The perceived effectiveness of the provincial crisis council during the Brussels Airport terror attack on March 22, 2016

An analysis of the procedures, achievements and the design of the network in which multiple local actors had to play a role.

Master Thesis

Written by: Joachim Brusten

Student Number: s1796704

Supervised by: Dr. Joery Matthys

Second reader: Dr. Sanneke Kuipers

Leiden University

Faculty of Governance and Global Affairs

MSc Crisis and Security Management

June 8, 2017

Table of contents

Abbreviations

ANIP = Regular Emergency and Intervention Plan (Algemeen Nood- en Interventieplan)

BNIP = Special Emergency and Intervention Plan (Bijzonder Nood- en Interventieplan)

BAC = Brussels Airport Company

CC BAC = Crisis Council Brussels Airport Company

CEM VB = (Head) Crisis and Emergency Management department Vlaams-Brabant

CIC = Communication and Information Centre

CP = Civil Protection

CP-Ops = Commando Post - Operations

Dir-CP-Ops = Director Commando Post - Operations

Dir-Co = Director – Coordinator Federal Police

D1 = Discipline 1 (Fire brigade)

D2 = Discipline 2 (Medical team)

D3 = Discipline 3 (Police)

D4 = Discipline 4 (Logistics)

D5 = Discipline 5 (Information unit)

ECM = Emergency Contingency Manager

FCC = Federal Crisis Council

FGI = Federal Health Inspector (Federale Gezondheidsinspecteur)

HC112 VB = Aid Centre 112 Vlaams-Brabant (Hulpcentrum 112)

ISIL = Islamic State of Iraq and the Levant

PCC = Provincial Crisis Council

PSM = Psychosocial Manager

1. Introduction

1.1 Problem outline

"Due to safety and traffic reasons I opted to establish our provincial crisis council in Leuven, although the plan states that after an incident at the airport we have to gather at Brussels Airport. This decision went against us where as other decisions favoured us."

(Governor Vlaams-Brabant, April 7, 2017)

The double terrorist attack in Brussels on March 22, 2016 was a wake-up call for all Belgian crisis leaders. First there were two bombings in Brussels Airport followed by a suicide bomber who targeted the metro an hour later. The impact of the disaster was immense and it demanded a crisis response. The different emergency service actors had to form a crisis council on a strategic level – making several urgent decisions – in order to coordinate the crisis response.

If a crisis occurs – on the local, provincial or federal level – emergency and intervention plans are activated and all actors will gather in a crisis council to manage the crisis. These plans are made by the administrative governments in consultation with the emergency services (Royal decree of February 16, 2006). These plans state that a crisis council only needs to gather when a crisis occurs. Therefore the crisis council can be perceived as a temporary security or crisis network (Parlementaire onderzoekscommissie, 2016).

After the terror attack in Brussel Airport two of these security networks became active: the provincial and federal crisis council. Although the severity of the terrorist act required a federal crisis response, the provincial crisis council was active as well. Article 20 of the royal decree of February 16, 2006 – concerning the emergency and intervention plans – takes the possibility into account that both crisis councils are active. In this case, the governor is responsible for the provincial coordination, although they have to work under the command of the minister of internal affairs. As will be discussed in the analysis part the federal and provincial crisis council divided the tasks. The federal crisis council was engaged in the judicial and security aspects, where the provincial crisis council took charge over the crisis coordination and relief during and after the crisis.

The main actors of such a provincial crisis council are representatives of several emergency services, namely fire brigade, medical team, police, logistics (civil protection and defence unit), an information unit and the administrative crisis and emergency management department. In this case Brussels Airport – as described in the provincial emergency contingency plan for Brussels Airport – is a rare new member of the (provincial) crisis council (personal communication, D1 – 2, head CEM VB). The federal crisis council holds higher representatives such as the prime minister, the minister of internal affairs, the minister of justice, the minister of public health and some other high officials (Royal decree of February 16, 2006).

These days security or crisis networks are becoming more and more important as we are more exposed to environmental disasters, a terrorist attack or so on (www.hln.be; www.unisdr.org). These disasters demand a crisis response in the form of a network. Whelan (2015) argues that after the terrorist attacks on September 11, 2001 in The United States many Western countries responded by improving the coordination of their national security. The latter includes crisis and emergency management and counter-terrorism. Belgium is one of the countries with the highest number of radicalized youngsters per head that went to Syria to join ISIL, the Islamic State of Iraq and the Levant (ICCT, 2016).

This research will give some insights on the crisis and emergency management policy in Belgium by evaluating the performance of the provincial crisis council after the terrorist attack on Brussels Airport. This study therefore focuses on the perceived effectiveness of the crisis network through the eyes of its members.

1.2 Research question

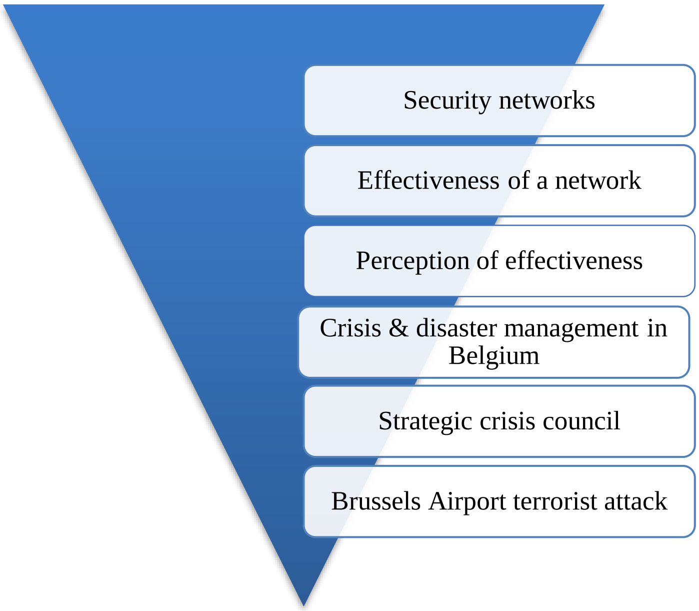
This study is an (ex-post) evaluative and explanatory research in which the researcher tries to determine whether the members of the provincial crisis network evaluate the network to be effective during the crisis response to the Brussels terrorist attack. Causal relationships between the perceived effectiveness of the network and the independent variables will be discussed in this research. The following research question is being asked:

'How effective was the strategic crisis network perceived to be in response to the Brussels Airport terrorist attack on March 22, 2016 and what factors influenced the perception of network effectiveness?'

Sub questions:

- What are the characteristics of the provincial crisis council?
- What are the goals of the provincial crisis council?
- How do the security actors in the crisis council perceive the achievement of the network goals?

This is the funnel that led to my research question. It also contains some concepts that will be further discussed.


Security networks
Effectiveness of a network
Perception of effectiveness
Crisis & disaster management in Belgium
Strategic crisis council
Brussels Airport terrorist attack

1.3 Academic and societal relevance

1.3.1 Academic relevance

Studying security networks is a relative new academic field. Moynihan et al. (2012) claim that there is little known about networks. Provan & Kenis (2009) and Whelan (2015) did some research on network designs, but the networks they studied have a permanent character. Therefore it may be necessary to contribute to the framework of network designs. The provincial crisis council can be perceived as a temporary network. They only gather in case of a crisis. Although other temporary networks have been evaluated, it might be interesting to look at the network design of this specific crisis network by evaluating its effectiveness. This is one of the reasons this research – the effectiveness of a security network – may add new knowledge to this field.

Furthermore Moynihan et al. (2012) did see a development in the rise of networks. Whelan (2012) confirmed this development in regards to security networks. The importance of local security networks is increasing in both studies' opinion. As more security networks rise, it is also essential that these networks are well established and effective. A Belgian parliamentary commission is investigating the double terror attack in Brussels, their main focus lies on the functioning of the federal crisis council and the operations on the field. In this thesis the perceived effectiveness of the provincial crisis network will be checked. It has never been evaluated before, despite occasionally being operational, in case of provincial emergencies.

It is difficult to evaluate network effectiveness. This is one of the reasons why it’s not often done (Provan & Kenis, 2009: 441). By selecting this case – the provincial crisis council during the Brussels Airport terrorist attack – we aim to contribute to the existing literature on networks and network effectiveness. Because of its unique and critical character the case may lead to new perspectives on networks. Special attention will be given to the network design of the provincial crisis council because it is an important factor of network effectiveness.

1.3.2 Societal relevance

The societal relevance of this research is that the effectiveness of a local security network will be evaluated. It is important to evaluate the crisis council because of the increasing risks of terrorism and natural disasters, as it is presumed that more disasters happen and will occur on European soil (www.unisdr.org). If another crisis has to be coordinated an effective, accurate and responsive crisis council has to be able to react accordingly.

The cooperation between the different actors will be scrutinized. If the network proves to be ineffective, its design should be evaluated and lessons should be learned. With this knowledge the administrative government may need to improve the network design so that the society benefits from it. These benefits involve more insights for policy makers and a better working crisis council.

There have been previous provincial states of emergency in which the provincial security actors had to react. This occurred in Vlaams-Brabant with e.g. a collision of two trains in Buizingen in 2010, but also in other provinces with a train crash with toxic liquids in Wetteren in 2013. Although there are some procedures, the effectiveness of these procedures and the network as a whole are never evaluated before (Parlementaire onderzoekscommissie, 2016). By testing the effectiveness of the network – through the perception of the security network actors – shortcomings and positive measures in the crisis and emergency management policy will be highlighted.

This particular crisis left many people wounded and several persons died. These people, along with the whole Belgian population, have the right to know how this security network performed and operated.

1.4 Thesis outline

The following chapter, the theoretical framework, will elaborate on the concepts of terrorism, security networks and network effectiveness. A third chapter will then list the methods that are being used to form this research. The research design, the choice for a single case study, the data collection methods and the operationalization of the used factors that can influence the network effectiveness will be explained. These factors will be the network design, trust, information sharing and goal consensus. The analysis of the network design and the perceived network effectiveness – in relation to the case – will be done in the fourth section of the thesis. In this fourth chapter a case description and the provincial emergency and intervention procedures will be explained. Furthermore the PCC is being analysed as a network by linking the network to the factors. All results on the effectiveness of the crisis network will be analysed in order to give a clear answer to the research question. The latter will be done in the final chapter, namely the conclusion. Besides the answer to the research question the researcher will also reflect on the results of this study.

2. Theoretical framework

2.1 Terrorism

2.1.1 Definition

Terrorism is a contested concept. Many scholars tried to define the concept, but because of its many dimensions it is difficult to determine a widely accepted definition. An example of a definition of terrorism is given by Schmid and Jongman (1988: 28):

“Terrorism is an anxiety-inspiring *method of repeated violent action, employed by semi-clandestine individual, group, or state actors, for idiosyncratic, criminal, or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators.”*

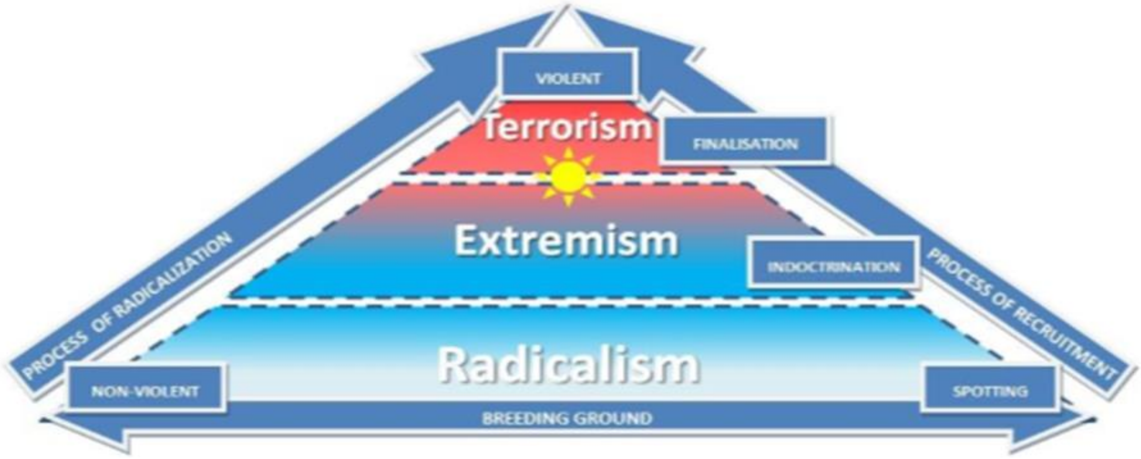
Although there is no accepted definition, many concepts return in most definitions. In case of terrorism the authors refer to the usage of violence to install fear among the people. This can be either for political, religious or ideological reasons. The main goal of terrorism is to target the people or government behind the people and gain publicity with it (Schmid & De Graaf, 1982).

One who engages in terrorism can be called a terrorist. This is a radical person that uses violence as a weapon to make his statement. Usually this person joins an organized terrorist cell in order to commit himself/herself to a cause (Noppe et al., 2011).

2.1.2 Radicalism, extremism and terrorism

According to Noppe, Ponsaers, Verhage, De Ruyver & Easton (2011) most persons that engage in terrorism – terrorists – undergo a process of radicalisation. This process is illustrated in figure 1. The process contains three steps: radicalism, extremism and terrorism, in the following order. There is an evolvement from varying worldviews and political or religious fanaticism to more extreme beliefs and even violence in order to protect their beliefs. Terrorists want to overthrow society by using undemocratic and violent means. Noppe et al. argue that every terrorist is a radicalist and extremist, but not every extremist or radicalist is a terrorist. In a case of e.g. Islamic radicalism or terrorism the three sorts of beliefs have somethings in common, like their belief in the salafistic way of living the Islam. Salafism is the form of living by the letter of the Koran and wanting the ‘Sharia’ as the criminal law.

Figure 1: The process of radicalisation in relation to terrorism (Noppe, Ponsaers, Verhage, De Ruyver & Easton, 2011: 51).



2.1.3 Terrorist organizations

A terrorist organization is a clandestine business in which planning and training for fighters and mass suicide killers finds place. Several persons join the network to fight for their cause. Terrorist attacks often are coordinated by members of these terrorist organizations. After an attack the organization usually claims responsibility. Such an organization can vary in structure from a hierarchy to a more horizontal structure or a terrorist cell with several autonomous members. Most terrorist organizations are autonomous and flexible networks (Matusitz, 2013: 4; 14).

Terrorist organizations can be considered as a combination of a hub and an all channel network. The hub network has a central actor with which the actors speak. The central actor can be seen as the leader of terrorist network, with the terrorists around him. An all channel network doesn't include a central actor. In an all channel network you can communicate with all other actors. Yet, terrorists often only gather if they are to commit a terrorist attack (Matusitz, 2013: 14). The following part (see 2.2.3) further elaborates on the different network governance forms.

Arquilla, Ronfeldt, and Zanini (1999: 51) noticed that terrorist leadership follows certain principles. These principles provide guidelines and restrictions on how to (re)act in certain situations. Because of this guideline there is no real hierarchy necessary in the terrorist network.

These terrorist organizations form a serious threat to the national security of all countries that are involved in the war against ISIL. Belgium is one of those countries participating in the coalition against ISIL. Raab & Milward (2003) stated that (security) networks had to be formed in order to fight 'dark' networks. Only then networks could be dissolved.

2.2 Security networks

2.2.1 *Definition*

Security networks are a relative new research field. To know more about the concept of 'security networks' we first have to explain the separate meanings of the concepts 'security' and 'network'.

Security comes from the Latin word *Securus* which means 'free from danger' (Craighead, 2003: 21). Kavalski (2009: 535) argues that people will seek protection to free themselves from any danger or harm. This protection – through the product of security – can be provided by public and private organizations and aims to protect people, goods and information (Craighead, 2003: 21). Security further implies that a certain level of safety is guaranteed without any disruptions. Stability and the absence of fear or any harm are the main characteristics of a secure environment according to Fischer and Green (2004: 21). Security isn't limited to the protection of persons or goods, it can also apply to the defence of a country (Brooks, 2007: 226). This shows that there are multiple points of view to define and understand security. People will perceive security differently as they interpret the meaning in various ways. The context, time and place affect the perception of security (Davidson, 2005 in Brooks, 2007: 226).

Networks became an important tool in countering complex (security) problems e.g. major disasters (O'Toole, 1997). Whelan (2012: 11) defines a network as a group of three or more organizations. To optimize the work of the network all organizations are interlinked through various relationships. These actors are individuals, units of an organization or the organisation itself. The agents may have personal relationships between individuals, functional relationships between the units of the organization or strategic relationships between the organizations themselves (Whelan, 2012: 11).

Networks were a relative new and positive governance form in which the concept 'coordination' received a different meaning. In 1975 Williamson was the first to add to the theory that markets and hierarchies were the sole governance forms. In a market goals were achieved through non-hierarchical coordination. The hierarchy was a system in which coordination was led by some high officials of the organization. The new governance form 'network' is a form of coordination with multiple organizations. This governance form has the possibility to reach certain outcomes which aren't possible in a hierarchical or market form. Networks hold the advantage of a higher efficiency and flexibility (Provan & Kenis, 2008: 232-233; Whelan, 2012: 15).

Nowadays networks – just as hierarchies and markets – are subject to more studies because they became more omnipresent (Moynihan, 2012). Castells (2000) even speaks of a network society. Grabher and Powell (2004 in Whelan 2012: 12) claim that the institutional and managerial approach are the best way to study network forms of organisation. The institutional approach focuses on the network and the environment of institutions around it, whereas the managerial approach sheds light on the network design and the attainment of the network goals.

The network is there to collaborate and facilitate the achievement of the goals of all organizations. The actors of a network work together because they can't achieve their goals on their own (Provan & Kenis, 2008). In this process it is possible that network goals arise. A network in which the different actors share a common goal is called a 'whole-goal directed network'. Although they are committed to the same goal, the level of commitment may differ per actor. Networks are considered to be flexible, efficient, goal-directed, better in processing information (than bureaucracies), responsive to unforeseen problems and sensitive to their clients' needs. Those are the main characteristics of a network (Moynihan et al., 2012: 639, Whelan, 2012: 11).

So what are security networks and what do they do? Whelan (2012: 18) says that network perspectives are used to better understand recent developments in the security field. Brodeur & Dupont (2006) often use a metaphor to describe the meaning of a security network. The metaphor reflects a certain relationship (or several ones) between various security actors. Thus, security networks also consists of three or more organizations and are interconnected with one another through several relationships. Their aim is to authorize and/or provide security for its stakeholders. These internal and/or external stakeholders will then benefit from the security that the network offers. Security networks are believed to be more effective and efficient than hierarchical bureaucratic organizations because of its distribution of resources, responsibilities and risks (Dupont, 2004: 78 in Whelan, 2012: 19).

As elaborated regular networks have increased and the same applies to the amount and influence of security networks. The increase of security networks has several reasons. First of all, the end of the Cold War led to new threats. Clarke (1998 in Krahmann, 2005: 17) argues that the territorial integrity of states is no longer challenged, it is rather the European and American life style. That includes the safety and security of civilians and a stable economy. The second argument is closely related to the first one. According to Raab & Milward (2003) security networks are established because of the growth of non-state threats e.g. dark networks. They believe that these dark networks have to be fought by networks itself. Furthermore globalisation as we speak of a stable economy, limited resources for public security organizations and subsequently the fragmentation of security policy-making require more cooperation between (security) actors. These days fragmentation occurs more often because several actors play a role in the security field. This in contrast with earlier years where private security companies and citizens were more isolated by the state when it came to security (Krahmann, 2005: 18; Terpstra, 2005: 38).

These different actors respond to societal changes. These changes lead to new security actors and issues which are dealt with by a security network. The actors of the network can either be individuals, public or private organizations. Over the past few years the involvement of private actors and the community has increased in the field of security, but still public actors are the highest represented group in the security field. Brodeur (2007) argues that the state remains the 'referent object' when it comes to the governance of security. These diverse networks offer some interesting insights with regard to the decision making processes and procedures of the different network actors (Krahmann, 2005: 27).

2.2.2 Security network typologies

Some authors have developed a typology of security networks. Not all networks have the same characteristics. Dupont (2004) comes up with four different types of security networks: local security, institutional, international and virtual networks.

First, you have the local security network. This network is actively integrated in the local community and open to new members. Public actors (police, local magistrates, social services, …), private security organizations and the community are involved. They share information in order to solve local crime problems.

Secondly, is the institutional security network. Almost all security networks involve some institutional actors, but only the institutional security network has the aim of government agencies working together on a project. Another objective is that these government agencies pool their resources across different government agencies. This sort of network only consists of public actors and isn't open to new members.

The third network is the international network. This network focuses on international relations. Usually it is one public actor that represents a country.

The final security network of Dupont's typology is the virtual – or also called informational – security network. This network facilitates the flow of information between all actors. These networks are in place to transcend time and space.

Terpstra (2005) further focuses on local security networks and institutional networks in his typology. He divides these two types of security networks into two. Local security networks can be either participatory or mixed enforcement networks. Both security networks are open to new members, but differ in orientation. The participatory network is preventive while the mixed enforcement network is reactive. In both security networks citizens play a role, but this role is more prominent in the participatory security network. In the participatory security network the involvement of citizens mostly lies in the initiation of the network, where in the institutional security network citizens are mostly involved through responsabilization. The participatory network is also more communicative and informal than the mixed enforcement security network.

The second distinction Terpstra (2005) makes is between two types of institutional security networks. These security networks can be either preventive or reactive and are both restricted to organizational actors (public and private). The latter implies that citizens aren't involved in these types of security networks. The reactive security network is more instrumental, formal and has a stricter fixed structure and technology than the preventive security network.

Still according to Terpstra (2005) local security networks have to deal with some internal problems. The most general problems are coordination, informality and goal consensus. Coordination can become a problem when there isn't a clear central actor or when actors refuse to surrender their authority. Informality is a problem when the balance between formal rules and cooperation can't be found. In some networks different actors can have a dispute about the network goals. Not every actor may be in accordance with the goals that are set. The lack of goal consensus in addition with often different positions and cultures of the actors may lead to tense situations between the network members.

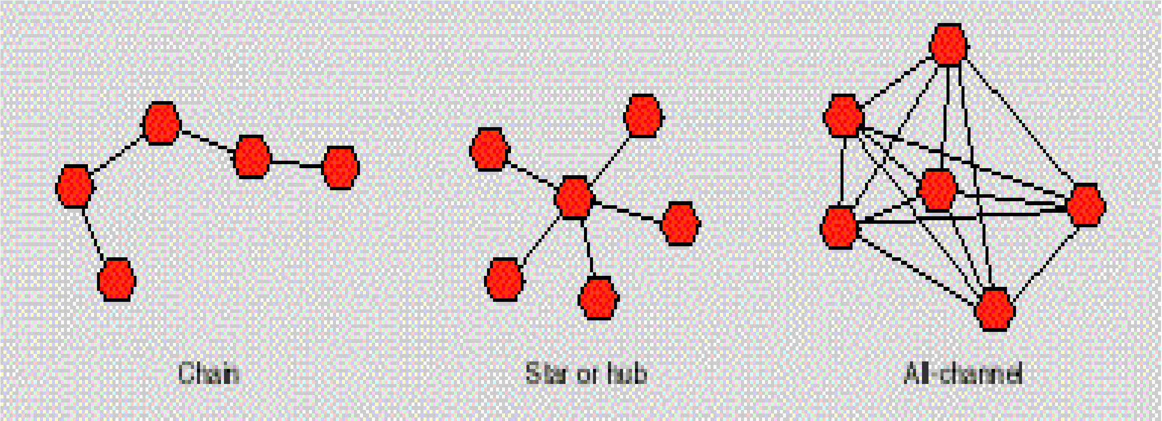
The above typologies by Dupont (2004) and Terpstra (2005) should help us understand security networks better. Normally you can situate a network in one of the above forms, but Dupont (2004: 79) states that a local security network regularly is based on a combination of the local security models.

Besides the differences in being an institutional or local security network and its orientation (preventive/reactive), a network can be either mandatory or voluntary. A mandated network often is created by a policy dictate, typically a government agency. Voluntary networks on the other hand are created bottom-up by actors that participate in the network. A mandated network is less activated than a voluntary network, which makes it more difficult to find the right balance between their organizational and network interests. So the inception of the security network also affects the selection of the most appropriate performance criteria (Provan & Kenis, 2009).

2.2.3 Network governance forms

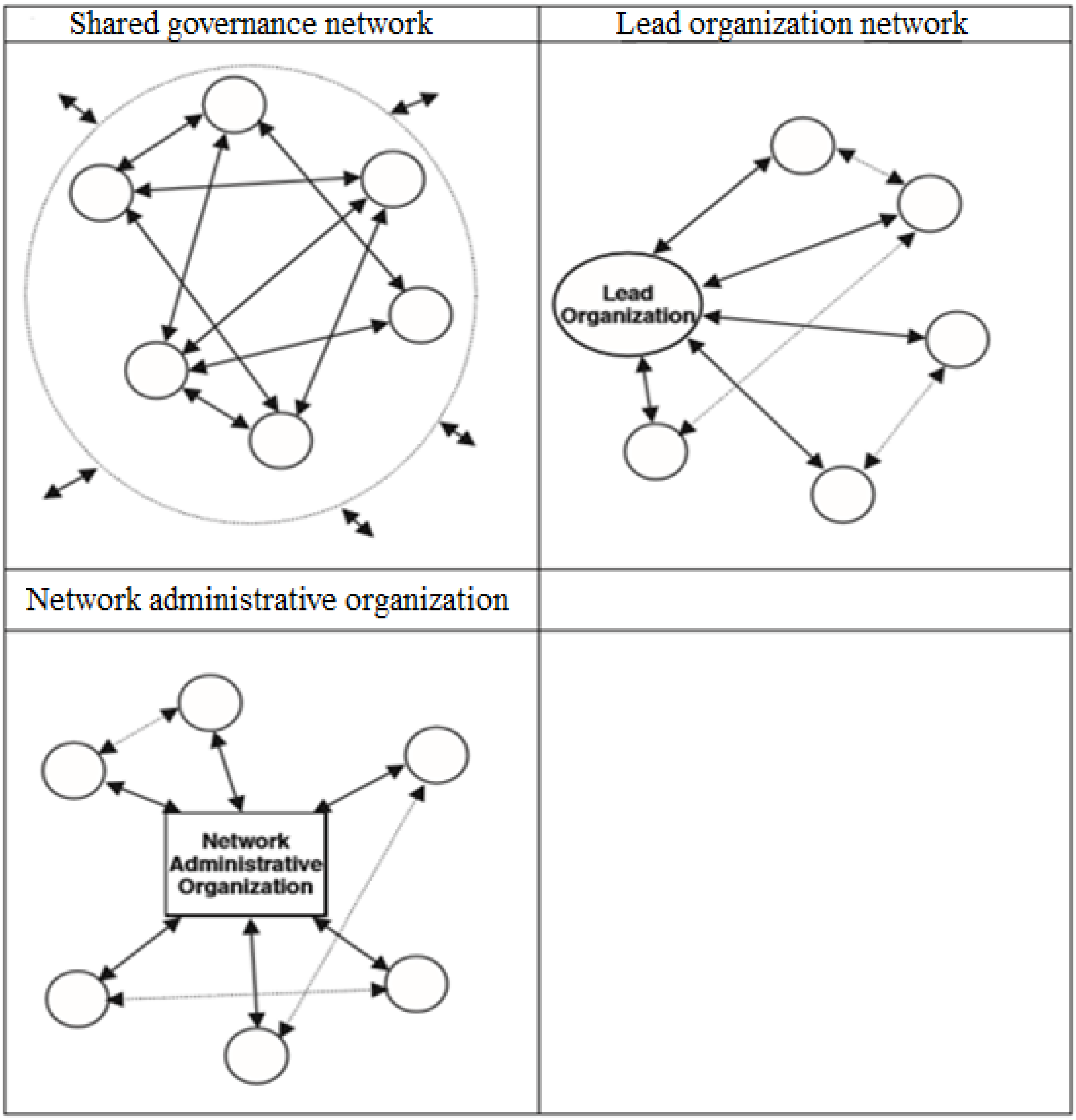
Provan and Kenis (2008) underline the importance of the network design. These designs give a certain structure to security networks. Arquilla & Ronfeldt's framework (2001) consists of three forms of network designs. According to them a network can either be a chain, hub or all channel network design. A chain network is a network form in which a security actor always needs intermediate actors to give or get to information from other security actors. It is some kind of a line network. A hub network means that all actors are tied to a central actor. This central actor will gather all information from all the individual actors and spread it to all other actors. An all channel network ultimately focuses on all the ties of the security actors. In this model every security actor is interlinked with all other security actors. These network designs are also illustrated in figure 2.

Figure 2: Network designs (Arquilla, Ronfeldt & Zanini, 1999: 50)



Provan and Kenis (2008; 2009) developed another framework on network designs. This framework includes three different network forms, namely a shared governance form, a lead organization form and a Network Administrative Organization (NAO). Provan and Kenis (2008) first make a distinction between brokered and non-brokered network governance. A non-brokered network governance form means that the network will be governed by its participants. This network form is dense and highly decentralized. The non-brokered network is the shared governance form. The second form Provan and Kenis found is the brokered network governance form. This governance form has two sub forms, the lead organization and the network administrative organization. These brokered network organization forms are led by one single organization or controlled by a broker. The difference between the two lies in the fact that a lead organization is a participant of the security network that takes the lead, while a NAO normally is externally governed by an actor. In a brokered network the sole actor is responsible for the maintenance of the network. The designs of these network governance forms are illustrated in figure 3 (Provan & Kenis, 2008; 2009).

Figure 3: Network designs according to Kenis and Provan's framework (2009: 447)


Shared governance network
Lead organization network
Lead Organization
Network administrative organization
Network Administrative Organization

The strengths of the **shared governance form** are the equal inclusion and involvement of all network actors in all decisions. The participants of the network themselves are responsible for the management of internal and external relations to ensure its maintenance. The participating actors can gather in a formal or informal way. On the one hand the network can have formal regular meetings in which the representatives of the different actors assemble and on the other hand there can be uncoordinated informal gatherings. Also when it comes to participating in a shared governance network form the network requires some flexibility towards new members and procedures. External relationships may be important to e.g. fund the network or to satisfy the needs of the costumers. The weakness of this network model is its relative inefficiency. This form is best suited for a low number of organizations in the network (5-6 members). Once its number becomes higher the network will become more inefficient. There is no distinct, formal administrative entity, although some administrative and coordination activities may be performed by a subset of the full network. The solution for a more efficient and centralized network – when the number of participants increases – would be a shift to a lead organization or a network administrative organization (Provan & Kenis, 2008; 2009).

The opposite of a shared governance model is the **lead organization**. This is a legitimate and efficient network governance form led by one sole actor, taking all important decisions and coordinating the situation. Thus, all power is centralized by the leading network member. The leadership role is either handed to the organization by the other members or it may be mandated. When the lead organization is mandated this is often a case of an external funder appointing the lead organization. The costs of all activities may be funded by an external actor, the lead organization itself or through contributions of all network members. These funds enable the network to achieve the network goals. The network members in this governance form still interact and work with one another towards (a) common goal(s). These goals are often quite similar to the goals of the lead organisation. The dominance of the lead organization can also have a negative aspect when they only focus on their agenda. In this case the other actors may lose interest in the network goals (Provan & Kenis, 2008; 2009).

Another brokered network governance form is the **Network Administrative Organization (NAO)**. In this network a separate administrative organization has the central broker role. Their aim is to ensure the sustainability of the network by installing a good coordination. These central organizations are mostly sustainable and legitimate organizations. Usually the central role is administered by a government entity or a non-profit organization. The administrative actor may be an individual person or a formal organization as a whole acting as the moderator or broker of the network. In case of a formal organization – with a board structure – the strategical decisions normally are addressed by the board, where the operational decisions are the responsibility of the director of the network administrative organization (Provan & Kenis, 2008; 2009).

Just like the lead organization the NAO is either mandated or chosen by the other network members. Unlike the lead organization this administrative entity doesn’t have its own agenda or network goals. The network administrative organization’s sole task is to make sure that the network works and thus the network goals are met. The NAO does have to make key decisions, like a lead organization, but unlike that governance form the NAO does this as an independent organization. The latter means that the network administrative organization handles in the best interest of the network, without any commitment towards monodisciplinary goals. The coordination of the network may be a downside for the NAO as the possibility exists that actors may rely heavily on them (Provan & Kenis, 2008; 2009).

2.3 Network effectiveness

2.3.1 Definition

Network effectiveness is a complex concept. It is difficult to define and evaluate the effectiveness of a network as it has various meanings in every sector and network. Network effectiveness is defined by Provan & Kenis (2008: 230) as *"the attainment of positive network-level outcomes that could not normally be achieved by individual organizational participants acting independently."*

In this context it is a view on the effectiveness from the network level perspective. The definition further implies that the participants enter the network for their own positive outcomes as well as the positive outcomes for the network. This network-level effectiveness holds the risk of undermining the performance of one or more network members, but the individual performances of network members can also undermine the overall network effectiveness (O'Toole and Meier, 2004 in Whelan, 2012: 17).

2.3.2 Level of analysis

Provan & Milward (2001) describe three levels of analysis from which the effectiveness of a network can be evaluated. These are the community, network and organizational level of analysis. The participants of those networks are: principals, agents and/or clients. Usually a combination of two categories forms the network. Whether principals, agents and/or clients are involved, depends on the level of analysis. Each level of analysis and some determinants will be discussed in order to measure the perceived network effectiveness. The factors of network effectiveness will also be further discussed in part 2.2.4 network effectiveness determinants.

First of all there is the community level of network effectiveness. In this network form the community has to be served. A local district or neighbourhood has to benefit from the network's actions. The key stakeholders of this network are principals and clients. Typically funders, politicians, regulators and the public are involved. These stakeholders should see their needs and expectations satisfied. As some participants may disagree on some network goals it becomes more difficult to work towards some network goals. In this case all actors may try to minimize the problems to come to an agreement on their mutual needs. A factor that may help in satisfying the needs of the network is trust. The social capital (relationships and trust) that these network members build by working together is very valuable for the current and future actions of the community-based network. If trust between the network members is high, the network becomes more efficient and effective (Provan & Milward, 2001).

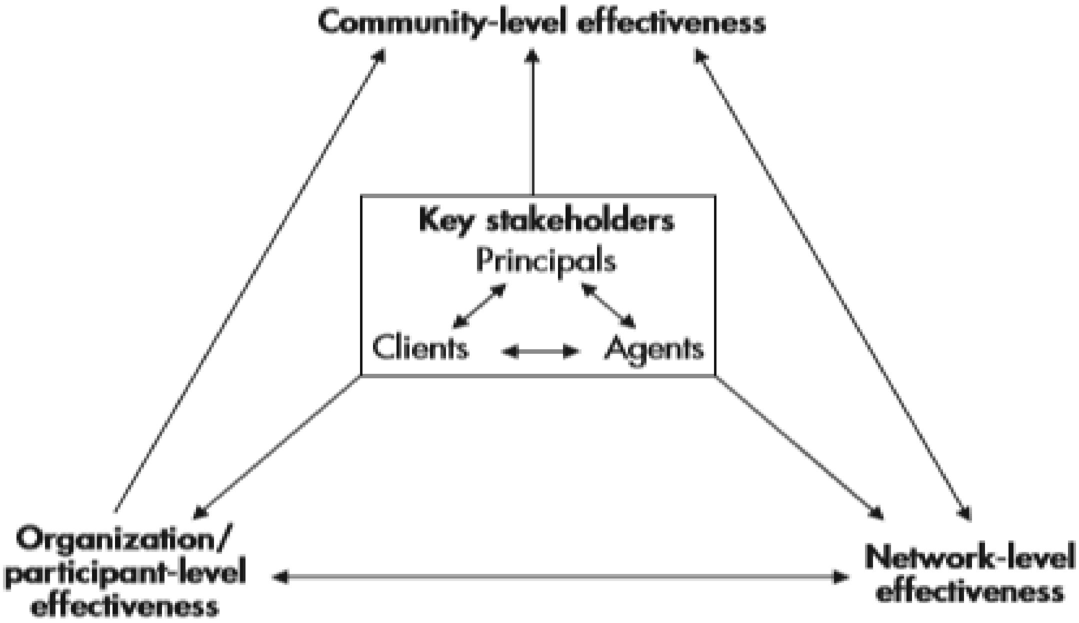
A second level of analysis for the network effectiveness that Provan & Milward (2001) discuss is the network level. Where in the community level the network satisfies the needs of clients and various community interest groups, the network level only has eyes for the network goals. The latter means that network goals are more important than the organizational needs. The key stakeholders of the network level are principals and agents. The network members, funders and regulators and a network administrative organization can be involved at this level. The NAO can play or plays an important role as the broker of the network. They coordinate and govern the network and look after its finances. The administrative entity operates as an agent of the community, but also as the principal of all network members.

Provan and Milward (2001) indicate some factors that might influence the network level of analysis. These factors of network effectiveness can be measured. Network growth is one of the methods to measure the network effectiveness. It is important that some core organizations form the network and provide critical services. Another measurement method is addressing the strength of the different relationships between the network participants. Organizations become multiplex if they have several connections to one another. This means that the relationship sustains if one of the ties between the two actors is broken. Effectiveness can also be measured by evaluating the administrative structure. For small organizations it is difficult to commit to and maintain mutual network goals over a period of time. Earlier Provan & Milward (1995) already argued that control is an important factor of network effectiveness. A network administrative organization plays a crucial role in the network success, although it isn’t the only factor influencing the outcome of the effectiveness (Provan & Milward, 2001).

A third and final level of analysis is the effectiveness at the organizational level. Many actors still join a network out of self-interest. The organizational level focuses on the benefits for the organization. Thus, organizations can benefit a lot of networks through funds, resources et cetera. This is an important factor for the network itself as organizational success is essential to the network success. In some occasions though network success can only be achieved if some individual network members abandon their own goals. One of the methods to measure effectiveness from the organizational network level is through client outcomes. These outcomes give a clear view on the effectiveness. The organization – benefiting from the network – will see some benefits to their organization and clients which wouldn’t have been possible without the network (Provan & Milward, 2001).

Each level’s outcomes – community, network or organizational – affect the outcomes of another level of analysis. Principals, agents or clients normally focus on the effectiveness of one level of analysis but these stakeholders actually satisfy the needs of another group as well. This is illustrated in figure 4. This illustration shows that only by satisfying the needs of all stakeholders we are able to realize the optimal network effectiveness. An example: principals are mostly concerned with the community level effectiveness but therefore have to rely on network providers to serve and satisfy the clients. The fact that these stakeholders hold different interests makes it more difficult to evaluate the effectiveness of a network (Provan & Milward, 2001).

Figure 4: Network analysis at different levels and the relationships between these levels, the stakeholders and (its) effectiveness (Provan & Milward, 2001: 421).


Community-level effectiveness
Key stakeholders
Principals
Clients
Agents
Organization/ participant-level effectiveness
Network-level effectiveness

2.3.3 Effectiveness characteristics

Some authors elaborated on some characteristics or factors of effectiveness. Provan & Kenis (2009) for example state that network effectiveness is influenced by three exogenous factors. These factors are the network form, its inception and the developmental stage of the network. The first factor ‘network form’ corresponds with the characteristic ‘appropriate governance’ from Moynihan’s et al. theory (2012) and with the structural level of analysis to measure the performance of a network (Whelan, 2015). This factor is already discussed in this thesis (2.2.3) as the three network governance forms are shared governance, lead organization or network administrative organization. Whelan also includes the aspect of hub, all-channel and chain network forms. As actors, boundaries and ties of the network differ we may conclude that the structure of the network form has an impact on the possible achievements of a network.

The characteristics of the three network governance forms are illustrated in table 1. By looking at the characteristics of the network the authors create a link with some determinants that might influence the network effectiveness. These four main factors are trust, size, goal consensus and the nature of the task which concerns the competencies of the actors (Provan & Kenis, 2008).

Table 1: Network governance forms and their key predictors of effectiveness (Provan & Kenis, 2008: 237)

Network governance form	**Characteristics**			
	Trust	**Number of participants**	**Goal consensus**	**Need for network-level competencies**
Shared governance	High density	Few members	High	Low
Lead organization	Low density, highly centralized	Moderate amount of members	Moderately low	Moderate
Network Administrative Organization	Moderate density, NAO monitored by members	Moderate to high amount of members	Moderately high	High

The second and third exogenous factor of effectiveness of Provan & Kenis theory (2009) is the inception and the developmental stage of the network. The criteria to measure effectiveness differs for both aspects. According to Mandell (1990, in Provan & Kenis, 2009: 449) this inception – either a mandatory or voluntary network – has an impact on their strategic management. For the developmental stage a model with four stages of live cycles was used. These stages were the emergence of a coalition, transition to a federation, maturity of federation and critical crossroads (D'Aunno and Zuckerman, 1987 in Provan & Kenis, 2009: 451). Each stage has specific criteria that reflect better on their effectiveness outcome, for example the attainment of network goals isn't possible to measure in new networks, but it is measurable in mature networks which already achieved (or didn't achieve) network goals (Provan & Milward, 2001).

Aside from the appropriate governance Moynihan et al. (2012) describe four more characteristics: involvement at multiple levels, network design, legitimacy and stability. First of all there is the involvement of the network at multiple levels. When the ties of an organizational network are built around a single person, it creates a likelihood that other members in the organization won't be committed to the network goals. They link it to the concept 'multiplexity'. This means that the diversity of the relationships among partners, based on the number of different types, is maintained. Yet, multiplex ties have a stronger character then single ties as multiple interests are involved. The network effectiveness can be enhanced since the goals and interests of the network are understood and accepted through the involvement of various members of the network.

Moynihan et al. (2012) describe network designs as the structure of relations in networks. These can either be dyadic, triadic or whole goal network relations. They developed the concept 'selective integration'. The integration across members is needed in order to perform the tasks that are well suited to network solutions. The integration can't be too little nor too much, since interacting frequently and intensively with the other members could create an over-embeddedness of the time and coordination costs. The ties between the network members have to be appropriate and targeted in order to work together effectively. Two goals should be set when they design a network. The first goal is to emphasize selective integration based on a mix of close ties,and brokerage. The second goal relates to the idea of closure. Even though strong relationships are needed within networks, weak ties with low to moderate interaction are also appropriate for most relationships.

Another characteristic of effectiveness is legitimacy. According to Den Boer et al. (2008) there's a trade-off between effectiveness and legitimacy. Moynihan et al (2012) argue that internal and external legitimacy are essential to ensure the success of one network. Internal legitimacy consists on demonstrating the value of participating in the network, developing trust among the members, resolving conflicts successfully, and building network and communication mechanisms. External legitimacy is seeking new members, it promotes the network, and provides resources to reach the goals. Internal legitimacy is more important in the development of the network, but the risk exists that the internal legitimacy will be ignored or underrated when it is a mandated network.

Stability is a characteristic of network effectiveness that both Moynihan et al. (2012) and Whelan (2015) discuss. There is an important trade-off between flexible and stable networks in relation to network effectiveness (Whelan, 2015). With flexible relationships whole goal-directed networks have great advantages performing tasks such as emergency responses. In this case actors are able to reach out to one another and work together in a more efficient way. This gives the network the possibility to change. But high flexibility also means instability, which then tends to lead to ineffectiveness. Although emergency responses need a highly flexible approach, it also needs some form of stability regarding the network members, coordination and distribution of resources (Moynihan et al., 2012). Whelan (2015) argues that the policy of a network covers these issues by determining their actions and procedures. The procedures are in place to attain the predetermined network goals, but may also evoke some tensions concerning the flexibility of the network. He argues that stability especially is important for long term networks. Procedures and policy implementations help develop this stable network.

So Whelan (2015) proposes some similar and some different factors (or 'levels') to determine network effectiveness. He looks at five factors that shape the network performance. These factors are the network structure and policy as earlier discussed, its culture, technology and relationships.

In a network actors with different cultures can be represented. Culture stands for the beliefs, norms and values that develop in a group over time and influence how the group thinks and responds to certain issues. As cultures differ, this factor may influence the performance in a negative way. However, the differences can also stimulate critical thinking and positive performances from the group (Whelan, 2015).

Furthermore Whelan suggests that technology is a network performance factor. It concerns the technological infrastructure of the network. The infrastructure is in place to support the networks information flow. The network participants have to be connected through the network design in order to share information more efficiently and effectively. Two problems were detected regarding information sharing. In public networks there have been some problems with the information and communication mechanisms concerning the interoperability on the one hand and on the other hand participants find it difficult to find the right balance between information sharing and protecting confidential information (Whelan, 2015).

The final characteristic that will be discussed is the network relationships. Some scholars say that the nature of the relationship is the most important factor to assess network effectiveness (Lavie, 2006 in Whelan, 2015: 546). It is especially central to the network performance when someone tries to determine how well a network operates. The most common determinants to measure this aspect are the level of trust and respect among the network members (Whelan, 2015).

2.3.4 Factors that can influence network effectiveness

There are many ways to determine the effectiveness of a network. In this part the most important determinants to measure effectiveness will be presented. The determinants of the earlier presented table 1 (pg. 23) will be discussed. These were trust, number of participants, goal consensus and network-level competencies. The perception about these determinants can vary from person to person and from situation to situation.

Trust and the distribution of trust are essential to the network-level effectiveness. If trust is widely distributed the network and ties among the network members are dense. It is possible that there are only sporadic individual relationships among network members. This makes it a network with a low density. The question has to be asked though if a every actor has to have ties with one another and put faith in them or if some relationships are sufficient to let the network succeed (Provan & Kenis, 2008)?

Whelan (2015) makes the distinction between interpersonal and interorganizational network trust. Interpersonal trust refers to the trust you place in the representatives of the other actors. Interorganizational trust is the trust one has in the partner organization itself.

Trust is the highest and most effective in a shared governance form. Networks in which trust has a lower density can still be effective, but to attain their goals their governance form is likely to be brokered. A lead organization or the network administrative organization are the brokered governance forms. A NAO normally is more dense than a lead organization because their members monitor the activities of the broker, while in a lead organization there are only dyadic ties (Provan & Kenis, 2008).

The number of the network participants is a second important network determinant. Once a network grows, new members enter the possible ties between these members also increases. Once a network becomes bigger it will be more effective in the form of a NAO or lead organization. Shared governance is the optimal choice when the number of network members is low. The amount of network members relates to a similar determinant, namely network inner stability (Provan & Kenis, 2008).

Network inner stability refers to the participating network members. The longer these members take part in the network the easier it is to create trust, share information and build continuous relationships. These factors are likely to lead to higher integration and network effectiveness (Turrini et al, 2010). It is as Ferlie and Pettigrew (1996: 95 in Turrini et al., 2010: 542) state: *"A face that you know and recognize is key"*.

Another network determinant is the goal consensus between the network participants. Consensus in goals and ‘domain similarity’ makes network organizations perform better than when there is a conflict. It isn’t always easy to prevent a conflict of interest as network members have to respond to both the organizational as the network goals. The formal accountability to the network goals of the network members is typically rather limited and the conformity to the procedures and rules is voluntary (Provan & Kenis, 2008).

The network literature focuses more on the aspect of similarity and homophily in goals. Network members will be attracted to work with actors that share the same interests. High commitment to network-level goals will normally lead to an effective network. This is often the case in shared governance forms, if they agree on the network goals. A moderate commitment can still lead to an effective network as well. This can either be a network administrative organization or a lead organization form. The NAO has a higher moderate goal consensus than the lead organization. The latter is moderately low (Provan & Kenis, 2008).

The lead organization makes most critical decisions when the other members can’t resolve the conflict. A lead organization isn’t always a long sustainable network as network members may lose interest in the network goals. The network members of an NAO are more committed to the network goals. The members of the network will be more involved as well. Nevertheless there may only be a moderate level of consent on what the network should do and how they can involve the members (Provan & Kenis, 2008).

The final network effectiveness determinant that will be discussed, is the network-level competencies. As earlier stated actors join a network because they can’t achieve their goals on their own. Interdependence between the network participants is essential in most cases. A brokered network governance form is most suited as they possess the ability to develop special skills to attain the network goals. The network appeals to the skills of independent network members. Therefore a shared governance form isn’t that likely. It can be concluded that in a shared governance form the network-level competencies are low. A lead organization has a moderate level of network competencies and a NAO has the highest level of all three governance forms (Provan & Kenis, 2008).

The emergency and intervention plans contain specific procedures for the approach of a crisis. First of all a crisis council has to gather with designated members. Only in specific cases extra members can be invited. Furthermore some procedures are described on where to gather, how to make contact with other members of the crisis council on the terrain and so on. These plans are made by the administrative government’s crisis and emergency management department in consultation with the emergency services[1]. Representatives of these emergency organizations normally also have their place in the crisis council (Parlementaire onderzoekscommissie, 2016).

3. Methodology

3.1 Research design

This explanatory research uses a single case study, reflecting on the performance of the provincial crisis council during the Brussels Airport terrorist attack. The main aim of this research is to evaluate the perceived effectiveness through the usage of document analysis, interviews and a small survey with the security actors within the crisis network. Both qualitative and (slightly) quantitative methods are being used. It will be the perception of the network participants that will be used to evaluate the effectiveness of the network. This research should add to the network literature and uncover some advantages and disadvantages of the current crisis and emergency procedures in Vlaams-Brabant (and Belgium as a whole). It has to be stated though that some new procedures have been introduced after the terrorist attack on March 22, 2016[2]. The following research question is being asked:

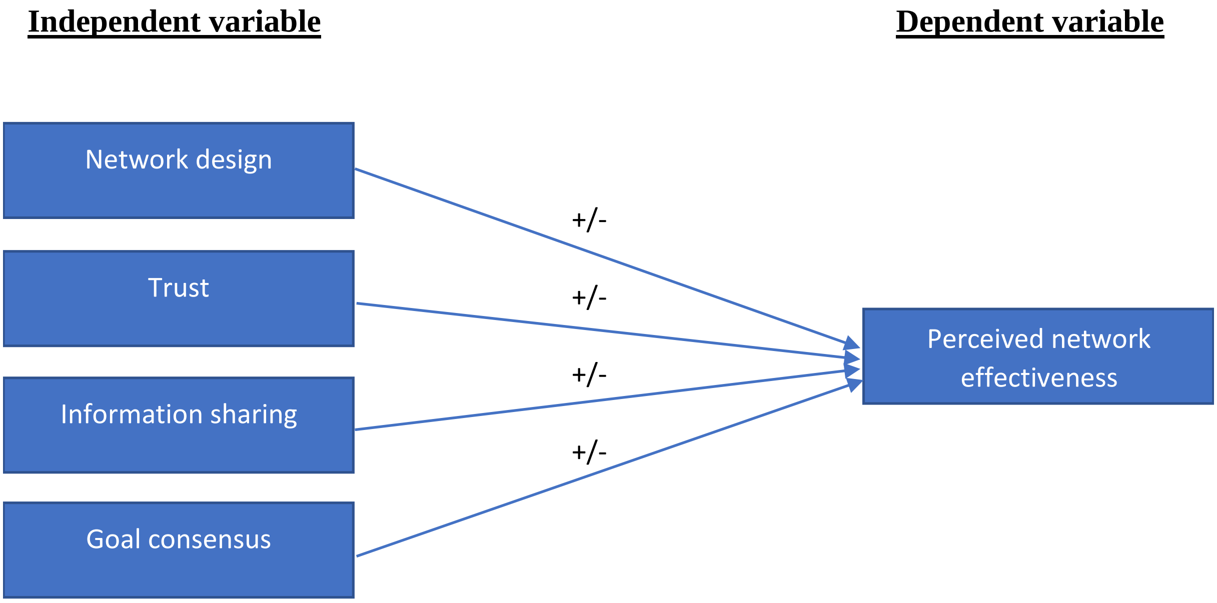
'How effective was the strategic crisis network perceived to be in response to the Brussels Airport terrorist attack on March 22, 2016 and what factors influenced the network effectiveness?'

In order to evaluate the crisis network performance a case study will be used. In this case the dependent variable is the perceived network effectiveness. The reason that we focus on the perception of this dependent variable is that studying network effectiveness itself is often too difficult. Many researchers therefore take one step back by assessing the perceived network effectiveness in order to find answers (Provan & Kenis, 2009: 441). Responses from the network participants will be analysed. These responses will contain information on the independent variables that are studied and that may affect the network effectiveness outcome. The independent variables set by the researcher are: the network design, trust, information sharing and goal consensus. This is visualised in figure 5. More about the operationalization of these variables in 3.4 operationalization.

[1] In Belgium there are three levels of administrative governments: governmental, provincial and federal.

[2] These new procedures are the royal decree of May 1, 2016 concerning the enrolment of a special emergency and intervention plan for terrorist events (Royal decree, May 1, 2016).

Figure 5: The possible effect of the independent variables on the dependent variable



3.2 Case study

3.2.1 Choice of methodology

A case study research can either exist out of a single case study or a multiple case study. In both methods it is important to clearly state the beginning and ending of the case(s). Another aspect is the usage of the holistic or embedded approach. In a holistic case study the amount of units of analysis is equal to the number of cases, where in an embedded case study a case can have several units of analysis. These different types of case studies are illustrated in figure 6. A case study is being used to give a thorough description of (a) multiple case(s) and to make people understand the nature of a phenomenon and its context (Yin, 2012).

In this case a holistic single-case design is the chosen methodology (see figure 6). An evaluation of the perception of effectiveness of the crisis network – the provincial crisis council – may give new insights or create new forms of networks in the Belgian crisis management sector. The context of this case is the terrorist attack at Brussels Airport in which we evaluate the performance of the crisis network. The provincial crisis council is our case subject. The case is specified in time and space. The provincial crisis council was operational for three days and was located at Brussels Airport[3]. The security actors – taking part in the crisis network –

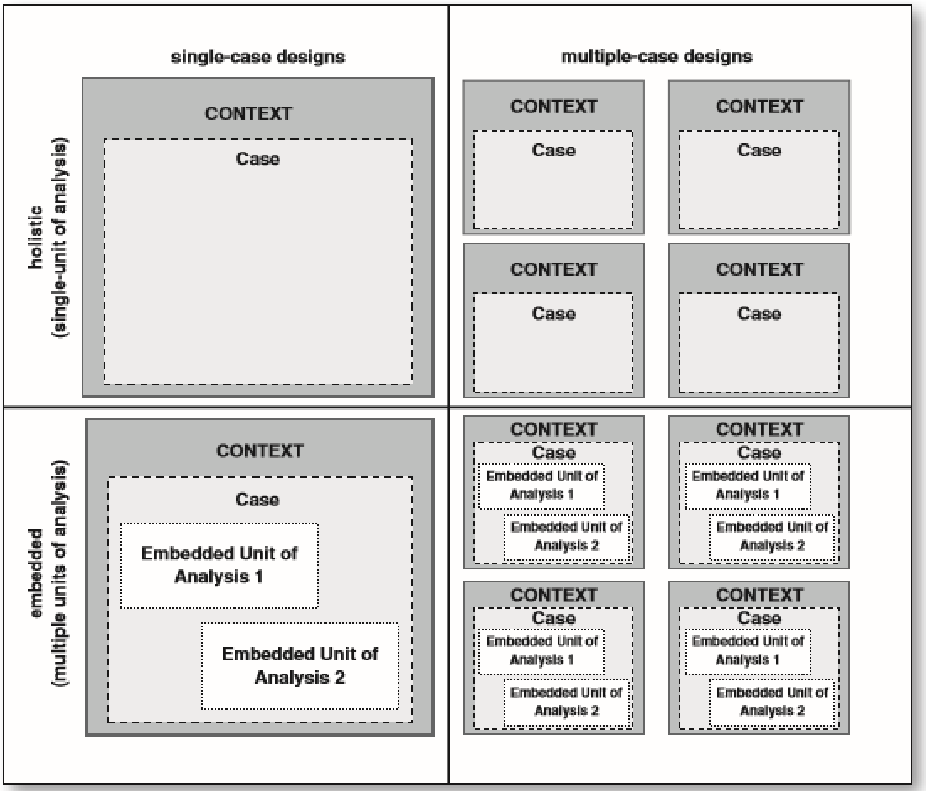
[3] In the beginning there were some problems with the start-up of the network as there was an internal crisis council at Brussels Airport and a provincial crisis council at the Vlaams-Brabant's department of crisis and emergency management. Due to safety reasons the governor decided to hold the crisis meeting in their provincial offices. Yet, some people of the provincial crisis council went directly to the airport, as is described in the crisis and emergency plan as the meeting point. To prevent more dissemination the governor relatively quickly revoked his decision after which they moved the provincial crisis council to the airport.

assessed and coordinated the situation from inside the crisis council. This case has an organizational decision-making aspect, which is typical to case studies according to Yin (1981: 97).

The unit of analysis is the Vlaams-Brabant's provincial network of response organizations in crisis and emergency management. A closer look tells us that the unit of observation is the provincial crisis council. The crisis council is concerned with the strategic crisis response. In this case it is specifically concerned with the crisis response during the Brussels Airport terrorist attack.

Single case studies are mostly used to test theories. Multiple case studies are mostly used to compare similar or opposite cases against each other. In general a case study is relevant for utilizing knowledge and analysing decision-making processes. Knowledge utilization has the following characteristics: multiple decisions which are taken over a long period of time, a big amount of relevant actors and special, historical events (Yin, 1981). During the crisis coordination at Brussels Airport a decision-making process took place. Several actors participated in the coordination of the special crisis – in the form of a network – over a period of three days.

Figure 6: case study designs (Yin, 2012: 8)


single-case designs
multiple-case designs
holistic (single-unit of analysis)
embedded (multiple units of analysis)
CONTEXT
Case
Embedded Unit of Analysis 1
Embedded Unit of Analysis 2

Case studies hold some advantages when it comes to understanding and explaining a specific process and their outcomes to large N studies. Because of the special, historical event of this case it is a significant single case study worth studying. To date it was the most extreme crisis Belgium and the province of Vlaams-Brabant had to deal with. By using a single case study it is possible to give a detailed description on the involvement of the security actors and the network structure. Furthermore network theories will be tested, especially the ones from Provan & Kenis (2008, 2009) and Whelan (2015). Testing a theory on the characteristics of a special, critical case boosts the theory's literature (Eckstein, 1975). A case study also makes use of the perceptions and motivations of the participants – in this case the security actors of the crisis network – to follow the development of the process and the factors influencing the process (Blatter & Haverland, 2012: 6).

3.2.2 Type of case study

Looking at the different types of case study research from Stake (1994) it is difficult to select one for this case. He distinguishes three different types of case studies. According to him a case study can have an intrinsic, instrumental or collective inception. An intrinsic case study really focuses on the case because of its importance. You have to understand the case by looking at its (special) features. The instrumental case study on the other hand looks at a problem or theory and tries to refine or understand it. The case is of less relevance. Finally, the collective case study applies to a multiple-case study in which a researcher tries to understand a phenomenon or group of people.

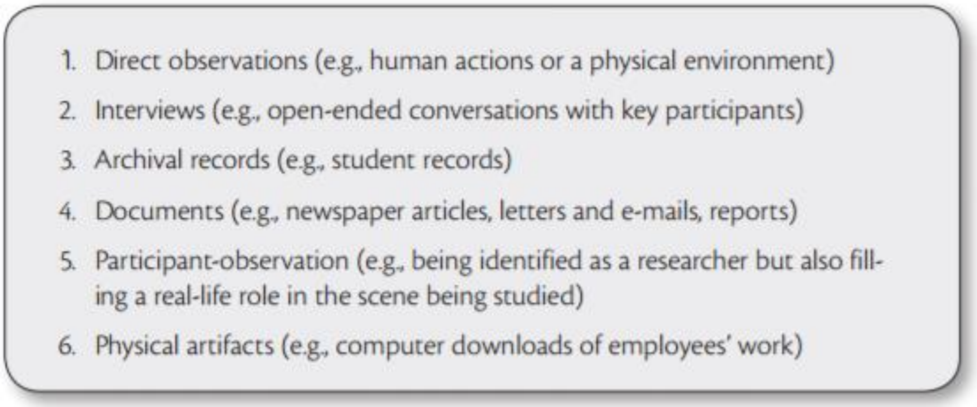
The crisis network in place after the Brussels Airport terrorist attack is a case of a significant relevance due to the magnitude of the event. For this matter it has to be concluded that evaluating the crisis network is an intrinsic single case study. The network theory is used to identify some special features of the crisis network. Nevertheless, it may also be argued that is an instrumental single case study. Although one of the aims is to evaluate the crisis network structure, this will be done by using some network theories[4]. These theories are fundamental in the process of evaluating the performance of the network. The network theories will be tested by using the provincial crisis council as a study subject.

[4] The frameworks of Provan & Kenis (2008, 2009) and Whelan (2015) will be tested.

3.3 Data collection methods

Yin (2009: 113, 2012: 10) argues that there are six valid methods to gather data in a case study research. These methods are described in figure 7. Two of these methods plus a quantitative survey are being used to analyse the case. The triangulation of gathering data enforces the validity of the research.

Figure 7: Six sources of data collection doing a case study (Yin, 2012: 10)



1. Direct observations (e.g., human actions or a physical environment)
2. Interviews (e.g., open-ended conversations with key participants)
3. Archival records (e.g., student records)
4. Documents (e.g., newspaper articles, letters and e-mails, reports)
5. Participant-observation (e.g., being identified as a researcher but also filling a real-life role in the scene being studied)
6. Physical artifacts (e.g., computer downloads of employees' work)

The first data that was gathered were governmental documents. These documents, such as the provincial emergency and intervention plan Brussels Airport (confidential) and the provisional report on the coordination in consequence of the Brussels terrorist attacks on March 22, 2016, were very useful in analysing the procedures and composition of the crisis network.

Furthermore interviews were introduced as a research method. This were semi-structured interviews in which several security actors of the crisis network were interviewed. The reason for the interviews to be mostly semi-structured was because each security actor had to elaborate on some network effectiveness determinants, the network role and goals. The interviews also gave more information about the real composition of the provincial crisis council and the procedures that were taken during the crisis coordination. The interview guide is added as annex 1.

After drafting my interview guide I started making a sample of relevant persons to interview. Every actor normally has one or two vast members in the crisis network. This is predetermined in the provincial emergency and intervention plan. This was my selection for interviewing respondents of the network. Their contact information was gathered through my direct link with the crisis and emergency management department of the province[5]. Eventually the sample

[5] During my Belgian curriculum as a student I was able to do two internships at the crisis and emergency management department of Vlaams-Brabant.

existed out of the governor of Vlaams-Brabant, the head of the provincial department of crisis and emergency management, two fire department commandants (discipline 1), the federal inspector of health and the psychosocial manager (discipline 2), the director-coordinator of the federal police Halle-Vilvoorde (discipline 3), the provincial army colonel for logistics (discipline 4) and the crisis contingency manager of Brussels Airport. These are all very important and reliable respondents who represent their organization/discipline in the crisis council of Vlaams-Brabant. Therefore this sample is believed to be valid and reliable. Afterwards I did one more informative interview with the director of the Communication and Information Centre (CIC) about the alert procedures once a provincial state of emergency is declared.

Besides the usage of these methods I was able to see the location and equipment of the crisis council and the rooms for the work cells. An explanation was given – by the contingency manager of Brussels Airport – on the activities of the different actors within the network. A small tour at Brussels Airport was also given on the scene, where the coordination of the emergency services was held.

Finally a small survey has been sent to seven out of nine network participants[6]. Five of them filled in the survey. This survey contained a statement about three of the four network determinants: trust, information sharing and goal consensus. The network design wasn't included in this survey, as it was already heavily discussed during the interviews. Each respondent had to give a score on a scale from one to five on each of the network determinants to evaluate the network performance. This scale went from '(1) not applicable during the crisis coordination' to '(5) fully applicable during the crisis coordination'. This survey is added as annex 2.

[6] The contingency manager of Brussels Airport argued that the evaluation of the crisis council was up to the disciplines. The multidisciplinary evaluation by Cemac also only included the different disciplines. Following this argument, the governor was also excluded.

3.4 Operationalization

While evaluating the perceived effectiveness of the crisis network some independent variables also play an important role. These factors have to be operationalized in order to measure the perceived effectiveness. The variables that are operationalized are: the network design, trust, information sharing and goal consensus. Other determinants, such as the network inner stability, were also mentioned during some of the interviews. The latter will also be discussed in the analysis but isn't operationalized. As earlier mentioned, the network effectiveness will be assessed by looking at the four factors. This means that a positive/negative impact of these factors will be used to analyse the network effectiveness through the eyes of the security actors. These network determinants are operationalized in table 2.

The independent and dependent variable are operationalized through the usage of information from interviews and government documents such as the provisional report on the coordination in consequence of the Brussels terrorist attacks on March 22, 2016. The interviews cover all variables where the documents mainly shed some light on the network design and information sharing.

This thesis thus reflects on the perceived effectiveness of the crisis network. This assessment will be done by evaluating the responses of the network participants concerning the selected variables. The most important question to measure the dependent variable is 'did the network achieve its goals?' Furthermore each respondent is being asked about the specific variables affecting or not affecting the perception of the network performance.

The network design is the first variable that is being used to evaluate the network performance. After reviewing some governmental documents the structure of command in the provincial crisis council became clearer. The analysis will have to show us if the design of the PCC is the same in practice as in theory. In order to further determine the network design the interviews were of help. In those interviews the respondents were being asked about their perception of the network governance forms. The literature study already showed that the design of the network might influence the network effectiveness.

Trust is the second variable that is being operationalized. In the interviews the respondents are being asked about their perception of the (interpersonal and interorganizational) trust between the different participants of the crisis network. The respondents were being asked to talk about their relation with the other disciplines and the person representing the discipline. In the survey a similar concept is used to operationalize trust. The survey analyses the confidence in each other’s capabilities. The amount of confidence one actor has in another then should give an idea about the level of trust between the network participants.

Information sharing is a third crucial factor of network effectiveness. In order to measure information sharing the respondents elaborated on the collaboration and distribution of information in the crisis council. The governmental documents showed that there were some problems with the information stream and log book. Further analysis of the documents and interviews will have to shed a light on the information flow between the different actors of the provincial crisis council. As a part of the analysis a map will be made with all ties between the different network participants. Furthermore in the survey a score is being given by the respondents on the level of information sharing.

The final network determinant we discuss is goal consensus. In order to measure this determinant we asked respondents about the similarity and homogeneity of the (network) goals of the different disciplines. This is both being asked in the interview as in the survey. The answers will indicate the differences and similarities in network goals, but also the level of its network goal consensus.

Table 2: Operationalized variables

Concepts	Indicators	Questions
Perceived network effectiveness	Perceived achievement of the network goals	*- What is your perception of the (non-)achievement of the network goals?*
Network design	Network structure, size, density and centrality of the network	*- Do you believe that the PCC fits one of the following network governance forms and why?:* ⇨ *Hub, all channel or chain?* ⇨ *Shared governance, lead organization or a network administrative organization (NAO)?*
Trust	Amount of ties between the actors, trust in each other's capabilities, interpersonal and interorganizational trust	*- To what extent is trust established between the network participants?* ⇨ *Is it rather trust in the people of the organizations or trust in the organizations itself? Why?* *- To what extent do you trust in the capabilities of the other network participants?*
Information sharing	Flow of information, amount of (multidisciplinary) interactions	*- To what extent did the information sharing happen (directly and indirectly)?* *- How did you perceive the information sharing process?*
Goal consensus	Similarity of network goals, homogeneity of network goals (Provan & Kenis, 2008)	*- To what extent do the network goals of all network members coincide with each other?*

3.4.1 Validity and reliability

The internal validity is assessed by collecting data through document analysis, interviews and a small survey. This data gives us insights on the perception of effectiveness of the crisis network. The interviews are crucial in detecting the goals and roles of each actor in the network. These are in-depth interviews in order to prevent a solely descriptive research. In the interviews patterns between the different variables will be analysed. Pattern matching is especially used in explanatory research. Searching patterns in the different perceptions of the security network actors strengthens the internal validity (Yin, 2012: 16). In order to further improve the validity the analysis is also reviewed by the security actors.

The external validity refers to the extent that findings are applicable in other social settings. In this research the external validity is rather low. This is mostly a problem within qualitative research, because it is so specific to the case. This is no different in my research. We try to strengthen the external validity by using network theories from Whelan (2015) and Provan & Kenis (2008, 2009). Lessons can be learned from testing the theory to the case, and may be somewhat applicable to other (future) crises in which the crisis council is required to gather. Every crisis and crisis response is different though, so the validity is rather low as cases differ in time and space. Because of the contribution to the network literature, the increasing terrorist threat and increasing importance of crisis and security networks the study is believed to be relevant.

The main critique and limitation of a single case study is the generalizability of the research. A critical case may not generalize its results to a broad population, but as Flyvbjerg (2006) mentions does reveal a lot of information. The reason that more information may come out of an extreme case is that more different actors are involved and some mechanisms or procedures are being studied.

Shifting focus to the reliability of the research we evaluate the internal and external reliability. The internal reliability is based on the correlating different factors in a test. It measures if similar scores are produced. The more respondents and same (re)actions by them, the more reliable this study. The research contains interviews with one or two persons from each response organization during the crisis. This doesn't seem to be a big sample, but during these crises every discipline only has one operational and strategic leader. If I would assume these leaders as the sample it is sufficient in my opinion (Yin, 2009).

Interviewing people sometimes leads to socially desirable answers or secretive people. The Belgian Parliament has a parliamentary commission to investigate the double terrorist attack in Brussels. Some crisis leaders have already been heard by this commission. These statements are credible and transparent for the public, which makes them valuable for this research (Parlementaire onderzoekscommissie, 2016).

During the interviews only two persons asked not to record the content of the interview. Nevertheless I was able to write down the most essential information of both interviews. Furthermore every respondent was sincere and critical about the shortcomings and positive factors influencing the effectiveness of the provincial crisis council.

The same network frameworks and case can be used to evaluate the perceived effectiveness of the crisis network. This is an important tool to determine the external reliability. Yet, it has to be argued that time will influence the amount of data that can be gathered (as people might forget details over time). We are now a year after the event and recently a commemoration event took place. A good period to reflect on the terrorist attack at Brussels Airport and the performance of the crisis network as it isn’t too soon, nor too long after the exceptional event in Belgian history.

4. Analysis

4.1 Case description

On March 22nd, 2016 a terrorist attack occurred at Brussels Airport. Three men entered the departure hall with trolleys and suitcases. Each one of those suitcases contained a bomb. At 07.58u the first bomb was detonated. Seconds later the second bomb went off as well. The third and – later seen as – the strongest bomb was dismantled by the bomb squad through a controlled explosion. Although it was a controlled explosion it still managed to damage a big part of the infrastructure (Parlementaire onderzoekscommissie, 2016). The director-coordinator of the federal police and the head of the crisis and emergency management department clearly mentioned that there was the perception that the third bomb could have been intended to target the emergency services.

The three terrorists had a clear target. They were targeting all passengers heading towards the United States of America, Russia and Israel. These countries are leading the coalition in Syria to fight the Islamic State of Iraq and the Levant (ISIL). Belgium is also taking part in this coalition. The terrorist attack was later claimed by ISIL (Parlementaire onderzoekscommissie, 2016).

Once it became clear that the country was dealing with a terrorist attack the administrative governments declared a provincial and federal state of emergency. The governor of Vlaams-Brabant declared a state of emergency at 08.30u. About half an hour later (09.03u) the federal administrative government scaled the incident up from a provincial to a federal state of emergency (Parlementaire onderzoekscommissie, 2016).

Declaring a state of emergency means that some procedures have to be started up. In this case both the federal and provincial crisis council were established. Although normally a phase is scaled up from one level to another, article 20 of the royal decree of February 16, 2006 – concerning the emergency and intervention plans – states that there is a possibility to activate different levels of crisis councils at the same time.

The federal crisis council handled the judicial and administrative aspects of the case. The crisis communication was also done by them. Normally the latter is the task of discipline five in the PCC: the provincial information unit, but their role was now limited. The provincial crisis council was handed the task of the crisis coordination and relief (Parlementaire onderzoekscommissie, 2016; personal communication, head CEM VB). The province is more experienced with the relief during and after a crisis. Normally the province does both the judicial and operational tasks in a provincial phase as is described in the royal decree of February 16, 2006 and the specific provincial emergency and intervention plan Brussels Airport. Yet, due to the magnitude of the crisis and the coordination by the federal crisis council the administrative governments decided to divide the tasks (personal communication, governor VB; head CEM VB).

The governor and his crisis and emergency management department made the decision to meet in Leuven. The provincial crisis council (PCC) gathered in the provincial offices in Leuven. All actors of the provincial crisis council were being asked to send their representative. The special emergency and intervention plan (BNIP[7]) Brussels Airport indicates the main representative of each discipline and the special guest(s) that are involved (personal communication, head CEM VB; D3; D4).

The decision to meet in Leuven was being made because of security and mobility reasons. It deviated from the predetermined location – the building 'Satellite' at Brussels Airport – that is described in the BNIP Brussels Airport. It would have been difficult to get to Brussels Airport in rush hour and the safety wasn't guaranteed there. Nevertheless, Brussels Airport Company started its own internal crisis council at Brussels Airport (CC BAC). Yet, the provincial crisis council gathered in the provincial offices in Leuven for the provincial coordination. The province there has an emergency room at their disposal. Therefore it is also considered as a valid location for the PCC. In case of crises for which there isn't a special plan this location is normally used as PCC. For such crises a regular emergency and intervention plan (ANIP[8]) is drafted (personal communication, governor VB; head CEM VB; BAC).

Once almost all disciplines were represented in the PCC in Leuven a video conference with the federal crisis council (FCC) was held. During this conference the actors shared information and got a situation report. There the PCC received the question from the federal crisis council (FCC) to transfer the PCC to the airport (personal communication, governor VB, head CEM VB).

Some representatives of the provincial crisis council already were present in the internal crisis council of Brussels Airport Company. They had the immediate reaction to go to the predetermined location from the plan (personal communication, FGI; PSM). Furthermore Brussels Airport Company (BAC) ignored the request to send someone to Leuven. They felt that they could better coordinate and fulfil their responsibilities on the scene (personal

[7] Bijzonder Nood- en Interventieplan

[8] : Algemeen Nood- en Interventieplan

communication, BAC). There was a dissemination of actors which the FCC tried to resolve by integrating the PCC members from Leuven in the CC BAC at Brussels Airport. So shortly after gathering in Leuven the actors from the PCC went to Brussels Airport. Police escorts were being used to speed up their arrival. These actors left at around 09.15u - 09.30u. During the transport there was no more communication possible due to the saturation of the mobile network (personal communication, D3; D4; head CEM VB).

To ensure the continuity of the PCC, during the transport, two mechanisms temporarily stepped in. On the one hand some substitutes of the main representatives stayed in Leuven in order to coordinate the situation and on the other hand the crisis council of Brussels Airport Company coordinated the relief. In the CC BAC three out of five disciplines were represented. The fire brigade (D1) was represented through the fire unit at Brussels Airport. The two main representatives of the medical team (D2) – the federal health inspector (FGI) and the psychosocial manager (PSM) – directly went to the CC BAC. Furthermore, for the police (D3) the special advisor of the director-coordinator of the federal police was present, namely the chief commissioner of the Brussels Airport's police. Because of the representation in the CC BAC and the continuity of the PCC during the transport, the decision-making and coordination process didn't stop (personal communication D4, BAC, PSM).

Eventually, at around 10.30u - 11.00u the members of the PCC arrived at the 'Satellite' at Brussels Airport. From there on the crisis coordination was being done by the provincial district commissioner and the CEO of Brussels Airport. Normally the governor of Vlaams-Brabant leads the PCC, but he was part of the FCC until 16.00u. In his absence the provincial legislature states that a district commissioner becomes responsible for the crisis coordination. In this case it was a co-leadership role with the CEO from Brussels Airport. The return of the governor led to a shift of leadership. From there on the governor coordinated the PCC for the upcoming days. In the end the provincial crisis council remained active for three days (personal communication, D3, governor VB, head CEM VB).

4.2 Emergency response procedures

4.2.1 BNIP Brussels Airport

Since 2000 there is a special emergency and intervention plan (BNIP) in place for calamities at Brussels Airport. This plan is developed by the Vlaams-Brabant's crisis and emergency management department in consultation with Brussels Airport and its so called crash management team. The latter contains the different disciplines (D1, D2, D3) who are every day operational at the airport (Cemac, 2016[9]).

An emergency and intervention plan can be activated in case of an emergency situation. This is defined as: *'every incident that causes or may cause damaging consequences for the society e.g. disorder of public security or a serious incident that is life-threatening for persons and/or important goods in which coordination of all disciplines is required to tackle and limit these damaging consequences.'* A provincial coordination is demanded when an incident surpasses the territory of one municipality or when the governor decides that a provincial coordination is required (Royal decree of February 16, 2006).

The BNIP Brussels Airport is divided in three parts, containing three scenarios. The first scenario is about the procedures when an airplane deals with technical difficulties. The second scenario describes the steps that the provincial crisis council should undertake when an airplane crashes in a radius of 500 meters of the airport. The third part explains the procedures in case there is no airplane involved. This scenario thus involves an incident on the territory of Brussels Airport. The internal crisis council of Brussels Airport Company immediately activated the third part of the BNIP at 08.14u. Once the provincial state of emergency was declared at 08.30u the provincial crisis council also activated this part of the BNIP (personal communication BAC, head CEM VB).

The plan clearly defines the main representatives of the disciplines that have to gather in the provincial crisis council. All respondents agreed on the following composition of the provincial crisis council. The governor leads the PCC, consulted by his provincial crisis and emergency management department. The information unit (D5) is also a part of the provincial tasks. The governor's other advisors send a predetermined representative. The main representatives of the other disciplines are: the head of the zonal fire brigade (D1), the federal health inspector (D2), the psychosocial manager (D2), the director-coordinator of the federal police (D3), the head of civil protection (D4) and the head of the provincial defence unit/army (D4). Furthermore the

[9] This is a confidential document which is only used once as a source to clarify how and by whom the BNIP Brussels Airport was made.

involvement of Brussels Airport Company – and possibly involved airline companies, airport security and/or distributors – is required as a special guest. BAC is represented by the CEO and its emergency contingency manager. Another actor that has a place in the provincial crisis council is the mayor and the emergency contingency official of the municipality. In case of a criminal incident the federal prosecutor`s office is involved. The latter is less known by the vast members of the network according the one of the fire brigade officers (personal communication, D1 – 2) .

Meeting points are another important procedure that is described in the BNIP. Locations for operational and strategic meeting points are included. Each discipline has – besides the strategic main representative in the PCC – an operational representative that takes the lead on the field. They are in direct contact with the representative of their discipline in the PCC. Operational meetings include the first operational meeting point[10] and the further meetings in the Commando Post -Operations (CP-Ops) between these operational representatives. The highest ranked commandant of the fire brigade in the field becomes the Director of the Commando Post -Operations (Dir-CP-Ops).

On the strategic level the location of the PCC is defined in the BNIP. It states that the building 'Satellite' at Brussels Airport is to be used as the location for the PCC. In case this location is occupied, not reachable or because of another valid reason that it can't be used an alternative location is foreseen at the fire department in Zaventem (personal communication, D1 – 1; D3). The governor stated that the alternative location was never considered as an option.

The BNIP is revised every year in case new procedures are agreed or flaws are discovered. This happens in the provincial safety council. This council assembles all the main representatives of the crisis council added by the governor's provincial department and the contingency manager of Brussels Airport (personal communication D1 – 2; D4, BAC). According to the psychosocial manager this safety council gathers ten to twelve times year. Their main task is to revise all emergency and intervention plans, organize emergency exercises and discuss new risks and/or procedures (Royal decree of February 16, 2006). In order to retain its license Brussels Airport every two year has to do an emergency exercise in which it tests some procedures. The last exercise was held on 25/04/2015 (personal communication, D1 – 2; D3; D4; BAC; head CEM VB).

[10] Also called 'motorkapoverleg' in Dutch.

Besides the biennial emergency exercise at the airport, the province, municipalities and disciplines have the obligation to hold emergency exercises themselves. There was almost no preparation for terrorism related incidents according to the respondent of D4, despite previous terrorist events in Belgium e.g. the terrorist attack at the Jewish museum in 2014 and a shooting in a Thalys train between Brussels and Paris in 2015. The commandant of Defence argued that there was only held one small table-top exercise with a terroristic scenario in the safety council. This scenario involved a shooting in the hospital and student aula. So, the scenario wasn't practiced with the airport instances (personal communication, D4).

There was no BNIP terror plan in circulation at the time of the terrorist attack. This was only developed after and due to the events on March 22, 2016. Because of the important location and risks an airport entails a BNIP is in place. For other (random) targeted locations a BNIP terrorism could be useful. The province of Vlaams-Brabant is now awaiting the approval of its draft BNIP terrorism (personal communication head CEM VB). The royal decree of May 1, 2016 only included terrorism as a scenario in the ANIP's and BNIP's of municipalities after the terrorist attacks. The Dir-Co is now doing a round-up in all municipal safety councils in order to integrate this scenario in all municipal emergency and interventions plan.

4.2.2 Alert system

At 07.59u the Vlaams-Brabant's aid centre 112 (HC112 VB) received first notice of an explosion of a bomb at Brussels Airport. A civilian called in by dialling the emergency phone number 100/112. Immediately the operator had to assess if the event was a small or large scale incident. It became clear that this was a large scale incident (personal communication CIC).

The operator of HC112 VB has the possibility to classify the incident as a multidisciplinary incident. It rapidly became clear that a multidisciplinary approach was necessary. In this case the other partner, the Communication and Information Centre (CIC), also becomes involved in the alert procedures. The CIC is actually a police related aid centre[11]. The CIC and the HC112 VB are located in the same room and therefore work with one system. This makes it easier to share information (personal communication, CIC).

The first alert message from the HC112 was directed to the emergency services. This message was already sent at 08.00u. It gave the emergency services the possibility to mobilize the necessary resources and to send them to Brussels Airport. In the aftermath of this message all

[11] It has an emergency phone number as well: 101. Civilians called in the explosions at Brussels Airport on both numbers: 101 & 112.

disciplines started their emergency procedures e.g. the monodisciplinary emergency plan from D2 (personal communication, CIC).

HC112 VB furthermore took contact with the head of the Vlaams-Brabant's crisis and emergency management department. This was around 08.05u. The aid centre informed him about the incident. The head of the department tried to inform the governor, but the governor wasn't picking up his phone. In that case the head of the department has to inform the substitute of the governor, namely one of the two district commissioners. At 08.20u the governor called his crisis and emergency management department after which they decided to initiate the provincial state of emergency, more specifically the third part of the special emergency and intervention plan Brussels Airport. This was also communicated with the HC112 VB so that they could inform all members of the BNIP to gather in the provincial crisis council. The governor decided to locate the PCC in their provincial offices in Leuven (personal communication, governor VB; head CEM VB).

4.3 The provincial crisis council as a network

4.3.1 The provincial crisis council

Looking at both definitions of a security network (pg. 13) and an emergency situation (pg. 42) it can be concluded that the provincial crisis council is a network. Several security and other relevant actors come together to solve a multidisciplinary problem. These actors need each other in order to tackle a provincial emergency. A meeting between these actors suggests itself in such cases. Only in case of a provincial crisis the network is established. Once the specific crisis is solved the network can be dismantled. Therefore the PCC can be considered as a temporary network. Due to the fact that the PCC only gathers after a crisis the network has a reactive orientation (Provan & Kenis, 2009). The governor has the possibility to declare a provincial state of emergency and request the presence of all crisis council members. Basically, the governor of the province decides to establish the provincial crisis council (Royal decree of February 16, 2006). The Brussels Airport terrorist attack was a major crisis in which coordination by the actors and cooperation between them was required.

The network members are described in the BNIP Brussels Airport. In 4.2.1 BNIP Brussels Airport the main actors and representatives of the PCC are named. These are the vast members of the PCC. Normally no new participants are allowed. In this case all interviewees stated that there were too many people involved in the provincial crisis council. The main reason that it was too crowded can be explained due to the fact that the internal crisis council of Brussels Airport Company and the provincial crisis council became one. This happened after the transfer of the PCC from Leuven to Brussels Airport. Once the PCC was fully operational two and a half hours passed[12]. Yet, there was some coordination on the terrain and in the CC BAC (personal communication D3; head CEM VB).

Optimally, there should be one representative for each discipline/actor in the PCC. Two representatives per discipline is still respectable, but all others should form monodisciplinary work cells aside from the PCC[13] (personal communication, PSM; D1 – 2). During this provincial state of emergency many actors were double, triple or even by a higher amount represented in the PCC. Especially Brussels Airport Company and its partners and the police (D3) are named in having the highest representation[14]. The police was mentioned six out of nine times in the interviews and Brussels Airport and/or its partners five out of nine times. The

[12] The PCC arrived at 10.30-11u at Brussels Airport.

[13] Every discipline and some guests had a work cell with some staff members and partners in support. These work cells were located in other rooms in the 'Satellite' building at Brussels Airport.

[14] The location and magnitude of the incident demanded a crisis response of several different police services.

new procedures in case of a terrorist incident would involve even more representatives of some organizations (Royal decree of May 1, 2016). The overpopulation in the PCC wasn't ideal for the mono- and multidisciplinary decision-making process and for the general overview of the information stream (personal communication, D1 – 2; head CEM VB). The latter is further discussed as a factor that can influence network effectiveness (see 4.5.3 Information sharing).

In the following paragraphs an overview is given of the relationships between the different actors in the provincial crisis council. To do so all persons of the PCC – after the terrorist attack at Brussels Airport – have to be defined. A scheme of the different ties between all actors of the provincial crisis council is presented. This is illustrated in scheme 1 (pg. 50).

The administrative government was present and led the PCC. Although the governor didn't join the PCC until 16.00u one of his district commissioners took over his role. The governor was convoked by the federal crisis council as is described in the federal emergency procedures. Once he returned he claimed the leadership role. In his absence the district commissioner took charge over the PCC, together with the CEO of Brussels Airport. The commissioner was advised by the governor's provincial staff members of the emergency and crisis management department (personal communication, governor VB; head CEM VB). The representatives of the disciplines also operated as advisors of the governor (personal communication, D1 – 2; D4). The information unit (D5) at most times only had one representative. The fire brigade (D1) was represented by 2-3 officers. The medical team (D2) was led by the federal health inspector. Another aspect of D2 is the psychosocial aftercare. This was coordinated by the psychosocial manager. The responsibility for logistics is the task of D4. Civil Protection (CP) is the first actor that has to intervene when resources are asked. If they don't have the necessary resources at their disposal the provincial defence unit (the army) has to assist. Both services had their head of command in the PCC (personal communication D4). Finally, the police (D3) is more fragmented in Belgium. The main representative was the director-coordinator of the federal police, but due to the location and criminal nature of the facts other police instances were involved (personal communication, D1 – 1; D3; FGI).

As previously mentioned the majority of the interviewees stated that the police was considered overrepresented. The structure of the police made that both the administrative and criminal police needed representation in the PCC. For the administrative police these were the director-coordinator and one of her officers, the chief commissioner of the Brussels Airport police and the local police's zonal chief. The criminal police wasn't at all times present in the PCC as their representative from Halle-Vilvoorde and the one from Brussels went back and forth between the PCC and their monodisciplinary work cell (personal communication, D3; D4).

The core of the crisis and emergency management normally is done by the administrative government and its disciplines. They have multiple ties with one another. They see each other at earlier provincial states of emergency, in the provincial safety council, in some cases in municipal safety councils[15], emergency exercises and in the daily (work) life (personal communication, D1 – 2; PSM; D4; BAC). They have multiple communication methods at their disposal to reach one another. Some examples are: cell phone, landline, e-mail and ASTRID-radio. The latter is a satellite phone that is used during the crisis coordination. This is especially handy when there is saturation of the phone network. It is often used to ensure the communication between the main operational and strategic representative of each discipline. In this specific case a lot of communication went through ASTRID. During the transfer of location of the PCC from Leuven to Brussels Airport this radio device played an important role in the coordination and relief after the terrorist attack. This is due to the fact that the other communication tools weren't usable because of saturation (personal communication, FGI; D3; governor VB).

Apart from the above already mentioned members the PCC on March 22nd contained some more actors. The criminal character of the case demanded the involvement of the federal prosecutor`s office (personal communication, D1 – 2; governor VB). They were concerned with the criminal investigation. Related to the criminal aspect the intelligence and security agency, the State Security Service, was also involved. Furthermore the mayor of Zaventem and his emergency contingency manager were invited as experts of the territory. Because of the location Brussels Airport Company was involved. Several partners of Brussels Airport Company such as TUI, Belgocontrol and some airlines also took place in the PCC (personal communication, D3). These partners of BAC were already in the emergency meeting room. Normally these partners of BAC have to be invited, but because of their presence from the start it was difficult to get them out of the room (personal communication, head CEM VB).

In the afternoon security was posted at the entrance of the PCC. Only the people on their list were still able to enter the PCC (personal communication, D1 – 2; FGI; head CEM VB; BAC). This means that, while during the morning forty to even fifty persons gathered in the PCC (personal communication, head CEM VB). After the introduction of the name list the amount

[15] Municipalities from Vlaams-Brabant

of persons was reduced to halve of that number. Twenty to thirty people still was perceived as a lot of persons. The people that had to leave formed or joined a monodisciplinary work cell (personal communication, D1 – 2).

Almost all network participants were public actors, except for the few private actors such as Brussels Airport Company and its partners. The PCC was also a relatively closed network. Therefore the provincial crisis council – coordinating the crisis of the terrorist attack at Brussels Airport – can be defined as an institutional network (Dupont, 2004).

This crisis network existed out of multiple agents and one or two principals. The disciplines acted as agents in their advisors role, while the other (security) actors also had their input. All agents are on the same level in the network. The governor was the principal of the network. Thus the network level of analysis for network effectiveness is applicable in case of the provincial crisis council (Provan & Milward, 2001).

4.3.2 Monodisciplinary work cells

In order to maintain and improve the regular operation of the PCC monodisciplinary work cells were established. Every discipline had one of these work cells in which the main representative from the PCC gathered some important partners and other staff members of their discipline as a support. There was also a work cell for Brussels Airport Company and one for the airlines. The work cells were the link between the PCC and the field (personal communication, PSM).

The main representative of each discipline cannot engage in hearing out all messages of the ASTRID-radio and making every (minor) decision. The representative has to rely on his/her work cell: they have to pass on information and specific, critical problems from the field to their main representative in the PCC. Then the problem can be discussed in the PCC after which they will decide upon the necessary measures. The details of these measures have to be further worked out by the work cell (personal communication, D1 – 2).

It is often the case that multiple work cells have to collaborate to tackle a problem, just like the multidisciplinary approach in the PCC. A work cell can also be perceived as a monodisciplinary network or an inner-network of the provincial crisis council. You can either approach it from a network or organizational perspective.

Scheme 1: Representation and relationships of the actors in the PCC after the Brussels Airport terror attack

Orange = authorized (invited) guests

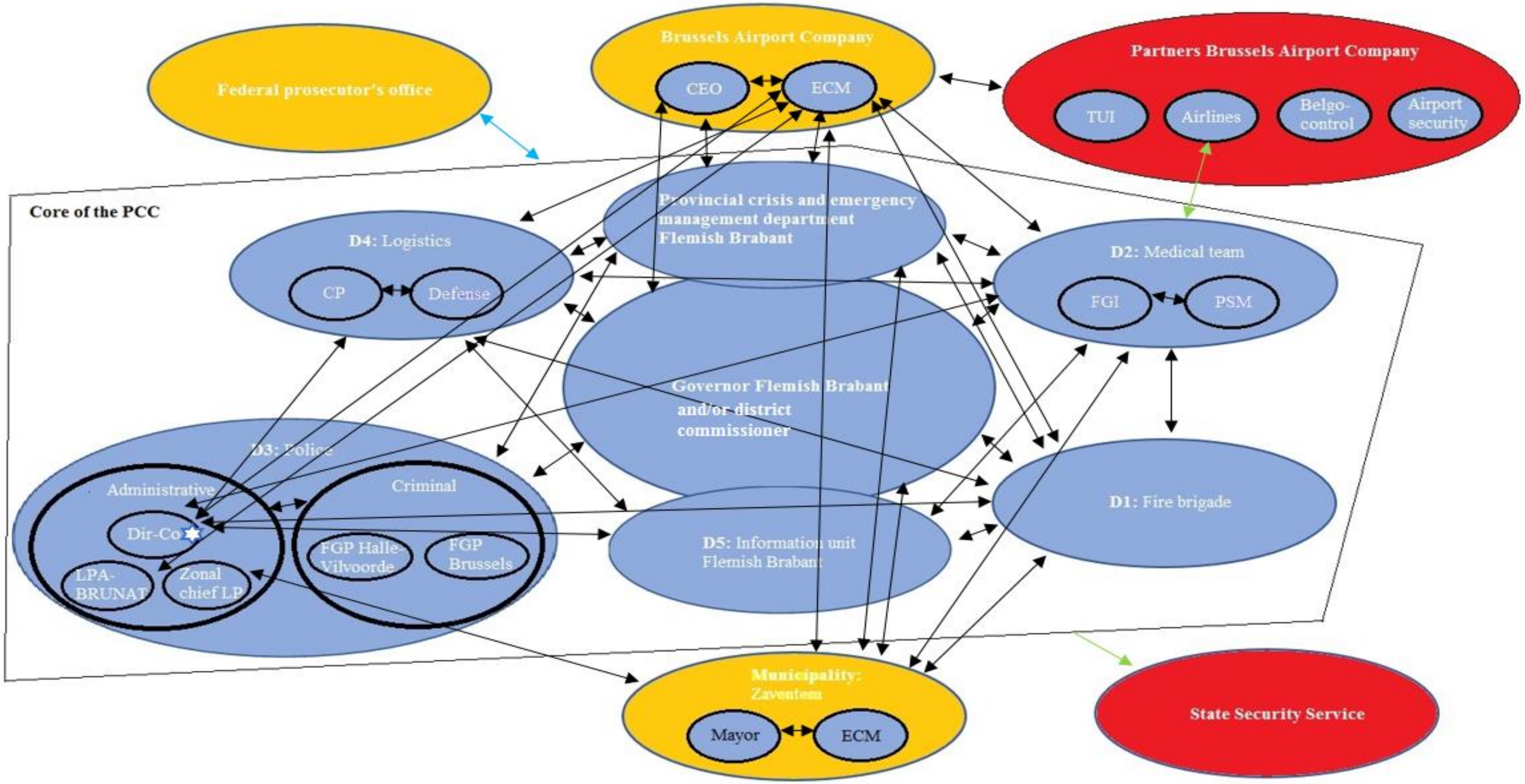
Red = Normally not represented in PCC

☆ = main representative in PCC

⟷ = Multiple ties and information sharing in PCC

⟷ = limited ties and information sharing in PCC

⟷ = only information sharing because of this incident (no further ties)



4.4 Perception of network effectiveness

In order to determine the perception of network effectiveness it has to be seen whether the goals of the network are met. The royal decree of February 16, 2006 – concerning the emergency and intervention plans – defines the crisis coordination and relief as the main tasks of a provincial crisis council. The governor, his head CEM, the FGI, D3, D4 and BAC also mentioned this as (one of) the goal(s). The head of CEM and the FGI went further by saying that the provincial crisis council is an executive body of the federal crisis council. The PCC fulfils the tasks that the FCC gives them. In this case the distribution of work was clearly defined by the FCC. They took charge over the judicial and security tasks, while the PCC was concerned with the crisis coordination and the relief (personal communication, governor VB, head CEM VB). It has to be stated though that the PCC can only operate as an executive body of the FCC if both (the federal and provincial) emergency phases are declared. This only happen in very uncommon situations (Royal decree of February 16, 2006).

Most of the critical relief was already done by the emergency services once the PCC gathered in Brussels Airport. In the meantime this was coordinated by the internal crisis council from Brussels Airport Company. The CC BAC handled quickly and adequately to sort out this problem (personal communication D4; BAC). So the tasks of the PCC were more focused on the aftermath of the relief and aftercare. In this case the latter contained the care for the wounded people, providing aid for the people those were physically in good shape but required psychosocial or logistical aid and the care for families and relatives of victims (personal communication, FGI; D3; D4; governor VB; head CEM VB; BAC).

The wounded people were treated in the medical post that was installed in the fire department building at Brussels Airport. From this location the triage of the injured people took place[16]. The stranded passengers were first given shelter in two hangars at Brussels Airport. Transportation for these passengers to accommodation centres was arranged by the PCC. These centres were opened at three locations to assist these people with their needs[17]. Once the people arrived in these centres they were registered. D2 was responsible for most of these tasks. They closely worked together with D4, mostly the provincial Defence unit, in order to provide the necessary goods such as camp beds, showers, food and drinks, landlines, etc. Within the timeframe of twelve to twenty-four hours these resources became available for the

[16] The medical post had to be relocated due to the discovery of a third bomb. Initially, the medical post was ‘only’ two hundred meters away from the departure hall where the bombs went off.

[17] Accommodation centres were opened at Peutie, Zaventem and Leuven (Brabanthal).

approximately three thousand stranded passengers (personal communication BAC; PSM; D4). According to the respondents these goals were met (relatively) well considering the conditions of the crisis.

The procedures of the BNIP and monodisciplinary plans were implemented and worked well. Yet according to the governor you often attain the goals without following all the procedural steps. During a crisis it is impossible to control everything which makes it inevitable that the BNIP isn't followed at all times. This mostly happens because of the direct aid by citizens at the scene. They aren't medically trained, but they can and have saved several lives of others after the bomb explosions. Besides the plans the previous emergency exercises are believed to influence the coordination. The following was said by both the governor and the provincial Defence unit. The representative of Defence (D4) stated:

"The structure of the royal decree and the emergency plans work because you practice them by having small and large emergency exercises. Furthermore just the fact that you see each other helps the process."

Yet the main representative of Defence and the police also argued that the emergency exercises might help, but aren't a good representation of the real incidents. The Dir-Co (D3) argued that:

"We have to acknowledge that emergency exercises aren't the same as real-life incidents. You can practice a lot, but you won't come close to full reality. An example of this is the communication problem we had to deal with during day one. You can't practice not having any communication. We always do these exercises in the best possible circumstances, yet at the time we were in the worst possible circumstances with our communication tools."

The psychosocial manager stated that not all goals were met at the end of the three-day PCC gatherings. They had to continue their activities for two more days on a monodisciplinary level, occasionally reaching out to some other actors of the PCC. This actor declared that they missed coordination and/or a crisis network during these two more days to address their questions.

4.5 Factors

In the analysis of the perceived network effectiveness the focus lies on four factors that might influence the effectiveness. These four factors are the network design, trust, information sharing and goal consensus. In the interviews network stability was also brought up as a possible factor. The following part elaborates on these factors and their perceived influence on the effectiveness of the network, being the provincial crisis council after the Brussels Airport terrorist attack.

4.5.1 Network design

4.5.1.1 Leadership

In the initial stages of the provincial crisis council in Leuven the governor led the PCC. He had his main advisors or substitutes from the disciplines at his disposal to advise him. Over the whole provincial emergency phase some disciplines were more proactive than others in providing advice or resources. It may also be that the conditions of the crisis demand a lot of coordination from (a) specific discipline(s) (personal communication, D4; PSM; head CEM VB).

In the first hour after the terrorist attack the crisis coordination and relief was done by the internal crisis council from Brussels Airport Company. They had the possibility to gather in an instance with some key partners and representatives from D1, D2 and D3. The CC BAC was led by the CEO of Brussels Airport Company. Some operational and strategic tasks of the CP-Ops and PCC were done by the CC BAC. Once the internal emergency plan was activated by BAC they started some procedures of their internal plan, but also the third part of the BNIP. A company will be quicker to respond to a (provincial) crisis than the PCC in most cases. Therefore the internal crisis council didn't wait for instructions from the PCC (personal communication, governor VB; FGI; PSM; head CEM VB).

In the meantime the (main) representatives from the disciplines were arriving in the PCC in Leuven. There a video conference was held with the federal crisis council. A first situational report was given during this meeting. Furthermore the question came from the FCC to transfer the PCC to Brussels Airport. This decision was being made with the underlying thought that the coordination and information stream would be more easily managed through two crisis councils (FCC and PCC) than three crisis councils (FCC, PCC and CC BAC). The governor then made the decision to transfer the PCC to Brussels Airport, after which the PCC and the CC BAC integrated into one crisis council (personal communication, FGI; D4; head CEM VB; governor VB).

The governor himself was convoked by the federal crisis council as a specialist of the terrain, similar to the invitation for the mayor of Zaventem in the PCC. During the absence of the governor in the PCC the provincial district commissioner had to take over his role. There are two district commissioners (personal communication, governor VB). The provincial commandant of Defence stated that one of the district commissioners remained in Leuven for the continuity of the PCC during the transfer, while the other took charge over the PCC once they arrived and established the PCC at Brussels Airport. Normally he – as the substitute of the governor – has the lone leadership role. In this case it became more of a co-leadership role of the PCC (personal communication, head CEM VB, D1 – 1). The psychosocial manager and director-coordinator of the federal police clearly mentioned that the crisis coordination was well led under charge of the district commissioner. They described him as a broker and a person that really acts upon monodisciplinary problems in a multidisciplinary context.

In the afternoon the governor returned to the provincial crisis council. His duties in the FCC were fulfilled, which gave him the chance to return to the PCC and take over the leadership role. He further led the PCC until the final stage. At the third day the provincial state of emergency was lifted (personal communication, governor VB). Under his command more structure was installed in the crisis network (personal communication, BAC; FGI; D4; D1 – 2). The fire brigade captain (D1 – 1) argued that there wasn't a clear chain of command during most of the first day. The respondent argues that there was no actual leader making all key decisions and coordinating the main activities.

During the coordination the king, prime minister and the ministers of Internal Affairs and Defence visited the PCC. These officials are directly or indirectly the boss of the disciplines in the PCC, but were mainly present in the federal crisis council (except for the king). The psychosocial manager and the head CEM VB made the remark that these visits hold up all activities for quite a while. These protocolary visits thus rather stall than speed up the crisis coordination.

4.5.1.2 Type of network design

Arquilla & Ronfeldt (2001) introduced a framework with three network governance forms. This framework includes an all channel, chain or hub network. Provan & Kenis (2008; 2009) developed another framework. The latter also contains three network governance forms, being a shared governance form, a lead organization or a network administrative organization. Both frameworks were discussed in 2.2.3 network governance forms. In this part an analysis is given about how the provincial crisis council is perceived as a network governance form.

According to the respondents the provincial crisis council certainly isn't a chain network. A chain network was only mentioned once in combination with a hub and all channel network. The governor described the chain as the link between the strategic main representative of the PCC, the work cell and the operational main representative.

If the combination of network governance forms from the governor is also taken into account, eight out of nine respondents described the network as a combination of a hub and all channel network. These respondents said that in theory a hub network is in place, but in real life it is often more of an all channel network. Only the fire brigade captain (D1 – 1) stated that it was none of the above network governance forms. He argued that almost all decisions were taken monodisciplinary and only sporadic the governor or his substitute had to intervene to take a decision.

The PCC started off as an all channel network with a lot of communication and information sharing between the different actors, but with limited coordination or a lead by a central actor. Not all actors were involved in every conversation, so some might have missed out on some crucial information. This structure of communication and information sharing is mentioned by eight respondents as an all channel network governance form during the crisis coordination of the PCC (personal communication, D1 – 2; PSM; FGI; D3; D4; BAC; governor VB; head CEM VB).

In the afternoon more structure was brought into the PCC by the district commissioner and later on by the governor. From that moment on more multidisciplinary meetings were held. Everyone had a turn to speak so that the information went – through the coordination of the leader – to all other actors of the network. In theory the hub network has the governor as the central actor. The disciplines and actors around him have the task to inform him. By informing the governor in a multidisciplinary meeting, all disciplines receive the necessary information. The same eight respondents also mentioned this way of coordination.

The governance form of the PCC became a combination of both an all channel and hub network due to the fact that not at all times all main representatives of the disciplines gathered in meetings. These meetings were set at certain times, while in between the meetings the disciplines and actors could work mono- and multidisciplinary according to their needs. In this case the work cells come into action as well. These work cells are attached to the main representatives (personal communication, D1 – 2; PSM; FGI; D3; D4; BAC; governor VB; head CEM VB).

While there is a lot of consent between the different respondents about the framework of Arquilla & Ronfeldt (2001), the respondents differ much more in their opinions about the framework of Provan & Kenis (2008; 2009).

The governor and his head of CEM claim that the provincial crisis council started as a shared governance form. A lot of the communication was mono- or multidisciplinary without any coordination. Only in a few cases decisions had to be made by someone. Therefore these two respondents say that it was a combination of a shared governance form with a network administrative organization. In the afternoon more multidisciplinary meetings were being held and a moderator/broker took the 'leadership' role. That was the time that more decisions had to be taken. This was the role of the governor and his substitute.

All other seven respondents excluded the possibility of a shared governance form because in those network forms there is no decision maker. Yet, three of these seven respondents (also) stated the importance of the autonomy of the disciplines. According to the PSM, the representative of D3 and BAC many decisions were taken monodisciplinary. Only when multidisciplinary problems were brought up a broker or leader was required. He then had to make a decision on which measure to take to solve the problem.

All nine respondents actually responded that there was some form of decision making by a broker or leader. Therefore it can be concluded that the provincial crisis council had a brokered network form[18]. Four of the respondents (PSM; D3; D4 & BAC) said that the PCC was a NAO. If the two above respondents (Head CEM VB & governor VB) are considered as well, six of them mentioned the NAO governance form. The governor in this case was described as the network administrative organization, deciding upon some key multidisciplinary problems. Though, often it was the case that decisions already were taken on a mono- or multidisciplinary level by the main representatives. If decisions couldn't be found on these levels the broker had to step in to decide for them. So the broker was a sole government entity that made some decisions and ensured that the network goals were met.

The three remaining actors (D1 – 1; D1 – 2 & FGI) argued that the PCC was a lead organization governance form. Key problems and activities were reported to the leader – in this case the governor – after which he took a decision on how to proceed. The two fire brigade officers argued that a NAO network would be applicable on the operational crisis network, namely the

[18] A brokered network form is either a network administrative organization or a lead organization governance form.

Commando Post - Operations. In this case the highest ranked officer of the fire brigade would be the Dir-CP-Ops (personal communication, D1 – 1; D1 – 2; FGI).

4.5.2 Trust

Six out of nine respondents claim that it is (very) important to have interpersonal relations with the other main representatives of the disciplines and guests. The representatives know each other from earlier provincial states of emergency e.g. the train collision in Buizingen from 2010, provincial safety councils, in some cases municipal safety councils, emergency exercises, especially the biennial exercise at Brussels Airport and the daily (work) life. They argue that ‘trust’ between the representatives improves the cooperation between the different actors. Multidisciplinary decisions are taken more rapidly. The fact that they know each other makes the decision-making process easier (personal communication, D1 – 2; PSM; FGI; D3; D4; head CEM VB).

Out of the six respondents that acknowledged the importance of interpersonal relations the interviewee D1 – 2, D3, the PSM and the head CEM VB mentioned that not knowing each other would have made it more difficult to agree on some multidisciplinary issues. Not knowing each other means that that the trust isn’t validated yet. The head of CEM VB summarized the relationship between the actors well. His comment went as follows:

“There’s trust in the organization, but also between the persons of the different actors. Of course you’re bounded to work with the main representatives of each discipline. After some years you are able to figure out how one will react, which isn’t the case with persons that you meet for the first time. The latter could lead to some problems. In the PCC you know the disciplines and most actors from previous exercises and earlier provincial emergency phases in which everyone fulfilled their role. Because you know them you can figure what to expect from the representatives and what no to expect, but at least you know the latter.”

The respondent of D1 – 2 who claimed that interpersonal relations are important added:

“The fact that you meet on a regular basis in the provincial safety council is a real advantage. This is the place where the emergency and intervention plans are made. You could even ask the philosophical question about the most important thing: the content of the plans or the preparation phase towards the plan. According to me the preparation phase is more important than the content of the plan.”

About the provincial crisis council he (D1 – 2) said:

“It is like a football team, for example the Belgian Red Devils. Persons from different teams gather for the national team. They have to perform on the occasion that they are together. This is possible through preparation.”

This metaphor describes the coordination of the provincial crisis council. The different security actors had to gather on a multidisciplinary level to ‘perform’, which in this case was solving the crisis.

The representative of D4 and BAC downplayed the importance of trust. The provincial Defence commandant acknowledged the fact that knowing each other could lead to easier cooperation, but both were convinced that interpersonal relations aren’t crucial. They believe that all actors bear responsibility for the crisis coordination and relief and that they would act upon it no matter what the problem is or who to work with. They do their job – taking measures to solve the crisis – and reach out to other actors if a multidisciplinary approach is required.

The scores of the survey for trust vary from ‘sufficient’ to ‘optimal’. Trust was measured by assessing the trust in each other’s capabilities. On a scale from one to five (not present to optimal) the actors responded thrice that there was sufficient trust between the actors in the PCC, but that there is still a considerable progression possible (=3). Once a score of four was given. This means that trust was relatively well established between the actors, but that there is still a bit of progression in order to collaborate in the best way. Once the highest score was given meaning that the trust in each other’s capabilities was optimal.

Overall the respondents never said that there wasn’t enough trust between them during the crisis coordination in the PCC. The provincial crisis council was perceived as a relatively dense network. On some occasions the level of trust can be improved though.

4.5.3 Information sharing

All nine respondents stated that there were some multidisciplinary meetings at certain times. At those moments each discipline had the chance to address their problems and share information. The governor or his substitute coordinated these meetings. In the earlier stages of the PCC the structure of these meetings was still missing. Information was only shared with the actors who collaborated on some multidisciplinary problems. Other problems were solved on a monodisciplinary level. In the afternoon of the first day a stricter gathering structure was installed with several meetings. The following comment of the D1 – 2 respondent summarized the structure of the meetings well:

"The governor pulled the strings over the provincial crisis council and called for some meetings at fixed times. In those meetings he mostly wanted to hear from the five disciplines. Once everyone addressed their problems and occasionally gave a situational report from the scene the meeting was finished. These gatherings were often followed by 'dead' moments."

Yet, not always everyone received the necessary information from these meetings. This was mentioned by the psychosocial manager:

"It were meetings where everyone could have their say. This however made it difficult to have full oversight over all the information and problems. Furthermore there wasn't a lot of feedback on the measures that were taken in previous meetings."

It was even mentioned by two interviewees (D1 – 1; D1 – 2) that there weren't actual meetings or only in a few cases. This was because of the following reason:

"Everyone sat together in the emergency room. In the critical phase you normally have several meetings in a short notice. After a while there is more time between the meetings because the situation is more under control. The PCC should pay more attention to arrange concrete meetings with the main representatives instead of the current situation where many people take place in the PCC to just listen to all information and approve decisions (personal communication, D1 – 2)."

The head of CEM VB, the fire brigade officer (D1 – 2) and the emergency contingency manager of BAC commented that the multidisciplinary information stream didn't went that fluently. They believe that this had two main reasons. On the one hand there was a lot of monodisciplinary work and meetings between the main representative of the discipline and its work cell. On the other hand there was quite some chaos in the PCC from time to time. Many disciplines were busy with their own problems during the multidisciplinary meetings. They listened to their ASTRID radios, took calls, worked on their computer or were briefed about a monodisciplinary issue during the multidisciplinary meeting. Due to this chaos they and others might have missed out on some vital information. A solution was handed by the fire brigade officer (D1 – 2):

"We have to separate the location of the crisis room and the work cells. These work cells have to be in the surrounding rooms of the crisis room. The crisis room has to be small, so that actually only the main representatives of the disciplines and guest actors can sit around the table. In this way meetings remain 'clean' and 'limited'."

Previous to the integration of the internal and provincial crisis council there was no communication between the internal and provincial crisis council according to the BAC contingency manager. He told:

"During the first part there was no communication between the internal and provincial crisis council. Only once all actors arrived at Brussels Airport information could be shared accurately, but it was chaotic at times."

Four of the respondents (D1 – 2; PSM; FGI; D4) also missed the fact that on their arrival in the PCC no situational report was provided. They argued that they weren't briefed or that there wasn't a whiteboard with the main information. There was only the log book, but this was a lot of information to read and could be interpreted in many ways. Also, the log book wasn't accessible by everyone because of some problems with the internet. The actors thus had to wait until the following meeting to have an idea about the situation, magnitude of the problems, etc. The first clear situational report they received was around 13.00u, in a multidisciplinary meeting. The fire brigade officer commented:

"You had the log book in which you could read everything, but this was logged in an inconvenient way which made it difficult to go through everything. It takes a lot of time if you want to read everything. You needed someone – a personal contact in the PCC – to brief you on the most important issues e.g. the things to focus on and what further steps that already were taken. If you don't have a personal contact a whiteboard would help. If someone enters the PCC he/she immediately could have a look at this board and be up to date about the most important things. Useful things to mention on such a whiteboard would be: the number of the chat group of the ASTRID radio, the time of the next multidisciplinary meeting, the division of tasks, the needs of each discipline, which phase you're in, the mono- and multidisciplinary plans that are activated and finally the amount of victims and wounded persons (personal communication, D1 – 2)."

Although the crisis information didn't always reach the necessary actors the coordination occurred sufficiently, given the circumstances according to the respondents. Aside from the multidisciplinary information sharing, there was also information that the federal prosecutor's office had to collect and share with the other actors in the provincial crisis council. The governor, his head of CEM and the director-coordinator of D3 elaborated on the relationship and information sharing with this actor of the crisis network. The role of the federal prosecutor's office became more important due to the criminal nature of the facts. Some of their analysts watched the footage of the departure hall in the PCC. On this footage they discovered that there was a possibility of a third bomb. Three people with trolleys entered the building, but only two bombs went off. Due to this discovery the emergency services were warned about the possibility of a third bomb and an (second) evacuation of the terrain took place (personal communication, D3; governor VB; head CEM VB).

The representative of the federal prosecutor's office mostly sat in a room across the PCC. They had to start a criminal investigation and therefore collect confidential information. Although the information was confidential the Dir-Co, governor and head of CEM VB argued that the representative came into the PCC at several times to share some information. This was important in order to know if everything was still safe. They perceived the contact between the PCC and the federal prosecutor's office as a good contact (personal communication, D3; governor VB; head CEM VB).

The main representative of D3 clearly mentioned that she knew the representative of the federal prosecutor's office and that it was a very capable representative. She believed that the culture of the federal prosecutor's office representative aided in the information sharing, as the father of the federal prosecutor's office representative was a former head of the federal police.

The survey showed that the actors perceived that the overall information sharing was limited to sufficient. This means that scores from two to three were given on a scale from one to five. Information sharing was measured by assessing the amount of times and the way the actors shared information with each other. In three occasions the information sharing was evaluated as limited (=2). In this case there is still a significant progression possible to optimize the level of information sharing. The other two times the respondents gave a score of three. This means that the information sharing in the PCC was done sufficiently according to these actors, but that there is still a considerable progression possible.

Not taken into account in this survey was the contact and information sharing with the federal crisis council. According to the governor and his head of CEM the communication only went in one way. The PCC had to inform the FCC, but only received some information from their governor when he was present in the FCC. On other occasions e.g. the video conference calls the PCC only had to answer questions from the federal crisis council.

4.5.4 Goal consensus

The perception and attainment of the (different) network goals is already discussed in part 4.4 perception of the network effectiveness. Most of the respondents (governor VB; head CEM VB; FGI; D3; D4 and BAC) stated that the crisis coordination and (aftermath of) the relief were the main tasks of the provincial crisis council. Network members are normally attracted to engage in work or network relationships with actors that share the same interests (Provan & Kenis, 2008).

In a normal scenario only one state of emergency is declared. In this case both the federal and provincial emergency state were declared. Normally the highest entity, the federal crisis council, then has to do the administrative and operational coordination. The other entity, being the provincial crisis council has to support the leading entity. Due to the magnitude of the event and the experience of the PCC with the operational coordination they were asked to do the crisis coordination and the relief. This is one of the tasks of the PCC in a provincial phase according to the royal decree from February 16, 2006 on the emergency and intervention plans. Normally the PCC is also responsible for the administrative aspects and the crisis communication, but the FCC decided to take up these tasks so that the provincial crisis council could fully focus on the crisis coordination and the relief (personal communication, governor VB; Royal decree of February 16, 2006).

Although the goals of a PCC are clearly defined in the royal decree, the psychosocial manager, the representative of D1 – 1 and BAC stated that in this case – the Brussels Airport terrorist attack – there was no clear vision about the network goals from the PCC. The emergency contingency manager of BAC had the following comment about this:

"The disciplines do know their own goals, but the network goals sometimes – don't necessarily get lost because of that – do receive a bit less attention because of that."

The latter resulted in varying scores of goal consensus in the survey. This was measured by asking about the homogeneity/similarity of the network goals. The lowest score was a score of two on a scale of five. This score was given by one of the respondents who claimed that there was no clear vision. This score means that there is still a significant progression to be made to reach the optimal level of goal consensus. Now the consent about the network goals between the network participants was evaluated as limited by this actor. The four other actors gave a higher score. Three of them gave a score of four. This score signifies that the network goals were well established and that there was a high mutual consent about these goals. Yet, there is still a bit of progression that can be made. One actor gave the middle score of three. According to this actor there was consent about the network goals up to a certain (seen as sufficient) level. There was thus room for considerable improvements to have full consent about the network goals between all network participants.

4.5.5 Network inner stability

This factor wasn't actually measured but was mentioned a few times by some respondents. The provincial commandant of Defence and the psychosocial manager claimed that there is a core group that always comes into action when a provincial emergency state is declared. The core actors of the PCC are illustrated in scheme 1 (pg. 50). These respondents believed that the stability of the crisis network facilitated the work and relationships in the network.

The representative of the Defence unit defined the network inner stability like this:

"It is a stable network with the five main representatives of the disciplines and the governor. The longer you are a part of the network, the more experienced you get and the more 'easier' it becomes. Furthermore you engage in interpersonal personal relations which makes it easier to get some things done in the PCC or to get some resources or information from another person."

The representative of D4 and the head of CEM VB mentioned that the personnel of the disciplines is very stable in contrary to the airport where there is a bigger flow of personnel. Therefore it is good that every two years an emergency exercise is hold.

'The personnel flow at Brussels Airport is big. You might not see the people from the previous emergency exercise when the next one is being hold. The government on the other hand were practically the same people as fifteen years ago so to speak. So in a short time span it changes a lot at the airport. Therefore it is a good initiative to practice every two years because otherwise they wouldn't know the procedures at all (personal communication, head CEM VB)."

Turrini et al. (2010) already stated that the better the network inner stability the easier it gets to create a good atmosphere, information stream and trust relationship within the network. But there has to be a trade-off between the flexibility of the network relationships and the stability of its actors in order to improve the efficiency and effectiveness of the network. The latter is especially necessary in networks with the emergency response as their main task (Moynihan et al., 2012).

4.6 Link between the perception of network effectiveness and the factors

Relatively seen the goals of the provincial crisis council were achieved, considering the difficult conditions they had to work in. The relief, crisis coordination and aftercare were the main tasks of the PCC.

The actors gathered in the provincial offices to start the crisis coordination and the relief, but were asked to move their operations to Brussels Airport. Due to this shift of location, the transport of the security actors first to Leuven and afterwards to Brussels Airport and the saturation of the phone network difficult conditions arose. The shift of location of PCC made it difficult to coordinate the actual relief. Therefore the relief was eventually done by the CC BAC and the emergency services on the terrain. The PCC then focused on the aftermath of the relief which was mostly aftercare and furthermore they coordinated the crisis. The actors perceived that the goals were met relatively well under the given circumstances. There was one exception though: the psychosocial manager thought that all goals weren't met yet when the provincial state of emergency was called off.

If we link the perception of the attainment of the goals to the perception of the factors that might have influenced the network effectiveness we can formulate more insightful conclusions about the perception of the network effectiveness of the provincial crisis council. The research of Provan & Kenis (2009) and Whelan (2015) also indicated the importance of the network design when it comes to network effectiveness. The latter will therefore also be considered as a factor in this matter. The network design is closely linked with the network inner stability. The other three factors (goal consensus, information sharing and trust) were measured both through qualitative and quantitative research.

The design of the network was perceived to be a combination of an all channel and a hub network in the one framework and a brokered network governance form in the other. There was some dispersion though if it was rather a network administrative organization (NAO) or a lead organization. In both forms the governor was seen as the 'leader' or 'broker'. Furthermore the network was perceived as a network in which all actors could talk and share information with one another. This didn't necessarily needed to happen through a central actor, but in this case the multidisciplinary meetings were perceived as rather helpful. The meetings gave an oversight of all the problems, needs and resources of all actors, for all actors. The latter is important because sometimes only information was shared with some actors while it would have been more appropriate if all actors could appeal to the information.

The *design of the network* is heavily linked with the stability of the network. The inner stability of this crisis network was perceived as quite strong by the respondents. The core of the crisis management disciplines, being the governor, the department of crisis and emergency management, the fire brigade (D1), the medical team (D2), the police (D3), logistics (D4) and finally the information unit (D5) know each other well by having worked together in some situations. They see each other in provincial crisis situations, both provincial and municipal safety councils, emergency exercises and in the daily work life. In this particular case many other guests were also involved, some invited and some not invited. Due to the magnitude of the incident the provincial crisis council too many people were perceived to be resent in the PCC. Most disciplines and actors had multiple representatives in the PCC. It would have been better if everyone had one main representative that could speak for the whole organization. So, the number of participants in the provincial crisis council had a negative effect on the stability of the network and the oversight at the multidisciplinary meetings. Nevertheless the network inner stability was perceived as relatively strong. The disciplines were quite autonomous in the beginning and reached out to the other actors if needed, as all necessary actors were involved in the provincial crisis council.

The *goal consensus* in the provincial crisis council was rather high. Most actors were emergency services that aim to help the people in need and guarantee safety. During the Brussels Airport terrorist attack the need for help was immense. The main task of the crisis council was the relief, crisis coordination and aftercare for the stranded passengers. Certainly the disciplines worked towards this goal. Brussels Airport Company was concerned about the wellbeing of the people, but also had to prepare plans for the rebuild of their departure hall because of economic reasons. Nevertheless they knew that the crisis coordination as a whole – and thus the medical and psychosocial aspect – was the first priority. Every actor acknowledged the importance of the evacuation of the stranded and wounded passengers. The actors shared the same belief and culture in this case. Because of this common goal the performance of the crisis network was quite positively perceived by the interviewees.

The last to one factor was *information sharing*. This was perceived as a negative factor influencing the performance of the network – although the previous actors were evaluated in a relatively positively manner by the respondents. The actors indicated that there was a significant to considerable progression still possible when it comes to information sharing. This had three main reasons.

First and foremost there were too many people in the emergency room which led to chaos during the multidisciplinary meetings. Half of them were sent out in the afternoon of day one, but still there were twenty to thirty people, which is considered a lot for a provincial crisis council. The reason people came to the crisis council was because of the saturation of the phone network. If you had to reach someone it was either through mail, WhatsApp, in person or by ASTRID-radio. These radios aren't that common and only used by the emergency services and governmental instances.

The saturation of the phone network was the second issue. In a normal crisis most communication goes through mobile phones. During this case the phone lines were rapidly saturated. This meant that alternative communication methods had to be used.

A third big reason was the lack or bad connection to the internet in the PCC. Not all actors had access to the log book in which all decisions were logged. These decisions were nowhere else retraceable as there was no whiteboard with the most important information. Situational reports were only given at some times and in the beginning or on the arrival of new members there were no briefings according to most respondents.

The one positive thing concerning information sharing was the contact with the federal prosecutor's office. Although most information was confidential this was shared by them with the PCC. Notwithstanding these partially signs the overall information sharing was perceived as limited to sufficient.

Finally *trust* was an important factor to assess the perceived network effectiveness of the provincial crisis council. As already mentioned the PCC was crowded. Although it was crowded the core of the PCC could rely on their strong ties from previous encounters. Not all actors within the PCC had ties with one another, but the core actors did, along with the BAC. In this case it could be argued that it wasn't necessary that all actors had ties with every other actor (Moynihan et al., 2012).

There was mostly interpersonal trust between the disciplines, but the trust in the organization was also in place. The disciplines share a responsibility towards the people to help them overcome the crisis and give assistance to the people where needed. These tasks are practiced with several actors during the biennial emergency exercise at the airport. This is a moment in which people get to know each other and the procedures of the plans. In this case – as we speak of trust – the relationships that might develop are the most important. This was also something one of the respondents (D1 – 2) insisted as he stated that the process towards the plans (getting to know each other) might be even more important than the content of the plan. The level of trust was therefore perceived as rather high by the interviewees.

Almost the same applies for the trust in each other's capabilities. Trust in each other's capabilities was sufficient to relatively well established, although it was perceived as a little bit lower than the interpersonal trust discussed above. The interviewees argued that it was important that the capabilities of the network participants are high, but there is still some progression to be made.

Thus, overall the goals were relatively well met under the given circumstances. It has to be stated though that some of the PCC's tasks were outsourced because of the inoperability for two to three hours. There was some continuity of the PCC during the transport of the PCC to Brussels Airport, but few decisions have been made by the PCC in the first few hours (personal communication, D3; D4). Furthermore trust has a strong and positive influence on the network. The stability of the network and the goal consensus also have a rather positive influence on the performance of the provincial crisis council, but less than the trust factor. Information sharing on the other hand was the weak point in the performance of this network in the case of Brussels Airport.

5. Conclusion and reflection of the research

5.1 Conclusion

The research started with a literature study about security networks, terrorism and the events and crisis coordination after the double terror attack on March 22, 2016. Not only Brussels Airport, but also the metro in Maalbeek was targeted that day. This thesis focused on the coordination of the first attack at Brussels Airport. The impact of the attack was bigger than in Maalbeek because of the economic importance of an airport. Furthermore it was a unique case of crisis coordination by a crisis network whose effectiveness was never evaluated before.

The network that was being studied was the provincial crisis council of Vlaams-Brabant. Through the usage of interviews with nine core provincial crisis council members the perceived network effectiveness was measured. In order to assess the perceived network effectiveness four factors were measured. These factors were the network design, trust, information sharing and goal consensus. During the interviews the respondents gave some more insights about other influencing factors such as the network inner stability and the location/start-up of the PCC.

We may conclude that under the given circumstances the provincial crisis did perform relatively well after the Brussels Airport attack. The main perception was that all goals were achieved in a relative short notice. The PCC mainly focused on the crisis coordination, aftermath of the relief and aftercare. Normally the relief is the main task of the PCC, but due to the transfer of location from Leuven to Zaventem the PCC lost a lot of time. The internal crisis council of Brussels Airport Company and the emergency services on the field in practice performed this task. So although the goals of the PCC were met, one of the main tasks was almost entirely and spontaneously coordinated by others. The start-up procedure of the PCC therefore is a point of critique, as this has to happen more rapidly and efficiently.

Multiple factors influenced the performance of the network in a positive or negative way. Positive enablers were the trust and inner stability of the network, especially between the core members of the network. The trust in each other and their capabilities was perceived as 'well established'. The respondents said that the most important thing was that they knew each other previous to the incident. Another relative positive aspect was the goal consensus. The core members had the same goal, being the crisis coordination and the relief. The invited and/or private actors set their own goals mostly aside to aid in this process, at least at the start of the PCC. The federal prosecutor's office for example had a criminal investigation that became really important and only during day two Brussels Airport Company started drafting plans for the rebuilding of the departure hall.

Besides the positive factors there were also two big negative factors influencing the crisis network. The information sharing between the actors wasn't that fluent at all times and the decision to gather in Leuven backfired. The initial choice of location for the PCC in Leuven actually caused a serious delay of crisis coordination and information sharing between the different actors. The PCC was only fully operational at 10.30u in Brussels Airport. This was two and a half hours after the bombings in Brussels Airport. The information sharing only happened in a structural way after the introduction of multidisciplinary meetings of the representatives in the PCC. These meetings were (only) introduced in the afternoon of day one. In the first hours most disciplines worked monodisciplinary or had to reach out to other actors. Information was shared, but not always with all the relevant actors. The fact that there was no whiteboard with an overview of the main decisions and that not everyone was able to follow the log book made that some actors didn't have some crucial information at their disposal.

Although these difficulties, the provincial crisis council was ultimately perceived as relatively effective. The actors perceived that the structures of the emergency plan and the royal decree worked, but admitted that the circumstances made it more difficult in the start-up of the council.

In conclusion, we can state that the provincial crisis council was perceived as relatively effective for the task they did perform. They didn't took charge over all their activities because of the inconsistency in decision-making from the crisis councils and representatives. The main representatives of the disciplines were divided over the different crisis councils (PCC & CC BAC) which made the crisis coordination more difficult. Later in the morning of day one both crisis councils became one. The integration of both councils led to a more organized structure and coordination, but some tasks were already performed by other actors at that time. So, the positive factors influencing the network effectiveness – according to the crisis council members – were the trust, network inner stability and the goal consensus. Negative factors were the information sharing and the initial location/start-up of the PCC.

5.2 Reflection and recommendations

The provincial crisis council was perceived as relatively effective during the coordination of the Brussels Airport terrorist attack. This means that they performed quite well, but that there are some improvements to be made still. First the information sharing has to happen on an immediate and regular basis in the PCC. This has to happen through coordinated multidisciplinary meetings with one main representative of each actor. The maximum number of participants of each actor should be limited to one to two members in the PCC, with the rest forming a work cell. This is in contrast with the new procedures of the BNIP terrorism, which would introduce more members of certain actors in the PCC. Most actors believe though that the multidisciplinary meetings in the PCC would be more effective if only the main representatives of each discipline and special guests are involved. A follow-up study would therefore be interesting.

Furthermore there should be more research about the network design of temporary crisis networks. Many respondents perceived the network to be as a combination of a hub and an all channel model (Arquilla & Ronfeldt, 2001). In the framework of Provan and Kenis (2008) the respondents stated that the network had a brokered network governance form, being either a lead organization or a network administrative governance form. In both frameworks there was no clear design that could be given to the provincial crisis council. New research about a possible new (crisis) network governance form could therefore be relevant.

This research used interviews to assess the perception of network effectiveness. Interviews were taken from nine of the network participants. These respondents were the main representatives of their organization, so it covered most of the network. It wasn't feasible to interview all actors or members due to the size of the network. Therefore the most prominent and relevant actors of the crisis coordination were interviewed. Because we had to deal with a specific provincial situation it is hard to generalize the results of this study to other cases. Nevertheless, this unique case may lead to new insights on the emergency and disaster policy in Belgium and the network literature, as the above recommendations for further research state.

Bibliography

Academic articles

Arquilla, J. & Ronfeldt. D.F. (2001). The Advent of Netwar (Revisited). In J. Arquilla and D.F. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 1–25). Santa Monica: RAND Corporation.

Arquilla, J., Ronfeldt, D.F., & Zanini, M. (1999). Networks, Netwar and Information-Age Terrorism. In I.O. Lesser, B. Hoffman, J. Arquilla, D.F. Ronfeldt, M. Zanini, & B.M. Jenkins (Eds.), *Countering the New Terrorism* (pp. 39–88). Santa Monica: RAND Corporation.

Blatter, J. & Haverland, M. (2012). *Designing case studies: Explanatory approaches in small-N research*. New York: Palgrave Macmillan.

Brodeur, J-P. & Dupont, B. (2006). Knowledge Workers or ''Knowledge'' Workers? *Policing & Society, (16)*1, 7-26.

Brooks, D.J. (2010). What is security: Definition through knowledge categorization. *Security journal*, *23*(3), 225-239.

Castells, M. (2000). *The Rise of the Network Society*. *The information age: economy, society and culture*. Malden: Wiley-Blackwell.

Craighead, G. (2003). *High rise security and fire life safety* (2nd ed.). Woburn: Elsevier.

Dupont, B. (2004). Security in the Age of Networks. *Policing & Society*, *14*(1), 76-91.

Eckstein, H. (1975). Case Study and Theory in Political Science. In R. Gomm, M. Hammersley, and P. Foster (eds.), *Case Study Method*. London: Sage Publications.

Fischer, R.J. & Green, G. (2004). *Introduction to Security*. Boston: Butterworth-Heinemann.

International Centre for Counter-Terrorism. (2016). The Foreign Fighters Phenomenon in the European Union. Den Haag: International Centre for Counter-Terrorism.

Kavalski, E. (2009). Timescapes of Security: Clocks, Clouds, and the Complexity of Security Governance. *World Futures: Journal of General Evolution*, *65*(7), 527 - 551.

Krahmann, E. (2005). Security governance and networks: New theoretical perspectives in transatlantic security. *Cambridge Review of International Affairs,18*(1),14-30.

Matusitz, J. (2013). *Terrorism and communication: What is terrorism?* Florida: Sage Publications.

Moynihan, D.P, Provan, K.G., & Lemaire, R.H. (2012). Core Concepts and Key Ideas for Understanding Public Sector Organizational Networks: Using Research to Inform Scholarship and Practice. *Public Administration Review, 72*(5), 638–648.

Noppe, J., Ponsaers, P., Verhage, A., De Ruyver, B., & Easton, M. (2011). *Preventie en radicalisering in België*. Antwerpen: Maklu.

O'Toole, L. (1997). Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration. *Public Administration Review*, *57*(1), 45-52.

Provan, K., & Kenis. P. (2008). Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229-252.

Provan, K., & Kenis, P. (2009). Towards an exogenous theory of public network performance. *Public Administration, 87*(3), 440-456.

Provan, K. & Milward, B. (2001). Do networks really work? A framework for evaluating public-sector organizational networks. *Public Administration Review, 61*(4), 414-423.

Raab, J., & Milward, B. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory, 13*(4), 413-439.

Schmid, A., & De Graaf, J. (1982). *Violence as Communication: Insurgent Terrorism and the Western News Media*. Beverly Hills: Sage.

Schmid, A., & Jongman, A. (1988). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*. Amsterdam: Transaction Books.

Stake, R.E. (1994). Case Studies. In N.K. Denzin & Y.S. Lincoln (eds.), *Handbook of Qualitative Research* (pp. 236-247). Thousand Oaks: Sage Publications.

Terpstra, J (2005). Models of local security networks: on the diversity of local security networks in the Netherlands. *Crime Prevention and Community Safety*, *7*(4), 37-46.

Turrini, A., Cristofoli, D., Frosini, F., & Nasi, G. (2010). Networking literature about determinants of network effectiveness. *Public Administration, 88*(2), 528-550.

Whelan, C. (2012). *Networks and National Security: Dynamics, Effectiveness and Organisation*. London: Ashgate.

Whelan, C. (2015). Managing Dynamic Public Sector Networks: Effectiveness, Performance, and a Methodological Framework in the Field of National Security. *International Public Management Journal*, *18*(4), 536-567.

Yin, K.R. (1981). The case study as a serious research strategy. *Knowledge: Creation, Diffusion, Utilization, 3*(1), 97-114.

Yin, K.R. (2003). *Case study research: Design and methods* (third edition). Thousand Oaks: Sage Publications.

Yin, K.R. (2009). *Case study research: Design and methods* (fourth edition). Thousand Oaks: Sage Publications.

Yin, K.R. (2012). *Applications of case study research*. Thousand Oaks: Sage Publications.

Governmental documents

Parlementaire onderzoekscommissie naar de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel: Tussentijds en voorlopig verslag over het onderdeel ‘hulpverlening’ (August 3, 2016). Retrieved on November 30, 2016, from http://www.dekamer.be/doc/FLWB/pdf/54/1752/54K1752006.pdf

Legislature

Koninklijk besluit betreffende de nood- en interventieplannen (February 16, 2006). *Belgisch Staatsblad*, 15407-15414.

Koninklijk besluit tot vaststelling van het nationaal noodplan betreffende de aanpak van een terroristische gijzelneming of terroristische aanslag (May 1, 2016). *Belgisch Staatsblad*, retrieved on April 25, 2017, from http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&caller=summary&pub_date=16-05-18&numac=2016000272#top

Websites

Redactie Het Laatste Nieuws. (August 9, 2008). Meer rampen treffen België. *Het Laatste Nieuws*. Retrieved on March 20, 2017, from http://www.hln.be/hln/nl/2624/Planet/article/detail/374110/2008/08/09/Meer-rampen-treffen-Belgie.dhtml

United Nations Office for Disaster Risk Reduction. (September 18, 2013). More disasters but reduced losses in Europe. Retrieved on June, 2, 2017, from http://www.unisdr.org/archive/34720