Local Security Networks: Structure and Counter-radicalisation Outputs

Emrah Karadogan
S1787624
Words: 24000

23 June 2017

Master's Dissertation

Crisis and Security Management Programme

Supervisor:

Dr. Ruth Prins

Leiden University

Faculty of Governance and Global Affairs

Abstract

In response to increasing terrorist attacks in Europe, the Danish authorities have sought to push back against extremism by countering radicalisation at its source. Fighting terrorism may take several forms, but Denmark's flagship approach is to incorporate counter-radicalisation measures into local cross-sectoral collaboration networks known as SSPs.

Despite a rich body of literature on networks and their performance, little is known about how a network's outputs are produced, and to what degree they are determined by the network's structural patterns.

This research investigates how the structural patterns of two local security networks (SSPs) in Denmark affect their counter-radicalisation outputs. The two cases selected for analysis are the local SSP networks in Copenhagen and Aarhus.

The study finds that there are key differences in the structure of the two networks, although their counter-radicalisation outputs are alike in many ways. A direct link between structure and output is not proven, but several explanatory factors are identified which contribute to the network literature and identify potential improvements in network.

Contents

List of Abbreviations:

CPH	Copenhagen
CT	Counter-radicalisation
DCY	Department of Child and Youth
DSS	Department of social service
NAO	Network Administrative Organisation
PET	Danish Security and Intelligence Service
SSP	Schools, Social Services and Police
ULD	Unit of Learning and Development

1 Introduction

On 30 September 2005, the Danish newspaper, Jylland-Posten, published 12 cartoons depicting the Prophet Muhammad. The cartoons triggered mass protests, both in Denmark and abroad, which resulted in several Danish embassies being attacked and burned down in the Middle East (Berlingske Research, 2015). The so-called "cartoon crisis" has been described as the biggest political crisis in Denmark since World War II (Butt, *et al.* 2014: 15).

In the aftermath of the crisis, several terrorist groups, including Al-Qaida and Al-Shabaab, urged Muslims to attack Denmark and Danes living abroad (Berlingske Research, 2015). Their calls did not go unheeded; two people were arrested for planning an attack on Jylland-Posten offices in 2009, and in 2010 a man attempted to kill the cartoonist behind the cartoons, Kurt Vestergaard. Later that same year, a man detonated a bomb in a hotel in Copenhagen (Butt, *et al.* 2014:15).

The fallout from the cartoon crisis led the Danish security authorities to place the country on its highest terror alert level, issuing a stark warning that there was a significant threat of terrorism in Denmark (ibid.). Today the alert level remains unchanged, partly owing to the 2015 Copenhagen shooting in which a 22 year-old man attacked a cultural centre and the city's Great Synagogue, killing a police officer and a security guard and wounding six others (PET, 2016).

Against this backdrop, radicalisation has naturally been a hot topic in the national debate since the cartoon crisis. Focus on the issue has only increased since Danish Muslims began to travel to Syria to join the civil war which broke out in in 2011 (Butt, *et al.* 2014: 16). In 2012, the first Danish Muslims began volunteering to fight in Syria, and according to the Danish Security and Intelligence Service (PET), at least 125 Danish citizens have since left the country to fight with Islamic extremist groups in Syria and Iraq (PET, 2015). Compared to other European countries, Denmark has the second-highest number of foreign fighters per capita (Higgins, 2014).

Several domestic organisations and groups in Denmark appear to have contributed to the high number of foreign fighters, as a number of Islamic organisations openly support the so-called Islamic State (ISIS), including the Danish Hizb ut-Tahrir, Kaldet til Islam (Call to Islam), and the Grimhøj Mosque. Located in Aarhus, the Grimhøj Mosque in particular has been in the spotlight for many years, as many Danish foreign fighters were frequent visitors to the mosque. It is believed that the Grimhøj Mosque actively radicalised youngsters (Nielsen, 2015).

In order to combat this radicalisation, Denmark's first official strategy and action plan was launched in 2009, and later modified in 2014 when a centre-left government replaced the centre-right government after the general election in 2011 (Lindekilde, 2015a; DIIS, 2015; Butt *et al.* 2014). Since then, the Danish government has readjusted the action plan several times, with the latest version being released in October 2016 (Regering, 2016).

Counter-radicalisation and Local Security networks

Since the first counter-radicalisation action plan was adopted in 2009, all the following versions of the Danish action plans stress the importance of strategic collaboration with local authorities, and sees the local SSP[1] networks as key actors in countering radicalisation among youngsters (Regering, 2016: 6).

Since the end the of 1970s, SSP networks have existed in every municipality in Denmark (DKR, 2012). The SSP was initiated to develop more efficient methods of crime prevention in order to cope with crime among youth, which increased rapidly during the 1960s and 1970s (ibid.) In order to reduce crime among youngsters and secure their wellbeing, municipalities started to coordinate their efforts across different sectors (ibid.) The precise form of collaboration differed from one municipality to the next, but the aim and purpose were the same; namely, to combine different professions and working methods to facilitate early crime prevention work. Over time, these local cross-sectional collaborations were formalized and made permanent in municipalities across the country (ibid.).

New objectives have been devised for SSP networks as new threats to the wellbeing of Danish youth have emerged. For instance, besides addressing criminal activities, tackling youth drug and alcohol abuse has become an SSP objective. The most recent objective adopted by SSP networks is that of counter-radicalisation among youngsters (DKR, 2012; DIIS, 2015). In 2011, the SSP networks in the Copenhagen and Aarhus municipalities were the first to integrate counter-radicalisation efforts into their work. Since then, many other municipalities have followed suit (DIIS, 2015).

[1] SSP stands for **S**chools, **S**ocial services and **P**olice. The Danish SSP networks are local collaboration initiatives between educational institutions, social services, police and civil society, which aim to prevent crime among children and adolescents in municipalities and local areas (DKR, 2012).

Various experts and Danish politicians have described the SSP networks' approach to counter-radicalisation as a successful one (DIIS, 2015). It has been argued that their methods work well since counter-radicalisation policies can be incorporated into already well-established local SSP networks (Vidino & Brandon, 2012: 53). Recognition has spread beyond Denmark's borders, and the European Counter-Terrorism coordinator, Gilles De Kerchove, has designated Denmark as a "lead country" on preventing radicalisation (Lindekilde, 2015b: 223).

Although the SSP's counter-radicalisation efforts have been widely considered a success story, they have also been subject to criticism (Lindekilde, 2015b: 231). The SSP network has traditionally focused on unlawfulness among youngsters. However, by integrating counter-radicalisation efforts into the SSP networks, radicalisation has become a new issue area with its own parameters and indicators (Lindekilde, 2015b, 235). In this regard, by integrating the fight against radicalisation with more general crime prevention, the political nature of radicalisation risks becoming obscured, since extreme political ideas deemed risky by the authorities are not necessarily inherently illegal (DIIS, 2015: 36).

Another criticism is that counter-radicalisation is not necessarily synonymous with ordinary crime prevention (Lindekilde, 2015b: 235). For example, the SSP framework allows the social services to intervene and remove a child from its parents' custody if there is clear evidence that the child is being abused. However, in the context of counter-radicalisation, child protection dilemmas may easily arise. A recent case that has been criticized for being too drastic is that of a fifteen-year-old boy, who was forcibly removed from his father's care as it was feared that the father was radicalising him and raising him to carry out violent jihad (Borg, 2015).

This case raises a further issue with anchoring counter-radicalisation efforts in the SSP framework. There is a lack of common understanding of what radicalisation is, and the absence of a consensus on the indicators of radicalisation leaves a relatively large scope for professional judgment (Lindekilde, 2015b: 230). Different SSP networks will make different professional judgments on the same 'sign' or 'signal' of radicalisation. They will assess the situation based on diverging professional norms, experience and knowledge (Jakobsen & Jensen, 2011: 9).

SSP Networks and Counter-radicalisation Outputs

Given the differences in assessing radicalisation and how to counter it, each SSP network has put together their own counter-radicalisation outputs (DIIS, 2015: 32). Counter-radicalisation outputs refer to the actions SSP networks take to combat radicalisation in their respective municipalities. These measures include conducting workshops, providing counselling, developing resources and the like. Although all SSP networks have the same objectives, their counter-radicalisation outputs differ from one network to the other (ibid.).

Considering the variation in SSP networks' outputs as well as in their respective structures, it is worthwhile asking whether there exists a link between structure and outputs. This thesis seeks to ascertain whether the structure of the SSP network makes a difference to the network's counter-radicalisation outputs. Thus, the aim of this research is to analyse the degree to which SSP network structures influence their counter-radicalisation outputs.

In order to investigate potential link between structure and outputs, two SSP networks have been identified for analysis, namely the Copenhagen SSP and the Aarhus SSP. These two cases have been selected based on similarities in their size, age and budget.

1.1 Research Question

In order to fulfil the aim of the thesis, this research addresses the following question:

To what extent does the structure of the SSP network have an impact on counter-radicalisation outputs in the Copenhagen and Aarhus SSPs?

This research question seeks to identify (1) the structure of the two SSP networks; (2) their counter-radicalisation outputs; and (3) any link between SSP structure and their counter-radicalisation outputs.

1.2 Academic and Societal Relevance

The literature on counter-radicalisation suggests that the optimal way to prevent and counter radicalisation is through engaging a variety of cooperating actors across both private and public organizations; essentially, by creating networks (Bartlett *et al*, 2010; Schmid, 2013; RAN, 2016). However, both terrorism studies and public administration studies have only recently turned their attention to studying counter-radicalisation in a network context, and therefore the existing body of knowledge in this field is relatively limited (Dalgaard-Nielsen, 2016).

The academic relevance of this research is twofold. First, this research can contribute to the literature by addressing the concept of a network. Despite the large amount of literature on networks, very little is known how counter-radicalisation efforts work within a local network setting. This thesis draws on both public administration studies and terrorism studies, and in doing so, aims to contribute new insights to the emerging literature on counter-radicalisation. Through analysis of the structure of SSP networks and their counter-radicalisation outputs, the study will provide new empirical data on how networks are configured, organized and coordinated, as well as on the kind of counter-radicalisation outputs being produced by these networks.

Second, this thesis explores and explains the possible relationship between two key variables, namely the structure of a SSP network and the network's counter-radicalisation outputs. The results will either support the assumption of a link between the two variables or reject it. Either way, the conclusion of the research will supplement the academic discussion on network outputs.

The results of this thesis are intended not only to have academic relevance, but also societal relevance. Networks cannot be administered successfully if the nature of the network is not properly understood (Klijn and Koppenjan, 2016: 259). As such, this research will not only help the actors involved in an SSP network deepen their understanding of the structure, but also help them in achieving their desired solutions. This is due to the fact that outputs are one of the key steps to developing a comprehensive solution to the problem being addressed in the network. The results of this research may additionally help the SSP networks manage their outputs more efficiently, as the study will indicate whether the SSP networks need to change their structure in order to maximize the quantity and/or quality of their outputs.

2 Context

Schools, Social Services and Police (SSP)

On the issue of crime prevention among youngsters, Denmark has extensive experience of collaboration across the governmental spectrum. Since 1977, the involvement of multiple agencies and organisations has been embraced across various networks to prevent crime locally (DKR, 2012). In Denmark, every municipality is obliged by law to carry out crime prevention work (DKR, 2012). This prevention work is organised according to local circumstances and needs.

One of the most common crime prevention initiatives is the so-called SSP collaboration, which focuses solely on young people[2]. Although the network consists primarily of Schools, Social Services and the Police (SSP), various other actors from both the public and private sectors are also involved (DIIS, 2015:18).

The main purpose of the SSP network is to identify the risk factors and reasons behind wrongdoing and criminality among children and youths, in order to address the factors from a preventive perspective (DKR, 2012). In addition to the focus on crime prevention, the work of SSP networks also includes efforts to support and protect vulnerable youngsters both physically and mentally (ibid.).

The basic idea of the SSP network is to aggregate and share information between professions with the aim of improving the quality of crime prevention work. This interdisciplinary collaboration increases the ability of the Danish authorities to act earlier and more effectively on the risk signs and risk factors in the daily life of children and youngsters.

The main objective of the SSP network is to build, operate and maintain a local network to prevent crime among adolescents as efficiently as possible, while supporting young people in their daily lives (DKR, 2012). This is done through three key areas of focus in the network: namely, general efforts, specific efforts and individual efforts (ibid.).

General preventive efforts target all youngsters, regardless of whether they have shown signs of criminal behaviour. The aim is to prevent youngsters from violating the law in the first place (bid.).

[2] The ages of the target group vary between networks. Some focus only on children and adolescents under the age 18, while others include young adults up to the age of 25 years (DKR, 2012).

Specific efforts are directed towards those youngsters who are at risk of violating the law or shows sign of vulnerability or neglect. Specific efforts include a special plan for the vulnerable youngster in question, depending on their situation and family circumstances.

Lastly, individual efforts focus exclusively on youngsters who have already committed crimes, and the aim is to prevent them from committing further offences (DKR, 2012). On this level, the SSP networks have a range of special measures at their disposal, including regular contact with the youngster and his/her parents, home visits, family plans, and so on (ibid.).

The Organisation of the SSP Cooperation

All 98 municipalities in Denmark have some form of SSP network (Servicestyrelsen, 2008). However, the structure and working frameworks of SSPs differ from each other, and there is no general blueprint for how preventative work should be carried out. This means each municipality has developed its own structure and methods depending on local circumstances including size, key actors and budget. The budgets of the SSPs are generally allocated by the municipal council during budget negotiations, meaning that the actors involved do not have any independent financial obligations (ibid.).

Despite the differences in SSP configuration, many SSP networks in larger cities have been organised similarly to one another. Usually, the bigger SSPs are organised at three levels: management level, coordinating level and implementation level (ibid). Each of these levels has their own responsibility within the SSP network.

The *management* level identifies the problems and issues that the SSP network is to deal with. It devises the general framework for crime prevention efforts (ibid.) by formulating the purpose and aim of the network, and establishing the resources required to carry out these efforts. Usually, the management level of SSPs consists of the major actors in the networks, such as such as the local police and the social services (ibid.).

The *coordination* level works as a control mechanism for the network. It steers and monitors the network to ensure that the SSP complies with the law and that the general framework devised by management is carried out in practice. The coordination level of the SSP network usually includes the local police and the different actors within the municipalities (ibid.).

The *implementation* level is responsible for the actual crime prevention work. Actors operating at this level implement the activities agreed in the frameworks, and are responsible for the daily tasks of the SSP network (ibid.).

The responsibility given to SSP networks has grown steadily since their inception. Nowadays, they focus not only on preventing violations of the law but also on youngsters' wellbeing. The latest responsibility that the SSP networks have begun to adopt is the prevention of radicalisation among youth in Denmark (DIIS, 2015).

SSP & Counter-Radicalisation Efforts

Recent security developments in Denmark have intensified the authorities' focus on reducing the growth of extremism. The SSP networks have started to play a crucial role in this regard. Since Danes began to travel abroad to join extremist groups, the SSP networks in the bigger cities have started to adopt counter-radicalisation measurements (DIIS, 2015). Today, all the SSP networks in major cities deal with radicalisation, although the structure and volume of their efforts varies significantly. However, only a few actually provide programmes and services to the target groups, as is the case in Copenhagen and Aarhus. The rest focus mainly on identifying sign of radicalisation, and reporting to the police or to national authorities when a cause for concern is identified.

3 Literature Review

To properly understand and analyse the SSP networks in this study, a coherent theoretical framework and a clarification of relevant concepts are needed. This chapter therefore examines and defines the key concepts to be used in the thesis. The first section explores the radicalisation and counter-radicalisation literatures. The (counter-) radicalisation literature emphasizes the wickedness of radicalisation -meaning that it is an ambiguous and complex problem with no common problem definitions (Baker-Beall, *et al.*, 2010; Fischbacher-Smith, 2016). Wicked problems in modern times have pushed the policy-makers to consider new ways of dealing with the complexities, which open up for new ways of governing the public (Head & Alford, 2015). The most noteworthy development in this regard, is the cross-sectional collaboration. Thus, the third section of this chapter examines the literature on networks. The network literature review assesses a range of concepts, from network type to network performance, and from network management to network output. The last section in this chapter derives a theoretical framework based on the two first sections which is used to conduct the research.

3.1 Conceptualisation of (Counter-) Radicalisation

Despite the rapid growth in use of the term radicalisation since the terrorist attacks in New York on 11 September 2001, the concept of radicalisation is not a new one, even though we may feel that way (Baker-Beall, *et al.*, 2015). The term radicalisation is derived from the word "radical" which is defined as "*advocating thorough or far-reaching political or social reform; representing or supporting an extreme section of a party"*, and thus to distinguish a *radicalised* person or idea from a *radical* idea can be challenging. Similarly, the term radicalisation can also be problematic to distinguish from the term radicalism, which is defined as *"politically or socially radical attitudes, principles or practice"* (ibid.).

Many societies interpret radicalism and radical ideas as an expression of legitimate political thought, whereas radicalisation is seen as a process that leads to political violence (Baker-Beall, *et al.*, 2015: 4-5). Given the ambiguous definition of radicalisation (or to be radical/ radicalised) and the subtle difference between radicalisation and radicalism, the contemporary discourse regarding radicalisation as a security issue gained prominence in the aftermath of the Madrid (2004) and London (2005) attacks (ibid.). Although the debate over radicalisation has been marked by a substantial degree of conceptual confusion, there is nonetheless a broad political consensus on using radicalisation as the main term to understand political and/or religious violence (Baker-Beall, *et al.*, 2015: 4).

As the search for what radicalisation really constitutes can be challenging, the same is naturally true for finding measures to counter it. Both the terms radicalisation and counter-radicalisation remain poorly defined and mean different things to different actors (Schmid, 2013: 1). The following sections are therefore devoted to addressing and clarifying the conceptual issues related to radicalisation and counter-radicalisation.

3.1.1 Radicalisation

Radicalisation is a topic of intense media interest and has drawn plenty of political attention in Europe, including in Denmark (Vidino & Brandon, 2012). As in other Western countries, the radicalisation debate in Denmark was catalysed by the Madrid train bombing in 2004 and the London attacks in 2005 (Schmid, 2013:1).

The public debate and political discourse around the causes of terrorism changed in the aftermath of these attacks (Kundnani, 2015: 14-15). Previously, discussions about causes were tempered by the assumption that there could be no rational explanation of terrorism beyond the evil mindset of the terrorists (Kundnani, 2015: 14). Hence, it was an "evil ideology" that did not require further analysis, and the only solution to terrorism was to capture or kill the terrorist before they could carry out another attack; this was the guiding principle of the so-called "war on terror" (ibid.). However, after the 2004-2005 attacks in Europe, governments began to look for new answers in their counter-terrorism efforts, as they no longer believed that merely capturing and/or killing the terrorist(s) was sufficient to prevent further acts of terrorism (ibid.). The concept of "radicalisation" therefore emerged as a vehicle for policymakers to explore the process by which an individual turns towards terrorism, and to provide an analytical grounding for preventive strategies that went beyond the threat of violence or detention (Kundnani, 2015: 15).

In Europe there are a diverse range of governmental definitions of radicalisation. (Schmid, 2013: 12). Below are some examples of radicalisation as defined by European governments:

- The British Prevent programme, developed in 2003, was one of the first governmental programmes in Europe to define radicalisation (Edwards, 2015: 54). Prevent defines radicalisation as: "*a process by which a person comes to support terrorism and forms of extremism leading to terrorism"* (Home Office, 2011: 108)

- The Dutch programme to combat jihadism defines radicalisation as *"an attitude that shows a person is willing to accept the ultimate consequence of a mind-set and turn them into action. These actions can result in the escalation of generally manageable opposition up to a level that they destabilize society due to the use of violence"* (Dutch Ministry of Security and Justice et al. 2014: 33).

- According to the Norwegian action plan against radicalisation and violent extremism: "*Radicalisation is understood here to be a process whereby a person increasingly accepts the use of violence to achieve political, ideological or religious goals"* (Norwegian Ministry of Justice and Public Security, 2014: 7).

- The Danish action plan to prevent radicalisation and extremism does not explicitly define radicalisation, but states "*radicalisation is not a clearly defined concept. It is a process that takes various forms. Sometimes it happens relatively quickly; sometimes it is long and drawn-out. There are no simple causal relationships – radicalisation is triggered by different factors and leads to different forms of involvement. It can assume forms such as support for radical views or extremist ideology, and it can lead to acceptance of violence or other unlawful acts as a means to achieve a political/religious goal*" (The Danish Government, 2014: 5).

In the British case, the emphasis is on the process that leads to support for terrorism. The Dutch government sees radicalisation not purely as a process, but as an attitude and the willingness to accept the consequences of an action. The Norwegian government sees radicalisation as a process whereby an individual accepts violence as a tool to achieve ideological or religious goals. The Danish action plan, like the Norwegian action plan, stresses that radicalisation is the acceptance of violence as a means to achieve political or religious goals.

These definitions thus provide different answers to what radicalisation entails. The British government sees radicalisation as the process underpinning terrorism, whereas the Dutch government sees it as a factor that destabilizes society. In the Norwegian and Danish cases, radicalisation is essentially about accepting the use of violence to achieve political and/or religious goals.

The recent focus on the process of radicalisation as a precursor to terrorism has given birth to a variety of assumptions and discussions about the root causes of radicalisation itself (Kundnani, 2015: 15). Some of the generally assumed root causes include poverty, inequality, political oppression and injustice (Schmid, 2013: 2). However, these assumptions do not fully explain the frequency of radicalisation in north-western European countries with liberal democracies and strong welfare systems. It is therefore argued that alienation, social exclusion, anger, hopelessness and a lack of integration are among the key reasons why youngsters in north-western Europe become radicalised (ibid.).

On the other hand, running counter to those explanations which "victimise" the terrorist and see the cause of radicalisation as an external symptom, are strong arguments that radicalisation is essentially a cultural, theological and ideological process (Kundnani, 2015: 17f).

It is not only policymakers who have found it difficult to agree on the root causes of radicalisation and terrorism; academic researchers have encountered the same challenges (Schmid, 2013: 2). Since the attacks in 2001 in New York, the number of academic articles mentioning radicalisation has risen exponentially (Kundnani, 2015: 18).

There are various academic definitions of radicalisation. Jensen (2006) defines radicalisation as:

"*A process during which people gradually adopt views and ideas which might lead to the legitimisation of political violence"* (Schmid, 2013: 17).

According to Sinai (2012):

"Radicalisation is the process by which individuals – on their own or as part of a group – begin to be exposed to, and then accept, extremist ideologies" (ibid.)

Although the competing definitions often differ on the details, there is general agreement that radicalisation is a process (Schmid, 2013). In accordance with the consensus, this research adopts the Danish SSP network association's definition of radicalisation, which is:

“*A process through which a group or an individual increasingly develops extreme attitudes and/or supports the use of undemocratic, illegal or violent actions to promote them”* (SSP-Samrådet, 2014).

The SSP network association’s definition is thus broadly in accordance with the academic consensus. Additionally, the national SSP network association’s definition of radicalisation is considered most appropriate for this research, as all the local SSP networks carry out their work based on this definition.

The existence of so many competing definitions indicates that we have neither a universal definition of what radicalisation is, nor a common political or academic understanding of what it constitutes. The issue of definitional ambiguity therefore poses a challenge not only for scholars and politicians but for counter-radicalisation practitioners, too, since effective solutions can only be developed if there is a degree of certainty about the issue being addressed.

3.1.2 Counter-Radicalisation

Following the attacks in Madrid and in London, and the assassination of the Dutch filmmaker Theo van Gogh in Amsterdam in 2004, the issue of “home-grown” terrorism in Europe has become increasingly prominent (Kundnani, 2015: 16). Policymakers across Europe have sought to devise policies and programmes to prevent their own citizens from becoming radicalised (Schmid, 2013: 50; Kundnani, 2015: 16).

These policies and programmes to fight and prevent radicalisation have various purposes and names. They can generally be divided into two categories, namely *De-radicalisation* and *Counter-radicalisation* (Schmid, 2013; Kundnani, 2015; EL-Said, 2015). De-radicalisation refers to programmes that are focused on already-radicalised individuals, while counter-radicalisation programmes seek to prevent individuals from becoming radicalised in the first place (Schmid, 2013: 50). For example, de-radicalisation measures typically include exit programmes, re-socialisation, family training and other integration methods. (Schmid, 2013: 41). Counter-radicalisation programmes on the other hand include measures such as the empowerment of communities, capacity building of vulnerable individuals and groups, and so forth (Schmid, 2013: 50).

As with radicalisation, counter-radicalisation is also a contested concept that can be defined in a variety of ways. Usually, counter-radicalisation is understood as a "*package of policies and measures designed and implemented by country to prevent youth or most vulnerable groups and communities from becoming radicalised in their home country"* (El-Said, 2015: 10).

This understanding of counter-radicalisation is broadly in line with the Danish SSP networks' definition of it. The latter's definition, which is adopted for the purposes of this research, is: *"Measures aiming to prevent individuals and/or communities from becoming radicalised"* (SSP-Samrådet, 2014).

Definitional issues aside, the precise form taken by counter-radicalisation programmes naturally varies from country to country, due to the fact that different countries have different cultures, values and political systems (El-said, 2015: 254).

Counter-radicalisation programmes implemented in northern European countries also differ from one another in term of their constituent programmes and projects (Vildino & Brandon, 2012: 7). Some of the most widespread counter-radicalisation programmes to be found in northern Europe focus mainly on empowering communities and individuals (ibid.). For example, education and training for vulnerable persons as well as debates and discussion sessions are commonly found in these countries' counter-radicalisations programmes (ibid.).

The success criteria of counter-radicalisation efforts also varies depending on country, context and programme specifics. Several evaluations of counter-radicalisation programmes have shown that it is not an easy task to agree on success criteria, neither is it easy to assess the degree to which these programmes have actually prevented radicalisation (Vildino & Brandon, 2012).

Despite the difficulty of precisely measuring effectiveness, several in-depth studies have developed numerous recommendations on how best to devise counter-radicalisation programmes (Bartlett *et al.*, 2010; Baker-Beall, *et al.* 2015). For example, Bartlett *et al.* (2010) recommend distinguishing between violent radicalisation and non-violent radicalisation (p. 7). In practice, this distinction is often overlooked by counter-radicalisation programmes (ibid.) Therefore, Bartlett *et al.* (2010) advise against broadening counter-radicalisation efforts to include large numbers of people, recommending instead that the authorities limit interventions to where there is a clearly identified risk from specific groups or individuals (p. 14-15). However, most of the counter-radicalisation programmes also have a broad preventive target, generally directing their efforts towards Muslim communities (Vildino & Brandon, 2012: 7). Consequently, the risk of stigmatisation of a certain ethnic or religious minority is acute, which may in turn have a counterproductive effect on the fight against radicalisation (Bartlett *et al.*, 2010). Most of the research on counter-radicalisation also acknowledges the complexity and wicked nature of the problems inherent to the radicalisation process (Bartlett *et al.*, 2010; Baker-Beall, *et al.* 2015).

Almost all counter-radicalisation studies stress the importance of cross-sectional collaboration between different public, private and civil entities (Bartlett *et al.*, 2010; Schmid, 2013; RAN, 2016). In other words, the key feature of countering radicalisation is the pooling of resources, information and experience. The most common way of doing this is through networks.

3.2 Wicked Problems Triggering New Way of Governing

In the twentieth century, traditional hierarchical government bureaucracy was the predominant organizational model used to deliver public services and fulfil public policy goals. Today, however, the increasing complexity of modern societies has compelled policymakers to develop new models to cope with and govern these complexities (Goldsmith & Eggers, 2004). In the literature, some contemporary public problems are described as wicked problems (Rittel & Webber, 1973; Head & Alford, 2015). Wicked problems have been characterised as ambiguous, complex, uncertain and open-ended and have even been described as a lost cause as there are no clear problem definitions (Rittel & Webber, 1973: 158). The wickedness of today's problems is mainly caused by the inception of the problems themselves, as many modern societal problems do not have a technical nature as they did in previous decades (Head & Alford, 2015: 715). Today, many problems have no well-defined solutions, and the solutions to the problems are subject to be redefined over time (Coyne, 2005: 6). Thus, potential solutions to wicked problems depend on the perspective of stakeholders and how the problems are looked upon (Rittel & Webber, 1973: 712).

Tackling wicked problems continues to pose a challenge to the authorities, not only because of the problems' inherent complexity but also because traditional hierarchical forms of public administration have not been conductive to addressing them effectively (Head & Alford, 2015: 719).

As consequence, public authorities have been forced to develop new ways of dealing with wicked problems (Walters, 2004; Head & Alford. 2015). The shift from 'government' to 'governance' is one of the more noteworthy developments related to dealing with deeply complex and challenging issues (Crawford, 2006).

Government refers to traditional policymaking and service delivery, in which coordination is realized by command and control within the public bureaucracy (Klijn & Koppenjan, 2016: 5).

In the literature, the term *governance* has various meanings. Within the public management literature, governance is seen as a way to improve performance and accountability. The role of the government is to set goals and formulate policies, while the actual implementation of these policies is left to other actors (Klijn & Koppenjan, 2016: 5-6). As a result, multi-level and inter-governmental collaboration has emerged (ibid.). This trend has only accelerated as the private and civil society sectors have started to take part in the implementation of policy (Sorensen & Torfing, 2008). The involvement of non-governmental entities in policy implementation has stimulated the emergence of cross-sectional collaboration (Klijn & Koppenjan, 2016: 1).

The shift from government to governance marks a transition from traditional hierarchical to more horizontally-based forms of policymaking. This shift has also diffused the boundaries between different entities over time (Walters, 2004). According to Walters (2004), governance is no longer something that is fixed, but is a dynamic and complex process, which is constantly evolving and responding to changing circumstances (p. 29). Accordingly, governance networks have emerged (Klijn & Koppenjan, 2016: 4).

3.3 Governance Networks

The inability of government agencies to tackle wicked problems and complex processes on their own can be attributed to natural limitations in their resources and problem-solving capacities, and it is from these limitations that multi-level and cross-sectional collaboration has emerged (Head & Alford, 2015). Governance networks are considered a product of this collaboration (Klijn & Koppenjan, 2016: 4). However, the concept of a governance network is in itself contested, since it can be understood and defined in a variety of different ways (ibid.). Klijn & Koppenjan (2016) define a governance network as:

"More or less stable patterns of social relations between mutually dependent actors, which cluster around a policy problem, a policy programme, and/or a set of resources and which emerge, are sustained, and are changed through a series of interaction" (p. 11).

Governance networks can take many different forms (Klijn & Koppenjan, 2016: 21). For example, they may consist of various actors from the public, private and the civil society sectors (ibid.). Governance networks can also have a loose configuration or a strongly-integrated framework with a well-defined working structure (ibid.). The number of entities involved in governance networks can also vary significantly (ibid.: 29), but there is a scholarly consensus that a network must consists of at least three actors (Klijn & Koppenjan, 2016; Whelam, 2012; Dupont, 2004; Kenis & Provan, 2009).

Despite the differing definitions and characterisations of governance networks, public administration scholars agree that networks are characterised by complex processes in which actors strive to minimise and/or solve problems. As the problems cannot be solved by any single actor individually, collective action is required (Klijn & Koppenjan, 2016: 10).

3.3.1 Actors within Governance Networks

It is evident that several actors must interact with another for a network to operate. How, though, is an actor to be defined? If two different departments from the same ministry take part in the same governance networks, they can be considered a single actor on the basis that they represent the same ministry. On the other hand, each department could also be considered an actor in its own right as each represents different interests within the ministry in question. So, what makes an actor? Klijn and Koppenjan (2016) suggest that an actor is "*an individual, group, organization or coalition of organizations that can act autonomously"* (p. 263).

According to the definition put forward by Klijn and Koppenjan, an entity can only be considered an actor if the entity acts autonomously, meaning it interacts independently with other actors in the network (ibid.). In this regard, another question arises: how should the independence of entities be measured? Klijn and Koppenjan (2016) argue that an actor acts autonomously when no other actors within the network are acting on their account (p. 264).

Careful deliberation on who and what can be considered an actor in a governance network is essential if the networks are to be analysed properly (Klijn & Koppenjan, 2016: 263). Another key element is the relative importance of the actors (ibid.). Governance networks may comprise just three actors, or be made up of many dozens. However, not all of them are of equal importance to the network (ibid.). Depending on the available resources, the actors' importance is determined by what they can offer the network. When an actor has exclusive access to a unique or crucial resource on which the network depends, then the actor has a critical position in the network (Klijn & Koppenjan, 2016: 269). Five important resources can be identified within a governance network (ibid.: 267):

- *Financial resources*: money and budgets.
- *Production resources*: means other than money which are needed to realize the network's goals.
- *Competencies*: the authority to make a certain decision and to take responsibility.
- *Knowledge*: information, expertise, experience and knowhow.
- *Legitimacy*: the support needed for a certain solution.

The relative importance of the resources is of course determined by the type of network and its goals, and thus not all five resource types are equally important across all governance networks (ibid.). Furthermore, fluctuations in relative importance of the resources may also occur due to changes in problem formulation or changes in policies and services (ibid.: 271).

The profile and relevance of governance networks has grown in line with the emergence of wicked problems (Klijn & Koppenjan, 2016: 43). This is especially true of the national security domain (Whelan, 2012: Dupont, 2004). Ever since the terror attacks in 2001 in New York, and later in multiple European countries, national security has been increasingly characterised as a network issue (Whelan, 2015: 537).

3.4 Delivering Security through Networks

Analysts and researchers have used networks to understand recent developments within the field of security (Whelan, 2012: Dupont, 2004). Both the public administration literature and the organisational theory literature argue that networks are an efficient way to achieve security goals, and an effective way to manage wicked problems (Head & Alford, 2015; Whelan, 2012). Within both security studies and the public administration literature, networks dealing with security issues are generally categorised as security networks (Whelan, 2012: Dupont, 2004). According to Dupont (2004), a security network can be defined as:

"*a set of institutional, organizational, communal, or individual agents or nodes (...) that are interconnected in order to authorize and/or provide security to the benefit of internal or external stakeholders*" (p. 78).

In other words, a security network is a network in which a set of actors have formed relationships to advance security-related objectives (Whelan, 2012: 19).

Just as governance networks vary in their size, form and shape, so too do security networks (Dupont, 2006: 167). Despite differences in size and structure, however, all security networks have a common goal, namely to provide security (ibid.).

Security networks are formed around the authorisation and delivery of security through a range of processes and services (Dupont, 2006: 168). Security networks' foundations differ from one network to the next. The inception of a security network can be a voluntary collaboration among autonomous actors, or may have a contractual framework with formal ties (ibid.). Besides the voluntary form of security networks, there are also security networks that are brought together by policymakers (ibid.). These type of mandatory security networks usually have a contractual working structure and well-defined goals (ibid.).

Regardless of these different types, the key feature common to all security networks is the pooling of resources to increase the effectiveness of delivering security (ibid.).

3.5 Types of Security Networks

Dupont (2004) identifies four different types of formal security networks: (1) local security networks, (2) institutional security networks, (3) international security networks, and (4) technological security networks (p. 79). Each security network type has its own characterisation depending on the aim of the network, the actors involved, and their activities.

3.5.1 Local Security Networks

Local security networks are designed to tackle local security problems, connecting a diverse array of state and non-state actors (Dupont, 2004: 79). Dupont (2004) defines local security networks as:

"*initiatives that seek to harness the public and private resources available in local communities in order to overcome complex crime problems that find their origins in deteriorating social conditions"* (p. 79).

Local security networks usually include actors from the law enforcement authorities such as magistrates and the police (ibid.). They generally also include other local governmental entities, such as social services, as well as communities and the private sector (ibid.).

The main activity of local security networks is the exchange of information on local crime problems and the mobilisation of resources to solve these crimes locally (ibid.). In general, local security networks rely on local knowledge and solutions that transcend institutional boundaries (ibid.).

3.5.2 Institutional Security Networks

The second type of security network is the institutional security network. This is understood to comprise an *"inter-institutional bureaucratic project or the pooling of resources across government agencies" (*Dupont, 2004: 80). In other words, institutional security networks aim to enable the amalgamation of resources across the public sector. Of course, all security networks enjoy some kind of inter-institutional framework and resource pooling to a greater or lesser extent; the difference is that the explicit purpose of institutional security networks is to facilitate inter-institutional resource efficiency (ibid.).

Institutional security networks rarely involve non-governmental actors. They are efficiency-based, meaning they are engaged in an effort to rationalise resources, optimise performance and maximise outputs (ibid.).

3.5.3 International Security Networks

A third type is the international security network. This type of security network – unlike the previous two types - extends beyond national borders (Dupont, 2004: 80). International security networks share many features with institutional networks, such as the aim of pooling resources together, but the former has an important distinguishing element: the concept of national sovereignty (ibid.).

Due to the sovereignty issue, international security networks are usually made up exclusively of state actors. It is only recently that non-states actors have come to participate in international security networks (ibid.). This type of security networks generally restrict membership to a single public actor per country involved (Dupont, 2004: 81).

3.5.4 Technological (Virtual) Security Network

The last security network is the technological security network, also known as a virtual security network. This type of security network facilitates the communication and exchange of information between the security actors with the aim of making information flows more efficient (Dupont, 2004: 82). This type of security networks is essentially a technological tool to pool and share information and knowledge in an easy way (ibid.).

All security networks in the present day can be categorised into these four types (Dupont, 2004). This does not mean, however, that the four types of networks are sharply divided or that a network must fall into a single category. In practice, many security networks include characteristics from two or more types (ibid.).

Security networks not only come in different types; they also take different forms and shapes. Each security network, regardless of its type, is organised somewhat differently. One of the main reasons why security networks vary from on another is that networks are generally very complex by nature (Sorensen & Torfing, 2008). Networks are full of conflict as numerous interests fuse and collide (ibid.). This chaotic process results in different forms of network organisations (Kenis & Proven, 2009), which will be discussed in the next section.

3.6 The Organisational Design of Networks

Networks come in different organisational designs (Kenis & Provan, 2009: 446). The organisational design of networks differs in terms of the number of actors, boundary of the network, and presence or absence of different links between actors (ibid.). It is crucial to understand the organisational form taken by a networks as these forms have significant consequences for what the network can achieve in practice (ibid.). Put simply, network design determines the quantity and quality of network outcomes. Kenis and Provan (2009) argue that a specific form of organisational design produces specific results (p. 446). In other words, a direct link can be identified between the form of organisational design of the network and the network's outcomes.

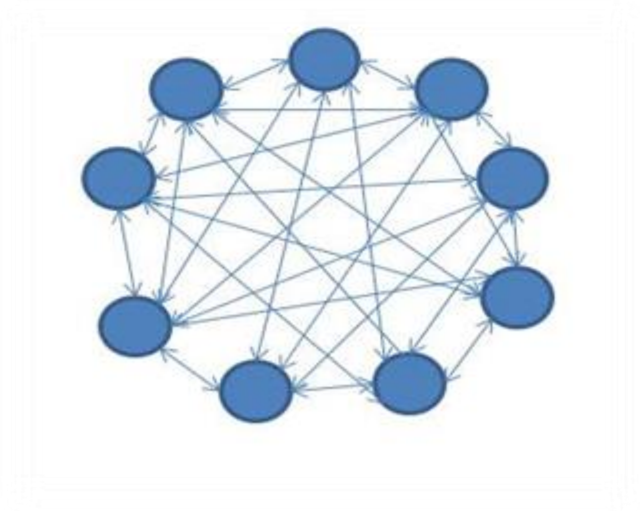
Kenis and Provan (2009) identify three models of network organisational design. These are (1) the *shared governance network*, (2) the *lead organisation network* and (3) the *network administrative organisation network* (NAO) (p. 446).

Each of these designs differs according to its own unique structure, and Kenis and Provan (2009) argue that each has its own specific functionality. This means that each design differs in what it is best at (ibid.). None of the three organisational designs are objectively superior than the others, however, each organisational design has its own strengths and weaknesses (ibid.).

3.6.1 Shared Governance Network Design

The simplest form of organisational design is the Shared Governance Network (Kenis & Provan, 2009: 446). This design is best suited to small networks and is self-managed, meaning all actors within the network participate in decision-making and in managing the network's activities (ibid.). In this type of organisational design there is no distinct formal administrative entity (ibid.)

Figure 1: Shared Governance Network Design



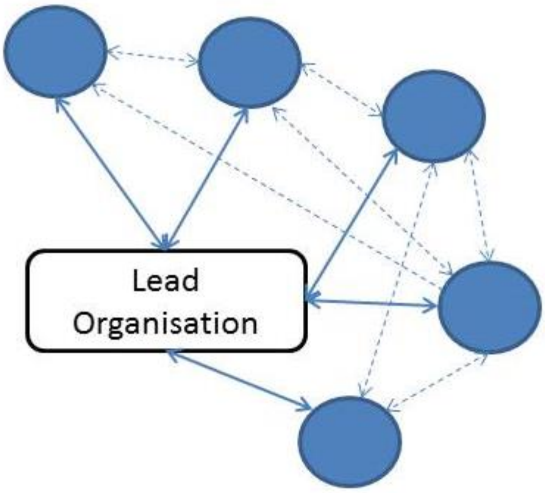
The strengths of the Shared Governance Network design include, first of all, the inclusiveness among the actors within it (Kenis & Provan, 2009: 446). As a result of the equal involvement of all actors in the network, the level of trust in this kind of organisational design is usually high (ibid). The design is also flexible, and the actors can interact with one another easily (ibid.).

The weakness of the Shared Governance Network design is its relative inefficiency: every actor must be involved in every decision made (ibid.). This weakness can be avoided if the number of actors involved in the network is limited, but when the network reaches a certain size the design can become counter-productive (ibid.).

3.6.2 Lead Organisation Network Design

Another form of network design is the so-called Lead Organisation Network (Kenis & Provan, 2009: 446). In this design, all activities and key decisions are coordinated by one of the members acting as a lead organisation (ibid.: 448). This does not mean that all the actions in the network must go through the lead organisation; the other actors do interact with one another, but the lead organisation plays a facilitating role (ibid.). According to Kenis and Provan, this type of organisational design is suitable for medium-sized networks (ibid.).

Figure 2: Lead Organisation Network Design



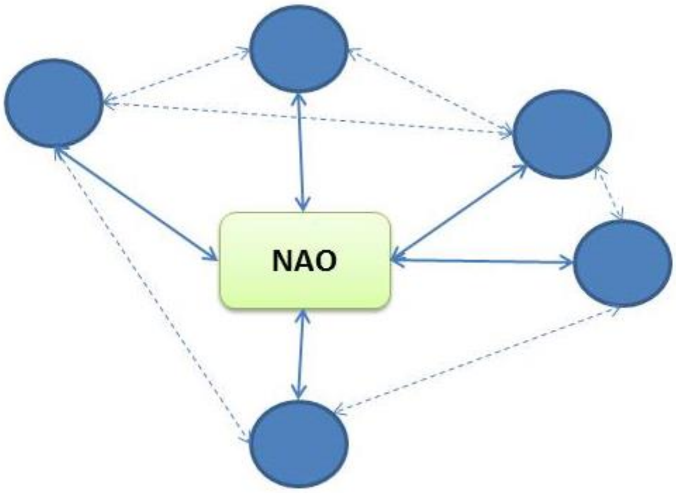
The main strength of this organisational design is the degree of efficiency that it affords the network (Kenis & Provan, 2009: 448). This is due to the fact that the lead actor assumes most of the responsibilities for running and coordinating the network, minimising the complexity and messiness inherent to medium-sized networks (ibid.). However, this design also has limitations. The most conspicuous drawback is the risk of the lead organisation dominating the network and advancing its own agenda. Any such domination may cause resentment and resistance from the other actors (ibid.).

To avoid both the inherent messiness in the Shared Governance design and the potential domination of one actor in the Lead Organisation design, an alternative design has been put forward, namely the Network Administrative Organisation Network design.

3.6.3 Network Administrative Organisation Network Design

The final network design form identified by Kenis and Provan is the Network Administrative Organisation Network (NAO) (Kenis & Provan, 2009: 448). The idea behind the NAO model is to separate the administrative entity of the network by setting up a special unit solely for managing and coordinating the network's activities (ibid.). The NAO is not another actor within the network; it does not represent any interests. The NAO is a purely established for the purpose of steering the network (ibid.).

Figure 3: Network Administrative Organization Network Design



The NAO itself can take different forms and be different sizes. It may be a single individual who acts as network facilitator, or it can be a complex NAO secretariat with an executive director and its own staff (ibid.).

The main strengths of this design are its sustainability and legitimacy. The design boosts both the internal and external legitimacy of the network, and maintains stability (ibid.). On the other hand, the NAO may adopt a framework which leads to an excessively bureaucratic decision-making process. The NAO may also potentially stimulate a shift from the original horizontal framework to a more hierarchical organisational model (ibid.).

Each of the three network organisational designs is unique, and each has its own strengths and weaknesses. All three designs have characteristics that affect the likelihood of particular output criteria being more or less appropriate (ibid. 449). The three designs explain the organisational structure of the networks, but in these models there is no indication of how information is shared among the actors. Each design may devise its own methods for pooling and sharing information.

3.7 Security Networks and Information Sharing Designs

In discussing network designs, Whelan (2012) is among those highlighting the importance of information sharing within security networks. Information sharing is considered crucial to a security network's performance (Whelan, 2012: 46). However, when numerous actors within a security network need to share sensitive information with one another, two problems may potentially arise: the risk of information overload and the risk of information protection (Whelan, 2012: 108).

Information overload refers to the risk of sharing too much information in proportion to the network's ability to process the information. Hence, there is a risk of important information being overlooked. On the other hand, information protection refers to the fact that some actors might withhold crucial information because of concerns that it will not be treated with sufficient care and discretion (ibid.).

Whelan (2012) identifies two type of information sharing design: the all-channel design and the hub design (p. 43). Both designs have distinct strengths and weaknesses.

The all-channel design refers to a network in which each actor shares information with all the other actors. All-channel information design is used for a number of reasons, one of which is that all the actors within a security network may require access to all the information collected by the network. The rationale behind sharing information with everyone is that it is difficult for just one actor to assess the relevance of information to all the other network members. The all-channel design gives actors the opportunity to assess the relevance of the information for themselves (ibid.).

However, in this case, the risk of information overload and/or the withholding of information is very high. Too much information to be processed by the actors would be considered inefficient, as processing information requires resources and energy. Moreover, the all-channel design carries the risk of information being withheld due to its sensitivity (ibid.).

The hub information sharing design poses a possible solution to problems around the sharing and withholding of information in security networks. In a hub network all information passes through a central actor, meaning that information sharing is centralised and therefore more efficient. The hub design does also have its weaknesses, however. One of the major risks is that the central actor through whom the information passes may not fully understand the information or may fail to identify who should receive it (ibid.).

Overall, the security network literature presents a wide range of network models and potential solutions to network problems. Several leading authors have provided the literature with different forms, designs, structures and models of how to configure and analyse different security networks and their performance.

3.8 Security Network Performance: The Outputs

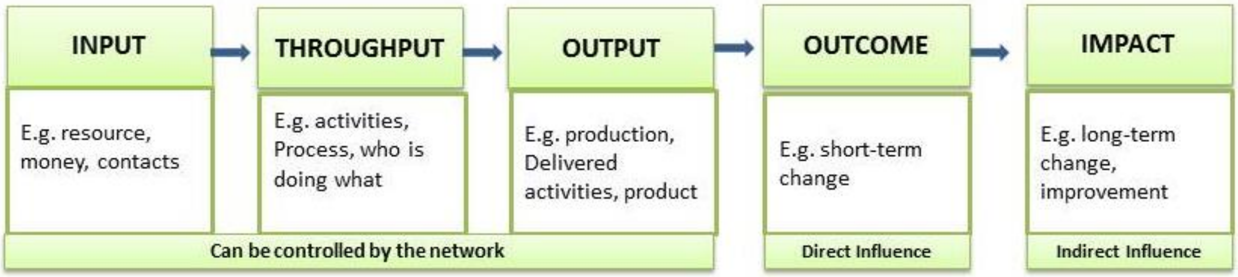
Assessing the performance of a security network is a challenging task (Turrini, *et al.* 2010). The inherent difficulty in performance assessment is that it depends on a variety of different factors, levels and criteria, which can differ significantly (ibid.).

Scholars and researchers have taken several approaches to measuring the performance of networks, and their conceptualisations of network performance have been based on divergent criteria (Raab, *et al.*2013: 480). Some scholars focus on the perspective of stakeholders; others analyse the network performance from the community standpoint, while still others take the entire network into account (Turrini, *et al.* 2010: 534). Besides the level of assessment of network performance, the criteria used in the network literature also varies (ibid.). For instance, some scholars assess performance based on information sharing between actors, while others consider performance to mean internal stability. Some focus on the achievement of goals, and some measure performance by the network's ability to survive in the long term (Turrini, *et al.* 2010; Raab, *et al.*2013).

Despite the differences in measurements, network scholars agree on the fact that an overall assessment of network performance is not feasible since the performance of a network is not objective but considered as a normative statement (ibid.). However, despite the inherent subjectivity of the exercise, Provan and Milward (2001) argue that networks can and should be assessed in terms of their performance (p. 422).

Since the first major assessment of network performance was conducted by Provan and Milward in 1995, many other researchers have started to explore the emerging field (Raab, *et* *al.* 2013: 482). Scholars have conceptualised network performance in diverse terms and variables, such as inputs, outputs, outcomes, effectiveness, efficiency and so forth (Turrini, *et al.* 2010: 529; Whelan, 2012: 16). Each of these variables measures a different level and process of a given network. For instance, assessment of network efficiency is usually done by analysing the relationship between inputs and outputs, and effectiveness can be measured by investigating whether the outputs leads to the expected outcome.

Figure 4: Phases of Network Performance Processes


INPUT
E.g. resource, money, contacts
THROUGHPUT
E.g. activities, Process, who is doing what
OUTPUT
E.g. production, Delivered activities, product
OUTCOME
E.g. short-term change
IMPACT
E.g. long-term change, improvement
Can be controlled by the network
Direct Influence
Indirect Influence

In the case of security networks, it is difficult to measure the outcomes or the impact (Whelan, 2015: Dupont: 2006). Firstly, security is a normative concept, meaning that how safe or secure a person feels depends on that individual's own perceptions (Whelan, 2012: 5). For example, different individuals will assess the same event or incident differently. Some may see it as a threat to security, while others might conclude precisely the opposite.

The second reason is due to the influence of external factors (ibid.). In addition to security networks, numerous security organisations also provide security and safety. So, when assessing a specific security network's performance in term of outcomes and impact, it is hard to fully eliminate external factors (Whelan, 2012: 6). Based on this premise, it is reasonable to argue that the correct (and most straightforward) way of measuring the performance of security networks is by assessing its outputs.

Output refers to what a security network actually produces (Klijn *et al.* 2010: Whelan, 2012). For instance, if a network's goal is to reduce crime, an output from the network could be community outreach, measured by the number of information meetings held or the number and length of conversations held with individuals in the community. Network output can be measured based on the *quality* of the outputs, and/or on the *quantity* of outputs (Whelan, 2012: 17). The quality of the outputs refers to how well the output was completed. Quantity of outputs, on the other hand, assesses the number of tasks achieved, meaning the amount of the outputs generated by the network (ibid.).

Despite the extensive literature on network performance, the discussion around how best to measure performance is still ongoing (Raab, *et al.*2013: 481). Scholars have tried to conceptualise and analyse network performance in very different ways, focusing on different levels and on diverse parameters (Turrini *et al*, 2010). However, although researchers have explored the link between network structure and general performance, little attention has been paid to the individual phases of a network's performance processes. In particular, there is a distinct lack of focus on network outputs.

3.9 Deriving a Framework

Since the first seminal study on network performance was published (Provan & Milward, 1995), scholars have been investigating how to successfully manage security networks. These researches have included an examination of how structural configuration can affect network performance (Turrini, *et al.* 2010: Raab, *et. al.* 2013; Whelan, 2015; Dupont 2006). However, the different aspects of network structure and how they relate to network performance remain under-researched (Klijn *et al.* 2010). This thesis seeks to contribute to the debate by investigating the linkage between structure and outputs in a security network.

Before we can analyse the structure of a network, we must first identify which actors should be taken into account. Considering the many objectives of SSP networks, numerous different actors are involved in some capacity. The actors in the present study will be identified based on Klijn and Koppenjan's (2016) actor analysis framework (p. 260). This framework allows for the identification of relevant actors based on actor's ability to act autonomously, and what resources the actor brings to the network (ibid.).

Table 1: The model for identification of actor relevance

	Identification
Actors Autonomous	*No other entity acts on behalf of them in the SSP network*
Actors Resources	*The importance of the resources they own or have access - which the network depends on*

Based on Klijn and Koppenjan’s (2016) framework, the model above will be used as a tool to determine the relevance of the actors in the SSP networks under study. On the issue of actor resources, various types have been identified in the network literature but the majority are not relevant to the SSP. For example, we can eliminate all kinds of financial resources as the SSP network’s budget is funded exogenously – by the municipality – rather than by the actors themselves. This study will therefore only take into account the knowledge the actors bring to the SSP network in the context of counter-radicalisation.

When the relevant actors within the SSP networks are identified they will be labelled as key-actors, while the non-relevant actors will be categorised as sub-actors.

SSP Network Structure Analysis Framework

Three main characteristics and predictors of the structure of a security network have been identified from the literature review.

The first is the type of the network. As mentioned previously, security networks can be categorised into four different types: local, institutional, international and technological (Dupont, 2004). Each type has its own purpose and specific features. However, this categorisation of security networks does not give any indication of how interaction between actors takes place within the network.

The second is the security network’s organisational design, meaning the way in which the actors interact with one another. Based on the literature, three organisational designs have been identified. The first is the shared governance network, the second is the lead organisation network and the third is the NAO network design (Kenis & Provan, 2009). All three of these organizational designs have their own interaction patterns, which are inherent to the structural characteristics of the network.

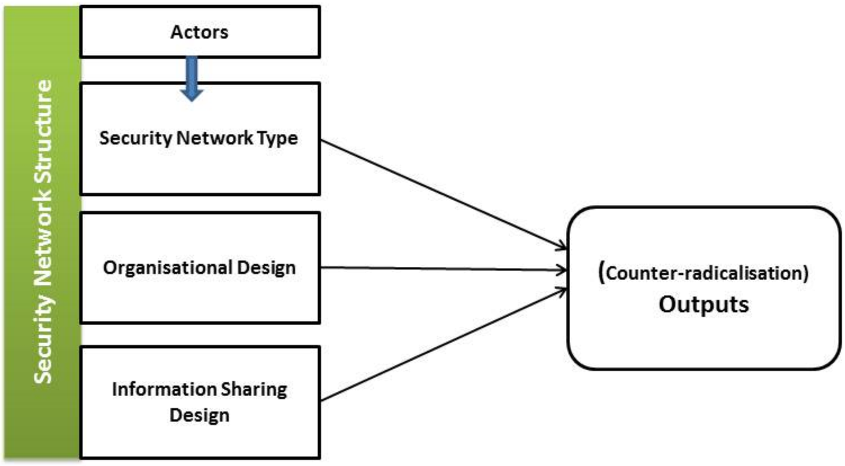
The last predictor for a security network structure is its information sharing design. Two designs were identified, namely the all-channel information sharing design and the hub version (Whelan, 2012). Information sharing is critical to the success of a security network and thus an important point to consider in the analysis of SSP networks. Without it, any assessment would be incomplete.

By combining the type of security network with the organizational design and the information sharing design, the model will provide a full picture of the structure of the SSP networks.

These three designs therefore provide both the foundations of this study and the analytical scope, in terms of SSP network's structure and the bearing of the structure on the outputs.

It should be noted that this paper focuses solely on counter-radicalization outputs, for two reasons. The first reason is that SSP networks deal with various problems, meaning that they produce a wide range of outputs, which would require extremely broad and time-intensive analysis. The second and main reason is that this study seeks to analyse SSP networks in the context of counter-radicalisation. As such, the other outputs produced by SSP networks are not of direct interest to the research.

Figure 5: The Analysis Framework


Security Network Structure
Actors
Security Network Type
Organisational Design
Information Sharing Design
(Counter-radicalisation) Outputs

Based on the literature review, it may be reasonably assumed that the outputs of a security network are a product of the network structure. Based on the analysis framework, it is expected that if one or more elements of the SSP structure are dissimilar, the outputs will also differ.

3.10 Operationalisation

Prior to conducting the analysis, it is necessary to devise specific definitions for the concepts being used.

Before we can measure the structure of the SSP networks, we need a clarification of what constitutes a key-actor is an SSP network. To this end, the independence and knowledge of the actor must be assessed. Each of the three designs of the study's proposed framework are operationalised in Table 2.

Table 2: Overview of Concept Measurements

Theory/Concept	Definition/ Description	Indicator(s)
(Key-) actor	*"An individual, group, organization or coalition of organizations that can act autonomously'* (Klijn and Koppenjan, 2016: 263)	- Acts independently within the SSP network in the context of counter-radicalisation - Owns or has access to knowledge that the SSP network depends on
Knowledge	*The availability of crucial information, documents, people, etc*. (Klijn and Koppenjan, 2016: 269)	- Access to sensitive information; journals; experts; professionals; practitioners - Irreplaceable Information
Security Network Type	"*A set of institutional, organizational, communal, or individual agents or nodes (…) that are interconnected in order to authorize and/or provide security to the benefit of internal or external stakeholder*" (Dupont, 2004)	- Actors involved - The purpose and aim of the network - Geographical work area
Organisational Network Design	Three organisational designs: shared governance network; lead organisation network and the NAO network design (Kenis & Provan, 2009)	The interconnectedness of the actors. Interaction in form of: - Meetings - (In-)formal contacts - Decision-making procedure
Network Information Sharing	Two information sharing designs:	Information patterns within the

Design	- All-channel - Hub	SSP network: - Information flow: gathering; sharing: diffusing of information
Counter-radicalisation Output	What the SSP networks do and produce in the context of (counter-) radicalisation	Number and type of: - Programmes - Services - Cases - Activities - Seminars - Counselling - Coaching

4 Methodology

This research seeks to explain whether there may be a link between the structure of an SSP network and its counter-radicalisation outputs. To meet this objective, a clearly defined methodology is essential. This chapter sets out the methodological approach taken by the study. First the research strategy is presented, and then the data collation is described. After the description of the aggregated data, the next section will explain how the data is analysed. The final section is devoted to discussing the research's reliability and validity.

4.1 Research Strategy

This paper's research question takes an explanatory approach, as its tries to connect ideas to understand the relationship between structure and outputs within security networks. The research question aims to examine the link between the structure of a SSP network (the independent variable) and the network's counter-racialisation outputs (the dependent variable).

A case study is considered the most suitable approach for two main reasons. The first is that case studies are among the most appropriate means of studying processes, searching for linkages and providing explanations of these causes (Yin, 2009: 8). In other words, a case study strategy enables the researcher to explain the linkage in real-life situations that may be too complex for other research strategies, such as surveys or experimental studies (ibid.).

The second reason is that case studies produce detailed knowledge, which many other research methods do not (ibid.). For example, to answer the research question posed in this study, it is necessary to gather in-depth information from multiple sources about the SSP networks' interactions, working processes, information sharing mechanisms and outputs, among other things. A case study is ideal for generating these kind of insights (ibid.). Therefore, to generate the necessary insights and collect sufficient information on the SSP networks and their counter-radicalisation outputs, a case study is preferred.

Security networks are defined as *"a set of institutional, organizational, communal, or individual agents or nodes (...) that are interconnected in order to authorise and/or provide security to the benefit of internal or external stakeholder" (*Dupont, 2004: 79). According to this definition, the security network itself must be the unit of analysis, and hence in the present study the unit of analysis is the SSP network. Considering this study's exclusive focus on the counter-radicalisation outputs of the SSP network, the units of observation are the structure (expressed in terms of type, organisational design and information sharing) and counter-radicalisation outputs.

A case study may consist of a single or multiple cases (Gerring, 2007: 38). This research conducts a multiple case study, a design based on careful consideration of the research objectives.

The first reason is that this thesis seeks to test the assumption that there exists a link between a network's structure and its outputs. A multiple case study is well suited to testing assumptions or hypotheses, unlike single case studies which are better suited to generating them (ibid.).

The second reason relates to the insights this research is investigating. The research tries to explore and explain the *causal effect* (meaning the linkage between the structure and outputs), as opposed to the *causal mechanism* (meaning why a certain structure produces a certain output). On this basis, a multiple case study is again more appropriate as it is better suited to generating insights into causal effects (ibid.).

In short, a single case study would not be able to produce a satisfactory answer to the research question, as with a single SSP network it would not be possible to explore the linkage between structure and outputs. For these reasons, a multiple case study was deemed most appropriate.

4.2 Case selections

Two cases have been selected for examination, namely the Copenhagen SSP and Aarhus SSP. These two cases have been selected base on their contextual similarities. The rationale is to minimize the possibility that the SSP network surroundings might affect the counter-radicalisation outputs. For example, the outputs of the two SSP networks could differ because of differences in working environment or size rather than the network structure itself. To overcome this potential limitation, the research attempts to nullify the external influence on the outputs by selecting two cases which are contextually similar.

In addition to methodological considerations, there is also a practical rationale underpinning the selections: access to crucial information, which is necessary for the research. Although there are numerous SSP networks dealing with radicalisation in Denmark, the researcher was limited to choosing from six SSP networks which were willing to take part in the study.

As a result of these practical and methodological considerations, the Copenhagen and Aarhus SSP networks were selected according to four distinct criteria.

4.2.1 Case Selection Criteria

The four criteria were developed based on the need to limit the possibility of contextual influence on the SSP's counter-radicalisation outputs. The four criteria are 1) the size of SSP network, 2) their age, 3) their budget, and 4) the extent to which extremism is known to exist in the SSP's municipality.

The first criterion is the size of the municipality, which is crucial to take into consideration for two reasons. The first is that the degree of interconnectedness among actors will increase or decrease in accordance with the size of the SSP network, and hence the differences in size may also affect the outputs of the network.

The second reason concerns working framework differences across large and small SSP networks. For example, if two networks have the same working framework but differ in size, their outputs may be different, as the smaller network might be more manageable and efficient compared to the larger network.

Both the Copenhagen and Aarhus SSPs can be categorised as large networks. This is due to the fact that Copenhagen and Aarhus are the two biggest municipalities in Denmark, and thus each incorporates numerous local organisations and entities.

The second criterion is the age of the SSP network. Age in this context is measured from the point at which counter-radicalisation became an objective for the SSP network. This criterion is essential, as the literature underlines the importance of the time framework for the performance of security networks (Whelan, 2012; Dupont, 2004; Raab *et. al.* 2013). If a security network is newly formed, its outputs may yet be underdeveloped compared to a network that enjoys several years of experience.

Both the Copenhagen and Aarhus SSPs began their counter-radicalisation activities in 2011 and thus each can be said to have the same amount of experience in this field (DIIS, 2015: 31).

The third criterion is the budget. Each SSP network has its own budget, which is determined in large part by the size of the local municipality. Smaller municipalities have fewer resources than bigger municipalities, hence the differences in their budget. This criterion is also crucial to take into account, as budget size may affect an SSP network's counter-radicalisation outputs. Put simply, if one SSP network were to enjoy greater financial flexibility compared to other networks, it might produce significantly different outputs. Both the Copenhagen and Aarhus municipalities have allocated a large amount of resources to their SSP networks.

The Copenhagen SSP network has been given approximately DDK 6 million per year (Socialudvalg, 2016), and since counter-radicalisation fell into the network's purview, the municipality has allocated a further DDK 5 million annually until 2018 (BIF, 2016).

In the Aarhus municipality, the SSP network has a budget of nearly DDK 6 million; since counter-radicalisation efforts have been incorporated into network, the Aarhus municipality has raised this budget to DDK 9 million (Aarhus municipality, 2015).

The final criterion is the extremism milieu existing in the municipality. The extremism milieu consists of radicalised individuals and those groups that actively take part in the radicalisation of youngsters (Bartlett, *et al.* 2010). As with the previous criteria, any major differences in the extremism milieu may also influence the counter-radicalisation outputs of the SSP networks.

According to research by the Danish National Centre for Social Research, the majority of antidemocratic and extremist milieus (mostly from Islamic groups) are based in the Copenhagen and Aarhus municipalities (SFI, 2014).

Table 3: Overview of Case Criteria

Criteria	Copenhagen	Aarhus
Size	*Large SSP network*	*Large SSP network*
Age	*Since 2011*	*Since 2011*
Budget	*DKK 11 million*	*DKK 9 million*
Extremism milieu	*High density*	*High density*

By taking these four criteria into account when analysing the SSP networks, the extraneous factors that may influence counter-radicalisation outputs are distinctly limited. Consequently, the degree to which an SSP's structure impacts its counter-radicalisation outputs can be assessed.

4.3 Data Collation

Data was collected in a three-step procedure. First, desk research allowed for the collection of relevant documents. These documents were mainly produced by external organisations, including private consulting firms, academic research institutes and various Danish authorities. The documents include relevant reports, evaluations, recommendation papers and the like. The criteria for identifying documents was timeframe and relevance to the SSP networks within the counter-radicalisation context. The timeframe was 2011 until 2017, chosen because both SSP networks first adopted counter-radicalisation measures in 2011. The advantage of using such documents is that they are unobtrusive, meaning they are not created as a result of the research (Yin, 2009: 106). The desk research data provided useful information which underpinned the next stage of data collection.

Once the first round of data collection was completed, interviews were arranged with key personnel from the two networks. The aggregated data from the first round, together with the literature review, formed the basis of the interviews. The interview questions[3] were developed deductively, meaning that the inception of each question was based on the conceptual framework in this research.

The second stage of data aggregation was by semi-structured interviews with one key person from each SSP network.

The two interviewees were selected based on their role as SSP consultants in their respective networks. Both the SSP consultants are full time network employees responsible for maintaining full network functioning. They ensure agreements within the network are carried out, and may also help the network's actors if they require assistance in certain situations.

Furthermore, the two SSP consultants have each been working for the SSP for more than five years, and do not represent any of the actors in their network, reducing the likelihood of direct professional bias towards the SSP network or specific actors.

It should be noted that both interviewees preferred not to be mentioned by name in the research, and thus have been granted anonymity. It was also agreed that any unnecessary circulation of their statements and the information they provided would be avoided as far as possible.

[3] The topic list of the interview is added to this thesis (see appendix 1)

The interviews were conducted to collect data that is not present in publicly-available documents. Furthermore, the interviews provided the research with information that was otherwise hard to obtain, with the aim of better analysing the relationship between structure and counter-radicalisation outputs. The interviews additionally provided a degree of personal reflection on the part of those who maintain the functionality of the SSP networks on a daily basis.

The third stage of data collection was through the two SSP consultants. After the interviews, the two consultants provided access to documents that cannot be obtained by desk research. The documents provided were administrative documents such as progress reports, policy papers, proposals and other internal records relating to the SSP networks and their counter-radicalisation activities.

The two SSP networks provided a range of internal records. However, not all the documents were used, as many of them contained duplicate data or did not offer any relevant information. It should be noted that the Copenhagen SSP network provided more relevant information than the Aarhus SSP network did. This is a limitation for the research, as the aggregated data for this thesis was not balanced between the two cases. A full overview of the internal records which were used in the analysis is included as an appendix (see appendix 2).

4.4 Data Analysis

The aggregated data is assessed based on the analytical framework detailed above. A content analysis of the data is the method adopted, meaning the data was first categorised according to the indicators for the analytical framework. The next step was to process the data in order to sketch out the SSP networks' structural patterns and configuration. Afterwards, the counter-radicalisation outputs are measured based on what the SSP networks produce and what action they take in the field under study. The final step is to identify the predictor of the link between structure and outputs.

The analysis starts by means of a within case analysis; the Copenhagen SSP network is analysed first, after which the Aarhus case is examined. The two SSP networks are then compared to explore the similarities and differences in structural patterns and counter-radicalisation outputs.

The within case analysis is divided into three phases. The first phase identifies the key-actors, while the second phase explores the structure and the third identifies the counter-radicalisation outputs. Finally, a cross-case comparison of the two SSP is conducted to determine the degree of linkage between the two variables under observation.

Analysing the Key-actors

There are a considerable number of actors involved in both the Copenhagen SSP and the Aarhus SSP network working on counter-radicalisation. The different actors contribute to the SSP network in noticeably different ways. Given that the structure of the SSP networks is being analysed based on the interconnectedness of the actors, a thorough actor analysis is essential.

The key-actors are identified based on the extent to which they can act autonomously, and on their access to information which is important to the SSP network in the context of counter-radicalisation. The internal SSP documents and responses of the SSP consultants were used as data for the identification of the respective key-actors.

Analysing the Structure

After the key-actors have been identified, the next step is to explore the structure of the SSP networks. First, the type of the network is specified according to the security network types derived from the literature review. The collated data is used to identify the aim of the network, its inception and its geographical boundaries.

The second phase is the organisational design of the network, which comes in three different designs: shared governance, lead organisation and the NAO network design.

The organisational design of the SSP networks is determined based on interaction between the key-actors. The interaction between the actors in the network may be formal or informal. Formal interaction generally involves meetings, discussion sessions and the like, whereas informal interaction refers to interaction that is not scheduled in advance. Based on the interaction between the key-actors, the organisational design of the SSP networks can be readily identified. Thus, the organisational design allows for the identification of the SSP network’s nodes patterns.

The last phase of analysing the structure of the SSP networks in Copenhagen and Aarhus is their information sharing patterns. Information sharing refers to the way in which the network organizes its information gathering and sharing approach. Information sharing can be categorised as either all-channel or hub. This last piece of data completes the structure of the SSP network.

Analysing the Counter-radicalisation Outputs

The third and final step in the within case analysis is to assess the outputs of the two networks in question. The outputs refer to what the SSP networks actually do to prevent radicalisation among youngsters. They comprise the initiatives, services and programmes that the two SSP networks produce. The data used here includes the documents gathered by means of desk research together with the documents the SSP networks provided, as well as information from the two interviews.

Once the two within case analyses have been conducted, the next phase is the cross case analysis. In this final part, the findings from the two cases are compared and discussed within the context of the research question.

Analysing the Link between SSP Structures and Counter-radicalisation Outputs

When both structure and output have been satisfactorily analysed for both networks, the exploration of the linkage between them can be conducted. This is done by means of a direct comparison between the cases. If there are similarities in the structure of the two networks but their outputs are different, we may conclude that the structure does not have a significant impact on the outputs. On the other hand, if the structure and outputs are different, it may indicate a link between the two.

4.5 Reliability and Validity

This thesis relies on publicly available information from various organisations, semi-structured interviews and on documents provided by the SSP networks.

Given that counter-radicalisation and security networks are relatively new and complex phenomena, new sources of information can be expected to arise frequently. Naturally, this has the potential to affect the assumption underpinning the research. The reliability of this research is also challenged by the dynamics of the networks themselves. Networks can change rapidly, particularly as new actors join or leave, and thus a network's problem perceptions, interactions, processes, rules and so on are subject to fluctuation. As such, this research provides only a snapshot of the two SSP networks within a given timeframe.

In order to minimise this issue, and to increase the accuracy of the research, a systematic assessment of the link between the independent variable and the dependent variable will be carried out by means of data triangulation. Such triangulation necessitates the use of a variety of sources, something this study has actively sought to incorporate by using internal documents from the SSP networks, interviews with two SSP consultants and multiple publications from external third party actors. To improve the reliability of the paper's conclusions, the research makes its various steps as operational as possible, in terms of indicators, data collection and analysis, interview topics and so on.

Another issue which may potentially affect the reliability of the research is the neutrality of the two interviews. It is important to recognise that a certain level of bias is inevitable in the interviews, both on the part of the researcher and the interviewees. Subjectivity on the part of the researcher could conceivably have impacted the formulation of interview questions, and the assumption of there being a link between the two variables may have unintentionally influenced the interviews in the affirmative.

Beside reliability, it is important also to assess both the construct validity and internal and external validity of the study.

Construct validity refers to identifying the correct research strategy and measurements for the research (Yin, 2009: 41). As this paper attempts to explain the linkage between an SSP's network structure and its counter-radicalisation outputs, the explanatory nature of the study lends itself to a deductive research approach. Hence, the analytical framework of the research is based on pre-existing theories and concepts. The assumption of a relationship between structure and output is derived from the analytical framework, and a multiple case study is considered the most suitable means for testing the assumption.

An important question may be asked at this stage: What is rationale behind the assumption of the research? Internal validity in this context refers to the correct establishment of the relations between variables (ibid.). In this research, the deductive analytical framework measures to a certain extent whether a linkage exists between the independent variable (SSP structure) and the dependent variable (SSP outputs).

External validity, on the other hand, refers to whether the results of the research can be generalised (Yin, 2009: 43). It is crucial to acknowledge that the results of this thesis are specific to the context of SSP networks and counter-radicalisation. Since the field of security networks is dynamic, the nature of this type of research make it highly specific to a particular time and context.

This is not to say that that the results cannot be generalised at all. Although the statistical generalisability is limited, the conclusions generated by this research can be taken as an effort to identify the degree of causal patterns between network structure and output, thereby contributing to the literature on security networks.

5 Findings

5.1 Copenhagen SSP Network and Counter-radicalisation

In 2009, the Copenhagen municipality adopted its first counter-radicalisation strategy (DIIS, 2015: 32), forming the so-called VINK[4] division (BIF, 2009a). The VINK was initially a pilot project, gradually expanded over two years (ibid.). The main aim of the project was to gather knowledge and provide advice for professionals working with youngsters in the municipality on radicalisation issues (DIIS, 2015: 32). When the pilot project ended in 2011, Copenhagen municipality decided to transfer the VINK project into the SSP network, providing the network with additional resources to make the counter-radicalisation efforts permanent (BIF: 2009b; Copenhagen Municipality, 2016).

In the first part of the analysis the findings from the Copenhagen SSP case are presented and assessed. Initially, the key-actors in the SSP network in Copenhagen are identified based on their autonomy and access to irreplaceable information. Next, the structural patterns are examined according to the type of security network, and organisational and information sharing designs. Lastly, Copenhagen SSP's counter-radicalisation outputs are presented.

5.1.1 Key-actors in Copenhagen SSP Network

To assess properly the structure and outputs of the Copenhagen SSP network, it is crucial to first map out which actors are involved in the network's counter-radicalisation activities. The determination of whether an actor is a key-actor or just a sub-actor within a coalition of organisations depends on whether the actor in question can act on its own account in terms of counter-radicalisation, and whether it owns or has access to knowledge on which the SSP network relies.

After careful scrutiny of the SSP network in Copenhagen, numerous different actors were identified. Three were identified as key-actors: the Department of Child and Youth (DCY), the department of Social Services (DSS), both from Copenhagen municipality, and the local police (BUF, 2016; SOF, 2017; DKR, 2012). All three key-actors operate autonomously within the SSP network. All three take part in the network's decision-making, and all are involved in drawing up the network's vision and plans for the years ahead (BIF, 2016).

[4] VINK is abbreviation of **V**iden, **In**kusion, **K**øbenhavn (Knowledge, Inclusion, Copenhagen)

The rest of the actors does not take part in any decision-making processes within the SSP network in Copenhagen, nor do they have any direct influence on counter-radicalisation plans. Although these actors cannot be labelled as key-actors, most of them are sub-actors to the DCY and DSS (BUF, 2016; SOF, 2017).

The Department of Child and Youth's (DCY) Access to Knowledge

The DCY is the largest department in the Copenhagen municipality and has access to a range of information about the youngsters living in the area (BUF, 2017; SOF, 2017). The DCY administers the primary and lower secondary educational institutions in the municipality (BUF, 2012). Through the institutions and services it provides to Copenhagen residents, the DCY has access to personal information, which is the main source of the data and knowledge it brings to the SSP network.

As the DCY mainly administers the local education systems, it does not engage directly with the citizens. It is through the DCY's institutions, such as schools and leisure centres, that it source its information. It should be noted that many of these institutions are themselves directly part of the Copenhagen SSP network. However, they cannot act autonomously on matters relating to counter-radicalisation and are thus considered sub-actors of the DCY, which also acts on the behalf of the educational institutions in the decision-making processes of the SSP network (CPH SSP consultant, 2017).

The DCY's sub-actors can be divided in three main categories, each encompassing numerous institutions. All these sub-actors provide the department with important information and expertise, which then is brought to the SSP network (BUF, 2013a). The DCY's sub-actors are set out below:

- **Schools**: Nearly 60 schools, both public and private (including international, Islamic, Turkish, Arabic etc.).
- **Leisure centres**: Including youth clubs, after school care, sports and cultural clubs etc.
- **Special institutions**: Services for youngsters with particular needs, such as maladjusted youth centres, special schools for vulnerable youngsters, institutes for youth psychological counselling, and the like. (BUF, 2017).

The DCY has direct contact and dialogue with teachers, student consultants, school nurses and all the other frontline workers involved with children and youngsters' development and wellbeing.

Through the DCY, the SSP network in Copenhagen has access to crucial information about the youngsters in the education system (BUF, 2017). This personal data is not easily accessible for other actors, which puts the DCY in a critical and central position in the SSP network (CPH SSP consultant, 2017). For instance, each school has a student journal, where information regarding student behaviour and development is evaluated annually, and teachers are obliged to report to the DCY if a student changes drastically or expresses worrying ideas or behaviours (ibid.).

The Department of Social Services' (DSS) Access to Knowledge

Copenhagen municipality's Department for Social Services (DSS) provides a broad range of services to citizens. Through these services, the DSS has access to sensitive information about citizens, ranging from financial affairs to health problems (SOF, 2017). Like the DCY, the DSS also aggregates information from social service institutions. Some of these institutions are also a direct part of the SSP network, but they do not act autonomously. The DSS's sub-actors includes:

- **Centre for family and youth counselling:** Aims to help youngsters and their families to maintain good relations and manage conflict.
- **Centre for vulnerable neighbourhoods (ghettos):** Outreach work to help vulnerable citizens in finding jobs, new apartments etc.
- **Centre for social pedagogy and psychiatry**: Treats youngsters with social and psychological problems.
- **Centre for vulnerable youth and crime prevention:** Helps youngsters if they are vulnerable to criminal activities.
- **Centre for prevention and consultancy:** Helps youngsters if they are not in the education system, in the labour force, or are homeless.
- **Centre for foster care:** Placed youngsters in foster care when needed.
- **Centre for youngster and drug:** Helps youngsters with drug and alcohol abuse.
- **Unit for social benefits:** Helps citizens if they have financial problems, for instance if they cannot effort to pay rent or deposits, etc.

- **Centre of psychological home visits**: Visits psychologically vulnerable citizens regularly.
- **Centre for the Crime Prevention Council:** Helps youngsters exit from gangs, criminal groups, etc.
- **Crisis centre for vulnerable youngsters and families:** Provides youngsters a safe and anonymous place to stay, such as if their families are threatening them.

Throughout theses sub-actors, the DSS has information regarding the youngster's drug abuse, family matters, social control, financial situation, whether the youngster is or has been part of a criminal milieu and so on (SOF, 2017). All this unique information is crucial for the SSP network in identifying those who are radicalised or may be vulnerable to radicalisation (CPH SSP consultant, 2017).

Copenhagen Local Police's Access to Information

The local police have access to the most sensitive information about the citizens. They have access to the criminal records of the youngsters and their families, access to information regarding the behaviour of a person during probation or prison time, access to their travel habits such as departure and arrival information, easy access to the person's telephone and internet records and so forth. Furthermore, the local police in Copenhagen work closely with other law enforcement institutions, such as the prison and probation service and the Danish intelligence and security agency (PET), which also give them easy access to experience, knowledge and expertise and so on (Østjyllands Politiet, 2015). The other actors in the SSP network do not have the same degree of access to this information as the police, and thus the local police are another crucial partner in the SSP network. However, the information the local police have access to is not easily shared with the other actors in the SSP networks, as most of the information is highly confidential in nature (BIF, 2009b). Despite strict limitations to information sharing on the part of the local police, they are still categorised as a key-actor, first because they can act autonomously, but also because they provide essential input to the SSP network.

5.1.2 Copenhagen SSP: Type of Security Network

Having identified the key-actors, it is possible to determine what type of security network Copenhagen SSP is.

The four types of security network defined in the literature are local, institutional, international and technological security networks. Each of these network types has its own unique patterns and characteristics. However, one network may display characteristics of several network types. This is the case with the Copenhagen SSP network, which is readily identifiable as a local security network, but also displays some features of an institutional security network.

It is clear from analysis of the Copenhagen SSP that the network takes action locally. First of all, the network operates solely within the municipality's borders and mainly includes actors rooted locally.

The second reason is the purpose of the SSP network in Copenhagen. The aim of the network is to mobilise local public and private resources to find solutions to complex and wicked security problems. Furthermore, as the aim of the SSP network is also to exchange information regarding unlawful activities in local communities, the SSP network can be categorised as a local security network (DKR, 2012).

Nonetheless, there are some indicators that the Copenhagen SSP network is also an institutional security network. First, the network consists almost exclusively of public actors; few private organisations are involved. Moreover, state actors are the only ones privileged to take decisions on behalf on the network.

Despite displaying these limited characteristics of an institutional security network, the SSP network in Copenhagen is nevertheless most accurately categorised as a local security network.

5.1.3 Copenhagen SSP Network Organisational Design

Networks are generally organised according to three main designs: the shared governance network, lead organisation network and NAO (Kenis & Provan, 2009). The type of organisational design stems from the network's nodes and interconnectedness. Interaction within the Copenhagen SSP network in the context of counter-radicalisation happens in a variety of formal and informal ways. Assessment of this network interaction indicates that a structure is certainly in place.

Although the VINK division merged with the SSP network back in 2011, the VINK division continued as a special unit for the administration of counter-radicalisation efforts in the Copenhagen SSP (DIIS, 2015). The VINK division remains a separate and impartial administrative entity within the SSP network, focused solely on coordinating and managing the network's counter-radicalisations activities (ibid.).

Each of the key actors in the SSP network has a direct link to the VINK division, through which all interactions on counter-radicalisation issues must pass (Copenhagen Municipality, 2012). The VINK also sets the agenda for the weekly meetings in the SSP network (CPH SSP consultant, 2017).

In these meetings, the VINK division and the key-actors discuss new developments, specific cases, the programmes and services they provide, and other related matters (BUF, 2012). It is at these formal meetings that most of the network's counter-radicalisation activities are decided and evaluated.

In addition to the formal weekly meeting, the key-actors and VINK division also interact informally. The SSP network in Copenhagen stresses the importance of regular contact between the key-actors (CPH SSP consultant, 2017). To be certain that important information is not missed during informal contact between actors, the SSP network has established a framework for informal interaction (Copenhagen Municipality, 2013). The Copenhagen SSP consultant describes the framework as an agreement that ensures the VINK division is informed when actors interact with one another outside a formal meeting context (CPH SSP consultant, 2017).

Considering that the VINK division focuses solely on coordinating the Copenhagen SSP network's counter-radicalisations activities, together with the fact that both formal and informal interactions are overseen by the division, it may be concluded that the VINK division operates as an NAO for the SSP network in Copenhagen.

5.1.4 Copenhagen SSP Network Information Sharing Design

Whelan (2012) identifies two types of information sharing design, namely the all-channel design and hub design. In this regard, the VINK division plays a further important role: that of information aggregation and diffusion (BUF, 2016).

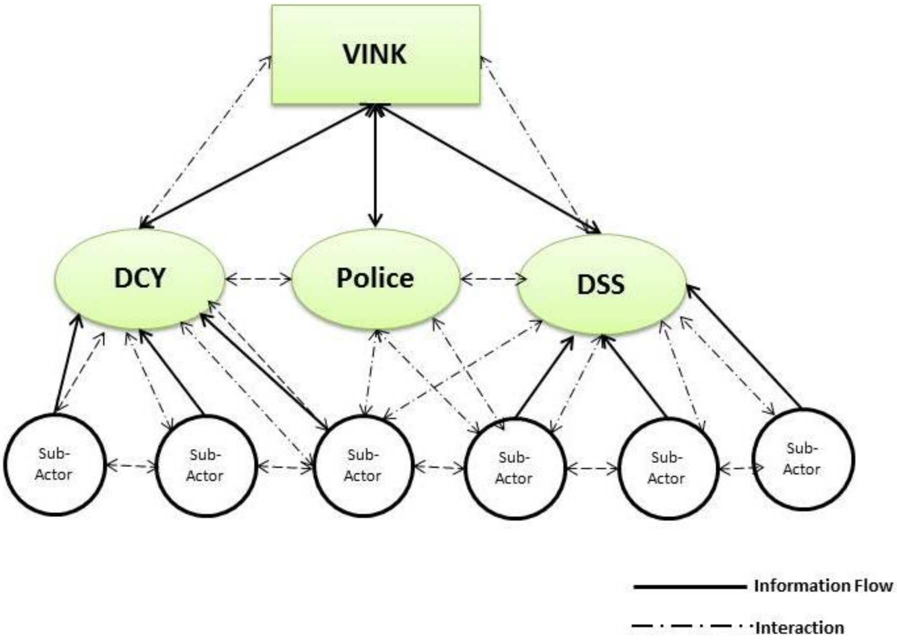
The VINK takes the leading role in ensuring that relevant information is collected and shared between the relevant actors in the network (ibid.). The division is therefore responsible for assessing what information should be shared, and with whom (CPH SSP consultant, 2017).

Each of the key-actors has access to sensitive personal information about citizens, and therefore the VINK division has devised an information gathering and sharing framework to avoid any form of information leakage (BIF, 2009b). The framework mandates that all information regarding radicalisation must pass through the VINK division, meaning key-actors shares information with the VINK alone, and the division assesses whether it should be passed on to other actors (CPH SSP consultant, 2017).

The SSP network has also a framework for handling non-sensitive information. This framework ensures the VINK division is always updated on the activities of the network's actors. If correspondence takes place between actors, the VINK is informed. For example, if the DCY is corresponding with the local police, the VINK will be copied on all communications (ibid.).

The centralised way in which information is managed by the VINK clearly indicates that the Copenhagen SSP network can be categorised as a hub design.

Figure 6: Copenhagen SSP Structure



5.1.5 Copenhagen SSP Network Counter-radicalisation Outputs

The SSP network in Copenhagen conducts a wide range of counter-radicalisation activities, from public information campaigns to mentoring radicalised individuals.

Strengthening the Awareness of Frontline Workers

One of the Copenhagen SSP network's flagship outputs is strengthening frontline workers' awareness of radicalisation among youngsters. Since 2011, the Copenhagen SSP network has developed a counter-radicalisation framework for frontline workers in the municipality to follow (Copenhagen Municipality, 2016). The municipality aims to conduct workshops for all frontline workers, to enable them to identify signs of radicalisation and give them the tools to address it when they encounter it among young people (ibid.).

The SSP network provides courses, workshops and conferences for all employees who work directly with youth in the municipality (BIF, 2016). Frontline workers are trained in how to spot a vulnerable person and what the next steps should be. They are also made aware of the SSP network's processes to give them an understanding of how the SSP handles the information they provide (CPH SSP consultant, 2017).

Since 2012, the Copenhagen SSP network has aimed to provide all frontline workers working with youths aged 15-20 with an awareness of radicalisation in Copenhagen and how to deal with it. By 2015, all frontline workers employed in schools and leisure centres in Copenhagen (approximately 1,500) had attended counter-radicalisation workshops provided by the network (Copenhagen Municipality, 2016).

Empowering Youngsters

The SSP network in Copenhagen also provides workshops and courses for youngsters to help them develop critical thinking skills and improve their ability to identify extremist propaganda (BIF, 2016). The workshops include themes like citizenship, democracy, critical thinking and use of social media (ibid.).

The workshops held by the Copenhagen SSP network are divided into two sections. The first is the specific workshop, tailored towards particular groups or communities, and the other is the general workshop for all pupils in the municipality (ibid.).

The specific workshop is geared toward communities and groups that are vulnerable to radicalisation.

The general workshops include all the youngsters in the municipality and are usually conducted in schools. The SSP network has held workshops between 2012 and 2015 for all senior classes[5], and continues to build upon previous workshops. Since 2011, 127 workshops for youngsters have been conducted by the SSP network in Copenhagen.

Dialogue with Communities and Civil Society

Ever since it was founded, the Copenhagen SSP network has made efforts to cooperate with local communities and civil society[6] (DKR, 2012). The network maintains a dialogue with local religious establishments (mainly mosques) and diverse minority organisations, in which local problems and challenges are discussed. Public debates are also conducted in vulnerable neighbourhoods, where different organisations and individuals discuss the issues openly, in order to challenge any radical ideas by developing counter arguments (CPH SSP consultant, 2017).

As radicalisation is a hot and politicised topic, confrontations may easily emerge. To avoid any form of escalation during dialogue with the local communities, the SSP network has developed a dialogue plan. This includes guidelines on how to monitor a debate, word usage, and how to keep a debate calm and respectful (Copenhagen Municipality, 2013).

Copenhagen Anti-radicalisation Hotline

Given the fact that a relatively high number of youngsters from vulnerable communities do not take part in any form of public educational or social institutions, a local telephone line has been established (Mht-consult, 2011). This hotline provides an opportunity for friends and relatives of a vulnerable person to call anonymously to the municipality if they are concerned about radicalisation.

The SSP consultant explains that this hotline is a crucial tool. People who are generally excluded from society and do not take part in local activities initiated by the SSP network are at risk of radicalisation without being noticed. Therefore, the hotline provides a means for the

[5] Approx. aged 12-16

[6] It is important to underline that these partnerships between diverse communities and the SSP network have been in place for years before counter-radicalisation become part of the SSP network. The cooperation between the SSP networks and the local communities in Copenhagen were created based on general crime preventive work, for which the SSP network is also responsible (DKR, 2012).

SSP network to gather information from anonymous callers who might not otherwise inform the authorities (CPH SSP consultant, 2017).

Since the VINK division became part of the SSP network in 2011, the hotline has seen an increase in the number of calls. Between 2011 and 2013 there was a total of 49 calls, of which 34 were assessed as crucial and led to a process being initiated (Copenhagen Municipality, 2014). In 2014, 60 calls were made to the hotline. In 2015 this number rose to 100, with 18 being assessed as crucial and 14 being identified as serious. In these cases, processes were started with the individuals of concern (BIF, 2016).

According to the Copenhagen SSP consultant, the reason for the rise in the number of calls is two-fold. The consultant suggested the increase is partly due to the SSP's campaign to advertise the hotline, and partly due to the Copenhagen shooting in February 2015 which raised concerns among local citizens about radicalisation (CPH SSP consultant, 2017).

Mentor-Mentee Programme

Mentors can play an important role in preventing radicalisation among youngsters (RAN, 2016). The role of a mentor in the Copenhagen SSP is to guide, motivate, be a role model and be a positive force in the life of a vulnerable youngster (Copenhagen Municipality, 2016). In order to establish a virtuous relationship between the mentor and mentee, the Copenhagen SSP requires that mentors possess certain personal qualities; this is intended to help the youngster identify him/herself with the mentor (CPH SSP Consultant, 2017). The SSP network has thus created a team of mentors who are divers in ethnic, gender, professional and religious background (ibid.).

The SSP network in Copenhagen ensures that mentors are reserved for those individuals who really need them. The mentor-mentee programme is therefore not the first option for the SSP network. Only if the youngster is assessed as being vulnerable to radicalisation is a mentor provided to them (CPH SSP consultant, 2017). Since 2012, 53 mentor-mentee relationships have been established, varying from between three and six months in length (ibid.).

Beside mentoring youngsters, the SSP networks have also provided mentors to parents with radicalised children. This initiative was launched in in 2014, since which time some 20 parents have been mentored (Copenhagen Municipality, 2015).

5.2 Aarhus SSP Network and Counter-radicalisation

The Aarhus municipality integrated its counter-radicalisation efforts into the local SSP structure in 2011 (DIIS, 2015: 32). Since then, the SSP network has taken several steps to deal with the emerging issue of radicalisation among local youngsters, including the development of various services and programmes for the target group. This section assesses the structure and activities of the Aarhus network. As with the analysis of the Copenhagen SSP, first the key-actors are identified, then the structure is explored, and lastly the outputs of the network are investigated.

5.2.1 Key-actors in Aarhus SSP Network

Numerous actors can be identified within the SSP networks in Aarhus in the context of counter-radicalisation. However, in keeping with the Copenhagen network, most of the actors do not operate autonomously but rather under different units of the Aarhus municipality, which also acts as a collective on behalf on the sub-actors (Aarhus Municipality, 2015).

Three key-actors can be identified in Aarhus SSP Network, namely:

1) The Unit of Learning and Development (ULD) - a unit under the department of child and youth in Aarhus municipality which represents educational institutions in the SSP network (FBU, 2016).
2) The Social Services Department (DSS) in Aarhus – another key-actor in the SSP network, as it works as a collective organisation for several sub-actors (SUV, 2017).
3) The last key-actor is the local police in Aarhus.

The Unit of Learning and Development's Access to Information

The Unit of Learning and Development (ULD) in Aarhus municipality has a central role in the SSP network, as it can act both on its own account and as an umbrella organisation for all the sub-actors within the education sector in the municipality. It is through these sub-actors that the ULD has access to personal information about pupils. The ULD's sub-actors can be divided into two categories:

- **Schools:** All schools in Aarhus municipality, both public and private.
- **Leisure centre:** All the youth institution such as sport and cultural clubs, after school care and youth drop-in centres.

As is the case in the Copenhagen SSP, the network in Aarhus has access to important information regarding youngsters in the municipality (FBU, 2016). The schools in Aarhus municipality have a database in which each pupil has a journal, updated regularly by school staff. The database contains personal information ranging from their grade to their behaviour in school (ibid.).

ULD has direct access to these journals which gives them a central role in the SSP network in Aarhus. The ULD is also in direct contact with frontline workers in the schools and leisure centres, who report to the ULD if they see signs of radicalisation among pupils (Aarhus SSP consultant, 2017).

The Department of Social Services' Access to Information

Aarhus municipality's Department of Social Services (DSS) provides a range of services to its citizens. Through these services, the DSS has access to sensitive information about citizens living in the municipality, sourced from the following organisations:

- **Family Centre:** Helps families to cope with familiar crisis and problems.
- **Youth Centre:** Helps adolescents if they have social or mental problems.
- **Child Centre:** An institution where children can stay short-term if there is trouble at home.
- **Centre for Alcohol Treatment:** Helps citizens overcome their alcohol problems, and provides counselling to relatives of individuals with alcohol problems.
- **Centre for Drug Treatment:** Helps citizens with drug abuse problems and their relatives.
- **Centre for Welfare and Care:** Provides shelter for citizens who are homeless or cannot stay at home for a while.
- **Centre for Vulnerable Adolescents:** A centre for youngsters who have asocial behavioural issues (SUV, 2017; FBU, 2017).

The DSS's privileged access to information, including sensitive information on problems like drug abuse, makes it a key-actor in the Aarhus SSP network.

Local Police's Access to Information

As is the case in Copenhagen, the local police in Aarhus also act on their own account, meaning no other entity acts on their behalf in the Aarhus SSP network. The Aarhus local police have the same access to sensitive information about the municipality's citizens as their counterparts do in Copenhagen. As the other actors in the SSP network have no direct access to this information, the local police in Aarhus are naturally a key-actor in the SSP network.

5.2.2 Aarhus SSP: Type of Security Network

An examination of the Aarhus SSP network and its actors allows us to easily eliminate international and technological security network types. Thus the Aarhus SSP is either a local security network or an institutional security network.

Since the purpose of the Aarhus SSP network is to mobilise local public and private resources to solve complex security problems, the network can be identified as a local security network. Moreover, the Aarhus SSP network operates exclusively within the municipality's borders and with local institutions and organisation.

5.2.3 Aarhus SSP Network Organisational Design

Each of the key-actors in the Aarhus SSP network has extensive experience of working together in the field of crime prevention in the municipality. Interaction among key-actors is therefore based on long-term relationships, suggesting stable cooperation with high levels of trust are the network norm (DKR, 2012).

Given that there is no clear division between counter-radicalisation activities and general crime prevention efforts, the interaction patterns are less structured in the Aarhus SSP than in the Copenhagen SSP. Like in Copenhagen, formal interaction in Aarhus includes weekly meetings (SBU, 2015). However, in these meetings the key-actors do not focus exclusively on radicalisation issues but also discuss general crime prevention work (Aarhus SSP consultant, 2017).

In addition to the formal weekly meetings there is regular informal contact between the key-actors (Aarhus SSP Consultant, 2017). This informal contact takes place since each of the key actors need the other actors for assessment and guidance (ibid.). Unlike in Copenhagen, the informal contact between key-actors in the Aarhus SSP network is not based on an agreed framework (ibid.). According to the SSP consultant in Aarhus, informal interaction between the key-actors happens regularly but not according to any pre-agreed format (Aarhus SSP Consultant, 2017).

Based on these findings, the organisational design of the SSP network in Aarhus as it relates to key-actors can be characterised as a shared governance network.

5.2.4 Aarhus SSP Network Information Sharing Design

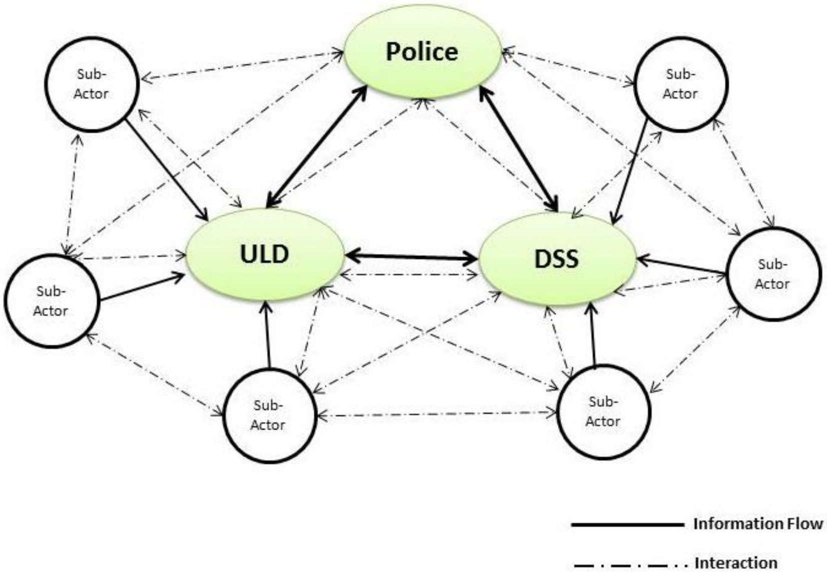
The Aarhus SSP network shares information regarding radicalisation in the same manner as the general crime prevention framework (Aarhus SSP Consultant, 2017). The information flow in the Aarhus SSP network regarding radicalisation issues passes through the key-actors in the network (Aarhus SSP consultant, 2017).

It would be fair to characterise the information flow in the Aarhus SSP as relatively loose. Most notably, there is no central actor that aggregates and assesses sensitive information about citizens prior to the information being disseminated. This means that sensitive information is shared with other actors without being assessed in advance.

Considering that the Aarhus SSP network does not clearly differentiate counter-radicalisation efforts from rest of its activities, the fact that every key-actor can share information with all the others may have negative implications for the Aarhus network, as information is subject to being misjudged or disseminated unnecessarily.

In terms of information sharing, the Arhus SSP network structure can therefore be considered an all-channel design.

Figure 7: Aarhus SSP Structure



5.2.5 Aarhus SSP Network Counter-radicalisation Outputs

Five types of counter-radicalisation output are produced by the Aarhus SSP. These are community outreach, workshops for youngsters, workshops for frontline workers, parents' networks and the mentor-mentee programme.

Community Outreach

Aarhus SSP network places significant emphasis on engagement with local communities. Their community outreach focuses on vulnerable communities in the Aarhus municipality (Aarhus Municipality, 2015). Since counter-radicalisation efforts fell into the purview of the Aarhus SSP, the network has initiated collaboration with various communities, as well as with civil and religious organisations. These communities and organisations have been chosen based on their ethnic and religious backgrounds (Aarhus SSP Consultant, 2017). For example, the counter-radicalisation outreach of the SSP network in Aarhus extends mainly to the Somali communities in Aarhus Municipality (Aarhus Municipality 2015). The Aarhus SSP consultant explains that it is primarily youngsters from this community who form part of the extremist milieu in Aarhus, and it therefore it makes sense to initiate dialogue with the community (Aarhus SSP Consultant, 2017).

In terms of religious organisations, the SSP network is in dialogue with the Grimhøj mosque in Aarhus. As mentioned previously, Grimhøj mosque is considered one of the main institutions in Denmark to have actively radicalised Muslim youngsters. Since 2014, the mosque and the SSP network have been in dialogue aimed at preventing radicalisation among youths in the local Muslim community (Aarhus Municipality, 2016a).

Aarhus SSP Workshops for Youngsters and Frontline Workers

Like Copenhagen, the Aarhus SSP network also provides workshops for both youngsters and frontline workers in the municipality. The workshops for young people aim to develop critical thinking skills so they can identify propaganda more readily online (Aarhus Municipality, 2016c).

The workshops for frontline workers aim to assist with capacity building, so they can better recognise signs of radicalisation and can deal with radicalised ideas in their daily contacts with the municipality's youngsters (ibid.). By the end of 2016, Aarhus SSP had conducted workshop for several schools and leisure centres in the municipality, attended by some 120 teachers and 23 leisure centre employees (ibid.).

The majority of schools in which workshops were held were those where a majority of pupils were from an immigrant background (Aarhus Municipality, 2016c). Similarly, workshops for frontline workers in leisure centres took place primarily in neighbourhoods with a high concentration of immigrants (ibid.).

Parents Network

In June 2013, the SSP network in Aarhus established the first network for parents whose children have been radicalised (Arhus Municipality, 2016b). The aim of the network is to ensure parents get the right support and develop the right tools to cope with the situation.

Since the creation of these parents' networks, seven meetings have been held with 10 to 15 participants in each meeting (Arhus Municipality, 2016b). The Aarhus SSP consultant explained that in the meetings, parents were able to share their feelings, experiences and how the process had affected them and their child (Aarhus SSP consultant, 2017). Aside from the formal meeting twice a year, the SSP network has no knowledge of whether the parents maintain informal contact (Aarhus SSP Consultant, 2017).

The parents' network is based on the principle of empowerment (Arhus Municipality, 2016b). The aim is not only to help parents to cope with a difficult situation, but also to focus on increasing parents' support resources and strengthening involvement in their children's lives (ibid) The workshop seeks to give parents the right tools to understand the challenges faced by their children, and to help them resist the lure of extremism (Aarhus SSP consultant, 2017).

Mentor-mentee programme

The Aarhus SSP mentoring programme was established at the same time as counter-radicalisation became a responsibility of the network (Aarhus Municipality, 2014).

In collaboration with PET, Aarhus SSP has trained ten mentors for their mentoring initiative (SBU, 2014). The aim of the mentor programme in Aarhus municipality is first and foremost to prevent the radicalisation of vulnerable youngsters and to motivate and support them in their daily lives (ibid.).

Since 2011, mentors have been assigned to 17 youngsters in the Aarhus municipality (SBU, 2015). Out of the 17, five were right-wing extremists and the rest were radicalised Muslims (ibid.).

5.3 Summation of the Findings

Based on the key-actor analysis, this research identified the Copenhagen SSP network as a local security network, featuring an NAO organisational network design in which information is gathered and shared centrally around a hub. Six counter-radicalisation outputs were identified, namely the strengthening of frontline work, empowerment of youngsters, dialogue with vulnerable communities and civil society, a counter-radicalisation hotline and mentoring for youngsters and their relatives.

Three key-actors were also identified in the Aarhus SSP network, which was designated a local security network. The Aarhus case exhibits a shared governance organisational design, with an all-channel information sharing framework. The counter-radicalisation outputs identified were community outreach, workshops for youngster and frontline workers, a parents' network and a mentor programme.

Table 4: Overview of findings

Network Structure Patterns	Copenhagen SSP	Aarhus SSP
Security Network Type	*Local Security Network*	*Local Security Network*
Organisational Network Design	*NAO*	*Shared Governance*
Information Sharing Design	*Hub*	*All-Channel*
Counter-radicalisation Outputs	**Copenhagen SSP**	**Aarhus SSP**
Types of Outputs	• *Workshop for frontline workers* • *Workshop for youngsters* • *Dialogue with communities* • *Mentoring youngsters* • *Mentoring parents* • *Hotline*	• *Workshop for frontline workers* • *Workshop for youngsters* • *Dialogue with communities* • *Mentoring youngsters* • *Parents' network*

6 Comparison

Analysis of the two SSP cases finds clear differences in key aspects of their respective network structures. Specifically, the organisational and information sharing designs in the Copenhagen and Aarhus SSPs contrast starkly with one another. Nonetheless, to a great extent the two networks produce similar counter-radicalisation outputs.

SSP Networks Patterns Connotation to Counter-radicalisation Outputs

The constituent actors of the two SSP networks have changed little since the networks were created (DKR, 2012). Since the inception, the two networks haven been acting locally, thus both the cases were identified as local security networks.

Three key-actors were identified in both Copenhagen and Aarhus. These key-actors are very similar in terms of their position and access to crucial information. The key-actors have a central role in their respective networks, taking part in decision-making processes and drawing up networks strategies and implementation plans.

The actors' positions seem to have remained essentially the same after the introduction of counter-radicalisation as a new field of responsibility, as the three key-actors were still the central nodes in both networks. In neither case did the sub-actors play any role in the fundamental processes of the networks, nor did they have any direct influence on developing counter-radicalisation outputs.

Despite the passive role of the sub-actors, they nonetheless provide the networks with important information. This is especially true of the sub-actors DCY in Copenhagen and ULD in Aarhus. The SSP consultant in Copenhagen explained: "*Teachers and other frontline workers are those who know the youngsters the best. Their knowledge about the youngsters is crucial for our work in the SSP"*. The consultant's counterpart in Aarhus concurred that "*schools and other day care institutions are essential for the SSP network"* (Aarhus SSP Consultant, 2017).

Although both SSPs recognise the importance of some sub-actors in the context of counter-radicalisation, the sub-actors are not included in decision-making processes nor are they involved in the development of counter-radicalisation efforts.

Organisational Design

Despite their similarity in outputs, the organisational designs of the two SSP networks are very different. The Copenhagen and the Aarhus SSP networks are highly distinct from one other in this regard, as the Copenhagen SSP's counter-radicalisation activities are centralised around a single entity (VINK) whereas the Aarhus SSP network organises them much more loosely.

In the case of Copenhagen, various interaction frameworks have been established. The frameworks provide the SSP with a stable and well-defined working structure and are well-integrated into the network. For example, the Copenhagen SSP network has an interaction mechanism which gives clear guidance on which actors should take which steps in particular situations, and describes each step to be taken in detail (BUF, 2012).

Mechanisms are also in place in the Aarhus SSP, but less streamlined as there is no central administrative unit in place to coordinate them. The counter-radicalisation efforts are steered by the three key-actors.

Information Sharing Design

The two networks have distinct information sharing designs, Copenhagen using a hub design and Aarhus operating on an all-channel design. In Copenhagen, the VINK division functions as the central entity to administer information flows, whereas in Aarhus all three key-actors administer the information together.

Although both SSPs are local security networks with similar counter-radicalisation outputs, their organisational and information sharing designs are different. However, these structural differences do not affect the networks' outputs.

7 Conclusion

This thesis has sought to ascertain the degree to which an SSP network's structure impacts its counter-radicalisation outputs. Contrary to the underlying assumption of this research, the dissimilarities in the networks structure did not influence the outputs in these two cases. The outset of this research was the question *"to what extent does the structure of the SSP network have an impact on counter-radicalisation outputs in the Copenhagen and Aarhus SSPs?"*. On the basis of the findings, it is argued that a relationship cannot be established between network structure and network outputs.

The results of this research may be of value both to the literature and in practical terms. From a theoretical perspective, the findings contribute to the existing literature by investigating the relationship between network structure and output. First, the research shed light on counter-radicalisation efforts within network settings. The literature on counter-radicalisation networks is relatively novel. The findings can therefore be a starting point for any subsequently research in this regard. Secondly, these results are noteworthy since they demonstrate that researchers should avoid focusing on a single structural characteristic, but should look at many different structural features and their joint effect on the outputs.

Moreover, the findings question some of the statement that can be found in the network literature. For example, Kenis and Provan (2009) argue that a specific form of organisational design produces a specific result. However, the findings question this statement, as the research suggests that two different organisational designs can also produce the same results. Additionally, the findings have also challenged Whelan's (2012) argument regarding information sharing designs in security networks. The research has shown that, regardless of the information sharing design, the output of the network has not been influenced by it.

In practice, the findings provide direction on how SSP networks can maximise their outputs. From the managerial perspective, this research provides possible guidelines for what the networks should refrain from if they want to changes their output, namely: avoid focusing on network structure.

As the networked approach to Counter-radicalisation is on an initial stage, this research has overall brought new information forward, in term of the network structure, outputs and the absence of a link between them.

8 Further Research

The conclusion of this research rejected the assumption of a linkage between structural patterns and counter-radicalisation outputs. This thesis has presented a considerable amount of information on SSP networks structure within the field of counter-radicalisation, which can be a starting point for further research in this regard. This research exclusively focused on the relationship between the structure and the outputs, thus several themes were left unexplored throughout this research as they fell outside the scope of this research. For this reasons, three suggestions are made for further research.

1) Type of Actors and Outputs

The first suggestion relates to the actors' positions in the two SSP networks under study. The finding indicates that the same actors have dominated the networks since their inception; thus a general habit of dealing with complex security problems may have been standardised, and persisted when counter-radicalisation outputs were developed in the two SSP networks.

On the basis of the indication here, there is a risk that by sticking too rigidly to existing policies and procedures the networks may not benefit from the new initiatives and perspectives that a network 'reboot' could generate. In other words, if the SSP network were to reconfigure the actors' positions, the problem perception of the well-established actors may be challenged by the newcomers. New and original outputs might therefore emerge. The similarity between counter-radicalisation outputs could be partially explainable by the entrenchment of long-term organisational habits.

By investigating the relationship between network and its outputs, the research can provide great insight into how the SSP networks counter-radicalisation outputs are produced. Such a research could be performed trough a cross-case actor analysis. This analysis would therefore reveal whether the control of the same actors in the SSP networks actually affect the outputs.

2) Network Norms and Outputs

With the decades of experience acquired by the two SSP networks, the level of intra-network conflict is minimum, and it seems the actors in both cases have developed similar norms, values and working methods.

In light of this, the similarities in counter-radicalisation outputs may be a product of shared norms and working processes. For example, it appears that counter-radicalisation outputs do not differ much from more general crime prevention outputs of the two SSP networks. When looked in the light of matured collaboration, the SSPs' counter-radicalisation outputs may simply be a reflection of entrenched habits in the networks. Put simply, the notion that 'things are a certain way because they have always been that way' may have a role to play in this instance.

A research on the relationship between network norms and the outputs would provide insight in to what degree the norms have an effect on the outputs. Such a research could take shape by exploring the differences in SSP networks norms and their counter-radicalisation outputs.

3) Network Structure and the Volume of the Outputs

This Thesis has focused on what kind of outputs the two SSP network produce, and not on the volume of them. Therefore, the last suggestion for further research is to take a further step and investigating to what extent the network structure has an impact on the volume of the outputs.

In this thesis, it appears that the number of counter-radicalisation outputs in Aarhus is much less than in Copenhagen. For instance, both SSPs aim to strengthen the counter-radicalisation capacity of frontline workers, but in Copenhagen 1,500 frontline workers have completed relevant workshops whereas in Aarhus the number is just 143. It is also worth noting that the Aarhus SSP has trained ten mentors, but only 17 mentor-mentee relationships have been initiated since 2011. There are two plausible explanations for this: either there is very little need for mentors in the community and the SSP trained more than necessary, or the SSP is not effective at identifying vulnerable youngsters in need of mentoring. Either way, this may be an indication that the less centralised network model in Aarhus might have an impact on the volume on the outputs.

The difference in the volume of outputs may be influenced by several factors, but it is plausible to assume that the centralised organisation of the Copenhagen SSP provides an advantage in generating counter-radicalisation outputs.

Another factor for the differences in the volume might be the SSPs information sharing design. For instance, it may be argued that the way the Copenhagen SSP have structured their information administration is less likely to lead to information withhold or information overload. With one entity steering all the information between actors, the right information can reach the right actors at the right moment. This indicator may help explaining the difference in output volume between the SSPs, since the Copenhagen SSP may simply be more efficient.

By contrast, the all-channel design used by the Aarhus SSP means that three entities are involved in the administration of network information. This may have an effect on the volume of counter-radicalisation outputs produced by the network. Compared to Copenhagen, Aarhus has fewer people using their services and programmes. In almost all the counter-radicalisation outputs identified, more than twice as many people have engaged with those produced by the Copenhagen SSP than the Aarhus SSP.

An analyses on the relationship between structure and the quality of the outputs can be conducted in various form. Either, the typology of this research can be used to determine the link between structure and the quality of the outputs, or the typology can be separated and thereby focus either only on the organisational design's or the information sharing design's impact on the quality of the outputs.

9 Limitations of the Research

This research has put forward several findings relating to the link between an SSP network's structure and its outputs. However, it is important to acknowledge the limitations that may have affected the research outcomes. This research has been limited by a number of factors, both methodological and external.

The first limitation is the choice of methodology. The research based its findings mainly on data produced by key-actors in the network, which may have affected how the interaction patterns in the two networks were analysed. If data from other actors from the SSP networks was also included, the network structure may have appeared different. The second limitation in the research design was the selection of interviewees. As the two consultants' main function is to maintain and manage the SSP networks, they can only observe the interaction between actors from a distance. If the research had included key-actor perceptions of the interaction, it may have produced other results.

An additional limitation to this research is its weakness in limiting the impact of external factors on counter-radicalisation outputs. As both the SSP networks' outputs are broadly similar, the outputs may both have been influenced by external factors. For example, the Danish central government's recommendations on countering radicalisation are not dissimilar to the services and programmes provided by the SSP networks in question. Thus, the outputs may have been heavily influenced by national recommendations rather than by the SSP networks' structures.

This research allows us to hypothesise how the structure of security networks in terms of type, interaction and information sharing can jointly influence their outputs. However, the findings cannot speculate about the nature of this effect, i.e. the reasons why the structural patterns have an influence on outputs. This research can provide an initial foundation and reference point; future studies with differing research designs and data analysis techniques may be better placed to explain the effect.

10 Bibliography

- Aarhus Municipality (2015) *Forlig om budgettet for 2016 til 2019*, September. https://www.aarhus.dk/~/media/Dokumenter/Borgmesterens-Afdeling/Budget-og-Regnskab/Budgetforlig-2016/Budgetforlig-2016-2019.pdf
- Aarhus Municipality, (2013), *Aarhus-modellen,* Notat, Socialforvaltningen og Børn og unge, Århus Kommune, Nov.
- Aarhus Municipality, (2014), *Værdiramme for indsatsen mod radikalisering tiltrådt af magistarten,* Borgmesterens Afdeling, June.
- Aarhus Municipality, (2015), *Forebyggelse af radikalisering og diskrimination i Århus,* Socialforvaltningen og Børn og unge, Århus Kommune, November.
- Aarhus Municipality, (2016a), *Indberetning,* Notat, Børn og ungeforvaltning, Århus Kommune, Jan.
- Aarhus Municipality, (2016b), *Indberetning,* Notat, Socialforvaltningen, Århus Kommune, Januar.
- Baker-Beall, C., Heath-Kelly C. & Jarvis, L. *Introduction* In "Counter-Radicalisation – Critical Perspectives", edited by Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis, pp. 1-13, Routledge critical Terrorism Studies, Oxon & New York.
- Bartlett, J., Birdwell, J. & King, M. (2010), *The edge of violence – a radical approach to extremism*, DEMOS, London.
- Berlingske Research, (2015), "*Tidslinje: Sådan Forløb Muhammed-Krisen",* Berlingske January 7, 2015. Accessed November 22, 2016. http://www.b.dk/globalt/tidslinje-saadan-forloeb-muhammed-krisen
- BIF (2009a) *Program for målrettet inclusion til forebyggelse af radikalisering og ekstremisme,* Beskæftigelses- og Integrationsforvaltningen, Memorandum, Copenhagen Municipality, Doc. Nr. 2009-221313.
- BIF (2016) *VINK – Styrket indsats mod radikalisering - Handleplan 2016-2017*, Beskæftigelses- og Integrationsforvaltningen, Copenhagen Municipality, April.
- BIF, (2009b), *Forebyggelse af radikalisering og ekstremisme – juridiske rammer for et målrettet inklusions program*, Beskæftigelse- og integration forvaltning, København kommune, April.
- BIF, (2012), *Notat, Doc. Nr. 2012-530268*, Beskæftigelse- og integration forvaltning, København kommune.
- BIF, (2014), *Notat, Doc. Nr. 2014-007925*, Beskæftigelse- og integration forvaltning, København kommune.
- BIF, (2016), *Handleplan 2016-2017, VINK – Styrket indsats mod radikalisering,* Beskæftigelse- og integration forvaltning 3. kontor, København kommune, April.
- Borg, O. (2015), "*Dreng tvangsfjærnet af frygt for radikalisering",* Jylland-Posten, February 28. Accessed December 09, 2016. http://jyllands-posten.dk/indland/ECE7494670/Dreng-tvangsfjernet-

af-frygt-for-radikalisering/

- BUF (2017), *Børn og – ungdomsforvaltningen*, Notat, Doc. Nr. 2017-045834
- BUF, (2012), *Notat, Doc. No. 2012-673569*, Børn og – ungdomsforvaltningen, København kommune.
- BUF, (2013a), *Notat, Doc. No. 2013-070099*, Børn og – ungdomsforvaltningen, København kommune.
- BUF, (2013b), *Notat, Doc. No. 2013-070569*, Børn og – ungdomsforvaltningen, København kommune.
- BUF, (2016), *Notat, Doc. No. 2016-970588*, Børn og – ungdomsforvaltningen, København kommune.
- Butt R. & Tuck T. (2014), *European Counter-Radicalisation and De-radicalisation: A Comparative Evaluation of Approaches in the Netherlands, Sweden, Denmark and Germany*, Institute for Strategic Dialogue, Cross-Country Evaluation Report.
- Copenhagen Municipality (2012) *Forebyggelse af Radikalisering – Strategi og Handleplan*, Copenhagen, May.
- Copenhagen Municipality (2013) *Københavns Kommunes Indsatser til Forebyggelse af Radikalisering – Strategi og Handleplan*, Copenhagen, May.
- Copenhagen Municipality (2014) *Københavns Kommunes Indsatser til Forebyggelse af Radikalisering – Strategi og Handleplan*, Copenhagen, June.
- Copenhagen Municipality (2015) *Københavns Kommunes Indsatser til Forebyggelse af Radikalisering – Strategi og Handleplan*, Copenhagen, May.
- Copenhagen Municipality (2016) *Københavns Kommunes Indsatser til Forbyggelse af Radikalisering – Strategi og Handleplan*, Copenhagen, May.
- Coyne, R. (2005) *Wicked Problems Revisited*, Design Studies, Vol. 26 No. 1, pp. 5-17.
- Crawford, A. (2006) *Networked Governance and the Post-regulatory state? – Steering, rowing and anchoring the provision of policing and security*, Theoretical Criminology, vol. 10 (4), pp. 449-479.
- Dalgaard-Nielsen, A. (2016), Countering Violent Extremism with Governance Network, *Perspective on Terrorism*, vol. 10. No. 6, pp. 135-139.
- DIIS, (2015) *The Danish Approach to Countering and Preventing Extremism and Radicalisatin*, Dansish Institute for International Studies, Report No. 2015:15, Copenhagen.
- DKR, (2012) *SSP Cooperation – Basis and Organization*, Danish Crime Prevention Council, Glostrup. Accessed October 20, 2016. http://www.dkr.dk/sites/default/files/Ssp-folder_UK_WEB.pdf
- Dupont, B. (2004) Security in the Age of Networks, *Policing & Society*, vol. 14, No. 1, March, pp. 76-91.
- Dupont, B. (2006), Delivering security trough network: Surveying relational landscape of security managers in an urban setting, *Crime, Law & Social Chance*, vol. 45, pp. 165-184.

- Dutch Ministry of Security and Justice, National coordinator for Security and counterterrorism & Ministry of Social Affairs and employment (2014), *The Netherlands comprehensive action Programme to Combat Jihadism- overview of measures and actions.* https://english.nctv.nl/binaries/def-a5-nctvjihadismuk-03-lr_tcm32-83910.pdf
- Edwards, P. (2015) *How (not) to create ex-terrorist: Prevent as ideological warefare,* In "Counter-Radicalisation – Critical Perspectives", edited by Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis, pp. 54-70, Routledge critical Terrorism Studies, Oxon & New York.
- El-Said, H. (2015), *New Approaches to Countering Terrorism – Designing and Evaluating Counter radicalisation and De-Radicalisation Programs,* Palgrave Macmillan, New York.
- FBU, (2016), *SSP Samarbejdet,* , Børn og ungeforvaltning , Aarhus Kommune.
- FBU, (2017), *Børn og unge arbejdes områder og organisering,* Aarhus Kommune.
- Fischbacher-Smith, D. (2016), Framing the UK's counter-terrorism policy within
- the context of a wicked problem, *Public Money and management,* vol. 36, no.6, pp. 399-408.
- Gerring, J. (2007), *Case Study Research – Principles and Practices,* Cambridge University Press, New York.
- Goldsmith, S. & Eggers, W. D. (2004) *Governing by Network – The new shape of the public sector,* Brookings Institution Press, Washington DC.
- Head, B. W. & Alford, J. (2015) Wicked Problems: Implications for Public Policy and Management, *Administration & Society*, Vol. 47(6), pp. 711-739.
- Higgins, A. (2014) "*For Jihadists, Denmark Tries Rehabilitation*", New Work Times, December 13. Accessed November 22, 2016. http://www.nytimes.com/2014/12/14/world/for-jihadists-denmark-tries-rehabilitation.html?_r=0
- Home Office, (2011), "*Prevent Strategy*", HM Government, London. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
- Jakobsen, S. F. & Jensen, S. (2011) *Fra bekryming til handling I arbejdet med unge og radikalisering,* Rehabilitation and Research Centre for Torture Victims, Report.
- Kenis, P.N. & Provan, K. (2009), Towards an Exogenous Theory of Public Network Performance, *Public Administration*, Vol. 87 (3), pp. 440-456.
- Klijn, E. H. & Koppenjan, J. (2016) *Governance Networks in the Public Sector,* Routledge, Oxon & New York.
- Klijn, E., Steijn, B. & Edelenbos, J. (2010), The Impact of Network Management on Outcomes in Governance Networks, *Public administration,* Vol. 88 (4), pp. 1063-1082.
- Kundnani, A. (2015) *Radicalisation – The journey of a concept,* In "Counter-Radicalisation – Critical Perspectives", edited by Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis, pp. 14-35, Routledge critical Terrorism Studies, Oxon & New York.
- Lindekilde, L. (2015a) Dansk forbyggelse af ekstremisme og radikalisering 2009-2014: udviklingstendenser og fremtidige udfordringer, Politica, Vol. 47, No. 3, pp. 424-444.

- Lindekilde, L. (2015b) *Refocusing Danish Counter-radicalisation Efforts – An analysis of the (problematic) logic and practice of individual de-radicalisation intervention,* In "Counter-Radicalisation – Critical Perspectives", edited by Christopher Baker-Beall, Charlotte Heath-Kelly and Lee Jarvis, pp. 223-241, Routledge critical Terrorism Studies, Oxon & New York.
- Nielsen, C. (2015) *"Hjernevask og radikalisering i Grimhøjmoskeen",* Politiken, January 16. Accessed November 18, 2016. http://politiken.dk/debat/kroniken/premium/ECE2513130/hjernevask-og-radikalisering-i-grimhoejmoskeen/
- Norwegian Ministry of Justice and Public Security (2014), *Action Plan against Radicalisation and Violent Extremism,* *https://www.regjeringen.no/contentassets/6d84d5d6c6df47b38f5e2b989347fc49/action-plan-against-radicalisation-and-violent-extremism_2014.pdf*
- Østjyllands Politiet, (2015), Handlingsplan for en sammenhænge indsats I forhold til ungdomskriminalitet I Aarhus kommune, Østjyllands Politiekreds, June.
- PET (2015), *"Terrortruslen mod Danmark fra udrejste til Syrien/Irak, Center for Terroranalyse",* PET, October. Accessed November 21, 2016. https://www.pet.dk/Nyheder/2015/~/media/Syrien20151023/TerrortruslenfraudrejstetilSyrienogIrakuklpdf.ashx
- PET, (2016), "*Vurdering af terrortruslen mod Danmark, Center for terror analyse, Politiet efterretningstjeneste*," April 28. Accessed December 12, 2016. https://www.pet.dk/Nyheder/2016/~/media/VTD%202016/20160428VTDpdf.ashx
- Provan K., & Milward, B. (2001), Do network Really Work? A Framework for evaluating Public-sector organisational Networks, *Public Administration Review,* Vol. 61, issue 4, pp. 414-423.
- Raab, J., Mannak, R., & Cambre, B. (2013), Combining Structure, Governance, and context: A Configurational Approach to Network effectiveness, *Journal of Public Administration Research and Theory,* vol. 25, pp. 479-511.
- RAN (2016) *Developing a local prevent framework and guiding principles,* RAN Policy Paper, Radicalisation Awareness Network, November.
- Regering, (2016) *Forbyggelse og Bekæmpelse af Ekstremisme og Radikalisering – National Handlingsplan.* October.
- Rittel, H. W. & Webber, M. M. (1973) Dilemmas in a General Theory of Planning, *Policy Sciences* vol. 4, pp. 155-169.
- SBU, (2014), *Forebyggelse af radikalisering og diskrimination i Århus,* Socialforvaltningen og Børn og unge, Århus Kommune, April.
- SBU, (2015), *Forebyggelse af radikalisering,* Socialforvaltningen og Børn og unge, Århus Kommune.
- SBU, (2016), *Forebyggelse af radikalisering,* Socialforvaltningen og Børn og unge, Århus Kommune.

- Schimd, A. P. (2013) *Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, International Centre for Counter-Terrorism – The Hague, Research Paper, March, The Hague.
- Servicestyrelsen, (2008), Kortlæggelse af Kommunernes SSP-Samarbejde, November. http://www.ft.dk/samling/20081/almdel/kou/spm/15/svar/584370/616626.pdf
- SFI (2014) *Antidemokratiske Og Ekstremistiske Miljøer I Danmark*, Det Nationale Forskningscenter For Velfærd, doc. Nr. 14:19, Copenhagen.
- Socialudvalg (2016), *Budget, Doc. Nr. 2016-0064503, Copenhagen Municipality*, Mart. *https://www.kk.dk/sites/default/files/edoc/ab306446-b4d4-4658-bc7c-43a3592941b6/1671bc89-9459-44c0-a4d7-b6db78828d0e/Attachments/14856036-17583841-8.PDF*
- SOF, (2017), *Socialforvaltningens Organisationdiagram 2016*, København Kommune, Doc. Nr. 2017-3491245
- Sorensen, E. & Torfing, J. (2008), *Theoretical Approaches to Governance Network Dynamics*. In Theories of Democratic Network Governance, edited by Eva Sorensen and Jacob Torfing, Palgrave Macmillan, New York.
- SSP-Samrådet (2014), *Militant Ekstremisme I forebyggelsesperspektiv – Analytisk vinkel på radikalisering*, SSP-Samrådet Årsmøde, Mart. http://www.ssp-samraadet.dk/media/1120/kasperno.pdf
- SUV, (2017), *Social forvaltning samarbejdspartner*, Aarhus Kommune.
- The Danish Government (2014) *Prevention of Radicalisation and Extremism – Action Plan*, September.
- Turrini, A. Daniela C., Francesca F. and Greta Na (2010), Networking Literature About Determinants of Network Effectiveness. *Public Administration*, vol. 88 pp. 528-550.
- Vidino, L. & Brandon, J. (2012) *Countering Radicalisation in Europe*, The International Centre for the Study of Radicalisation and Political Violence, A Policy Reports, London.
- Walters, W. (2004) Some Critical Notes on Governance, *Studies in Political Economy*, vol. 73, Spring/Summer.
- Whelan C. (2015) Managing Dynamic Public Sector Networks: Effectiveness, Performance, and a Methodological Framework in the Field of National Security, *International Public Management Journal*, Vol. 18 (4), pp. 536-567.
- Whelan, C. (2012), *Networks and National Security – Dynamics, Effectiveness and Organisation*, Ashgater Publishing Company, Farnham.
- Yin, K. Robert (2009) *Case Study Research – Design and Methods*, SAGE Publications, Forth edition, London.