to the RIEC's and EMM. It is a chain-wide collaboration, but lacks the physical contact that distinguishes an information node.
11. CoMensha has tasks similar to those found in an information node, but is an individual organization unrelated to the organizations it serves. Therefore, although it does facilitate it, it does not consist of a collaboration between parties in the chain and cannot be considered to be an information node.
12. The RCF – Kenniscentrum Handhaving exists of nine centers throughout the Netherlands and focuses on the sharing of expertise and experiences between the municipalities and their chain partners. It has its own coordination and the involved parties seem to have little influence on its actions.

Cases that were not selected because of practical criteria (cases 1-6) could very well be information nodes, but they should be looked into in more detail to confirm or disprove this.

The cases that were discarded because of theoretical criteria could possibly be information nodes as well, but due to time constraints it was impossible to do enough research to be completely sure. Examination of available documents has led to the belief that they are not.

The CIV has been excluded from further analysis because they were unavailable for an interview. The information regarding the CIV gathered from available documents can be found in the factsheet in Appendix 4, but because the data in the factsheet is incomplete and has not been confirmed with the information node, it is not used in the research.

## **4.2 Analysis of the information nodes**

The information nodes were analyzed through a number of sources. First, a document study was performed, analyzing available documentation on the information nodes. This includes year-end reports, year plans, press releases, interviews, and other documents when available. With this information, an initial factsheet was created which included how the aspects identified in chapter 4 are realized within the information nodes. This initial factsheet was presented to and discussed with an advisor with experience with this specific information node. From this discussion the factsheet was corrected where necessary and completed further.

Following this, interviews were held with representatives from the information nodes in order to verify the existing information in the factsheet and to complete the fact sheet. The interviews were also used to find lessons learned and experiences with the information nodes. Using the information from the interviews, the factsheets were completed and presented to the interviewees for validation.

### **4.2.1 Interviews**

Interviews have been used to gather more detailed information on how the information nodes were created and how they operate. The interviews were held, when possible, with people directly involved with the creation of the information node or with a leading role in the information node at this time. This is done because these people are able to provide an insight in both the intentions of the information node and how it functions in practice. Also, advisors that have been involved with the creation of the information nodes have been interviewed when they were available. These advisors provided additional insights because they have an outsiders view on the information node and have no current stakes in the project.



Yin (2003) provides a number of strengths and weaknesses of interviews. Strengths are that interviews allow for a direct focus on the topic of the case study and are insightful. On the other hand, when the questions are poorly constructed, they can lead to biased answers. This will be avoided as much as possible by having the interview questions reviewed by a number of experts, both academic and with experience in the field of information nodes. These experts with experience in the field of information nodes will also be used as what Yin defines as “informants”. Informants are people with knowledge of the field who do not only provide insights, but can also give pointers on where to look for new information.

Another weakness of interviews is the risk of inaccuracies due to poor recall. This will be countered by checking the information gathered from the interviews with the interviewees. When possible, the interview will also be recorded and transcribed. The risk that then remains is that transcribed text loses some of the implicit information it contains, but this is a known problem and almost unavoidable (Lapadat & Lindsay, 1999), checking the information with the interviewed employees will give some check of the correctness.

Because multiple information nodes are researched, the multiple case study design is used to describe the information nodes and the context in which they occur. For the nodes for which an expert is available, two interviews have been performed; one interview with the expert and one with an employee involved with the information node, preferably someone involved with the creation of the node or with a leading role within the node. For the information for which an expert is unavailable, interviews with one or two employees of the information node have been performed.

This number of interviews is chosen because most of the questions can be answered objectively and would therefore only require one well informed employee or expert to interview. Any extra interviews are for confirmation and for the few subjective issues such as trust when this seems necessary. For the information node for which an expert is unavailable, one interview is done with an employee of the information node, preferably with a leading role, which should provide information on how the node works and what problems have been encountered. Any additional interviews are done with employees active in the node and will provide more information on the practical functioning of the node. Some information might differ for the different organizations involved with the information node, such as the integration of the systems into the base level of the chain. Using multiple interviews with employees from different organizations should give a more complete view of how this is organized and if there is a difference in experience between the different organizations. Whether or not the additional interviews have been conducted depends on both the availability of employees for interviewing and the quality of the first interview. When the head of the information node is an independent party who represents the needs of all involved parties, additional interviews will likely yield less usable information.

It is important to interview either an independent party or multiple parties (preferably both), because the chain-computerization theory assumes that there is irrationality, where each party acts in a way that is rational for them, but that might be irrational when looking at the chain as a whole. Parties have different goals and needs and therefore might have different views on how the node functions. Interviewing employees from different organizations or with an independent role helps avoid generalizing the problems of one organization to the entire information node. Because the experts are not linked to the information node or any of the involved parties, they are able to provide objective information on how the information node functions.

The study of each of the nodes can be considered to be a literal replication of the others, aimed at duplicating the earlier results. Even though at forehand it is known that there are differences in the way the nodes function, the goal is to analyze each of the nodes in a standardized way, making it possible to compare the nodes on the earlier defined aspects. Each information node is analyzed to see how each of the aspects identified in chapter 3 is realized in the information node.

The interviews have been performed in a semi-structured fashion and serve as a way to complete and verify the information already gathered from available documents. As such, the questions can be found in Appendix 3, but not all questions are asked in each interview in this form. In practice, the initial conversation with the person involved with the information node and the explanation of the working of the information node contained an answer to a large number of questions. Also, answers to a number of questions were already found in available documents and only required confirmation.

This led to a less structured approach to the interviews than initially planned, but left more room for discussion and exploration of the unique points of each information node. The results for each node can be found in the factsheets in Appendix 4.

## 5 Comparison of the information nodes

The five information nodes that have been examined in this research (found in chapter 5.1) all match the definition provided in chapter 3. However, they are each unique and often have differences between them. This chapter looks into the way the information nodes are organized and how this differs between them. This difference shows the importance of having a fresh approach when creating an information node and why an existing information node cannot be copied to a new situation.

To this end, Table 13 contains a filled in version of the table presented in chapter 4, with all of the analyzed information nodes. More information on the specific information nodes, including the table in more detail can be found in factsheets in Appendix 4.

The information nodes used here by no means form an exhaustive list of the options that are available for information nodes. It is possible that other information nodes not used in this research take another approach. What is presented here is merely a list showing how the examined information nodes have filled in the aspects in a way they consider to be optimal for themselves. As each information node is unique, it might be that an information node benefits from a combination of approaches or even an approach not considered in this research.

It is interesting to note, when looking at the definition of an information node, that all information nodes are active in a social chain and focus on a dominant chain problem in similar ways (although the nature of the dominant chain problem differs). The way the formal, structured collaboration is realized differs from daily collaboration by representatives to periodical meetings to a black box construct on which the participants have little direct influence. Also, all information nodes use more than only critical information. This information does not always leave the information node, however. That the definition fits all information nodes, but excludes other forms of inter-organizational collaboration, as seen in chapter 3 indicates that it covers the information nodes sufficiently, while leaving room for the individual differences. The following sub-chapter goes deeper into the comparison between the information nodes.

### 5.1 Comparison

#### Node in Context

As can be seen in Table 13, the **level of the chain process** in which the information nodes are active varies. This could be related to the sensitivity of the information the information node handles and the relation of the goal of the information node to the primary processes of the involved organizations. For the CT Infobox, the reason for the supporting function is that the information node cannot share any information itself. Instead it provides an advice which is then used to gather the available information. As such, the CT Infobox supports the actions of the participants, but does not directly assist in the actions of the organizations.

The IKC considers the subject of cyber security and cybercrime which is not part of the core activities of the organizations. Because of this, it only has a supporting function.

At the other three nodes (FEC, MIK and RIEC) the information provided by the information node is used directly in the core processes of the involved organizations, so they are active at the level of the primary process.

The FEC and RIEC, finally, also include periodical meetings with representatives from higher functions in the participating organizations and in that way influence the participants directly on the policy level.

It is interesting to note that although the chain-computerization theory (Grijpink, 2010b) states that a solution on the policy level is harder to implement than a solution on the support level, no indication was found that the information nodes operating on the support level were more easily created. The level of the chain process seems to depend on the relevance of the information node for the core functions of the participants only. This could be because the largest obstacle is the collaboration itself, regardless of the level on which it happens. Effort has to be made to create the initial collaboration and to get all participants on the same page. When the realization of a common need is there, the largest part seems to be done. On what level the information node is positioned then seems to be a lesser issue, and because all participants at this point see the necessity of the information node, this appears to sort itself out.

The **position in the chain** shows similarities, not in their exact actions, but in the part of the chain that is covered. All information nodes cover the first step(s) of the chain as shown in the mission profiles in Appendix 4. These are the steps where information is gathered, analyzed and shared. This

is to be expected, since the definition of an information node states that it resolves around the sharing of information; it leaves the actions based on this information to the participants. So the actual physical action that is taken based on the provided information is performed by the organizations outside of the information node, although possibly supported by more information or expertise from the information node.

The **reason** for creating the information node also shows similarities for the different information nodes, all coming from a (often government funded) report which finds that there are problems. This report is then used as the basis for the information node. The CT Infobox has had a more direct reason in the terrorist attacks in Spain in 2004, but the reason also was a political (and societal) need.

All information nodes are created to combat a problem that affects all participants and that has a social relevance. Often the extent of this problem is not realized until it is found by an external party. This is often done by a government organ when it creates a report which finds and defines the magnitude and potential risks of a problem. This is similar to the chain-computerization theory (Grijpink, 2010b) where a dominant chain problem is the reason for collaboration and which states that none of the parties in the chain is able to define the dominant chain problem by itself. This is because it does not have a clear vision of what happens outside of its own boundaries and which of the problems it experiences also affect other parties.

The **scale** of the collaboration is regional and national with some local aspects in the RIEC. However, this is one of the criteria on which the information nodes were selected, so it will not be discussed further.

All **products** of the nodes are semi-tangible products such as advice, experiences, projects and structural information exchange. Since the information nodes mainly work with information, this is relatively similar for each node and will not be elaborated on because of this.

### **Collaboration**

With regards to the **form of collaboration** roughly three varieties can be discriminated. First, there can be permanent collaboration where employees work together on a daily basis (for example at the MIK). Second, it can be a collaboration which consists of periodical meetings where the information exchange happens, with a coordinating organ coordinating optional projects and administrative tasks (As is found at the IKC). Thirdly, there can be permanent collaboration, where employees work together on a daily basis and which is supported and guided by a coordinated organ which meets on a periodical basis (which happens at the FEC).

Each information node used in this research consists of seven to ten **participating organizations** (listed in the factsheets in Appendix 4). However, since existing of five or more participants was one of the requirements, this is not surprising. However, none of the information nodes consists of more than 10 participants (technically the IKC consists of more organizations, but the ISAC's (Information Sharing and Analysis Centers) are treated as (sub) information nodes for this research because they form the actual collaboration). This limit of 10 organizations can possibly be related to the principle from the chain-computerization theory that there is irrationality (Grijpink, 2010b); each organization will act in its own best interest. When there are too many organizations each acting this way, coming to an agreement could be nearly impossible, so some limit has to be set. This could be deliberate or it could have evolved this way. On the other hand it is possible that these information nodes were created to combat a problem which impacts only a limited number of organizations, no more than 10 in the case of the information nodes researched here. This would mean that it is possible for other information nodes combating larger problems to involve more organizations.

One of the characteristics of an information node is that it is controlled by the chain, not a single party. In practice, this is a little less black and white. None of the information nodes has a single party that controls it, but there are information nodes which indicated that there is a small number of participants who have the most advantage of an information node and contribute more to compensate for this. This however, gives them more power within the information node as well. It indicates that there might be a grey area between total equality between the participants and a leading party taking control which can also yield success when executed correctly.

It was found that although all information nodes had some **entry barriers** these were not always specified and in practice only required the potential participants to be active in a relevant area and to provide relevant information. None of the information node had exit barriers, other than requiring an x month notice, but it was stated that the information nodes gave such an advantage to participants that they did not want to leave.

Although hard to quantify, all information nodes stated that **trust** was important for the successful collaboration. Participants have to trust other parties and the information node itself to only use the information they provide for the agreed upon goal.

Not all information nodes considered trust equally important, as some, like the CT Infobox and the FEC, have created strict rules and agreements on what exactly can be done with the information or have agreed on not sharing information directly in the information nodes. This is what Tan and Thoen (2000) describe as control trust, trust in the systems or processes that regulate the information sharing. It seems that when the processes are more strictly regulated, the amount of reliance on trust decreases, as participants have to trust the rules rather than the other participants.

### **Information Sharing**

**How** the information is shared shows some differences between the information nodes. It ranges from daily collaboration which depends on sharing information between participants directly in the MIK to a black box construct in which information is used, but not shared and only an advice is created as happens in the CT Infobox. This black box construct means that the CT Infobox gathers information from the systems of the participants and uses this information to create an advice regarding a subject in the CT Infobox. The information used to come to this advice is not shared, only the advice leaves the box and participants can share relevant information and coordinate actions individually.

Other possibilities are periodical meetings where information is shared and discussed as happens in the IKC, a combination of periodical meetings and direct exchange of information in teams as in the RIEC, and a daily collaboration leading to information being shared between the participants during periodical meetings. As stated before, it is not unthinkable that there are a number of other forms of sharing information possible, or possibly combinations of methods found here. For example, a daily collaboration based on sharing information as exists in the MIK could be combined with periodical meetings to discuss this information and plan future actions for the involved organizations.

**What** is shared is often more than just the information critical for combating the problem the information node was created to solve. Critical information is the information required for combating the problem the information node as created to solve. For example, this might mean that not all information on a person is shared, but only information regarding his employment history. In practice, however, the value of information nodes can extend beyond the direct problem, as more general combination of information from different sources can show new patterns and before unnoticed problems.

When more information is shared than purely critical information, this information is shared with a clear goal and should only be used for that goal. In addition, information nodes like the FEC check the information before it is shared, although this is often only to check whether it can be legally shared. The CT Infobox uses more than critical information to create an advice, but does not share any of that information.

This is consistent with the characteristic that the information node should facilitate the sharing of information critical for combating the dominant chain problem and collaboration. It should be noted that the information node can share more information than only the critical details, this seems to go against one of the principles of the chain-computerization theory (Grijpink, 2010b). However, it can be argued that the goal of an information node is to solve a lack of overview in a specific area leading to criminal activity. In that case it could be that more general information, for example about activity on the North Sea, is considered critical. However, it seems like the sharing of information is sometimes done by providing all information on a subject, which will in many cases include more than critical information. In those cases, trust or strong rules are important to guarantee that the information is only used for the problem at hand.

Also, this characteristic does not mean that the information has to be shared between the participants in the information node directly. The CT Infobox only shares an advice, but all participants share their entire systems with the CT Infobox itself which includes more than just critical details..

Regarding **who** has access to the information; for each of the analyzed information nodes all parties are considered equal and there is enough trust to share information within the node with all parties when legally possible. For the CT Infobox, all information sharing happens outside of the node (outside of meetings and not using facilities provided by the information node), but there is stated to be enough trust for this to happen between all participants.

Besides the general sharing of information with the information node and all participants, it could be possible that information is shared between participants directly, without the control and influence of the information node. However, this has not been researched.

### **Supporting systems**

The **systems** used to support the information sharing differ for each information node, as can be expected because they use different ways to share information. Not all information nodes use a system, the IKC and RIEC do not use systems, merely standardized files to exchange information. Other information nodes use a system to share information in, either directly (in the MIK) or moderated (in the FEC). The CT Infobox, finally, uses a shell through which it can access the systems of the participating organizations. This works one way only, no information is returned to the participants this way.

These systems have no **integration** with the systems of the participants (with the exception of the system of the CT Infobox, which has some integration, but one-way only; the CT Infobox can access the systems, but the systems of the CT Infobox are closed for the participants) and all information is transferred between the system of the information node and the participant's own system manually.

From the theory on Inter-Organizational Systems (Chi & Holsapple, 2005; Kumar & van Dissel, 1996) it would be expected that each information node uses a system to share, or refer to, the information. However, this is not the case, as most of the information nodes examined do not use a system to exchange or refer to information directly, but (nearly) all exchange is done either physically between parties or moderated by the information node when the information node exists of employees independent of the involved organizations.

### **Preconditions**

The way the nodes are **financed** differs, although all nodes require some resources from the participating organizations. This can be only in the form of one or more fte's (for the FEC, IKC, and MIK) or can include a financial contribution as well (for the CT Infobox and RIEC). The rest of the costs are covered by either a Ministry (FEC; Ministry of Finance, and RIEC; Ministry of S&J) the coordinating organ (IKC; NCSC, and MIK; Netherlands Coastguard). The CT Infobox is the only information node paid for completely by the participants.

Information nodes have to consider a number of laws and **legal** restrictions, most often the Wbp<sup>3</sup> when using information about natural persons. Other laws that might be relevant are the Wpg<sup>4</sup>, WIV<sup>5</sup> and WOB<sup>6</sup>.

When regarding **information security**, the measures taken depend on the system used. Some are technical, requiring identification by phone in addition to a username and password (at the FEC), where the traffic light system for classification of information as used by the IKC is based completely on trust. Other information nodes secure the information by using protocols and formal ways of sharing the information (the CT Infobox and MIK).

---

<sup>3</sup> Wet bescherming persoonsgegevens (Personal Data Protection Act), the law regulating the use of information regarding natural persons. For example, the information gathered regarding a person can only be used for the purpose it was collected for. This can be a problem if the goal is related, but not identical to this purpose.

<sup>4</sup> Wet Politiegegevens (Police Data Protection Act)

<sup>5</sup> Wet op de Inlichtingen- en Veiligheidsdiensten (Law on Intelligence and Security services)

<sup>6</sup> Wet Openbaarheid van Bestuur (Law of Open Government)

Table 13 - Comparison on the information nodes (more detail can be found in Appendix 4)

	<b>CT Infobox</b>	<b>FEC</b>	<b>IKC</b>	<b>MIK</b>	<b>RIEC</b>
<b>Node in context</b>					
<b>Level of the chain process<sup>7</sup></b>	Support	Support, Primary process, Policy	Support	Support, Primary process	Support, Primary process, Policy
<b>Position in the chain.</b>	Process Step 'Acquire'	(supervision and detection) - notice – investigate	Monitor – analyze – prevent	Monitor and analyze	Find problem identify people coordinate actions
<b>Reason</b>	Real-life event	Report	Government issued after report	Report	report
<b>Scale</b>	National	National	National	Regional, covering the entire North Sea	Local and regional
<b>Product</b>	Advice	Coordinated information exchange, increase of knowledge, projects, analyses	Good practices. Experiences, studies	Structural information exchange, daily briefing	Administrative measures
<b>Collaboration</b>					
<b>Forms of collaboration.</b>	Permanent collaboration and periodical meetings of coordinating organ	Permanent collaboration and periodical meetings of coordinating organ	Periodical meetings. Coordinating organ managing secretariat and large projects	Permanent collaboration	Permanent collaboration through the teams Training and advice. Coordinating organ, the LIEC (Landelijk Informatie en Expertise Centrum; National Information and Expertise Center)

<sup>7</sup> Explained further in chapter 3.1.1

	<b>CT Infobox</b>	<b>FEC</b>	<b>IKC</b>	<b>MIK</b>	<b>RIEC</b>
<b>Participating organizations</b>	9 parties	8 parties	3 core parties, number of parties per ISAC differs. 10 for water ISAC	7 parties	8 main partners
<b>Entry/exit barriers</b>	When all parties agree.	When the coordinating organ agrees, parties can join.	Relevant field of operation.	Relevant area of operations, provide at least 1fte.	Must provide relevant information/public party.
<b>Trust</b>	Trust in the node itself, due to closed character not in the other parties. Has grown because of the node.	Trust in the node itself and in partners not to use information without consultation.	Great importance. All information is shared face to face and the classification system is based completely on trust.	Important, maintained by being transparent and having an independent head.	Important, results are always returned to all parties.
<b>Information Sharing</b>					
<b>How</b>	Using a black box format.	Within the node and when legally possible between parties in a dataroom.	During periodical meetings within the node.	Face to face structural information sharing.	Meetings and within the teams.
<b>What</b>	In principle all information owned by participants, only critical info is used. No sharing between parties within the node.	All information on a specific subject, only used for the intended goal.	Experiences and problems, any relevant information regarding cybercrime. Critical information.	Information regarding what happens on the North Sea. Mainly critical information.	Signals, information on (potential) cases.
<b>Who</b>	Decided on base level.	Only legal restrictions.	All parties.	Every party, when legally possible.	Parties who can legally access the information.



	<b>CT Infobox</b>	<b>FEC</b>	<b>IKC</b>	<b>MIK</b>	<b>RIEC</b>
<b>Supporting systems</b>					
<b>Systems</b>	Shell over participants' systems.	Tool in which each party has its own space and the FEC can access all.	No systems.	System for internal communication used by the information node.	Workflow systems, administrative dossiers.
<b>Integration</b>	One way from systems to node.	None. Manual transfer.	None.	No integration, manual transfer.	Administrative dossiers are used internally and externally.
<b>Preconditions</b>					
<b>Finance (Venrooy &amp; Sonnenschein, 2008)</b>	Paid for by all participants using a distribution key.	Each party provides a number of fte, ministry of finance provides 6 fte, including housing etc.	Paid by participants, secretariat and coordination by coordinating organization.	Staff is paid for by the respective participants, housing is provided by the Netherlands Coastguard.	Supported by Ministry of S&J (1/3) the rest is paid for by the participants.
<b>Legal (Whitman &amp; Mattord, 2011)</b>	WIV	wbp		Wbp, wpg	wbp, wpg
<b>Information security (Whitman &amp; Mattord, 2011)</b>	All information is signed by multiple parties to confirm its correctness.	Identification through name+password and mobile phone.	Traffic light <sup>8</sup> , based on trust.	All information is shared using a proces-verbaal <sup>9</sup> .	None specified, but laws are respected.

<sup>8</sup> The traffic light system is used to indicate to what extent information can be used by the participants. It is explained in more detail in Appendix 4.3.

<sup>9</sup> A formal form of documenting facts and observations, used by investigation officers. This includes documenting the source of the information and how it was acquired.

## **5.2 Relation to the chain-computerization theory**

Because the chain-computerization theory, among other theories, is used as a basis for looking at the information nodes, it is important to consider how it relates to existing information nodes. During the creation of the factsheets and the comparison of the information nodes it has proven to provide a number of useful principles, but not all statements have been found completely true for all information nodes. Even though the number of information nodes used in this research is too few to base conclusions on, these statements will be discussed shortly. It should also be noted that this does in no way mean that the chain-computerization theory is incorrect, because information nodes are not necessarily chain-wide nor positioned at the chain level and because the chain-computerization is largely conceptual and therefore leaves room for differences in practice. It does show that it might be possible to create more specific principles for the creation of information nodes.

The principles from the chain-computerization theory discussed here hold true to some extent, however, they are not strict rules and information nodes were found to move a bit into a grey area between what the chain-computerization states to be possible and impossible. These findings could be helpful in the creation of further theory specific to information nodes or an extension of the chain-computerization theory to include information nodes.

### **Location of the information node in the chain**

According to the chain-computerization theory the coordination of chain activities should happen on the chain-level. The actual activities within the chain happen on the base level of the chain; between the participants directly, without the use of systems that cover the entire chain. Since an information node often performs actions that go further than mere coordination it can be stated to be active on the base level of the chain as well. However, it clearly has this coordinating function, as it can influence future actions of the participants. When there is a coordinating organ within the information node, this organ could be considered to be active on the chain level, as it covers all organizations and does not perform actions itself. The information node itself would then be active on the base level of the chain, performing the tasks it receives from the coordinating organ. This is the case for the IKC, where the ISAC's are active on the base level, with the IKC itself coordinating actions on the chain level.

When the node itself does not include a coordinating organ and performs some tasks that influence strategic planning and coordination itself because of its impact on the primary processes, it shows activity on both the chain level and the base level of the chain. For example the MIK, as the backend of the coastguard does not have a coordinating organ, but does influence the actions and strategies of the participants.

This indicates that the classification of an entity to be active on either the base level or the chain level is too strict. It seems to be possible for an information node to span both levels.

### **Creation from a common need**

The chain-computerization theory works from the assumption that collaboration on the chain level can only exist if participants see the need of such collaboration. There should be a dominant chain problem that all participants are willing to solve and invest in because of its severity. When looking at information nodes, this seems to be not necessarily the case. The problem leading to the creation of the information node does not always impact all participants equally, leading to resistance to join and possibly requires some force from an authority. Or an information node does not apply to the primary processes of the participants and external support, often financial and from the government, is required to set up the information node. This could be because the societal need for the information node is greater than the need from the involved organizations, as the problem can be underestimated (for example this was stated to be a problem at the IKC when considering cybercrime in public sectors where organizations have functioned for years without worrying about cybercrime, or because an organization like the Belastingdienst has no interest in the investigation of criminal activity as was found to be the case at the RIEC).

The chain-computerization states that the creation of inter-organizational collaboration on the chain level can be hard and should be done gradually and that the existence of a dominant chain problem is not sufficient if the parties are unwilling to collaborate.

Experiences with the information nodes in this research are that often an external pressure (either financial or political) is required to start the information node. This is a possibility that is mentioned only briefly in the chain-computerization theory, as it implies an overarching authority, which would negate the need for a solution on the chain level.

It seems unlikely, however, that collaboration without the realization of a common need from the participants is sustainable, there has to be some motivation. This does not seem to have to be as strong as indicated by the chain-computerization theory, as it can be compensated for by external support. This support can be either financial (lowering the barrier to join) or political (forcing government controlled organs to join).

Dependence on external support can weaken the information node, as it might fall apart when the support stops. Ideally, working in the information node convinces participants of the need, eliminating the requirement

of external support, but this cannot be expected to always be the case. Because of this, it is understandable that creation from a common need can create stronger nodes and is emphasized by the chain-computerization theory.

The examination of the information nodes in this research provides new insights into the influence of an external pressure and raises the question if there is a difference in success between information nodes with and without an external pressure.

### **No authority; no party can take a leading role**

The need for creating an information node should be strong enough for participants to contribute money and other resources to creating collaboration together. However, when looking at the examined information nodes there are cases where one or more parties have taken the lead, something that is explicitly named as impossible by the chain-computerization theory. There are a number of nodes that depend largely on government support and are therefore influenced in their actions by the government. Other information nodes have one or a number of participants who contribute more and can therefore ask more from the information node. For example, the AIVD benefits more from the CT Infobox than the other participants do and therefore contributes more.

In addition, it is possible for an information node to be housed and coordinated by one of the partners even if this party does not officially take a leading role. Other information nodes have a chairman from one of the participants who has some influence on what actions the node will perform and will use this from the point of view of his organization.

The chain-computerization does not state that each participant should be equal, as it is possible to start collaborating with a number of parties and to include the rest of the chain later on. So it seems like the principle can be generalized to stating that all parties need to feel like they profit from the information node and are more than just providers of information. It contains the same value as the principle, but it is formulated less strictly. When participants contribute less, they were found to be satisfied with less power over the information node and less profit from participating in the information node. It seems most important that participants feel treated fairly and as equals by all parties, they should at least receive as much as they put into the information node.

### **Only share critical information**

Each of the information nodes shares more information than just the critical details to which the sharing should be limited according to the chain-computerization theory. It can be argued that the CT Infobox, where no information is provided by the information node does adhere to this principle, but the CT Infobox also requires more information than just the critical details to base their advice on. All other information nodes share more than is strictly necessary and trust the other participants not to abuse the information that is shared. However, participants are not willing to provide all their information to just anyone for any reason. For these information nodes to work, strict rules regarding what can be done with the information and who it is shared with had to be created. In a sense, this means that only the critical details can actually be used, despite the fact that more information is provided. This does require a fair amount of trust to work.

Most of the other principles of the chain-computerization theory seem to be applicable to information nodes. However, it is not the goal of this research to check the applicability of this theory to information nodes and the principles described here are the ones that became apparent during the analysis of the information node. Further research could confirm these and find other principles that could be adjusted.

## 6 Lessons Learned

After creating a complete list of lessons learned based on available documents, and interviews with practitioners and experts, these lessons were further discussed with experts with experience in the field of information nodes in order to combine lessons or to elaborate on or emphasize certain lessons.

The lists of lessons and tips that have been mentioned in the interviews for each information node can be found in the factsheets for each of the information nodes in Appendix 4. The lessons and tips have been combined into a list of 19 points, which are discussed in this chapter. A checklist containing a list of these points can be found in Table 15 in Chapter 8. The list is not exhaustive and it is possible that problems were encountered by information nodes that did not report the problem. In general, if a lesson was mentioned by multiple information nodes or if it has a solid theoretical founding, it is included in the list.

The problems and lessons have been sorted into five categories. These are Collaboration, Information Sharing, Preconditions, and Support as defined in figure 3 in chapter 3, and an additional category 'Node' which covers the fundamentals of the node itself. The classification of the lessons is somewhat arbitrary, as some of the problems can be argued to fall into multiple categories, but to prevent repetition each problem is listed only once. The Node, Preconditions, and Support categories are looked at first, because Node and Preconditions can be considered to be the basis of the information node, and Support is also considered important to consider soon during the creation of an information node. The other two categories are looked at after that in the order in which they have been discussed in previous chapters.

Each lesson consists of a short explanation of what the lesson means in practice, followed by examples of how information nodes have experienced this, and finally how this relates to the theory.

For each lesson the information nodes that named the lesson are listed. It should be noted that this in no way means that the other information nodes did not encounter this problem, only that it did not follow from the interview with and analysis of the information node. In addition, the amount of information nodes that named a lesson cannot be considered an indication of how important that lesson is.

### Node

These lessons consider topics that in a way form the foundation on which the information node is built and therefore should be considered at the start of the information node. However, this does not mean that these are only relevant when the information node is created, some can also be relevant later in the life span of an information node or throughout the existence of an information node.

#### **1. The information node should have a clear goal to manage expectations. (MIK, FEC, CT Infobox)**

When an information node is created, it should be clear what its goal is in order to manage the expectations of both the participants and from other inter-organizational collaborations or organizations that might exist in the same field.

It is important for organizations and other information nodes or inter-organizational collaborations that exist to know that the information node will not take over their work and that it could possibly be a valuable addition to their work. It can be imagined that participants are active in both the information node other inter-organizational collaborations, directly conveying relevant information.

Participants of the information node should know what is expected of them and what they can expect to gain from the information node. This includes clarity on what the information provided to the information node is used for and what they are allowed to use the information provided by the information node for.

The MIK has experienced mistrust and slight opposition to the information node from other inter-organizational collaborations already existing in their field. After consultations and clarifications of their goals and tasks they grew more supportive. In addition, participants can be active in both the MIK and other collaborations, providing a link between the MIK and the other collaborations.

The FEC and CT Infobox stated that partners should know that their information is only used for the goal it is provided for. In the CT Infobox, for example, this is guaranteed by the black box format.

Regarding the theory this can be related to the idea from the chain-computerization theory that the goal should be to combat a dominant chain problem and that only information critical for combating this dominant chain problem should be shared. This information should only be used to this end (Grijpink, 2010b).

This can be generalized to having a clear goal to which all participants agree and clarity of what information is shared for what reason. The tasks of the information node should be unique, if it takes over tasks that are already being performed, there is no real need for the creation, as the problem is already being combated. This indicates that in practice, it is a lack of knowledge of what the information node will do that creates the fear, not the actions of the information node.

## **2. Get operational soon, sort out the details later. (MIK, RIEC, CT Infobox)**

When an information node is active soon, including as many participants as are available at that time, it will yield results quickly. This can lead to more support from both responsible parties (such as a Ministry) and potential participants.

In addition, it prevents the information node from creating methods that participants do not agree with, or from losing time discussing potential methods. It can use proposed methods and let the success speak for itself. This way, participants are less likely to disagree with the information node, easing the collaboration. It is important when working from a broad setup towards a more specific way of working to keep the goal of the information node in focus.

In addition to the work processes, it could also be useful to wait with specifying the scope. When the scope is created too soon, it can lead to an information node not working to its full potential because participants are unwilling to change the scope and put in more or other resources than was specified in the original document.

It should be noted that starting as fast as possible is not the best approach for all information nodes. For some nodes, the sharing of information requires a strong protocol, or the participating organizations might want structure before they collaborate.

The MIK and RIEC stated the advantage of starting soon, creating effective work methods and results to gain both financial and political support and to include potential participants more easily. The CT Infobox felt that the creation of the scope for the information node in one of the initial documents has limited the tasks it performs. Regarding the actual collaboration the CT Infobox used a very structured approach, where the collaboration was first created theoretically and then executed in practice, which has worked well for this information node.

It seems possible that the preferred approach in this respect is related to both the sensitivity of the information that is used and possibly the reason for creating the information node. When an information node is created from a strong societal or political need, there can be more time and money for designing it before it is created, where information nodes that are created with less political support need results to prove itself. However, even for information nodes that have the time and money, it might be preferable to start soon, in order to get all parties to join and to further specify the way of working together.

This can be related to the chain-computerization theory (Grijpink, 2010b) which states that the collaboration should arise from all parties together (based on a common problem) and therefore, they should all agree on how the information node operates. The method of starting soon and specifying later (called the bottle neck-model by the MIK) has proven to be a way to establish the methods for collaborating.

## **3. Take enough time for completing the information node, decision making in organizations can be slow. (MIK, RIEC)**

Any information node will consist of a number of organizations that will have to join. For all examples of information nodes found in this research that meant at least providing a number of fte to the information node and often included other costs. Because of this and because of the other implications of joining the information node such as the information they have to share and the internal process they might have to change, organizations do not join the information node lightly and decisions have to be made by the top of the organization. The decision making process as well as the movement of information through the organization can be a long process and when creating the information node this should be considered.

This was experienced by the RIEC and MIK. It is important to take time for this to be sorted and to prepare for this when creating an information node, possibly by finding a way to begin the collaboration before all participants have joined in which case results might speed up the process. When the problem is a slow transfer of information through the organization, they stated that it can help to be persistent and make sure the information reaches the right persons. This could be done for example through contacts from the already participating organizations.

Slow decision making processes in organizations based on a complete set of information, using analytical techniques have been found to result in more successful decisions (Dean & Sharfman, 1996). However, these processes are time consuming. As using these processes tends to lead to better choices, they are desirable, as they can lead to more dedication to the information node when it has shown to be profitable for the organization. As can be imagined, more factors are of influence on the decision making speed, such as how severe the problem is and the internal stability of the organization.

## **4. Be persistent, when an approach fails, look for other options. (MIK, RIEC)**

It is unlikely that the creation and managing of an information node will completely follow the plan created by the initiators. When considering the existing information nodes, each has had some setbacks during its existence. When something does not work as planned, for example, an important party is unwilling to join, or the related Ministry will not provide additional funding, it is important to look for other approaches instead.

These approaches can consist of contacting another person in the organization, looking into collaboration with another organization which has access to the same information, or collaborating with the parties that are willing and letting the results be the motivation.

It is important not to stick to an approach that has proven unfruitful. Not everything will go as planned, expect failures and try to always have a plan B.

The MIK stated that they have had trouble getting all parties they would like in the information node to join them. When this became apparent at first, it was decided to start with the remaining parties and present the results to persuade them to join. When this did not work for all parties, mainly because they had trouble providing the capacity required for joining, other organizations with access to the required information had already joined. This way the MIK had access to the information through other channels.

The chain-computerization theory (Grijpink, 2010b) emphasizes that inter-organizational collaboration is hard because of (among other things) the different organizations involved and their different views of what is important. This should always be considered, as not each organization (either potential participant or external party) will see things from the perspective of the node and they cannot be trusted to act in a rational way from the point of view of the information node.

#### **5. Without political and/or societal support an information node has little chance of success; create publicity. (MIK, RIEC, CT Infobox)**

An information node should perform tasks that have political or societal relevance. When it does, it is easier to get support, both from external financiers and from potential participants. When there is no political or societal need for the information node it has very little chance of success. To ensure the political and/or societal relevance it clear for both potential participants and (potential) supporting parties such as Ministries, an information node should create publicity around its successes. This publicity can motivate current participants, interest new participants and show the value of the information node to both politicians and society.

The comparison of the information nodes in chapter 5 shows that each of the information nodes analyzed in this research was created following a report, often created or initiated by the government. This indicates a political and/or societal cause leading to the creation of the information node.

The necessity political support was explicitly noted by both the RIEC, which stated that it would not have succeeded three years earlier, because there would have been less political support then, and the CT Infobox which was created after the terrorist attacks in Madrid in 2004.

The RIEC also found that the publicity from their successes led to tips from citizens, because they became aware of the existence and tasks of the information node. For the MIK, the publicity on successes has led to more political and financial support.

The need for political and/or societal support can be related to the chain-computerization theory (Grijpink, 2010b) which states that there should be a dominant chain problem; a problem of such magnitude that is poses a threat to the entire chain. When considering the security sector this implies a societal danger, for example criminal activity remaining unpunished, and leads to societal support for combating this problem.

#### **6. Each node is unique, you cannot use a blueprint. (RIEC)**

Each information node exists of different organizations, which each have different goals and needs. In addition, each information node serves a different purpose and even though these might be closely related, differences exist. Because of this, no blueprint for what an information node should look like can be created. Each node should in a way be created from scratch. However, this does not mean that earlier experiences should be ignored. Lessons can be learned from past projects and elements can be recycled, as long as these are not used as set rules and they leave room for the unique character of the new information node. This is true even if the new information node is a new implementation of an existing regional information node, since regional differences can greatly influence the working of an information node.

The RIEC found that this is true when creating the RIEC's in other regions than Zuid- Limburg, where the first instance was created. It can also be seen when the different information node examined in this research are compared, they all differ greatly and using the methods from one information node to perform the tasks of another information node would likely create problems.

The idea that each project is unique and should be created from scratch can also be found as one of the main principles in the chain-computerization theory (Grijpink, 2010b).

### **Preconditions**

Preconditions include the lessons that are not directly related to the actions of the information node, but that are required to be managed in order for the node to be able to function as intended. These are often things that are less important when an information node is created (except for the need for handling the laws and regulations which is one of the most important things to consider), but that do require attention and should not be expected to sort itself out.

#### **7. Participants should have the right qualifications. (IKC, CT Infobox)**

The representatives from the different organizations who participate in an information node should have the right qualifications. This refers to their position in the company, for example, a meeting with only IT experts will yield different results than a meeting with a mixed group of IT experts, process experts and engineers. It also means that the representatives should have enough knowledge of what is happening in their organization to bring some insights to the meetings and they should be able to communicate any new information from the meetings back to their organization.

When the information node performs actions itself, such as the analysis of information, it means that the person working in the information node should be capable of doing this.

The Water ISAC of the IKC, consisting of the Dutch water processing organizations, has experienced that it is hard to get people with the right qualifications to participate in the meetings and believes that this partly is due to a lack of awareness. The organizations possibly don't fully see the importance of the information node and therefore don't give it the required attention.

In addition, the information node should have a capable head or chairman. Since an information node requires some amount of dedication and investment from the participants, it can be of value to have someone in charge who is enthusiastic and inspiring. When this is the case, he (or she) can help convince potential participants of the importance of the information node and can convince external parties to help or support the node financially. At the same time, already cooperating parties are motivated further and will keep supporting the collaboration.

The CT Infobox found that a certain amount of expertise is required when performing certain tasks. To ensure this expertise is available, it has created a profile for the potential employees of the node to ensure each is capable of performing the actions required by the information node.

Both the CT Infobox and RIEC stated that it is of importance to have a capable head of the information node and it was indicated that having a good plan for an information node is important, but that the presentation of this plan might be equally important. If a great plan is presented by someone who does not believe in it, it is less likely to get support than when it is presented by someone who is enthusiastic about and who can convey this enthusiasm to the people whose help is required.

As stated by the chain-computerization theory, the goal of an information node should be to combat a dominant chain problem (Grijpink, 2010b). In that case each party sees the advantage of working together and will prioritize this. When this is not the case, either the problem might not be severe enough or some of the parties are not fully aware of the severity of the (potential) problem.

This can also have an impact on trust, participants should trust other parties to provide the best possible information. When organizations send under qualified representatives this is not the case and the trust can be damaged and thereby the effectiveness of the information node can decrease.

#### **8. Financing can be hard, it should be considered at the start of the information node and entails more than just the setup. (CT Infobox)**

When creating the information node it should be considered how it will be paid for. For example, the information node can be paid for by the participants, by an external financier such as a Ministry or by a combination of both. When this is agreed upon it is important to not only consider the costs of initially creating the information node, but also the costs of maintaining it over time. This is only a potential problem for information nodes that rely (in part) on external funding.

For example, the CT Infobox received funding from the Ministry when it was set up, but the cost of managing the information node was not considered. Other nodes might require an initial investment for technology which can be covered by either an external financier or the participants, but this equipment will be outdated after a

number of years and should be replaced requiring another large investment. When this is not considered in time it could break up the information node.

Venrooy and Sonnenschein (2008) suggest that the costs of the collaboration itself should be covered by the participants, since this is what should provide results and has a direct advantage for the participants. Costs for coordination and secondary costs such as housing and IT systems should be covered either by creating a distribution key among the participants or by an external financier.

### **9. It is important to consider where to physically locate the information node. (IKC)**

An information node can be created as a new legal entity, housed in its own location and performing its actions there or it can be housed at an existing organization. As experienced by the IKC, it is important to find a location where the information node can exist for an indefinite period of time. When the housing of an information node turns out not to be suitable and the information node has to be relocated, this can create problems, such as high costs and less activity from the information node until it has found a proper location. Potentially, it could mean the end of the information node if no suitable housing is found.

The RIEC is an example of an information node in its own, independent location, while the MIK at the Netherlands Coastguard and the CT Infobox at the AIVD are examples of information nodes located at one of the participants.

The problem with unsuitable housing was experienced by the IKC which has been housed by the NICC until that was discontinued, was then moved to TNO and now resides at the NCSC, which is a government organization.

What could be an important factor when considering where to house an information node is the relation of the tasks of the information node to the core processes of the participating organizations. For the organizations participating in the IKC, cybercrime and cyber security are important, but not part of the primary processes of the organizations. This might lead to a lack of funding for independent housing, while at the same time none of the participants wants to host it because it is not part of their core business. Another possible factor might be the size of the information node. The IKC spans multiple sectors and dozens of organizations. The coordination of such an information node can be complicated, even when the collaboration per sector happens largely independent.

According to the chain-computerization (Grijpink, 2010b) the collaboration should be independent of the participants. This indicates that the information node should always be located in its own, independent location. However, this is not the case in practice, often due to financial considerations; using available space at one of the participants is less expensive than creating new offices for the information node.

### **Support**

Support entails the lessons regarding the supporting systems used by the information nodes. It entails only one lesson, which indicates that it is not something that is considered important by the information nodes. This also shows in the fact that none of the information nodes has a direct integration with the systems of the participants.

### **10. Being legally able to share information is more important than a system for sharing this information. (MIK, RIEC, FEC, CT Infobox)**

In order to be able to collaborate effectively, parties should be able to share information critical for the goal of the node in a legal way. Because information nodes often handle information regarding natural persons, the Wbp<sup>10</sup> is possibly applicable to the exchange of information, along with a number of other laws, including the Wpg<sup>11</sup> and WIV<sup>12</sup>. In addition, internal rules of the participating organizations regarding the sharing of information apply. Together, these rules and regulations can make it unclear what is possible and can hinder the exchange of information between participants and the information node.

In order to facilitate the exchange of information between participants, a protocol should be created early on in the collaboration. The creation of a working protocol for the exchange of information should happen before a system to facilitate this information sharing is created. If the system is created before there is clarity on how information can be shared, the information sharing will possibly be less than optimal or significant changes to

---

<sup>10</sup> Wet bescherming persoonsgegevens (Personal Data Protection Act), the law regulating the use of information regarding natural persons. For example, the information gathered regarding a person can only be used for the purpose it was collected for. This can be a problem if the goal is related, but not identical to this purpose.

<sup>11</sup> Wet Politiegegevens (Police Data Protection Act)

<sup>12</sup> Wet op de Inlichtingen- en Veiligheidsdiensten (Law on Intelligence and Security services)



the system have to be made which can cost time and money which often are scarce during the creation of an information node.

After a protocol that allows the information to be shared legally has been established, a system can be created to support this, but as stated before, the protocol to share information is more important.

The MIK, RIEC, and FEC have found that it is best to have meetings with the legal experts from the different organizations as fast as possible after the goal of the information node and the information needed to reach this goal is specified, and to create a protocol that can be used to share this information. When this is in place, it can be used by the parties to collaborate and share information in a way that is both legal and accepted by the participants. The CT Infobox has different legal challenges when sharing information, in particular the WIV and has created the protocol for sharing information in a different way (being created before the start of the information node rather than from consultations with all participants), but they also underline the importance of a working protocol<sup>13</sup>.

This problem, the large number and complexity of rules and regulation regarding information sharing, was also found by Whitman and Mattord (2011).

## ***Collaboration***

Collaboration includes lessons that regard how the information node works. They have an impact on the actual working of the information node and can have a strong impact on the success of an information node.

### **11. Resistance against the creation on a personal and organizational level should be accounted for; people might fear for losing existing work. (MIK, RIEC, CT Infobox)**

When a new way of working is introduced, as happens when an information node is created, things change within the involved organizations. It may lead to employees of the organizations having to give up tasks they have performed for years or to have to change the way these tasks are performed. For people who have developed an expertise in these tasks, this might be hard. Often it is not experienced as a lack of belief in the importance of the information node, but a more personal fear that they might become obsolete or at least less important. This leads to these employees agreeing with the changes in public, but refusing to accept them when they should.

This fear is often just, and information nodes should therefore consider these employees, possibly providing them extra training in the new way of working in order for them to develop new expertise.

In addition, these employees can also be included in the design of new work methods. It was experienced that while it is possible to decide what should happen in the information from a top down perspective, the actual way the tasks are performed should be created with or by the people who have to perform them. This potentially removes the fear of change and will create methods with which the responsible people can work efficiently. It might also prevent the employees from resisting change that has been forced upon them by their superiors.

Besides the resistance from employees, a new information node will often work in a field where other inter-organizational collaborations are already active. These collaborations and regular organizations might see the information node as a threat, as it is often larger and therefore more influential than these collaborations between a small number of organizations. To prevent these collaborations and organizations from standing up against the information node, the tasks of the information node should be clearly communicated to them and it should be shown how the information node can support and not take over their tasks. On the long run, their fear might be just, as successes from the information node could lead to growth and new tasks that were previously performed by smaller collaborations. However, that is a slow and organic process and it should be clear that this is not the goal of the information node.

The fear on a personal level was experienced by the MIK and RIEC and required some effort to identify, since these employees were often positive about the plans when they were presented and discussed. The fear for losing work from other inter-organizational collaborations or organizations was experienced by the MIK and CT Infobox and was solved through clear communication.

The resistance against change within an organization was also acknowledged by Val and Fuentes (2003) who state that it is an essential factor to be considered in any change process. They reckon that managing any resistance is the key for change success or failure. It is possible that the fear decreases as the need for the information node is more apparent, for example the CT Infobox was created with the common realization that terrorism was a real threat, because of this, organizations and individuals might be more willing to give up tasks and power in order to be better able to combat this problem.

---

<sup>13</sup> For example, the Informatieprotocol FEC 2011

**12. Joining the information node should provide an advantage both for the node and for the participant. (MIK, RIEC, FEC, IKC)**

When getting partners to join an information node, it should be considered that great differences can exist in the way the organizations work and the impact this has on for example the decision making process. A strongly hierarchic organization will most likely need more time to reach a decision because of the layers of the hierarchy the decision needs to pass. Also, if an information node supports the core tasks of an organization, it will be more willing to join than when it regards something with lower priority for the organization. This difference between organizations is not only visible in how long it takes them to join, but also in their capability to keep up with the changes in the node and the possible investments that go along with it. Each organization that joins the information node should be of value to the information node as a whole, either because it provides new information or because it can share experiences. In addition, it should be considered how to treat potential participants who are unable to contribute the required resources to the information node. They could be excluded from the information node, or can be included under certain conditions such as a lower priority for their requests. It could, however, be argued that when the parties cannot provide the required capacity, they do not consider the information node to be important enough and therefore should not benefit from it. When the information node would be relevant enough, they would find a way. However, if the information node has a need for the information this participant can provide, effort to include this organization might have to come from the information node.

Within the node, all parties should see how the information node provides an advantage for their organization. Without this, they will be less motivated to participate and the effectiveness of the information node decreases. This is also supported by a feeling of fairness, organizations should perceive that they at least get back what they put in and that each party provides a valuable contribution. This does not necessarily mean that each organization should provide equally, but it does mean that when an organization is unable to contribute to the information node fully they should communicate why and show what it is they do with the information and why this is valuable for the information node as a whole. This can happen when laws do not allow all parties to contribute equally. Following from this it is also of importance that the role each participant has in the information node is clear. Possibly not all parties are equally involved with the information node, not all participants are able to share an equal amount of information, or participants want to use the information from the information node for different goals. It should be specified to what extent this happens, for example the amount of resources provided could increase when an organization uses the information node more and it can be defined exactly what each organization can do with the provided information (keeping in mind the goal of the information node).

Each of the information nodes has experienced this to some extent. A number of information nodes (including the FEC, CT Infobox, and MIK) have the requirement that all participants have to agree for a new participant to join the information node, meaning that all participants should see the added value of the extra party.

All information nodes have established what the information shared by the information node can and can't be used for, in order to prevent misuse and misunderstandings.

With respect to potential participants unable to provide resources the MIK decided to exclude these parties from the information node. They still are allowed to request information from the MIK (while regarding legal limitations), but these requests have the lowest priority and this information is only provided if it is also relevant for the MIK or one of the participants or when there are no other current requests. The exclusion of these parties was possible because the MIK has access to their information systems through other participants.

The importance of knowing what each participant provides and what their value to the information node is, as well as knowing how the information node is of value to the organization was found to be of importance by all examined information nodes. This is likely because organizations are reluctant to provide their information (Grijpink, 2010b) and even more so if it is unclear if this will provide them with any advantages. Specifying explicitly what each participant provides and what they can do with the information could also be considered a control system for trust (Tan & Thoen, 2000).

**13. Trust is important, the information node can help to increase it over time. (IKC, CT Infobox)**

Since an information node requires people and organizations to work together and share information often of value to the organization, a certain amount of trust is required. When this trust is absent, the organizations are reluctant to share the information that is of value and the information node is unable to function. However, important as it is, trust is hard to control. Trust in the information node itself can be supported by working as transparent as possible, showing participants what exactly is done with the information they have provided and communicating any results back to them. Also, creating clear rules of what can be done with the information and checking if these are still followed can have a positive effect. The trust among the organizations can be harder. Often there is some trust at the start, when the organizations have had contact before, which is likely

since the organizations face the same problem and have likely been active in the same or related fields. This trust can then be used to work within the node and might increase over time as the organizations become more familiar.

All the information nodes examined in this research have stated the importance of trust as can be seen in the comparison in chapter 5. The amount of importance that each node gives to trust differs however. The IKC names it as the most important aspect of the information node, as there are no formal mechanisms to prevent misuse of information exchanged within the information node. The CT Infobox on the other hand, requires some trust in the information node itself, but has strong protocols and rules. These rules and protocols compensate for any lack of trust among participants. The CT Infobox did state that the existence of the information node has increased the bonds and trust between the participants, easing collaboration.

Tan and Thoen (2000) state that when there is insufficient trust, it can be attempted to increase or substitute this by implementing control mechanisms, for example having the information node check all information that is exchanged and what is done with it, or by requiring a certain amount of input from each participant.

Important to note is that, although it is often considered crucial for the functioning of the information node, there is no uniform way to create and maintain, or even measure trust. Ideally it will exist at the start of an information node and will only grow over time as the organizations become more accustomed to working together, but one mishap by an organization can diminish the trust in the entire information node (for example when an organization uses the information node for something else than the intended purposes). Clear agreements are often seen as the best way to prevent this, but these should not limit the participants too much. From analyzing the examined information nodes it seems that when the information becomes more sensitive for the organizations involved, there is less reliance on trust and more on control systems.

#### **14. Clarify the tasks of the supervisors early on. (CT Infobox)**

A number of the information nodes examined in this research have some sort of supervising organ, coordinating actions of the information node and providing overall guidance. These organs often exist of higher level representatives from the participating organizations and meet on a periodical basis, less often than the information node itself. In some cases the coordinating organ is more or less independent of the working of the information node and is only tasked with the administrative coordination.

It should be clear for the participants in the information node what the tasks of the supervisor entail and how they influence the actions of the information node. When this is clear, it can prevent participants from expecting more from the supervising organ than it can do and it can prevent them from feeling limited or intruded by the tasks the supervising organ performs.

The CT Infobox noted that there was a lack of clarity regarding the tasks of the Coördinerend Beraad with participants being unsure what to expect from the supervising organ. When this is the case, it is possible that the supervising organ does not perform as effectively as possible. Because the coordinating organ often exists of employees from higher in the participating organizations, it can perform certain tasks with relative ease. When these tasks have to be performed by the node itself, more resistance might be encountered.

According to the chain-computerization theory (Grijpink, 2010b) there should be no overarching authority which coordinates the collaboration. In the case of a supervising body, as found at an information node, this body consists of employees from the different organizations that are also active in the information node and can thus be considered part of the information node. However, if this is the case it seems that the coordinating organ and the information node itself should communicate more closely and possibly less in one direction. It is now the case that the coordinating organ instructs the information node. It could benefit from more communication, where it is possible for the information node to transfer tasks to the coordinating organ when the organ is more capable of performing these tasks.

#### **15. Specify the form of collaboration. (MIK, RIEC, IKC, CT Infobox, FEC)**

As was found during the comparison of the information nodes in chapter 5, the way the information nodes collaborate differs. Three ways of collaborating within an information node have been found in this research.

- On a daily basis, with a number of permanent employees who work together directly
- On a periodical basis, during meetings with representatives from the participants
- On a daily basis, with a number of employees who work together directly, supported by a coordinating organ consisting of representatives from the participants who meet on a periodical basis

The MIK shows the first form of collaboration, consisting of collaboration on a daily basis where the information that is shared is reported back to the participating organizations directly. The second form of

collaboration can be found in the IKC, where the different ISAC's meet on a periodical basis to exchange information and experiences. In addition, there is a coordination organ in the form of the NCSC which supports the administrative side of the information node and which can provide for example training for the participants. The other three information nodes all consist of collaboration on a daily basis supported by a coordinating organ.

Which form is optimal differs for each information node. When an information node shares information that is used in the daily processes of the participants, a daily collaboration and information exchange is of value. When the goal of the information node is to share information on a subject that is not considered one of the primary processes of the participants, a periodical meeting can suffice.

If the daily collaboration requires a coordinating organ, seems to depend on the actions or projects the information node coordinates besides the information exchange. It was found that if the information node is involved with projects performed by the participants, a planning of which projects should be performed is required. This planning can be made by a coordinating organ consisting of representatives of the different organizations. When the information node performs no other tasks than sharing information, there is no need for further coordination.

### ***Information Sharing***

Information sharing includes lessons that regard how the information is shared within the information node. They all regard what is shared within the information node, not how this is done.

#### **16. All information should be shared formally, ensuring the origin of the information is clear and the information can be used. (MIK, FEC, CT Infobox)**

As stated before, when sensitive information is shared, strict rules have to be adhered to; information should only be shared when this is legally possible. When information is shared in a formal way, the legal sharing of information can be ensured. In addition, the reliability of information can always be checked and information is less likely to be marked as classified when it is not.

When information is shared by participants who have to follow strict protocols, it might be automatically classified as sensitive, even when this information originates from an open source. The formal exchange of information can prevent this, as it will list the original source of the information. In addition, when the source and thereby reliability of information is clear, it will be more usable in an investigation.

In practice, the MIK uses a Proces-verbaal when exchanging information, including the source of the information to ensure it is traceable and its sensitivity can be checked.

The CT Infobox checks the reports it gives out by having it reviewed and signed by each of the parties that have been involved in it. This is time consuming and has been said to be limiting to the fast working of the information node, but it ensures the quality and usability of any information provided by the information node.

The importance for this formal exchange follows from the laws these information nodes have to adhere to. The information nodes are limited in what information they can share and if the information is shared or otherwise acquired when this is not allowed, the information can be dismissed when used in an investigation. This works two ways, as information might not be used when it is believed to be not allowed to share, while the original source is accessible by the requesting party.

The formal sharing of information is not equally important for all information nodes. It seems that information nodes whose participants perform investigations and use the information to take legal actions benefit more from the formal exchange of information. Information nodes such as the IKC which are used to exchange experiences and best practices have less need for a more complex, formal exchange.

#### **17. All primary participants should be present at all meetings. (IKC)**

When an information node exists (in part) of periodical meetings, it is of importance that all directly participating organizations attend these meetings. This has two main reasons, the first is that attendance and input of all participants gives a more complete view of the developments and that their input can be of value for the other participants. The second is that the organizations that do not attend might miss crucial information. This is especially true when the periodical meetings are the only formal contact the information node has.

This can be avoided by making the meetings mandatory, but this brings the risk of organizations sending under qualified and unmotivated employees who have neither the knowledge of their organizations to provide relevant input, nor the authority to use the information from the meetings. A better way could be to look at the reason for the absence and attempting to solve that. Possibly the organizations do not realize the importance of the information node.

The Water ISAC in the IKC found the (lack of ) attendance of primary participants to be a potential problem, as they use the meetings as the only way to communicate information on incidents and when organizations are absent they have no way of receiving this information.

The reason for not attending each meeting could be that the participant does not see the information node important enough. As with the right qualification of the employees in the information node, this could be because the problem it combats is not severe enough (Grijpink, 2010b) or because some of the organizations are not fully aware of the severity of the (potential) problem.

**18. In order to keep information richer, the employees of an information node should maintain sufficient knowledge of the organization they originate from. (MIK, FEC, CT Infobox)**

An information node exists of a number of parties each contributing information and knowledge and thereby increasing the value of the information node. To this end, it often happens that the actual information node exists of employees from the different organizations staffing the information node. When the information node works in this way, it is considered important that the employees staffing the node are more than mere access to the respective systems. The employees should have a connection with and knowledge of the organization they originate from. This connection can be maintained by leaving the employees officially part of their respective organizations, and having them report information directly, thereby 'staying in the loop' at their organization for training and such. Or by having employees work at the information node for a predefined period of time and then have them replaced by another employee from their respective organization. This exchange ensures knowledge of how the organization works as new employees can bring new insights.

Which of these methods is the best choice for any given information nodes seems to depend mainly on the nature of the information that is used. When this information is sensitive, it cannot be shared with the participating organization directly and the information node can best consist of dedicated staff working for the information node only. When the information is not sensitive and can be used in the processes of the organizations directly, the direct link that employees from the different organizations still have can be valuable.

The direct link between the information node and the participants through the employees in the information node can be found at the MIK. The CT Infobox and the FEC use employees from the different organizations who work dedicated at the information node.

Besides improving the quality of the information node, this also helps with involving the participating organizations with the information node. According to the chain-computerization theory each participating organization should see the advantage of the information node and should be involved (Grijpink, 2010b). When the information node exists of employees with a connection with the organizations, they will know the needs of the organization they originate from and will act in its best interest. This could contribute to the value the organizations see in the information node.

**19. Physical collaboration is important, it leads to richer information exchange. (MIK)**

The sharing of information can in theory happen mainly automated, using computer systems. However, when information is shared only automated, or through digital media without the interpersonal contact, it is possible for details to get lost. Information that might seem implied by the sender can be unknown by the receiver and checking the information costs more time and effort through digital media than it does when collaborating face to face.

This was experienced by the MIK, who stated that for example an incomplete description could have parties looking out for a yacht when they should be looking for a sailboat. In that case, the sender of the request might have thought using the term boat implied it to be a sailboat which was interpreted incorrectly. Face to face communication eases the checking of information and is experienced to prevent this type of mistake.

The loss of richness when communicating digitally has been acknowledge by a number of researchers (for example Daft & Lengel, 1983; O'Connell, Whittaker, & Wilbur, 1993). These researches also included the use of video conferencing and found that there still was some loss of information richness. So even though it can be more expensive to facilitate physical collaboration, it increases the effectiveness of the information node.

These lessons learned have been used to create a checklist ( which can be used during the creation and use of an information node. Because each problem is unique and each information node is a unique solution to this problem, it is possible that information nodes encounter problems in areas not covered by the checklist or this research. Creators of information nodes should therefore care not to stare blind on the checklist, but to use it as guidelines, rather than rules.

## 7 Conclusion / Discussion

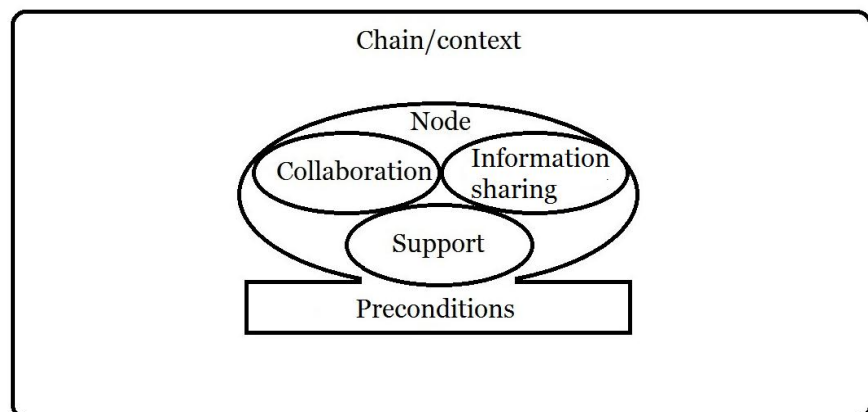
This research has provided a theoretical definition of an information node, along with the aspects that are relevant for such an inter-organizational collaboration. In addition, it has provided a list of lessons learned that have been relevant for existing information nodes and therefore could support the creation of new information node and the further development of existing information nodes. Most of these lessons can be related to existing theory from IOS and chain-computerization, which indicates that they could likely be generalized to some extent.

To answer sub-question 1.1 “What is an information node?”, the definition that has been created based on both theory and existing information nodes combined with discussion with experts is: ‘A formal, structured collaboration between a number of organizations within a **social chain**, which includes some form of **interpersonal contact**, that is focused on combating the **dominant chain problem** and that resolves around, but is not limited to, the **sharing of critical information**.’

Using this definition and theory, an answer to sub question 1.2 “What are aspects of an information node?” was created, consisting of four categories (shown in Figure 3) containing a number of aspects of an information node that can differ between information nodes (shown in Table 14).

**Table 14 – Aspects of information nodes**

<b>Context</b>
Chain
<b>Node in context</b>
Level of the chain process
Position in the chain.
Reason
Scale
Product
<b>Collaboration</b>
Forms of collaboration.
Participating organizations
Entry/exit barriers
Trust
<b>Information Sharing</b>
How
What
Who
<b>Support</b>
Systems
Integration
<b>Preconditions</b>
Finance
Legal
Information security



**Figure 3- categories of aspects of information nodes**

By using these aspects to analyze a number of information nodes that confirm to the definition, factsheets were created, containing both an overview of the working of the information nodes, how the aspects are realized, and what lessons the information node has learned during its existence, providing an answer to sub-question 2 “How are these aspects, found in sub-question 1.2, realized in each node?”

This information for the factsheets was gathered through interviews with the information nodes, analysis of existing documents, and discussion with experts and practitioners.

By comparing these factsheets, some patterns were found, providing an answer to sub-question 3 “What patterns can be found in the way the different nodes have been constructed?” For example, all information nodes were created following a government initiated publication highlighting a problem in their field. This indicates that each information node has had some political motivation to be created. Three forms of collaboration were identified; daily, periodical, or a combination of both. It was found that none of the collaborations within the information nodes consists of more than ten participants, although the reason for this was not researched.

The comparison also indicated some principles of the chain-computerization doctrine that do not fully apply to information nodes, mainly because of its strict rules on what is possible and impossible. Information nodes seem to sometimes be positioned in a grey area between these rules.

From the lessons learned in the factsheet, combined with the other information and discussion with experts a checklist containing the lessons learned was created, which is shown in Table 15. This list is a combination of lessons learned by the individual information nodes, generalized to cover information nodes in general and combined to prevent overlap and increase clarity. These lessons are an answer to sub question 4. "What lessons can be learned from the creation of earlier information nodes and how are these usable for the creation of new information nodes?"

**Table 15 - Checklist**

<b>1</b>	The information node should have a clear goal to manage expectations.
<b>2</b>	Get operational soon, sort out the details later.
<b>3</b>	Take enough time for creating the information node, decision making in organizations can be slow.
<b>4</b>	Be persistent, when an approach fails, look for other options.
<b>5</b>	Without political and/or societal support an information node has little chance of success, create publicity.
<b>6</b>	Each node is unique, you cannot use a blueprint.
<b>7</b>	Participants should have the right qualifications.
<b>8</b>	Financing can be hard, it should be considered at the start of the information node and entails more than just the setup.
<b>9</b>	It is important to consider where to physically locate the information node.
<b>10</b>	Being legally able to share information is more important than a system for sharing this information.
<b>11</b>	Resistance against the creation on a personal and organizational level should be accounted for; people might fear for losing existing work.
<b>12</b>	Joining the information node should provide an advantage both for the node and for the participant
<b>13</b>	Trust is important, the information node can help it increases over time.
<b>14</b>	Clarify the tasks of the supervisors early on.
<b>15</b>	Specify the form of collaboration
<b>16</b>	All information should be shared formally, ensuring the origin of the information is clear and the information can be used.
<b>17</b>	All important partners should be present at all meetings.
<b>18</b>	In order to keep information richer, the employees of an information node should maintain sufficient knowledge of the organization they originate from.
<b>19</b>	Physical collaboration is important, it leads to richer information exchange.

Together, the answers to the sub-question provide an answer to the main research question:

*"What aspects should be taken into account when creating an information node and can earlier experiences in this field be used to create a checklist to support both the creation of new and the functioning of existing information nodes?"*

The aspects that should be taken into account are the aspects presented in chapter 3 and shown here in Table 14. The creation of new information nodes can be supported by the lessons learned provided in chapter 6, which can form a foothold in a complex area. It should be stressed that they should only be used as guidance and in no way form a framework for the creation of an information node. They can help practitioners who would else start from scratch create an overview of how an information node can function.

These lessons can also be of value for existing information nodes, as a number of problems are not limited to new information nodes, but can surface later in the lifespan of an information node.

## 7.1 Limitations and future research

This research is explorative of nature and therefore delivers no quantifiable results. It can, however, form a basis for future research and it could in its current form be a useful tool for practitioners involved with the creation of information nodes. As stated earlier in the research, it can and should not be considered to be a blueprint for the perfect information node. It is meant to provide creators of information nodes with an overview of what aspects should be considered and a list of lessons that have been learned by other information nodes during their development and existence, providing some foothold when starting a project the size of an information node.

The research provides a first attempt at defining and supporting the creation of a previously undefined form of inter-organizational collaboration, information nodes. A definition has been created for an existing form of collaboration, based where possible on theory, but completed by examining the existing information nodes.

This means that the definition holds true for this research and it has been checked often and by a number of experts and practitioners, but it is based on a limited number of information nodes which all exist in the Dutch security sector. Further research should prove if the definition is true for information nodes in other countries and sectors as well.

This can be extended to the lessons learned. Future research is required to see to what extent the lessons learned by information nodes in the Dutch security sector also hold true for other sectors. Cross-sector research can be performed on a larger scale, potentially providing quantitative results, and allowing for the creation of a more complete list of potential issues and lessons learned.

Even when only considering the Dutch security sector, the list of lessons learned that is provided by this research is not exhaustive. Since each information node was interviewed once during the research, they might not have named all lessons they learned during the existence of the information node. Lessons that were reported by a small number of information nodes might have played at other information nodes as well even though they did not report them.

Finally, this research has used the chain-computerization theory as a basis. This has provided a number of useful principles, but does not fit information nodes perfectly, as was to be expected since the theory does not account for the existence of information nodes. There is some friction between how information nodes behave and how the chain-computerization theory states that solutions on the chain level should act. This includes the activity on the base level of the chain which can be found in information nodes, the existence of an external force other than a common need when creating an information node, the existence of (more) dominant participants, and the sharing of more information than is strictly necessary.

Future research could expand the chain-computerization theory and create a specific set of rules for information nodes, as it seems that the basic principles of the chain-computerization theory hold true for information nodes. However, information nodes sometimes seem to reside in the grey area between what is possible and what is impossible according to the chain-computerization theory.



## 8 References

- Adviescommissie Informatiestromen Veiligheid. (2007). *Data voor daadkracht - Gegevensbestanden voor veiligheid: observaties en analyse*. Retrieved from <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2007/08/30/rapport-data-voor-daadkracht.html>
- Baker, G. P., Gibbons, R., & Murphy, K. J. (2008). Strategic alliances Bridges between islands of conscious power. *Journal of The Japanese and International Economies*, 22, 146-163.
- Baus, F., & Ramsbottom, C. a. (1999). Starting and Sustaining a Consortium. *New Directions for Higher Education*, (106), 3-18.
- Chi, L., & Holsapple, C. W. (2005). Understanding computer-mediated interorganizational collaboration: a model and framework. *Journal of Knowledge Management*, 9(1), 53-75.
- Daft, R., & Lengel, R. (1983). *Information Richness: A new approach to managerial behavior and organization design*.
- Dean, J. W., & Sharfman, M. P. (1996). Does decision process matter? A study of strategic decision-making effectiveness. *Academy of Management Journal*, 39(2), 368–396.
- Devlin, G., & Bleackley, M. (1988). Strategic alliances Guidelines for success. *Long Range Planning*, 21(5), 18-23. Elsevier.
- Duivenboden, H., Heemskerk, P., Luitjens, S., & Meijer, R. (2005). Informatisering in ketens. In Lips, M., Bekkers, V., & Zuurmond, A. (Eds.), *ICT en openbaar bestuur* (pp. 349-373). Utrecht: Lemma BV.
- Dyer, J. H., Kale, P., & Singh, H. (2001). Strategic Alliances Work. *MIT Sloan Management Review*, 37-43.
- Eisenhardt, K., & Schoonhoven, C. B. (1996). Resource-based view of strategic alliance formation: Strategic and social effects in entrepreneurial firms. *Organization science*, 7(2), 136-150.
- Grijpink, J. H. A. M. (1997). *Keteninformatisering met toepassing op de justitiële bedrijfsketen*. Voorburg: J. H. A. M. Grijpink
- Grijpink, J. H. A. M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving*. Den Haag: Sdu Uitgevers
- Grijpink, J. H. A. M. (2010a) *Keteninformatisering in kort bestek. Theorie en praktijk van grootschalige informatie-uitwisseling* (2nd ed.). Den Haag: Boom Lemma uitgevers
- Grijpink, J. H. A. M. (2010b). Chain Analysis for Large-scale Communication Systems: A Methodology for Information Exchange in Chains. *Journal of Chain-computerization*, 1, 1-32.
- Homburg, V. & Bekkers, V. (2005). ICT, toezicht en informatierelaties. In Lips, M., Bekkers, V., & Zuurmond, A. (Eds.), *ICT en openbaar bestuur* (pp. 277-296). Utrecht: Lemma BV.

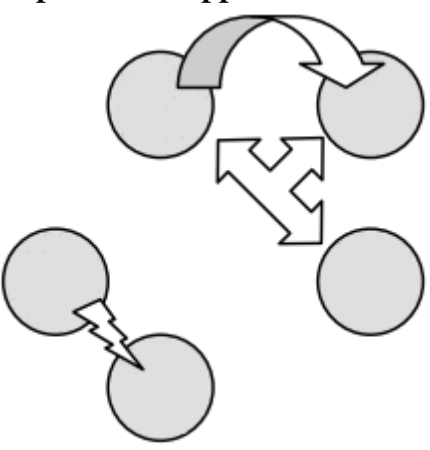
- Hong, I. B. (2002). A new framework for interorganizational systems based on the linkage of participants' roles. *Information & Management*, 39(4), 261–270. Elsevier.
- Horstink, J. (2009). Werken met het samenwerkingsprofiel. In J.H.A.M. Grijpink & M. Plomp (Eds.), *Kijk op ketens: Het ketenlandschap in Nederland* (pp 127-139). Den Haag: J.H.A.M. Grijpink.
- Jagdev, H., & Browne, J. (1998). The extended enterprise-a context for manufacturing. *Production Planning & Control*, 9(3), 216-229.
- Janssen, M., & Joha, A. (2006). Motives for establishing shared service centers in public administrations. *International Journal of Information Management*, 26(2), 102-115.
- Karahannas, M. V., & Jones, M. (1999). Interorganizational systems and trust in strategic alliances. Proceedings of the 20th international conference on Information Systems (pp. 346–357). Association for Information Systems.
- Kumar, K., & Van Dissel, H. G. (1996). Sustainable collaboration: Managing conflict and cooperation in interorganizational systems. *Mis Quarterly*, 20(3), 279–300. JSTOR.
- Kumar, R. L., & Crook, C. W. (1999). A multi-disciplinary framework for the management of interorganizational systems. *ACM SIGMIS Database*, 30(1), 22–37. ACM.
- Lapadat, J. C., & Lindsay, A. C. (1999). Transcription in Research and Practice: From Standardization of Technique to Interpretive Positionings. *Qualitative Inquiry*, 5(1), 64-86.
- Lorange, P., Roos, J., & Brønn, P. S. (1992). Building Successful Strategic Alliances. *Long Range Planning*, 25(6), 10-17.
- Mechling, J. (2007). Shared Service Center. *3ecompass.net*.
- Meier, J. (1995). The importance of relationship management in establishing successful interorganizational systems. *The Journal of Strategic Information Systems*, 4(2), 135-148.
- Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, 21(2), 241-242. Updated version, last modified: November 12, 2011 <http://www.qual.auckland.ac.nz>
- O'Conaill, B., Whittaker, S., & Wilbur, S. (1993). Conversations Over Video Conferences: An Evaluation of the Spoken Aspects of Video-Mediated Communication. *Human-Computer Interaction*, 8(4), 389–428.
- Parkhe, A. (1993). Strategic alliance structuring: A game theoretic and transaction cost examination of interfirm cooperation. *Academy of management journal*, 36(4), 794–829. JSTOR.
- Poppel, I. (2010). *De domeineigenaar geketend: Coördinatie en sturing in de toeslagenketen*. (Unpublished manuscript). Erasmus Universiteit, Rotterdam.
- Post, J., Preston, L., & Sachs, S. (2002). Managing the extended enterprise. *California Management*, 45(1), 6-28.

- Tan, Y. H., & Thoen, W. (2000). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce*, 5(2), 61–74. ME Sharpe, Inc.
- Thomas, G. (2011). A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure. *Qualitative Inquiry*, 17(6), 511-521.
- Todeva, E., & Knoke, D. (2005). Strategic alliances and models of collaboration. *Management Decision*, 43(1988), 1–22.
- Updegrove, A. (1995). Standard setting and consortium structures. *StandardView*, 3(4), 143–147. ACM.
- Val, M. P. D., & Fuentes, C. M. (2003). Resistance to change: a literature review and empirical study. *Management Decision*, 41(2), 148–155.
- Venrooy, A. van, & Sonnenschein, L. (2008). *Ketenunits: grip krijgen op publieke ketens*. Arnhem: Drukkerij Gelderland.
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4<sup>th</sup> ed.). Boston: Course Technology.
- Yin, R. (2003). *Case study research: Design and methods*. Thousand Oaks, California: Sage Publications.
- Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization science*, 9(2), 141-159.

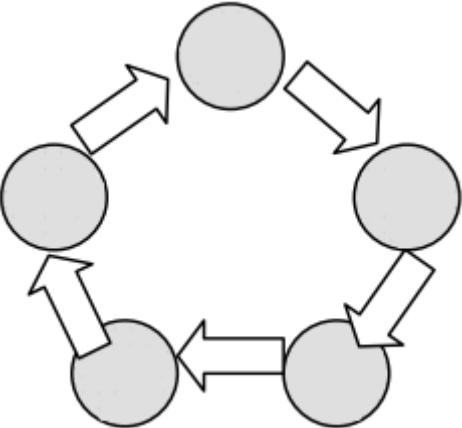
# Appendix 1 – Models for information sharing

The models for information sharing within a chain by Duivenboden et al. (2005) as described by van Poppel (2010)

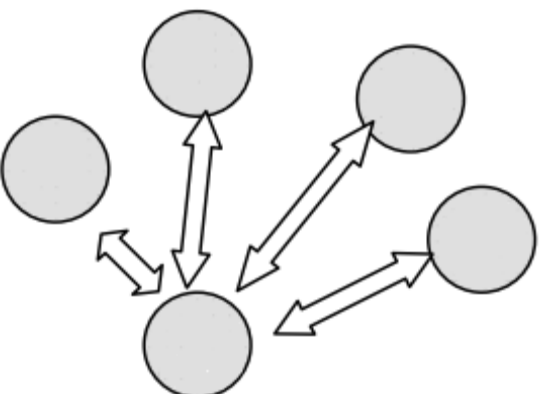
**Table A1.1 - the prosthesis approach (Duivenboden et al., 2005; van Poppel, 2010)**

<p><b>The prosthesis approach</b></p> 	<p>In this model each organization has its own information system and exchange of information only happens on an ad hoc basis. Responsibilities for the maintenance of the systems and the information are with the respective organizations.</p> <p>Advantages of this model are that each organization maintains its independence and isn't limited in its possibilities. Disadvantages are that there is no standard for the format of the information and no information infrastructure. This might lead to slow information exchange and lower quality of the information.</p>
---	---

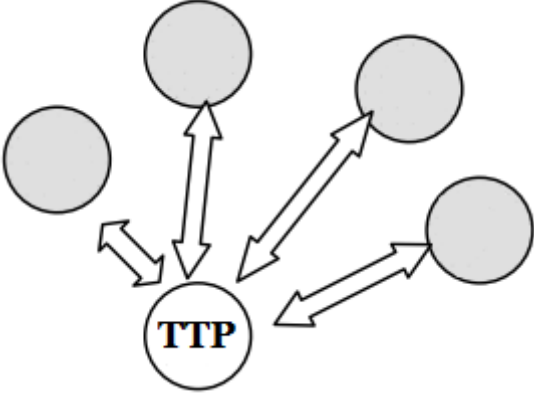
**Table A1.2 - the relay approach (Duivenboden et al., 2005; van Poppel, 2010)**

<p><b>The relay approach</b></p> 	<p>In this model each organization has its own information system, but the information system is structured in a common format. While a subject moves through the chain, the information on the subject moves with it from party to party. The organization remain largely independent and can manage their own information systems, but they do need to agree on what the standard format should look like.</p> <p>Advantages of this model are that it is relatively simple, information follows the subject and the organizations that are involved remain autonomous. Disadvantages are that the relay approach is error prone, when an error is made it is carried through the chain and it is possible for information to go missing or be sent to the wrong place.</p>
--	---

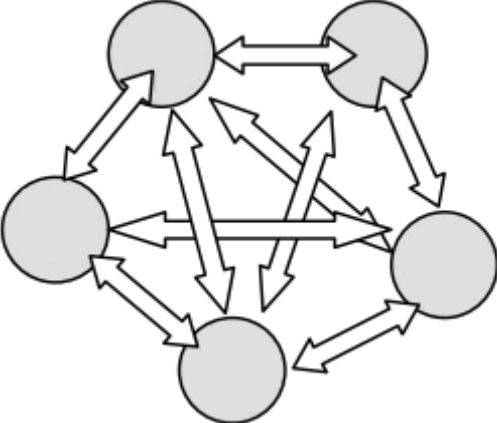
**Table A1.3 - the spider approach (Duivenboden et al., 2005; van Poppel, 2010)**

<p><b>The spider approach</b></p> 	<p>In this model one organization leads the other parties in the chain to adapting their information systems to its system. Information and files are kept in a central location, with the responsibilities for this information also on a central level. Advantages are that the information sharing becomes easier, more efficient and more transparent because it can all be controlled from a single location. Disadvantages are that the organization that controls the information can get too much power, which can become a problem when it pursues its own goals over that of the chain.</p>
---	---

**Table A1.4 - the notary approach (Duivenboden et al., 2005; van Poppel, 2010)**

<p><b>The notary approach</b></p> 	<p>This model shows similarities to the spider model, but instead of the information being controlled by a party within the chain, it is controlled by a trusted third party (TTP). This also gives some of the responsibilities for the information to this 'notary'. Advantages are more easy, efficient and transparent information sharing, but also more control of the information streams because the trusted third party has no personal interests in the information and can therefore use its independent judgement to optimize information flow.. Disadvantages are that this model can only work when all parties are dedicated to it, which can be hard when the profit differs for organizations. Also, the trusted third party is an extra link in the chain which might make the information exchange more complex.</p>
---	---

**Table A1.5 – the network approach (Duivenboden et al., 2005; van Poppel, 2010)**

<p><b>The network approach</b></p> 	<p>In this approach, all organization have their own information systems which they make (partially) accessible for the other parties. Information and files are kept in a decentralized location, but are linked within the systems. The advantage of this model is that information can be used without intervention from the party that owns the systems that stores it. However, the disadvantage is that this type of information exchange requires quite some effort from all parties, and without a good reason this might be too much. Because it is important to maintain a high information quality, when one party neglects its responsibilities the whole system can fail. Because there is no overarching authority, it is hard to prevent this.</p>
---	---

## Appendix 2 – The mission profile

The goal of the mission profile is to analyze a chain, usually with the goal to see if a chain-wide solution is necessary and possible or to see how a current chain-wide solution is working. It does this by analyzing the product of the chain, the dominant chain problem, how the subject moves through the chain and what information could solve the existing problems. A step-by-step explanation of the mission profile can be found in Table .

**Table A2.1 - The mission profile (adapted from Grijpink, 2010b)**

<b>Element</b>	<b>Explanation (underlying questions)</b>
Social chain product	What is the purpose of this chain in our society? Which basic social value is achieved through the chain-cooperation?
Chain challenge	Which concrete objective is being worked towards to contribute to the social chain product?
Dominant chain problem	Which chain problem that none of the chain partners is able to solve on its own is causing the chain partners such difficulty that it could result in the entire chain being discredited?
Target group	On what (object) or who (subject) does the chain focus? Which role do they play (risk location; victim, applicant) and what position do they take: are objects private moving property (building) or is the object a moving phenomenon (traffic congestion); are the subjects co-operating (e.g. a patient) or non-co-operating (e.g. a crime suspect)?
Chain partners	Which chain partners contribute to the social chain product by jointly tackling the dominant chain problem while trying to meet the chain's challenge?
Process steps at operational level (links in the chain)	In which logically consecutive process steps (links in the chain) is the social chain product brought about?
Intermediary product(s) of each link	With which intermediary products – used to pass on the result of the work from one link to another – is the social chain product brought about?
Critical details	Which essential details (usually 2-3) can prevent incorrect decisions and trigger the right action in the chain? What information do you need to know?
Important points of contact	Where or on which occasions do chain partners usually meet the target group?
Criterion for the chain	What determines the chain's boundary? Which cases belong to the chain, and which do not?

The item, 'important points of contact', is not used in this research, since the mission profile generally considers a target group that is helped by the actions of the chain, where in the security sector the target group is often a problem or a group causing a problem and this contact does not necessarily take place.

## **Appendix 3 – interview questions**

Because the research uses information nodes in the Dutch security sector, the interview questions used are in Dutch.

1. Wie bent u en voor welke organisatie bent u werkzaam?
2. Wat is uw rol en de rol van uw organisatie in het **\*informatieknooppunt\***?
  
3. Waarom is het knooppunt gestart?
4. Kijkend naar de taken van de keten waarin u actief bent, op welk niveau is het informatieknooppunt actief? Heeft het een ondersteunende functie, is het actief in het primaire proces of werkt het op beleidsniveau?
5. Zijn alle partijen in de keten actief in het informatieknooppunt? Omvat dit ook alle processtappen in de keten? Welk deel is direct betrokken?
6. Op welke schaal is het knooppunt actief? Is dit lokaal, regionaal, nationaal of internationaal?
7. Wat is het product dat het knooppunt creëert?
  
8. Welke organisaties zijn bij het informatieknooppunt betrokken en zijn er partijen die gekozen hebben niet mee te doen?
9. Hoe werken de betrokken organisaties samen binnen het knooppunt, is dit meer dan enkel informatie delen? Hoe vaak gebeurt dit? Voert het knooppunt zelf taken uit?
10. Hebben alle organisaties een gelijke rol binnen het knooppunt?
11. Wie is eindverantwoordelijke voor het knooppunt?
12. Aan welke voorwaarden moet een organisatie voldoen om toe te treden tot het informatieknooppunt?
13. Zijn er voorwaarden verbonden aan het verlaten van het informatieknooppunt?
14. In hoeverre steunt de informatie-uitwisseling en samenwerking op vertrouwen, zijn er systemen om dit vertrouwen te waarborgen?
15. Op welke manier wordt er informatie gedeeld binnen het knooppunt? Bijvoorbeeld dagelijks tussen medewerkers van de organisaties, of tijdens een periodiek overleg.
16. Welke informatie wordt binnen het informatieknooppunt gedeeld?
17. Wat voor informatie wordt gedeeld? Is dit informatie die kritiek is voor de oplossing van een probleem, of algemenere informatie? Is de informatie operationeel, of betreft het ook de werking van de betrokken organisaties?
18. Hebben alle organisaties betrokken bij het informatieknooppunt toegang tot alle informatie? Kunnen organisaties hun informatie met specifieke partners delen?
19. Zijn er computersystemen in gebruik die het informatieknooppunt ondersteunen?
20. Zijn deze computersystemen geïntegreerd in de informatiesystemen van de verschillende organisaties?
21. Door wie wordt het knooppunt betaald? Indien dit door een van de partijen is, heeft deze partij ook meer invloed op het knooppunt?
22. Welke wetten en regels moeten worden gerespecteerd met betrekking tot het delen van informatie? Hoe is dit geregeld in de praktijk?
23. Welke mechanismen bestaan er om te voorkomen dat de informatie in verkeerde handen valt?
  
24. Zijn er dingen waar u bij het opzetten of gebruik van het informatieknooppunt tegenaan bent gelopen die voor problemen hebben gezorgd of die juist een onverwacht voordeel opleverden?
25. Als het knooppunt nu opnieuw opgezet zou worden, zou u dan wat anders doen?
26. Zijn er nog dingen met betrekking tot het knooppunt die niet in het interview zijn langs gekomen die u wilt toevoegen?

## Appendix 4 – Factsheets

### A4.1 CT Infobox

#### A4.1.1 *General description of the information node*

The CT Infobox (Contra Terrorisme Infobox) is a collaboration between law enforcement services, security services, and other services involved in the fight against terrorism. Currently, nine organizations collaborate in the CT Infobox: AIVD, IND, KLPD, MIVD, OM, FIOD, KMar, FIU-NL, and NCTV<sup>14</sup>. Its goal is to contribute to the fight against terrorism by gathering and combining information on networks and individuals who are suspected to be involved with terrorism and the related radicalization.

Initially, this supporting role was performed by the ‘Analytische Cel’, a collaboration created following the 2004 terrorist attacks in Madrid with as goal to ‘keep an eye on’ individuals who might in some way be involved with terrorist activities. This collaboration included the OM, KLPD, and AIVD.

However, due to the laws and regulations regarding secrecy of the information concerning the AIVD, the collaboration was considered unable to function properly and information could not be shared adequately. This led to the restructuring of the collaboration and the creation of the CT Infobox.

The CT Infobox is legally part of the AIVD, which means that technically all information from the AIVD handled by the CT Infobox is kept internally. This way, the AIVD can function in the collaboration while adhering to the laws and regulations.

Because of the nature of the information that is used and because the involved parties do not wish to provide all their information to the partners, the CT Infobox functions like a black box. It has access to the information systems of the participating organizations and combines the information from the systems to look for patterns and analyze the potential threat that a person poses. This leads to an advice, including the threat the investigated individual poses and where the relevant information on this individual is located. This information can then be shared between the organizations on the base level of the chain. The CT Infobox itself does not share any of the information it uses.

This core task of the CT Infobox is performed by a number of employees from the different organizations working together permanently. These employees are seconded from the participating organizations and work in the CT Infobox for a period of 2 to 4 years.

In addition to this, the ‘Coördinerend Beraad’ meets regularly and consists of representatives from the different parties. In the meetings of this steering body the advice provided by the CT Infobox can be discussed and a course of action is chosen. Its main function is to give overall guidance to the CT Infobox and to address managerial issues regarding the CT Infobox.

Since the CT Infobox works as a black box, using information and providing advice, no information is shared in the information node itself. This means that the participants should trust the CT Infobox with their information, but trust between the partners themselves is not crucial (although desirable to ease the collaboration). Working together in the CT Infobox has, however, increased the amount of trust which exists between the participants. This goes both for the Coördinerend Beraad which contains policy makers and for the people directly involved with the CT Infobox. Because they work together on a regular basis. To ensure trust in the CT Infobox itself, any big decision made within the CT Infobox can be vetoed by any participant and discussed in its own organization or ultimately with the respective Minister.

---

<sup>14</sup> AIVD (Algemene Inlichtingen- en Veiligheidsdienst); General Intelligence and Security Service  
IND (Immigratie- en Naturalisatiedienst); Immigration and Naturalization Service  
KLPD (Korps landelijke politiediensten); National Police  
MIVD (Militaire Inlichtingen- en Veiligheidsdienst) Military Intelligence and Security Service  
OM (Openbaar Ministerie); Public Prosecution  
FIOD (Fiscale inlichtingen- en opsporingsdienst); Fiscal Information and Investigation Service  
KMar (Koninklijke Marechaussee); Royal Military Police  
FIU-NL (Financial Intelligence Unit – Nederland); Financial Intelligence Unit – Netherlands  
NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid); National Coordinator for Counterterrorism and Security



### A4.1.2 Context of the information node

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

Element	
Social chain product	Security from terrorism
Chain challenge	Decreasing the risk and fear of a terrorist attack and limiting possible damage of such an attack.
Dominant chain problem	Terrorist remain uncaught and are able to coordinate and perform terrorist acts because of a lack of coordination between parties active in the field of terrorism.
Target group	Individuals or organizations capable of and willing to perform acts of terrorism.
Chain partners	Ministries of Security and Justice, Interior and Kingdom Relations, Foreign Affairs, Defence and Finance, AIVD, MIVD, KLPD, OM, IND, KMar, customs, and local governments.
Process steps at operational level (links in the chain)	Acquire – prevent – defend – prepare - prosecute
Intermediary product(s) of each link	Threat analysis – decrease of possibilities for support – monitor and security measurements – crisis approach and aid coordination – seek out and judge terrorist networks and individuals
Critical details	Information on previous offenses of a suspected person. Information on the contacts a suspected person has.
Criterion for the chain	People threatening to perform , preparing or performing serious acts of violence aimed at people

### A4.1.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

Node in context		
Level of the chain process	Support – The CT Infobox locates information and creates advice based on information, but it does not share this information directly. It does not cover the primary process, since this uses the actual information exchanged on the ground level. The advice contains too little information to use directly.	At what level of the chain process is the node active? (Grijpink, 2010a)
Position in the chain.	Process Step 'Acquire'. Combining information from different parties to create a threat analysis and from this an advice.	Does the node cover all process steps, or a number and which?
Reason	The terrorist attacks in Spain in 2004 led to the creation of the 'Analytische Cel', a collaboration between a number of parties to combat terrorism. The way of collaboration proved too limiting, leading to the creation of the	Why was the information node started?

	CT Infobox.	
Scale	National	On what scale does the information node operate?
Product	A short statement, usually a single sentence, containing advice on where to find relevant information or if a person is worth looking into further. Because of the strict regulations in the WIV (Wet op de inlichtingen- en veiligheidsdiensten; law on intelligence and security services) the CT Infobox is unable to share more.	What does the node create?
<b>Collaboration</b>		
Forms of collaboration.	The CT Infobox consists of employees from the different organizations working together permanently. There is a monthly meeting of the “Coördinerend Beraad”, consisting of a representative from each of the participating parties. This meeting includes discussing what action should be taken on the available advices, coordination of actions on relevant cases, and managerial issues regarding the CT Infobox itself.	What forms of collaboration exist?
Participating organizations	AIVD, IND, KLPD, MIVD, OM, FIOD, KMar, FIU-NL and NCTV The CT-Infobox is located at the AIVD and the AIVD has taken a leading role in the creation. According to the report by the ‘Commissie van Toezicht naar de Contra Terrorisme Infobox’ (2007) the legal construct where the CT-Infobox is part of the AIVD was necessary to ensure an effective participation in the collaboration by the AIVD. However, in practice the CT-Infobox should be an equal collaboration of all parties. This has changed for the better and the organizations strive for consensus on each decision. Final responsibility lies with the minister of Interior and Kingdom Relations.	Which organizations participate in the information node?
Entry/exit barriers	Article 10 of the letter of intent that all involved parties signed states that other parties can join with agreement from all parties. The letter of intent does not state any exit barriers.	What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust	There is trust in the working of the CT Infobox, since it can access the systems if the participants.  Trust in other parties involved is not an important prerequisite for the collaboration, since the rules are fairly strict and information sharing within the information node itself is limited.	To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan & Thoen, 2000)

	On the base level however, trust is important to share relevant information. Here, the trust between participants has grown because of the collaboration.	
<b>Information Sharing</b>		
How	The CT Infobox functions as a black box, using information from the systems of participating organizations to create an advice.	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.
What	The CT Infobox does not share the information it uses, it merely advices and indicates where relevant information could be found. This information is critical information. All sharing of information is regulated by the WIV 2002 <sup>15</sup> .	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?
Who	The information sharing itself happens on the base level, so each organization decides who to share with. Some information is shared during the “Coördinerend Beraad” in which all parties participate.	Who has access to the information?
<b>Supporting systems</b>		
Systems	The CT-Infobox uses a shell covering multiple systems of participating organization enabling it to search them more easily.	What systems are used and what do they look like?
Integration	The shell grants access to all participating systems, but this is one-way only.	How are the systems in the node linked to the organizations?
<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	The CT Infobox is paid for by the participants. Each participants pays for its own employees active for the CT Infobox, the AIVD manages housing and the additional costs including ICT and development are shared by the participants. To share the costs a distribution is created depending on the amount of fte each organization adds and the interests each organization has in the CT Infobox. Roughly 1/3 of the costs is distributed among all parties equally. 1/3 is paid by the AIVD and KLPD as major users, and the final 1/3 is paid for by the remaining organizations.	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)	The CT Infobox should adhere to the WIV (Wet op de inlichtingen- en veiligheidsdiensten; law on intelligence	The use of sensitive information requires care, how is this organized?

<sup>15</sup> [http://www.st-ab.nl/wetten/0662\\_Wet\\_op\\_de\\_inlichtingen-en\\_veiligheidsdiensten\\_2002.htm](http://www.st-ab.nl/wetten/0662_Wet_op_de_inlichtingen-en_veiligheidsdiensten_2002.htm)

	and security services) which prevents the AIVD from sharing any of their information and which complicates the sharing of information outside of the CT Infobox. Special powers are given to the head of the CT Infobox which enable him to share threat related information in times of need.	
Information security (Whitman & Mattord, 2011)	All information that is leaves the CT Infobox needs to be signed by a number of parties.	How is unauthorized access and manipulation of information prevented?

#### **A4.1.4 Lessons learned**

Following are the problems and opportunities, insights and experiences that were overcome during the creation and use of the information node. These are interesting for both new and existing information nodes. Not because they give clear cut solutions, but because they help cover each aspect of an information node and can help avoid problems.

- A political necessity or cause is required, for the CT Infobox this was the terrorist attacks in Madrid and (3 years earlier) in New York and the subsequent rise in threat levels in the Netherlands.
  - o Political pressure made organizations more willing to join.
- Just setting up an information node is not enough, it needs to be managed
- Financing the collaboration can be hard
- The implications of the chain-computerization theory can be underestimated (i.e. there is irrationality, all parties should see the direct advantage, etc.)
- Create a solid legal framework which allows for the required actions.
- Organizations will initially mistrust each other, trust has to be earned.
- Clarify the role of the supervisors (in this case the Coördinerend beraad) and their position.
- The CT Infobox could potentially do more than it does today, but is restricted by the participants and (in lesser amounts) the law.
- Organizations can be scared that the node will replace them instead of supplement.
- An information node needs a clear scope and goal and should only be used for this goal, but
- Do not specify the exact scope too early on, you might get stuck doing less than you could.
- Pay enough attention to the basics; a good plan for financing the node and clarify the tasks and responsibilities of the supervisors (het coördinerend beraad).
- The quality of the employees active in the CT Infobox is very important
  - o To ensure the quality, profiles have been created that employees should adhere to.
- Formalize the exchange of information. Each report requires to be signed by a number of people. This is time consuming, but ensures that the information is correct and will hold up when used in an investigation.
- Employees work in the CT Infobox for a period of two to four years. This way, they keep a feeling and familiarity with the organization they come from.

Before the CT-Infobox was created, the 'Analytische Cel' existed. This was a collaboration between parties with the same goal as the CT-Infobox has now, but included direct sharing of information between the participating parties.. This was problematic because the laws (more specifically, the WIV (Wet op de inlichtingen- en veiligheidsdiensten) 2002<sup>16</sup>) lay down very strict provisions under which the AIVD (and later also the MIVD) is allowed to share their information with other parties.

This led to the decision to choose another form of collaboration, which was given a place at the AIVD and which adheres to the WIV 2002. Because the CT-Infobox resides at the AIVD, but more importantly because it operates within the service's legal framework, it can be considered to be a part of the AIVD. The other parties can be stated to perform tasks for the AIVD, adhering to the WIV 2002.

Following from this, the AIVD took a leading position in the collaboration, which should be avoided (Grijpink, 2010b) because it conflicts with the terms of creating a good and fair collaboration. This has changed, the organizations strive for consensus on any decision.

---

<sup>16</sup> This law (among other things) regulates the way and extend to which the AIVD can share their information with other parties.

## **A4.2 Financial Expertise Center (FEC)**

### **A4.2.1 General description of the information node**

The objective of the 'Financial Expertise Center' (FEC) is to enhance the integrity of the financial sector.<sup>17</sup>

It was established following the 'Nota Integriteit Financiële Sector' by the Ministers of Finance and of Security and Justice in 1998. It was acknowledged that a healthy and trustworthy financial sector is of importance and that the involved parties should work together to guarantee this. When trust in the financial sector is damaged, this can have consequences with high costs for society.

The FEC consists of two parts, the FEC-Council and the FEC-Unit.

The FEC-Council consists of representatives of the FEC-partners at executive level who meet three times a year. It functions as a decisional body and controls the FEC-Unit.

The Financial Markets Director of the Ministry of Finance and the Law Enforcement Director of the Ministry of Security and Justice attend FEC Council meetings as monitors. (FEC flyer 2012)

The FEC-Unit performs the tasks described in the Covenant FEC 2009 and the FEC-year plan. It belongs to the FEC-partners, performs tasks for the FEC-partners and is staffed by the FEC-partners.

The FEC-Unit performs the core tasks of the FEC:

Creating structural information exchange among the partners

Realization of a knowledge center for and by the partners containing information in the knowledge areas relevant for the FEC.

Carrying out projects with a view to concrete, operationally useful results.

The FEC-unit works as follows when conducting the core task structural information exchange. It receives a signal from one of the partners, requesting information. This information relates to (current) developments in the financial sector, threats to integrity, or to cases requiring an enforcement decision. The FEC-unit forwards this signal to the other partners, if allowed within the legal frameworks, who provide the relevant data that they have to the FEC-unit. The FEC-unit then assesses this information, determining if it is possible to share this information with the requested partner. The FEC-unit can also decide to discuss the information in a dataroom with experts from all relevant partners. Further actions are coordinated there. For example when the Belastingdienst and AFM are looking into the same case, they could coordinate and combine their actions.

After this, the FEC-unit edits a FEC-advice in collaboration with the FEC-partners. The FEC-advice is sent to the FEC-partners whom it concerns to take further action. The FEC-Unit does not use the information itself other than for analyzing it to see if it is usable and if it can be shared. After this is done, the information is removed from the FEC.

Information is shared using CoCOTo (College Collaboration Tool) which is developed by De Nederlandsche Bank. The FEC uses this system to collect and exchange information among the partners. Each partner has its own space within the tool; only the FEC-unit can see and collect all information. The system is not a database, but merely a way to exchange data, no data is stored for longer than necessary and partners should copy information to their respective systems.

---

<sup>17</sup> Covenant containing agreements on cooperation in the context of the Financial Expertise Center (Covenant FEC 2009); Staatscourant 2009, 71

### A4.2.2 Context of the information node

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

Element	
Social chain product	Financial integrity
Chain challenge	To strengthen the integrity of the financial sector by stimulating, coordinating and extending the mutual cooperation among the partners by exchanging information and sharing insight, knowledge and skills.
Dominant chain problem	Economic problems due to lack of trust in the financial sector because of fraud and other forms of criminal activity.
Target group	(Illegal) financial institutions and persons / organizations that undermine the integrity in the financial sector.
Chain partners	AIVD (Algemene Inlichtingen en Veiligheidsdienst), AFM (Stichting Autoriteit Financiële Markten), Belastingdienst, DNB (De Nederlandsche Bank N.V.), FIOD (Fiscale Inlichtingen en Opsporingsdienst), Regiopolitie Amsterdam–Amstelland, KLPD (Korps landelijke politiediensten), OM (Openbaar Ministerie);
Process steps at operational level (links in the chain)	(supervision and detection) - notice - datarooms / knowledge events / projects – take action - report
Intermediary product(s) of each link	Notification – FEC-advice / enhancing knowledge / reports – penalty and/or consultation – report
Critical details	The Notification, critical financial-economic information regarding the notification, critical information on people and institutions involved
Criterion for the chain	Individuals or organizations that commit or attempt to commit fraud or other forms of criminal activity within the financial sector.

### A4.2.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

Node in context		
Level of the chain process	Policy (and underlying levels) Policy – the FEC-council is active on policy level as a decisional body, planning future actions of the FEC-unit. Primary process Support: One of the goals of the FEC-unit is the creation of a knowledge center containing information in the knowledge areas	At what level of the chain process is the node active? (Grijpink, 2010a)

	relevant for the FEC	
Position in the chain.	(supervision and detection) - notice – investigate The node combines the information and shares it with the FEC-partners, supporting part of the investigation by creating analyses of the information. The actions are performed by the FEC-partners themselves.	Does the node cover all process steps, or a number and which?
Reason	The FEC has been created following the 'nota integriteit financiële sector' from December 1997. This nota emphasized the importance of a healthy and trustworthy financial sector.	Why was the information node started?
Scale	The FEC operates on a national scale	On what scale does the information node operate?
Product	Structural information exchange between the FEC-partners, coordinated by the FEC-unit. The FEC-unit acts as a middle-man judging the possibility of and coordinating information sharing aimed at solving cases. Strategic, tactical and operational analyses. Enhanced knowledge in areas relevant for the FEC Projects with a view to concrete, operationally useful results, such as the National Threat Assessment Witwassen (NTA).	What does the node create?
<b>Collaboration</b>		
Forms of collaboration.	Information exchange, for example on mortgage fraud or money laundering. Creating analysis to find trends and developments. Realization of a knowledge center containing laws and regulation and information on subjects relevant for the FEC-partners. The FEC-unit, which can support partners performing projects, such as the National Threat Assessment Witwassen(NTA).	What forms of collaboration exist?
Participating organizations	AIVD, AFM, Belastingdienst, DNB,	Which organizations participate in the



	<p>FIOD, Regiopolitie Amsterdam–Amstelland, KLPD, OM;</p> <p>These are all the parties active in the chain that forms the context of this information node.</p>	information node?
Entry/exit barriers	<p>With consent from the FEC-Council other organizations can join the FEC or participate in activities of the FEC.</p> <p>The Covenant FEC 2009 states that each party can terminate its participation under observance of a six-month period of notice.</p>	What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust	<p>Information exchange within the FEC is, besides exchange within the existing legal frameworks, based on trust. Information that is received from the partners may not be used unless the partner that gave the information is consulted (no action without consultation).</p> <p>There is also some trust in the FEC-unit which acts as a separate and impartial party. It is trusted with judging the sensitivity and ability to share information. This trust is maintained by having the FEC-unit staffed by the partners.</p>	To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan & Thoen, 2000)
<b>Information Sharing</b>		
How	<p>During periodical meetings and on a daily basis between members of the FEC-Unit. This is where information from the FEC-partners is analyzed and where the knowledge center is realized. This has mainly a supporting function.</p> <p>In datarooms, information is discussed and combined to be used in the primary process.</p>	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.
What	<p>The information that is shared consists of all information the partners have on a certain subject. This can include more than only critical information, but it is only used for the</p>	<p>What information is shared between parties within the node?</p> <p>Is this only critical information or also more substantive?</p> <p>Only operational or also</p>

	goal it is collected for.	managerial?
Who	The FEC-unit judges if the information can be shared and if it is possible all partners can get access to it.	Who has access to the information?
<b>Supporting systems</b>		
Systems	CoCoTo (College Collaboration Tool), a system developed by DNB to safely exchange information.	What systems are used and what do they look like?
Integration	There is no integration, information is transferred from CoCoTo to the internal systems manually.	How are the systems in the node linked to the organizations?
<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	Each of the FEC-partners has provided an average of 4 fte to the FEC. The activities of the FEC/Unit are financed by the Ministry of Finance. The financing include costs for housing and facilities, recruitment, training, and such. The FEC-unit consists of 6 fte. In addition the OM adds 1 fte. (Jaarverslag 2010)	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)	The FEC uses the Informationprotocol FEC 2011 which regulates the sharing of information between partners within the existing legal framework.	The use of sensitive information requires care, how is this organized?
Information security (Whitman & Mattord, 2011)	The CoCoTo system requires identification through username and password as well as a text message.	How is unauthorized access and manipulation of information prevented?

#### **A4.2.4 Lessons learned:**

Following are the problems and opportunities, insights and experiences that were overcome during the creation and use of the information node. These are interesting for both new and existing information nodes. Not because they give clear cut solutions, but because they help cover each aspect of an information node and can help avoid problems.

- Laws and legal restrictions are considered the biggest difficulty for sharing information
- The FEC has a very specific goal; enhancing the integrity of the financial sector. This is all the FEC can be used for.
- The FEC has the advantage of the Ministry of Finance taking some of the costs, lowering the barrier to join. However, partners do have to put in some money and time to use the FEC.

- Good agreements and a clear overview of the advantages on a high level can help with the inclusion of parties.
  
- The chairperson of the FEC changes periodically, which also changes the focus of the FEC a bit towards the party that provided the chairperson. However, there is no structural advantage for any of the partners as the focus will change with a new chairperson.
- Employees work at the FEC-Unit for a predefined time after which they return to their organizations and are replaced by others. This ensures that each employee still is aware of the internal structure of the organizations they originate from.
- Getting all partners on the same page is hard, especially when creating an information protocol. It took years and required some hard deadlines to get some progress.
- The FEC-unit used to perform their own projects, but has stopped this because it was too hard to pull the partners along when none of them were really motivated. Projects are now placed at one of the partners and supported by the FEC-unit.
- All information is analyzed by the FEC-unit before it is shared to ensure it can legally be shared.

## A4.3 Informatieknooppunt Cybercrime (IKC)

### A4.3.1 General description of the information node

The 'Informatieknooppunt Cybercrime' (IKC) was originally started as one of the experiments of the program 'Nationale Infrastructuur ter bestrijding van Cybercrime (NICC; National Infrastructure for combating Cybercrime). The goal of this program, started in 2006, was to get representatives from vital sectors and relevant public parties to collaborate in the IKC, raising awareness of cybercrime. The aim was to increase the overall awareness and moreover the security of the primary processes in the vital sectors, such as the water purification process.

The information node has grown into a permanent network of professionals in the field of cybercrime and cyber security. It is used to share information regarding good practices, incidents, and threats.

The IKC is based on the British model for Information Exchange from the Center for the Protection of National Infrastructure (CPNI). This model consists of a number of Information Sharing and Analysis Centers (ISAC's). These ISAC's consist of a number of organizations active in a particular sector who share information with each other. The ISAC's are centered around a core consisting of the AIVD, the Team High Tech Crime of the KLPD, and the National Cyber Security Centrum (NCSC). In addition to these sectoral ISAC's, there are a number of cross-sectoral ISAC's containing for example representatives from the energy and water sector. These ISAC's meet less often, only a few times a year.

Also, meetings are organized on a theme, a few times a year, consisting of members of different ISAC's.



Each of the ISAC's has its own meetings and the representatives from the different organizations are the same for each meeting, encouraging trust between the parties. This system where trust is of importance also led to informal meetings between the organizations and between organizations from different ISAC's, creating a network bigger than the ISAC's themselves.

All information shared within the ISAC's is classified with the traffic light system. Green information can be shared with people within and outside the participating organizations, but any publication is forbidden. Amber information can be shared only with the members of the information exchange and those within their organizations who require this information to take action and red information will not be used outside the meeting, unless it is strongly generalized. Code Red information consists of practical examples of problems that

have posed a problem and that can be sensitive information. In addition, there is white information which may be publicly disseminated without restrictions, so called open-source information. This classification system is also used by the core parties to share information between the different ISAC's when this is allowed by the providing parties.

All information is shared during the meetings in the ISAC's, there is no shared system. Although minutes are created for each meeting, always classified as amber to ensure no one misses important information. However, the minutes do not include the incidents and other relevant so called 'red' information that are discussed during the meeting, which can be of value for the parties and works as an incentive to participate in all meetings.

In January 1, 2010 the program NICC has been discontinued and the IKC has been positioned at TNO under the name CPNI.NL.  
 January 12, 2012 the IKC has been placed at the National Cyber Security Center (NCSC)

**A4.3.1.1 Interview with Martin Visser, Waternet**

For this information node, it was chosen to perform the interview with one of the ISAC's, since this is where the actual information sharing happens and because the ISAC's operate almost independently. An interview was held with Martin Visser, who works as Security Officer PA at Waternet and is vice president of the Water ISAC. Because the ISAC's can be considered to be a sort of sub-nodes they have encountered problems and chances as a 'normal' information node would. Also, the water ISAC was the first ISAC to be created from the NICC.

The Water ISAC consists of the ten organizations that make up the Dutch water industry. It has as its goal to share experiences, good practices and discuss problems regarding cybercrime and cyber security. In addition they collaborate on research that has value for the sector. For example, they have developed a list of 39 good practices regarding cyber security which is now widely used and the creation of a scenario for process failure which is now used to test how able the organizations are in coping with process failure. It is also used to create sector wide solutions for new problems that arise, creating a form of standard for the sector.

During the meetings, each participant can introduce subjects they want to discuss. When a subject requires more attention and possibly input from the core partners(AIVD, the Team High Tech Crime of the KLPD, or NCSC), it can be discussed with them at a later time. In addition, from time to time the core partners will give presentations from their work and projects they are performing that are relevant for the participants.

The Water-ISAC participants invest in hours under the convention that each company provides max. two representatives in the ISAC meetings and that they provide room to hold the meetings. The location of the meetings alternates between the participants. In addition, the NCSC provides the secretariat and coordinates any sector-wide actions. When sector-wide actions are undertaken, they are paid for by all participants.

With regards to laws and regulations that apply to the sharing of information, no personal information is shared so the laws regarding the sharing of personal information (more specifically the Wbp) are not relevant.

**A4.3.2 Context of the information node**

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

Element	
Social chain product	Cyber-security
Chain challenge	To prevent cybercrime from causing damage to vital sectors and to other parties through the sharing of knowledge between public and private parties.
Dominant chain problem	The disruption and disabling of vital sectors, for

	example water purification and electricity because of cybercrime.
Target group	Systems, networks, and practices used in the vital sectors.
Chain partners	AIVD, KLPD, and NCSC are the core parties. But cybercrime is an issue for each party active in the vital sectors, so numerous parties are involved in the different ISAC's.
Process steps at operational level (links in the chain)	Monitor – analyze – prevent – repair – prosecute
Intermediary product(s) of each link	Report on possible weaknesses – Detailed information on weakness – measures to fix the weakness – protocols for when a weakness is exploited – legal actions against cyber criminals
Critical details	Experiences with cybercrime, solutions to known problems
Criterion for the chain	Systems and practices used in the vital sectors that are potentially vulnerable for cyber attacks.

### A4.3.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

<b>Node in context</b>		
Level of the chain process	Support	At what level of the chain process is the node active? (Grijpink, 2010a)
Position in the chain.	Monitor – analyze – prevent The information node is mainly aimed at exchanging experiences and good practices, actual actions are taken by the individual parties.	Does the node cover all process steps, or a number and which?
Reason	Government issued through the NICC. The NICC was started following the 'Actieplan Veilig Ondernemen Deel 2' which was created by the 'Nationaal Platform Criminaliteitsbeheersing' (NPC)	Why was the information node started?
Scale	National	On what scale does the information node operate?
Product	Good practices, experiences, studies, events, platform on cybercrime/cyber security.	What does the node create?
<b>Collaboration</b>		
Forms of collaboration.	Periodical meetings between parties active in an ISAC. No collaboration beyond information sharing within the node.	What forms of collaboration exist?

Participating organizations	AIVD, KLPD, and NCSC as core parties. The ISAC's consist of sector specific parties and differ for each of the ISAC's. Within the ISAC's all parties are equal.  <i>Final responsibility?</i>	Which organizations participate in the information node?
Entry/exit barriers		What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust	Stated to be of great importance for the proper functioning of the IKC. Trust is the most important value for the well-functioning of the IKC in the Netherlands. Promoted by using the same representatives each meeting and by encouraging informal contact outside of meetings.	To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan & Thoen, 2000)
<b>Information Sharing</b>		
How	During periodical meetings information is shared within an ISAC. The core partners exchange information between the different ISAC's.	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.
What	Critical information regarding cybercrime. Experiences and solutions. Potential problems.	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?
Who	The traffic light model allows the information to be classified, indicating to what extent it can be shared. All parties in the ISAC are treated equal.	Who has access to the information?
<b>Supporting systems</b>		
Systems	No systems are used. All information is shared during the meetings and through the reports created from the meetings.	What systems are used and what do they look like?
Integration		How are the systems in the node linked to the organizations?

<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	The Water-ISAC participants invest hours under the convention that each organization provides max. two representatives in the ISAC meetings and that they provide room to hold the meetings. The location of the meetings alternates between the participants. In addition, the NCSC (National Cyber Security Center) provides the secretariat and coordinates any sector-wide actions. When sector-wide actions are undertaken, they are paid for by all participants.	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)		The use of sensitive information requires care, how is this organized?
Information security (Whitman & Mattord, 2011)	The traffic light model indicates who can access information. This protocol is largely based on trust	How is unauthorized access and manipulation of information prevented?

#### **A4.3.4 Lessons learned**

Following are the problems and opportunities, insights and experiences that were overcome during the creation and use of the information node. These are interesting for both new and existing information nodes. Not because they give clear cut solutions, but because they help cover each aspect of an information node and can help avoid problems.

- Not all parties are present for each meeting. This causes them to miss potentially useful information and keeps them from sharing their experiences which could be useful for other participants.
- Each participant should both give and take, everyone should provide some input. As it is now, not all parties provide as much information as they possibly can. This could be because of laws that keep them from sharing their information, but this is not well communicated.
- Make sure the role of each participant in the information node is clear.
- The synergy between the different vital sectors could be used more, each sector now has its own ISAC and there is little communication between them.
- The right representatives should participate in the information node.
  - o The representatives should be multi-disciplinary, not just ICT or technical employees.
  - o The representatives should be motivated to participate
  - o The representative should be high enough in the organization to be able to communicate results of the meetings to the right people and to use them.
- The steering committee could take more action to ensure the right representatives are present.

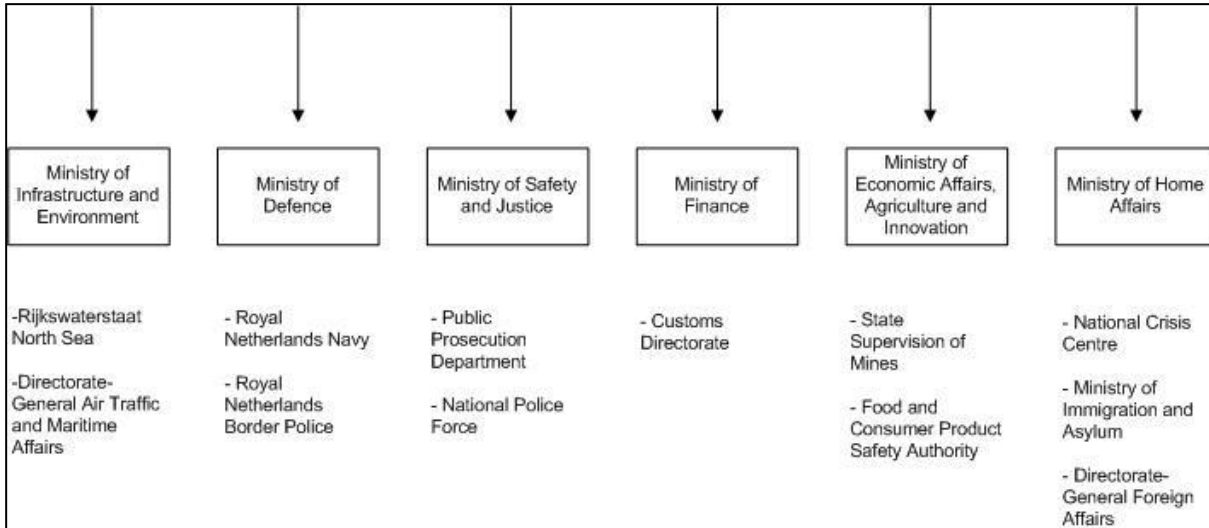


- The head of the information node should be enthusiastic and inspiring, just a good model is not enough.
- Trust is important, this can be secured by using the same representatives each meeting
- Participating in the ISAC greatly improves one's network
- The information node with a number of sectors represented in it is able to do more than the organizations itself can. For example, the NCSC was able to collaborate with the Idaho National Laboratory (INL) in the USA to provide trainings in cyber security.

## A4.4 Maritiem Informatie Knooppunt (MIK)

### A4.4.1 General description of the information node

The Maritiem Informatie Knooppunt (MIK) functions as the back office of the Netherlands Coastguard. The Netherlands Coastguard is a collaboration between a number of parties governed by a number of ministries. These are portrayed in Figure 4.



**Figure 4 - ministries and departments working with the Netherlands Coastguard (adapted from the Netherlands Coastguard information flyer)**

The Netherlands Coastguard consists of a front office and a back office. The front office is the center monitoring the activities on the North Sea 24/7, using various systems to visualize all activities. The front office can be contacted by ships in need and can set up actions, such as search and rescue operations. The back office, consisting of the MIK, combines information from the systems of the different participants to support the front office in their tasks. The parties active in the MIK are the KWC, ILT, RWS, Marine, Police, FIOD, Customs, KMAR, and AID (NVWA). The MIK consists of employees from the involved parties who physically collaborate and share information from their respective systems, while adhering to relevant laws and regulations. This means that sometimes, permission from the prosecutor has to be acquired before information can be shared. To ease this process, a letter of intent has been created, grounding the information sharing in specific rules.

The MIK was created after the 'Veiligheids Concept Noordzee (VCN)' was developed. This concept contains a method to create an overview of all potential threats to The Netherlands coming from the North Sea. The necessity of such a method was identified by the 'strategie nationale veiligheid' on which the VCN is based. It was found that the information to create the full picture of what is happening at the North Sea was available, but that it was scattered over a number of different organizations. As a result, suspicious activities were not always seen as such, because none of the organizations involved had enough information to act upon by itself and criminal activities therefore remained unnoticed.

All information gathered in the MIK is directly communicated back to the involved parties. For example, the customs employee working in the MIK updates the custom's computer systems with the new information, enabling them to act upon it immediately.

The actions that the MIK takes and the cases being examined are initiated by the participating parties. Each party can ask information from the MIK and therefore, each party benefits from participating in the MIK. The information sharing happens by using a 'proces-verbaal' which details where the information originates from. This is both to ensure the information is correct and will hold up in court, and to clarify to which extent information can be shared. For example, information that originates from a public system can be shared freely, even if it reaches the MIK through contact with the police.

In addition to supporting the front office and the involved parties, the MIK also provides a daily briefing for the units of the Coastguard, containing information on ships that might pose a potential problem or threat.

The MIK is set up as an addition to existing organizations and collaborations, such as the ‘CCC Douane’, KIC (Korps Informatie Centrum) KLPD, and the ‘Maritieme kamer Kmar’. Because it consists of employees from organizations that make up these collaborations as well, their information also supports these collaborations.

At this time, most of the organizations that could benefit from participation in the MIK are participating, except for Rijkswaterstaat and the ‘Inspectie Leefomgeving en Transport’ (ILT). These are both part of the ministry of Infrastructure and Environment. The reason for not participating is a lack of capacity to provide an employee for the MIK. This employee is, however the only entry-barrier for the information node (besides performing activities that relate to safety on the North Sea). For the MIK, the absence of these two organizations is no real problem, since their information systems are accessible through other parties.

The MIK is located at the Netherlands Coastguard. The reason for this is that the Netherlands Coastguard is already a collaboration between a number of parties that focus on the North Sea. The MIK serves as an addition to this, forming its back office. A great advantage this gives is that the involved parties are already used to some amount of collaboration, taking away some problems of initial trust and fear of the unknown that a new information node could encounter.

The MIK is led by an employee who originates from one of the organizations, but who has an independent role within the MIK. To ensure this independence, his salary is paid by all involved organizations combined. There are some requirements for this position however, one of which is that it has to be a ‘hulpofficier van justitie’ who has some special competencies, especially regarding the sharing of information. This leaves the kMar and police as possible providers of an employee for this function, given the prerequisites for becoming a ‘hulpofficier van justitie’.

The MIK operates on level 2, as defined in the ‘Nationaal Intelligence Model’ (NIM). This means that according to the NIM it has a regional focus, but more important, enables it to communicate with both level 1 and level 3 entities. This is important, because the setup of the NIM only allows for communication up or down one level. This way, the communication lines are relatively short and information can be acquired quickly. Also, the NIM provides standardized ways to exchange the information which eases the communication.

#### **A4.4.2 Context of the information node**

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

<b>Element</b>	
Social chain product	Information on all activities on the North Sea
Chain challenge	To monitor and get a complete knowledge of potential threats from the North Sea
Dominant chain problem	Criminal activities and potential threats from actions on the North Sea are missed because information is scattered over different organizations.
Target group	All activity on the North Sea that could potentially pose a threat for the Netherlands and/or international safety.
Chain partners	KLPD, Marechaussee, Marine, coast guard, Customs, FIOD, VWA, ILT, RWS.
Process steps at operational level (links in the chain)	Monitor – collect data -- analyze – act – (prosecute)
Intermediary product(s) of each link	Notification – dataset -- threat assessment – course of action – (‘proces verbaal’)
Critical details	Civil information on the one hand and operational information on the other hand.

Criterion for the chain	Activity in the North Sea under Dutch control that pose a potential threat for the Netherlands.
-------------------------	---

### A4.4.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

<b>Node in context</b>		
Level of the chain process	<p>primary process, support.</p> <p>Parties perform their daily work and can use information provided by the information node directly while doing this; primary process.</p> <p>It is the backend of the Netherlands Coastguard and therefore also has a support function, supporting the coordination of actions by the coastguard.</p>	At what level of the chain process is the node active? (Grijpink, 2010a)
Position in the chain.	<p>Monitor and analyze, the actual actions are performed by the parties themselves. Not all chain partners that are part of the chain are involved. Rijkswaterstaat and ministerie van ILT do not participate.</p>	Does the node cover all process steps, or a number and which?
Reason	<p>Recommendation from the 'Veiligheidsconcept Noordzee' (VCN), pointing out the lack of complete knowledge of what is happening at the North Sea.</p>	Why was the information node started?
Scale	<p>Regional, covering the entire North Sea</p>	On what scale does the information node operate?
Product	<p>The information node shares information within the information node, which is then directly used in the actions of the involved parties. The information is shared using a 'proces-verbaal' detailing the source of the information.</p> <p>Also, the information node creates a daily briefing, containing information on potentially interesting ships and activities.</p>	What does the node create?
<b>Collaboration</b>		
Forms of collaboration.	<p>Employees from the involved organization working together permanently, sharing information (for example, information on ships passing through the North Sea) in order to be able to collaborate when fighting threats. Any further action is coordinated by the front office of the Netherlands Coastguard and happens on the base level.</p>	What forms of collaboration exist?
Participating organizations	<p>Coastguard center (front office), KLPD, Marechaussee, Marine, Customs, FIOD, nVWA.</p> <p>The MIK is situated at the Netherlands</p>	Which organizations participate in the information node?

	Coastguard, so responsibility for the MIK lies with the director of the coastguard. Final responsibility lies therefore with the Minister of Defence who is responsible for the Netherlands Coastguard.	
Entry/exit barriers	To join the information node, besides the need to have a relevant area of operations (the North Sea), each participant must provide at least one full-time employee to the MIK.	What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust	Trust is of great importance, as each organization should feel like it benefits equally from the collaboration. Therefore, the information node is as transparent as possible and the employees working at the MIK remain employees of their respective organizations. This way, each organization has at least one set of eyes in the information node to ensure fair results. This trust is also strengthened by the independent coordinator of the information node, who is paid by all involved parties and therefore acts as a neutral party.	To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan & Thoen, 2000)
<b>Information Sharing</b>		
How	Working together in a dedicated location, sharing information from the different systems when needed. Participating parties can request information on for example a ship docking in the harbour of Rotterdam, which will then be provided by the other parties if legally possible. 2	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.
What	Information that relates to relevant activity on the North Sea, this is critical information for the problem the information node combats.	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?
Who	Sharing happens between all the involved organizations. The only restriction here are the rules and regulations, which don't always allow free sharing of information.	Who has access to the information?
<b>Supporting systems</b>		
Systems	Each organization uses its own systems and shares information manually. There is a separate system used by the information node containing information from the front office and that is used for internal communication.	What systems are used and what do they look like?
Integration	There is no integration into the systems of the organizations. Information is	How are the systems in the node linked to the organizations?

	copied from the shared system into the respective systems. This information is then usable in the whole organization.	
<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	Employees are paid by their respective organizations. Housing is provided by the Netherlands Coastguard. The head of the information node is paid by all involved parties together.	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)	Information is shared for as far as the law allows it, sometimes the prosecutor is asked for permission to share the information. Relevant laws are the 'wet bescherming persoonsgegevens (wbp), wet politiegegevens (wpg). A letter of intent is used to ease the information sharing.	The use of sensitive information requires care, how is this organized?
Information security (Whitman & Mattord, 2011)	To ensure the correct sharing of information, it can only be shared with consent of the 'hulp officier van justitie' and all information that is shared is done so by using a 'proces-verbaal' which notes the source of the information.	How is unauthorized access and manipulation of information prevented?

#### **A4.4.4 Lessons learned:**

Following are the problems and opportunities, insights and experiences that were overcome during the creation and use of the information node. These are interesting for both new and existing information nodes. Not because they give clear cut solutions, but because they help cover each aspect of an information node and can help avoid problems.

- Resistance against the creation; people see a new information node as a threat on a personal level, they might be afraid that they become less important when an information node becomes active. Also, people might be hesitant to share their information with 'lesser' partners, such as police information being used by customs (on a personal level, the organizations itself can fully cooperate, but the employees themselves can feel this way and resist against it).
- Organizations have to give up capacity to support the information node. This can be a problem when the node is approved on a policy level, but the employees have to come from lower in the organization.
- Organizations can have very slow decision making processes. Often they require pilots, which lead to new insecurities for the employees involved. This is especially relevant for information nodes that require employees to work in a specific location.
- The protocol for sharing information is more important than a system to share the information through. Make sure laws and regulations are adhered and for as much as possible, create a letter of intent which formalized the information sharing.
- A growth model, or bottle-neck model is easier to set up than a plan that has been exactly defined. Starting without filling all the details and working towards a more specific organization, based on what proved effective in practice. This way, any issues that organizations have can be resolved along the way and practices can be proven to work before they are formalized.
- Don't do everything yourself, a process writer would have helped greatly to create and specify the processes.

- Don't be afraid to be persistent, when trying to involve a party, if something doesn't work, try another approach.
- But also, don't spend too long trying to include non-essential parties.
- Make sure each of the involved parties sees a direct benefit from the information node, by using employees from the different parties who will still report back to these parties and keep their interests in mind.
  - o Each party who provides capacity can request capacity
- Be transparent, the information node is paid for and should be owned by all parties, they should know what it does exactly.
- Clarify the goal and tasks of the information node and how this relates to existing collaborations. This shows that the new information node will not make them obsolete and might improve support from them.
- Remain multi-disciplinary, have the employees be part of the involved parties, so that they stay involved with developments within those organizations as well. They should be more than an access to their systems.
- The information node has to be led by an independent party, paid by the information node (indirectly, by all involved parties).
- Physical collaboration is very important; it leads to more trust and more complete information. Communication over distance tends to involve a loss of details that could be crucial.
- Information should be shared formally, though the use of a proces-verbaal ensuring the origin of the information is clear.
  - o Always question the origin of information and the reliability of sources
- Successes will create more interest in the node and will motivate government and potential partners to support the information node

## **A4.5 Regionaal Informatie en Expertise Centrum (RIEC)**

### **A4.5.1 General description of the information node**

RIEC's (Regionaal Informatie en Expertise Centrum) are collaborations between a number of parties with as goal the administrative fighting of crime on a regional level. It aims at preventing the government from (unwittingly) facilitating criminals, preventing the criminal circuit from blending into the legal circuit, and breaking economic powerhouses built with criminally gained funds.

The primary parties participating in the RIEC's are the provinces, municipalities, police force, Openbaar Ministerie (Public Prosecution), belastingdienst (Tax Administration), FIOD (Fiscal Information and Investigation Service), inspectie SZW (inspection Social Affairs and Employment), Koninklijke marechaussee (military police). In addition a number of parties participate on a non-structural basis. These can be found in the 'node in context' table below.

It does this in a number of ways: By facilitating the sharing of information and based on this information coordinating enforcement tasks, by providing knowledge and expertise to administrative processes, and by supporting provinces and municipalities with preventing and enforcement.

The RIEC's have a regional focus and are coordinated by the LIEC (Landelijk Informatie en Expertise Centrum). At this time, 11 RIEC's exist providing national coverage.

The LIEC has as its task to coordinate actions between the RIEC's and to act on a national scale. It can notice when a problem is larger than one RIEC and can set priorities for the RIEC's. The LIEC also functions as a shared service center to support the RIEC's.

The sharing of information in the administrative and integrated approach happens on three levels.

The local municipal consultations (lokale gemeentelijke overleggen),

the thematic workgroups (thematische werkgroepen),

the intervention consultation (het interventieoverleg).

The local municipal consultation is led by the coordinator administrative measures (coördinator bestuurlijke aanpak) who creates the agenda on behalf of the Mayor. During the consultation, the municipality is advised by the account managers from the RIEC.

Selected cases can be handled locally by taking administrative actions (such as the denial of permits and financial penalties) or by using municipal flexteams. Cases that are larger are transferred to the thematic workgroups or the intervention consultation. Periodical consultations happen between the municipal coordinator and the account manager, and the Mayor. Annually an evaluation report is created by the coordinator, containing the results.

The thematic workgroups are active fighting specific problems.

The way they operate has changed in 2011, due to the termination of the Convenant Samenwerkende Overheden and the positioning under the Regionaal Convenant Geïntegreerde Aanpak Georganiseerde Misdaad voor de Provincie Limburg.

The themes that are treated in the thematic workgroups differ for the different RIECS. For Zuid-Limburg, the themes are human trafficking, organized hemp cultivation, 'patseraanpak', and organized environmental crime. In Noord-Limburg, the old covenant was still active and the themes were human trafficking/prostitution, chain approach cannabis, 'patseraanpak'.

The intervention consultation is a bi-monthly consultation by the heads of service for the partners. For the OM these are the 'rechercheofficier' and the 'informatieofficier van justitie'. Municipalities and the province are represented by the account managers from the RIEC.

The intervention consultation discusses all cases sent in by the local municipal consultations and the thematic workgroups, and decides on a best course of action on these cases. The actual actions on the case are discussed internally by each partner individually. This leaves the existing tasks, responsibilities and authority with partners.

The administrative approach consists of the efficient and effective use of administrative means to prevent the criminal circuit from mixing with the 'normal' circuit and preventing the (local) government from unknowingly supporting various forms of crime.



In this approach, the RIEC mainly acts as an information broker, promoting the disclosure of information by the municipalities. It also uses open sources such as Kadaster and Kamer van Koophandel, combining information to provide analyzed information packages.

The RIEC can also support the integrated approach by using closed sources, taken into account the principles of proportionality and subsidiarity. This information is then analyzed by the RIEC, taken into account legal limitations. When this analysis reveals possible criminal activities, a so-called intervention advice is created and action by the partners can be coordinated.

In addition to supplying physical products, the employees of the RIEC Limburg can provide knowledge and expertise regarding financial and economic, legal, analytic and administrative tasks.

#### **A4.5.1.1 Background (Interview with Lou Mennens, initiator of the RIEC Zuid-Limburg)**

The RIEC Limburg was the first of the RIEC, officially started in 2008. It came forth from the realization that a large amount of criminal capital remained unhandled (an estimated 18.5 billion euro). The fighting of this type of crime was too hard and yielded less visible result than fighting more visible crime.

The criminal funds pose a potential problem when it mixes with the legal funds through money laundering, for example in real estate. The municipalities give permits for these criminal activities, unwittingly supporting them. It was possible for this to happen while the police was in possession of information linking the person requesting the permission to organized crime.

As head of the interregionale recherche Zuid-Nederland (interregional detective force south Netherlands) between 1993 and 2003, Lou Mennens, cooperating with Cyrille Fijnaut, realized a broader approach was necessary. Research showed that the presumed pyramid-structure in criminal organizations was in fact more of a network structure. This meant that the information on 'low level' criminals could be more important.

In 2003 this led to a 3 month investigation on where improvements were possible within the detective force. This led to the realization that there was no need for more powers or financial means, but that there was a need for information. Most of this information was already available in the public sector, but not yet for the detective force.

To show this, a project was started in one neighbourhood in Maastricht where presumed criminal activities happened. A team of government officials from the municipality and a police officer analysed each of the buildings in this neighbourhood using open and half-open (available for the municipality) sources. This already showed some interesting things, for example a mortgage greatly exceeding the value of the building. Or a store that has existed for years, but that hardly shows any customers. For this, information on turnover from the Belastingdienst (Tax Administration) would be useful.

After consultation with the Minister of Finance and the head of the Belastingdienst they agreed and a letter of intent was created which allowed the sharing of information with the Belastingdienst under strict conditions. Consultation with the different partners was of importance, they were used to plan and discuss results. Initially 5 municipalities were involved. Within a year, all 19 were included.

The introduction of the 'BIBOB' law (Wet bevordering integriteitsbeoordelingen door het openbaar bestuur) gave a boost to the number of municipalities willing to join, since maintaining this law required more manpower than most municipalities could provide themselves.

The BIBOB law requires that governments check the integrity of permit applicants with the national BIBOB bureau. The municipalities that had not yet joined the RIEC and had not implemented the BIBOB law saw an increase in permit requests, suggesting an increase in criminal activity. This, combined with support from the Ministry of Safety and Justice led to a rapid growth and willingness of the municipalities to join.

There is a letter of intent which regulates the sharing of information between partners. However, strict rules still apply.

The sharing happens through analyses from the RIEC and between the partners directly.

### A4.5.2 Context of the information node

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

Element	
Social chain product	Security, more specifically administrative security using laws and regulations to minimize crime.
Chain challenge	Efficient and effective use of administrative means to prevent the criminal circuit from mixing with the 'normal' circuit and preventing the (local) government from unknowingly supporting various forms of crime.
Dominant chain problem	Insufficient action to fight organized crime because of a lack of overview and combination of the different indicators of criminal activity.
Target group	Criminal organizations active in the Netherlands
Chain partners	Primary: municipalities, openbaar ministerie, politie Nederland, belastingdienst en douane, fiscale inlichtingen en opsporingsdienst (FIOD), sociale inlichtingen en opsporingsdienst (SIOD), provincies en de Koninklijke Marechaussee Other: Kamer van Koophandel, Kadaster, UWV, Sociale verzekeringsbank, Algemene Inspectiedienst, VROM- IOD, Dienst Wegverkeer, Brandweer / veiligheidsregio.
Process steps at operational level (links in the chain)	(Monitor) Find problem identify people coordinate actions act monitor
Intermediary product(s) of each link	A description of the problem (i.e. drug dealers) A description of the people or organization involved Possible actions to combat the problem Coordinated actions are performed Effectiveness of the approach is analyzed
Critical details	Information on what the exact problem is and what earlier problems have been, both in the area and with the people involved Information on stores and real estate, its owner, its use and its history.
Criterion for the chain	Problems on a local level, should fit in the strategy that has been defined for the chain, which includes terrorism, drug dealing and manufacturing, human trafficking, use of and dealing in arms and explosives, and money laundering.

### A4.5.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

Node in context		
Level of the chain process	Policy, primary process,	At what level of the chain

	<p>and support  Policy: The course of action for combating organized crime by the municipalities is coordinate through the RIEC.  Primary process: The information combined in the information node allows parties to take action.  Support: The information is used to select which cases to investigate.</p>	<p>process is the node active? (Grijpink, 2010a)</p>
Position in the chain.	<p>Find problem  identify people  coordinate actions  The actual action, although often performed as a collaboration between a number of partners is not part of the information node. The analysis of the action is also done by the parties themselves. The RIEC however can support these steps.</p>	<p>Does the node cover all process steps, or a number and which?</p>
Reason	<p>Lack of administrative action on criminal activity, mainly money laundering involving real estate and the (unwilling) involvement of municipalities through the provision of permits. This was published in the program 'bestuurlijke aanpak van georganiseerde misdaad', 2008.</p>	<p>Why was the information node started?</p>
Scale	<p>Local and regional with some national aspects through the LIEC</p>	<p>On what scale does the information node operate?</p>
Product	<p>An administrative approach to fighting crime.</p>	<p>What does the node create?</p>
<b>Collaboration</b>		
Forms of collaboration.	<p>Information sharing  Multidisciplinary collaboration, supported through daily contact between the account managers of the RIEC and the contacts at the organizations, sharing information through oral communication, giving tips and bringing together key figures in current investigations. (jaarverslag Limburg 2011)  Own action: analysis of a problem and research</p>	<p>What forms of collaboration exist?</p>

	<p>through use of open and half-open sources.</p> <p>Creation of advice including where to find relevant information in systems of the partners.</p> <p>Proving training for the partners.</p>	
Participating organizations	<p>Partners: Provincie, <i>gemeentes</i>, politie, om, belastingdienst, FIOD, inspectie SZW, Koninklijke marechaussee.</p> <p>In addition, there is some non-structural collaboration with private organizations and other expertise centers. These include the Vastgoed intelligence Center (VIC), Expertisecentrum Mensenhandel en Mensenmokken (EMM), and RCF - Kenniscentrum Handhaving.</p> <p>Landelijk Bureau Bibob (LBB), landelijk programma Financieel Economische Criminaliteit (FINEC), Nationaal Intelligence Model (NIM), and Landelijk Taskforce Georganiseerde Hennepteelt. (jaarverslag Limburg 2011)</p>	Which organizations participate in the information node?
Entry/exit barriers	<p>Other parties can join when they provide useful information. The joining of private parties is being investigated at this time, but poses some problems with the laws on information sharing.</p>	What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust	<p>Most actions are taken in collaboration and the results are communicated to the partners so they will always see the result of the information they provide.</p>	To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan & Thoen, 2000)
<b>Information Sharing</b>		
How	<p>The RIEC organizes meetings for the parties to discuss their information needs and to coordinate actions.</p> <p>In addition, information is shared within the teams that analyse potential cases.</p>	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the

		systems that are used for the sharing.
What	Signals of potential problems. Information on real estate that might be property of criminals. This includes for example mortgage information, information on revenue of stores, and information on the number of buildings and stores owned by one person.	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?
Who	Sharing happens with parties that need the information and that can legally use the information.	Who has access to the information?
<b>Supporting systems</b>		
Systems	The RIEC's use workflow systems to support the process of identifying money laundering through real estate investments. It uses administrative dossiers to share and tune information, these dossiers are managed by the 'Landelijk Loket Bestuurlijke Dossiers' which can coordinate actions based on them. External partners require manual acquisition of information.	What systems are used and what do they look like?
Integration	The RIEC's use the administrative dossiers internally as well	How are the systems in the node linked to the organizations?
<b>Preconditions</b>		
Finance (Venrooy & Sonnenschein, 2008)	The RIEC's are financially supported by the Ministry of Security and Justice. According to the annual report 2011 from the RIEC Limburg, roughly one third of the costs of the RIEC was paid for by the ministry of S&J. Roughly one third of the costs was covered by the municipalities and province, and the remaining amount was covered in the form of personnel from the belastingdienst and police.	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)	Letters of intent for the sharing of information and the 'wbp' and 'wpg' are adhered to.	The use of sensitive information requires care, how is this organized?
Information security (Whitman & Mattord, 2011)		How is unauthorized access and manipulation of

#### **A4.5.4 Lessons learned:**

Following are the problems and opportunities, insights and experiences that were overcome during the creation and use of the information node. These are interesting for both new and existing information nodes. Not because they give clear cut solutions, but because they help cover each aspect of an information node and can help avoid problems.

- A problem when creating the other RIEC's was the lack of influence the minister had on the way they work. Each RIEC is influenced by different people with different views in the municipalities and cabinets. Because of this, the basic principle of the RIEC's isn't unambiguous.
- The first line of managers at the involved partners might see the changes as a threat for their job and expertise. They might agree that it is the best course of action, but can be unwilling to actually make changes.
- Collaboration cannot be forced and requires time. Each of the organizations has to give up some part of its autonomy.
  - o A network organization such as an information node should be treated different from an institutional organization.
- Integral collaboration is good, different organizations working together to solve a problem. Integrated collaboration can be even better, when the different organizations work together even more closely, functioning as one to make a plan and solve the problem.
- Public-private collaboration is planned, but is very hard considering the laws and regulations regarding the sharing of information. Especially for the 'belastingdienst' this is problematic. As it is, the information from the 'belastingdienst' can be used for a limited purpose as it is.
- The structure and work processes of the first RIEC can't be copied exactly to the other regions. Regional differences can have an influence on the way of working.
- Creating a blueprint does not work, each information node is unique.
- The human factor is of great importance; don't get stuck in a systematic way of thinking.
- What should happen can be managed top-down, but how it should happen requires a person-centered approach on a lower level.
- Different organizations have different cultures and will therefore have more or less trouble joining an information node.
- The right contacts and publicity have been of great importance for the success of the RIEC.
- Get operational as soon as possible; let the success of the cases be a motivator. Specify the details later.
- A uniform, national way of working is ideal, but there should be enough room for local differences.
- Be patient
- Political and societal timing is important; 3 years before the RIEC would most likely have failed.
- Some parties will be hard to get on board (for example, the police force who is very protective of its information). Patience and persistence might be required to get them on board, as well as showing

them the advantage of joining.

- When something is legally hard (for example, the use of information from the 'belastingdienst'), make sure the possibilities are examined and documented clearly.
- When laws pose problems, use a different approach. They will not likely change soon, so look for alternatives.
- Give all partners credit when it is due and show them the advantages of participating in the information node.
- Use the press to create more widespread awareness of your successes.

## **A4.6 Centraal Informatiepunt Voetbalvandalisme (CIV)**

### **A4.6.1 General description of the information node**

The ‘Centraal Informatiepunt Voetbalvandalisme’ (CIV) exists since 1986, when riots surrounding the Europacup finals in Belgium resulted in a number of people injured and dead. This led to the realization that there should be more information on individuals or groups who could potentially perform violence or vandalism, and which can be linked to soccer matches or teams.

The shared system that was later created to support the CIV (called the ‘Voetbal-Volg Systeem’ (VVS; soccer-monitoring system)) consists of two parts. On the one hand there is the KNVB-part which contains information about the soccer match, its preparation and anything happening after the match. On the other hand there is the person-part which contains information about individuals who pose a (potential) threat.

The person-part is available for the majority of the involved parties, the KNVB-part is only used by the KNVB and a limited number of other parties.

The information in the VVS is gathered from a number of parties and is used to coordinate actions and monitor potential risks. The system was created from the need to get a view on the preparation of soccer related violence and vandalism so that adequate action can be taken.

During its lifespan the focus of the system has shifted slightly, since better monitoring lead the violence and vandalism to move from the stadiums to other places. In combination with new ways to organize and hide, this posed a new problem, since this made the violence and vandalism even less visible and predictable.

The CIV is a body separate from the involved organizations, tasked with calculating the risk for each soccer match, preparation for matches and maintaining the public order in collaboration with the police and municipalities.

There are half-yearly meetings between the CIV and its partners which are used to create the higher level policy. More structural contact between the partners happens during the time leading to a soccer match. This contact happens between the police and soccer club for small matches and includes more parties such as the municipality for bigger matches. Besides this, there is a monthly or bi-monthly local or regional meeting to analyze past matches.

To be able to coordinate all the different soccer matches, which often involve a number of local parties that have to join the collaboration, it is housed and coordinated by the police force. In practice, responsibilities are spread over the different organizations, placing some at the coordinators of the soccer matches and some are specified in letters of intent between the organizations.

This information node is an example of a case where the dominant chain problem has changed over time. When the information node was first created, the problem mainly consisted of the riots occurring in the stadiums. Later, these riots (partly) moved outside of the stadiums and even to the days before the soccer match. This led to a change in how the information node operates.

### **A4.6.2 Context of the information node**

The information node exists in one or more social chains. In the following table, one of these chains is looked at in more detail. This is done using an adapted version of the mission profile as created by Grijping (2010b). It is used to place the information node in context which is useful for the second part of the factsheet.

<b>Element</b>	
Social chain product	Safety
Chain challenge	Preventing and fighting soccer related vandalism and/or violence.
Dominant chain problem	Difficulty predicting who, when, and where soccer related vandalism or violence occurs because the preparation is hard to identify and track.
Target group	People at or near a soccer match
Chain partners	The police, the KNVB, Majors of involved municipalities, Auditteam soccer vandalism,



	Police force managers, Betaald Voetbal Organisaties (BVO's; professional soccer organizations), Supporters clubs, railway police, firefighters, Regionale Inlichtingendienst (RID; regional intelligence service), Mobiele Eenheid (ME; Riot control), Geneeskundige Hulpverlening bij Ongevallen en Rampen (GHOR; Medical assistance for Accidents and Disasters), Openbaar Ministerie (OM), Ministry of IKR, Ministry of Justice, Ministry of HWS, Stuurgroep bestrijding voetbalvandalisme (Steering Committee combating soccer hooliganism), Jongerenwerk (youthwork), Verslavingszorg (Drug rehabilitation, Samenwerkende Organisaties Voetbalsupporters (SOVS; Collaborating organizations soccer supporters), Transport companies.
Process steps at operational level (links in the chain)	Prevent – observe – act – investigate - penalize
Intermediary product(s) of each link	Preventive measures – observation of unwanted behavior – direct measure – report – sanction or measure
Critical details	Personal information, risk code, current measures.
Criterion for the chain	Soccer related violence resulting in disturbance, substantial damage and/or (possible) physical harm.

(adapted from:

**Een informatiestrategie voor de bestrijding van voetbalvandalisme**

J.J. Dijkman, J.H.A.M. Grijpink, M.G.A. Plomp, P. Seignette & T. Visser)

### A4.6.3 Information node in context

The following table contains aspects of an information node on which information nodes can vary. It can be used to compare different information nodes and as a way to get a uniform overview of a number of information nodes.

<b>Node in context</b>		
Level of the chain process	Primary Process	At what level of the chain process is the node active? (Grijpink, 2010a)
Position in the chain.	Prevent – Observe – Investigate	Does the node cover all process steps, or a number and which?
Reason	The riots during the 1985 Europacup finale in Belgium showed the need for a systems to support the police forces. This system was first active in 1986.	Why was the information node started?
Scale	National, but collaboration often happens on a regional scale.	On what scale does the information node operate?
Product	<i>Approaches to preventing and combating soccer-related violence.</i>	What does the node create?
<b>Collaboration</b>		
Forms of collaboration.	There are half-yearly meetings between the CIV and its partners which is used to create the higher level policy. More structural contact between the partners	What forms of collaboration exist?

	<p>happens during the time leading to a soccer match. This contact happens between the police and soccer club for small matches and includes more parties such as the municipality for bigger matches. Besides this, there is a monthly or bi-monthly local or regional meeting to analyze past matches.</p> <p>To be able to coordinate all the different soccer matches, which often involve a number of local parties that have to join the collaboration, it is housed and led by the police force. In practice, responsibilities are spread over the different organizations, placing some at the coordinators of the soccer matches and some are specified in letters of intent between the organizations.</p>	
Participating organizations	<p>The main partners of the CIV are the police, the KNVB and the majors. In addition, some other parties are involved, but act mainly on the base level of the chain. These include:</p> <p>The police, the KNVB, Majors of involved municipalities, Auditteam soccer vandalism, Police force managers, Betaald Voetbal Organisaties (BVO's; professional soccer organizations), Supporters clubs, railway police, firefighters, Regionale Inlichtingendienst (RID; regional intelligence service), Mobiele Eenheid (ME; Riot control), Geneeskundige Hulpverlening bij Ongevallen en Rampen (GHOR; Medical assistance for Accidents and Disasters), Openbaar Ministerie (OM), Ministry of IKR, Ministry of Justice, Ministry of HWS, Stuurgroep bestrijding voetbalvandalisme (Steering Committee combating soccer hooliganism), Jongerenwerk (youthwork), Verslavingszorg (Drug rehabilitation, Samenwerkende Organisaties Voetbalsupporters (SOVS; Collaborating organizations soccer supporters), Transport companies.</p> <p>The CIV is part of the Dutch police and the final responsibility therefore lies with the police force and following from that with the Minister of Safety and Justice.</p>	Which organizations participate in the information node?
Entry/exit barriers		What rules exist for joining or leaving the information node? (Eisenhardt & Schoonhoven, 1996)
Trust		To what extent does the collaboration rely on trust and are there systems in place to secure this trust? (Tan &

		Thoen, 2000)
<b>Information Sharing</b>		
How	Using the VVS, different parties can access information relevant for their tasks.	How is the information shared between organizations in the node? For example, on a daily basis between employees from different organizations or periodical during scheduled meetings. This does not cover the systems that are used for the sharing.
What	Mainly critical information, but the KNVB-part also contains non-critical information. However, not all parties have access to this information.	What information is shared between parties within the node? Is this only critical information or also more substantive? Only operational or also managerial?
Who	The KNVB-part is only used by the KNVB. The person-part is accessible by all parties.	Who has access to the information?
<b>Supporting systems</b>		
Systems	<p>VVS – ‘Voetbal Volg Systeem’ a shared system consisting of two parts.</p> <ol style="list-style-type: none"> <li>1. The KNVB-part; containing information regarding the soccer matches itself. Both the preparation and issues after the match, and the match itself.</li> <li>2. The person-part; containing information about individuals, such as stadium bans.</li> </ol> <p>The systems consist of information on individuals arrested by the police (only people who have been arrested are included in the system). The information on the arrested individual is retrieved by the OM and when relevant, notifies the KNVB of this information. The KNVB then uses its own information to decide what action to take on this individual. Any measure taken by the KNVB (such as a stadium ban) are then visible for the OM and the KNVB. This system shares only information on the individuals on the chain level (name and picture when available). The rest of the information is shared on the base level of the chain. It uses the VVS to share the information, but access is restricted to a select number of parties.</p>	What systems are used and what do they look like?
Integration	Little, it is a separate system which is only used before, during and after a soccer match. Because the tasks of most involve parties include more than fighting and preventing soccer related violence, integration could be useful, but is not	How are the systems in the node linked to the organizations?

	critical for their daily actions (for example, the municipalities do not need the information daily).	
<b>Secondary Issues</b>		
Finance (Venrooy & Sonnenschein, 2008)	The node is housed by and paid for by the police force.	Where do the financial resources to run the information node come from?
Legal (Whitman & Mattord, 2011)	<i>Not much information is shared on the chain-level and the information that is shared is only used for the specific purpose of preventing and combating soccer-related violence. Some parts of the system are only accessible to certain parties.</i>	The use of sensitive information requires care, how is this organized?
Information security (Whitman & Mattord, 2011)		How is unauthorized access and manipulation of information prevented?

## ***Appendix 5 – Abbreviations***

AFM (Stichting Autoriteit Financiële Markten); Authority Financial Markets

AIVD (Algemene Inlichtingen- en Veiligheidsdienst); General Intelligence and Security Service

ANV (Analistennetwerk Nationale Veiligheid); Analyst Network National Safety

BPVS (Beveiliging en Publieke Veiligheid Schiphol); Security and Public Safety Schiphol

BVO (betaald voetbal organisatie); Professional Football Organizaion

CCV (Centrum Criminaliteitspreventie Veiligheid); Center for Crime Prevention and Safety

CIRL (Convenant Informatie en Registratie Ladingdiefstal); Letter of Intent for Information and Registration Cargo Theft

CIV (Centraal Informatiepunt Voetbalvandalisme); Central Information Point Soccer Vandalism.

CMI (Centraal Meld- en informatiepunt Identiteitsfraude en -fouten); Central Contact and Information Point Identity Fraud and Faults.

CoMensha (Coördinatiecentrum mensenhandel); Coordination Center Human Trafficking

CPNI (Center for the Protection of National Infrastructure)

CT Infobox (Contra Terrorisme Infobox); Counter Terrorism Infobox

DNB (De Nederlandsche Bank)

EMM (Expertisecentrum Mensenhandel en Mensensmokkel); Expertise Center Human Trafficking

EPICC (Euregionaal Politie Informatie en Coördinatie Centrum); Euregional Police Information and Coordination Center

FEC (Financieel Expertice Centrum); Financial Expertise Center

FINEC (landelijk programma Financieel Economische Criminaliteit); National Program Financial Economic Crime

FIOD (Fiscale inlichtingen- en opsporingsdienst); Fiscal Information and Investigation Service

FIU-NL (Financial Intelligence Unit – Nederland); Financial Intelligence Unit – Netherlands

Fte – Full-time employee

GHOR (Geneeskundige Hulpverlening bij Ongevallen en Rampen); Medical assistance for Accidents and Disasters

HRS (Human Resource Services)

IKC (InformatieKnooppunt Cybercrime) ; Information Node Cybercrime

ILT (Inspectie Leefomgeving en Transport); Environment and Transport Inspectorate

IND (Immigratie- en Naturalisatiedienst); Immigration and Naturalization Service

inspectie SZW (Sociale Zaken en Werkgelegenheid; Inspection Social Affairs and Employment),

IOS (Inter-Organizational Systems)

ISAC (Information Sharing and Analysis Center)

KNVB (Koninklijke Nederlandse Voetbal Bond); Royal Dutch Football Association

LBB (Landelijk Bureau Bobob) National Bureau Bobob

KLPD (Korps landelijke politiediensten); National Police

KMar (Koninklijke Marechaussee); Royal Military Police

LIV (Landelijk Informatiecentrum Voertuigcriminaliteit); National Information Center Vehicle Crime.

LLV (Living Lab Veiligheid)

ME (Mobiele Eenheid); Riot Control

MIK (Maritiem Informatie Knooppunt); Maritime Information node

Ministry of FA (Foreign Affairs); Ministerie van BZ (Buitenlandse Zaken)

Ministry of IKR (Interior and Kingdom Relations); Ministerie van BZK (Binnenlandse Zaken en Koninkrijksrelaties)

Ministry of HWS (Health, welfare, and Sport); Ministerie van VWS (Volksgezondheid, Welzijn en Sport)

Ministry of S&J (Security and Justice); Ministerie van V&J (Veiligheid en Justitie)

MIVD (Militaire Inlichtingen- en Veiligheidsdienst) Military Intelligence and Security Service

NCSC (National Cyber Security Centrum)

NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid); National Coordinator for Counterterrorism and Security

NICC (Nationale Infrastructuur ter bestrijding van Cybercrime); National Infrastructure for combating Cybercrime

NIM (National Intelligence Model)

NPC (Nationaal Platform Criminaliteitsbeheersing); National Platform Crime Control

OM (Openbaar Ministerie); Public Prosecution

PwCIL (PricewaterhouseCoopers International Limited)

RCF - Kenniscentrum Handhaving; RCF – Knowledge Center Enforcement

RID (Regionale Inlichtingen Dienst); Regional Intelligence Service

RWS (Rijkswaterstaat)

SIOD (Sociale Inlichtingen en Opsporingsdienst); Social Intelligence and Investigation Service

SSC (Shared Service Center)

VIC (Vastgoed Intelligence Center); Real Estate Intelligence Center

VROM- IOD; The of special Investigation Servicethe Ministry of Infrastructure and the Environment

VVS (Voetbal Volg Systeem); Soccer Tracking System

VWA (voedsel en Waren Autoriteit); Foor and Goods Authority

WBP (Wet Bescherming Persoonsgegevens); Personal Data Protection Act

WIV (Wet op de Inlichtingen- en Veiligheidsdiensten); Law on Intelligence and Security services

WOB (Wet Openbaarheid van Bestuur); Law of Open Government

WPG (Wet bescherming politiegegevens); Police Data Protection Act