Designed or Emergent - A Social Network Analysis of two prolific Terrorist Networks in the context of Dark Networks

Author:	Matthijs J. Huijing
Student number:	2394987
Supervisor:	R. Torenvlied
Date presented:	17-06-2022
Programme:	Management Society and Technology
Institution:	University of Twente
Location:	Enschede
Word Count:	10654

Abstract

This bachelor thesis answers the question: To what extent does the literature of dark networks accurately predict the structure of Islamic extremist terrorist networks and how comparable are the network structures of the Islamic extremist terrorist network to one another? To answer that question, the thesis uses a literature review in combination with a social network analysis on two case studies. The case studies used in this thesis are the 9/11 network and the Paris/Brussels network. They were selected because of their well documented history and prolific impact on society. The social network analysis found that the network structures of both cells were significantly different. The 9/11 network perfectly matches the concept of dark networks, whereas the Paris/Brussels network does not. It is likely that the 9/11 network is a designed network as it has a hub and spoke network structure that is ideal to function as a dark network. However, the Paris/Brussels network has an all spoke network structure which makes it likely that it is an emergent network. Yet, both meet the other requirements of the concept of dark networks, while the theory of dark networks only predicts one structure type. Thereby, the concept should be slightly adjusted so that it no longer aims itself specifically at designed networks but also emergent networks.

Table of Contents

1. Introduction

1.1 The issue of Muslim extremism

The impact of jihadism on the first two decades of the 21st century is not to be understated. However, the armed conflicts between Muslims and non-Muslims has been around for much longer (Hegghammer 2010). The form in which it is expressed today has been growing since the 1940s, yet little is known about that era of jihadism as the field is understudied (Hegghammer 2010). The first well studied change in jihadism after the Second World War, was the rise of foreign fighters, it stems from the 1980s. Foreign fighters are fighters that join the fight from their respective domestic countries to join a war in a foreign country. With the rise of these so-called foreign fighters followed the rise of terror attacks on domestic soil. However, as Hegghammer (2010) concludes, while foreign fighters are distinct from insurgents and terrorists, most terrorists were at one point in their lives foreign fighters. Apart from a past as foreign fighters, most terrorists were also indoctrinated or recruited in Western countries (Hegghammer 2010). In foreign countries and closed communities in the west extremist ideologies of the jihadists remained unchallenged and flourished. Thus increasing the ease to set up a terrorist network.

Eventually ideologies in the Muslim extremist worlds shifted to conducting attacks on Western society, prioritizing the United States of America and the European continent (Gunratna 2004). The unchecked terrorist networks and a new orientation towards Western society has led to jihadist networks to focus specifically on harming Western society. The drivers for these attacks consist of multiple goals: the formation of a strong international identity, forcing political decisions and damaging or even halting military operations and diplomatic relations (Federal Bureau of Investigation 2022).

The prolific group that became renowned as the international vanguard of Muslim extremist terrorism is Al Qaeda. The first attack conducted on American soil was the bombing of the World Trade Center in 1993 (Federal Bureau of Investigation 2022). This attack was aimed to bring down the World Trade center, but it had failed. The main perpetrator of the group had sent the New York Times his motives in a letter. These motivations were to stop the military, political and economical assistance to Israel, to halt all diplomatic relations with Israel and not to interfere with any of the interior affairs of countries in the Middle East (Gunratna 2004).

The respective motive for these attacks became a recurring pattern in the terrorist attacks that followed in Europe in the early 2000's (Gunratna 2004). The people that were affiliated with Ramzi Yousef, the main perpetrator of the 1993 attacks, became high ranking members in the new organization called Al Qaeda. This new organization quickly became known as an international threat and prolific terrorist organization due to the destructive September 11 attacks. Because of the 9/11 attacks, terrorism became an international focus point on which many resources were spent to get a better understanding of how to combat this 'new' problem. Among those resources was scientific research. Due to the sudden spike in scientific interest, the phenomena of terrorism has been massively researched over the course of the 2000's, often focusing on Al Qaeda specifically.

In the year 2011, internal conflict rose to a boiling point in Syria (Shamieh et al. 2015). More and more people started to oppose the rule of Assad and began to rebel against his regime. The largest among the groups that rebelled was the Islamic State Iraq Syria (ISIS). This organization originated from Abu-Musab Al-Zarqawi (Shamieh et al. 2015). He was imprisoned in Jordan because of his affiliations with a terrorist organization and owning weapons. After his release, he left for Afghanistan where he set up a new jihad group named 'Jama at al- Tawhid wal-Jihad'. In 2004 Zarqawi clarified that the organization had aligned their views with those of Al Qaeda and that they served as a branch of Al Qaeda in Iraq. When Al-Zarqawi died in 2006, Al Qaeda Iraq appointed a new leader which changed it into Islamic State Iraq, thereby splitting from Al Qaeda (Shamieh et al. 2015). This 'state' had a council which released a clear vision in which they clarified that there should be an Islamic State in Iraq and Syria. Due to the rise of internal conflict in Syria in 2011, Islamic State Iraq could branch into Syria, thereby renaming itself to Islamic State Iraq and Syria. During the war in Syria, foreign fighters came to join the cause of ISIS, which led to an international spread of the ISIS ideology along with an international recruitment (Shamieh et al. 2015).

Khalid Zerkani was one of those recruiters. In the Molenbeek area of Brussels he recruited several people to join the cause in Syria (Van Ostaeyen et al. 2019). The largest proportion of people that joined were young men who already had prior convictions. The Molenbeek area was in hindsight notorious for thriving unnoticed radical Islamic ideologies among some of the inhabitants (Van Ostaeyen et al. 2019). In combination with people coming back from the war in Syria and a support base for Islamic extremism and jihadism, a new terrorist network was born. Among these networks was the Paris/Brussels network, sometimes referred to as the Zerkani network. This group was responsible for the attacks on Bataclan, the State de

France and bars and restaurants along the Bataclan area. Another part of this network was responsible for the attacks on the metro stations in Belgium. The Paris/Brussels group had a strong affiliation with ISIS ideologies and possible connections with people within the organization of ISIS. Especially since ISIS claimed that the attacks were their own. The motives for these attacks were similar to those of Al Qaeda (Van Ostaeyen et al. 2019).

1.2 Terrorism

The definition of terrorism is conceptualized by many different historians, law enforcement agencies and scientists. Using this definition is a sensitive topic as the use of the word terrorist is very dependent on context and seen as concdemning. For one country a group may be considered a legal political party whereas the same collective may be viewed as a terrorist organization by another country.

The Federal Bureau of Investigation defines two types of terrorism: domestic and international (Terrorism 2023). In this bachelor thesis, the two types of the Federal Bureau of Investigation are used under the one definition of terrorism: violent, criminal acts committed by individuals and/or groups who are inspired by or associated with designated foreign or domestic organizations, to further ideological goals from domestic or foreign ideologies. This definition is a synthesis of the two separate definitions. It was created because of the ability of terrorists and their respective ideologies to cross borders with relative ease.

In the field of conducting social network analysis there are a lot of different approaches and attempts to use these results for new applications in the field. One approach is the use of machine learning on a case study on the terrorist organization Boko Haram in Nigeria. This paper was published by the department of computational robotics of the University of Nigeria (Pourhabibi et al. 2021). In China there are also researchers working on using algorithms to map the movement and formation of dark networks (Wu et al. 2011). However, the main characteristics of a terrorist network are not yet discovered. Several studies focus on the analysis of one or two case studies, of which the findings are then used as a proof of concept. For instance in Raab et al. (2006), the example of Al Qaeda is used to validify the existence of dark networks.

1.3 Dark networks

This thesis relies on the concept of dark networks to gain a better scientific understanding of how terrorist organizations are to be characterized as networks in the context of social sciences (Raab et al. 2003). Raab argues that networks can be conceptualized as methods to map and apprehend complex problems, such as public health and safety, as well as being a tool to map social connections in a group of people (Raab et al. 2003). Raab et al. (2003) have extended beyond the 'regular' definition of networks and came up with the concept of dark networks. These so-called dark networks are a means to describe networks that do not adhere to law as they make a distinction between how overt networks function and how covert networks function. The overt networks being the 'regular' networks and the covert networks being the dark networks. This literature forms the foundation for this thesis as the very concept of dark networks concerns itself with the characteristics of terrorist networks.

Dark networks are different from normal networks in many ways (Raab et al. 2006), the first being the goal. Overt networks are in place to achieve legal goals in a collaborative fashion, whereas the covert (dark) networks aim for illegal goals and illicit gains (Demiroz et al. 2012). The second difference is that dark networks have a more flexible structure than normal networks, which allows them to be more resilient in the face of law enforcement. The third difference is that institutionalization is not an option for these dark networks, as it would destroy the covert identity. Normal networks can be institutionalized, as is often the case. The fourth difference is that dark networks are capable of thriving in areas where they will not be pressurized by law enforcement or local populations. Normal (overt) networks do not suffer from pressure exerted by local police or populations as they are not punishable by law. Apart from a few distinctive characteristics, dark networks share key characteristics with overt networks. The first similarity between both network types is the need for a territorial basis. Both of these networks require some sort of territory in which and from which they are enabled to operate. The second similarity is that both covert and overt networks face issues of integration and differentiation. However, as pointed out earlier, dark networks do not have the ability to combat these processes using institutionalization.

In the same paper, Raab et al. point out that it is built on a major assumption, namely that if the dark networks are problems for the organizations that try to fight them, that these organizations will become better at fighting them via collaboration. This is because of the

nature of networks, as networks are able to cross borders, which Raab et al. summarizes as: “fight networks with networks”.

Jackson (2006) expands upon the requirements of a dark network, he adds that a set of individuals is required with fitting connections or social relations to one another. As well as the presence of some authority for the shaping of an agenda. Thereby, a network needs some sort of command structure, even in a decentralized network. Jackson (2006) makes a distinction between three types of authority namely; strategic, operational and tactical. Strategic control is the control in which one defines the highest goal. Operational control is controlling the specific activities of the organization and tactical control is managing individual actions. The networks under study in this thesis are only observed on the tactical control as the networks were aimed at committing a terror attack in which the operational and strategic goals were already predetermined (MetaTempo 2001)(Van Ostaeven 2019).

Demiroz et al. (2012) claim that an organizational structure specifically adapts itself to an illicit goal, thereby adding that every dark network will aim to decentralize itself to hide better from law enforcement. That goes hand in hand with the idea of a dark network thriving in areas with low amounts of social control, as the structure is aimed at avoiding publicity at all costs (Demiroz et al. 2012). Xu et al. (2008) expand on the preference of secrecy over efficiency by explaining that these networks focus on a ‘small world’ network. That means that the networks tend to rely on people that know each other and actively put in effort to minimize the size of the network (Xu et al. 2008).

1.4 Terrorist networks

Terror cells are known in scientific literature as a relatively small group that is making its preparations to attack a target in a hostile area (Santifort et al. 2012). Such groups can be between 3-5 members in general, with some cells being larger. The goal of these terror cells is often to optimize the amount of people hurt in their attack (Helfstein et al. 2011).

These smaller groups are often components of a larger network and in some cases multiple cells can be put under one label, such as the 9/11 network which comprised of multiple cells (Krebs 2002). This was one network consisting of multiple smaller cells with each their respective targets: the north tower cell, south tower cell, pentagon cell and the white house

cell (Krebs 2002). Understanding the organizational structure and how the planning of these cells within a network was orchestrated is done by using social network analysis. Thereby, the definition that this thesis follows is that the cell is the core of active perpetrators with a single goal, while the network consists of everyone (semi-) actively involved in the group.

Before the attacks on September 11th 2001 very little was known about the internal structure of terrorist networks and their subsequent cells (Jackson 2006). It was later found that the general structure that terrorist networks take on is a decentralized network as the strategies of law enforcement are often aimed at the leadership of organizations (Dishman 2005). Alhaijar et al. (2021) argue that terrorists are adapting a decentralized method in order to avoid the kingpin strategies, strategies that focus on arresting the leaders of a group, that are adapted by militaries and counter terrorism agencies (Helfstein et al. 2011). This flattening of the leadership or decentralizing within the terrorist networks might allow for more cooperation with 'regular' criminal organizations as argued by Dishman (2005).

The article from MetaTempo (2001) argues that Islamic extremist terrorist networks, specifically Al Qaeda, are multi-layered structures that operate on different levels. These different levels consist of different cells. At the center is the core group. This group is responsible for leading and planning the entire organization (MetaTempo 2001). It is argued by MetaTempo (2001) that this structure is likely to be a chain with the core group at the head of the chain or ring., Each of the leaders will then have their own respective groups which build several separated networks of the organization. The next layer is named the 'structural cell' layer. This layer is responsible for the necessary specialized functions and tasks that the organization requires. Such tasks can include: acquiring funds and gaining intelligence terrorist operations. The members of this layer are often positioned in urban environments (MetaTempo 2001). This layer of the organization is known to be socially, structurally and functionally embedded in their environment (MetaTempo 2001). It is likely this layer takes on a hub network structure that follows a hierarchy that is tied in to the core group network circle in the middle (MetaTempo 2001). The next and final layer of an Islamic extremist terror organization is the layer of the 'operational cells' (MetaTempo 2001). This layer consists of 'seeded' individuals that request assistance in conducting attacks in the name of the ideology that the terror organization supports. These individuals are then trained under the watchful eye or the core group to avoid intruders (MetaTempo 2001). These operational cell members have been properly trained and tested so they are loyal and capable of conducting the attacks that they are tasked with. Outside of the network itself the research of MetaTempo (2001) argues

that there is a support network, which is often unaware that they are linked to an Islamic extremist terror organization. Throughout the entire organization, trust is the essential binding factor to maintain the relational ties between the members (MetaTempo 2001), since the interactions between members may be relatively low. This thesis mainly concerns itself with the structure of the so-called operational cells and their respective surrounding support network.

Even though, terrorist organizations and criminal organizations are both dark networks and share some similarities, they are inherently different (Alhaijar et al. 2021). In conducting a network analysis on both a criminal network and a terrorist network, there are major distinctions between the two types of dark networks. Terrorist networks tend to have high densities and high degree centralities whereas these are known to be low in conventional criminal networks (Alhaijar et al. 2021). In conventional criminal networks, the average geodesic distance and maximum betweenness centrality tend to be high whereas these are low in terrorist networks. Therefore, the network structures are quite different. Alhaijar et al. (2021) find that these differences are likely explained by the way the networks operate. Terrorists operate in small, tight groups in which every member knows one another, whereas the low-level criminal actors are more independent on the individual level and are more reliant on the chain of command.

1.5. Research question

To what extent does the literature of dark networks accurately predict the structure of Islamic extremist terrorist networks and how comparable are the network structures of the Islamic extremist terror networks to one another?

This research uses a social network analysis on two case studies of Islamic extremist terrorist networks which were successful in conducting their attacks on foreign soil (Krebs 2002 and EUROJUST 2018).

1.6 Subquestions

Q1: What are the key characteristics of dark networks in general and terrorist networks in particular? What is the theoretical relation between dark networks and terrorist networks?

Q2: What were the network structures of both terrorist networks and what are the implications of their respective structures?

Q3: How can the terrorist networks under study be empirically characterized? To what extent are the key characteristics of dark networks present in these Islamic extremist terrorist networks?

2. Theory and Hypothesis

This bachelor thesis will provide a literature review on the topic of dark networks. As this concept is central, apart from a definition and requirements, an understanding of how this concept is viewed in the scientific community as well as deeper more contemplative perspectives are necessary. The first paper written specifically about networks under risk, either because of illicit goals or illicit affiliations, was Secret societies and social structure (Erickson 1981). This publication builds the groundwork for the structures of ‘secret societies'. There was an earlier essay that discusses these ‘secret societies’ namely The sociology of secrecy and secret societies by George Simmel. In that essay Simmel (1906) claims that the structures of ‘secret societies’ do not deviate from ‘regular societies’. Erickson (1981) finds the opposite by analyzing ‘secret societies’ as case studies.

The paper that was used for the introductory text on dark networks was the first specific scientific publication using the term (Raab et al. 2003). Ever since that publication, multiple additions to the topic have been made. Raab and other writers have made contributions to the scientific understanding of dark networks. The concept of dark networks as described in 2003 is summarized as illicit networks that avoid attention and strive for illegal goals. These networks thrive in environments with low social control and a low attention from law enforcement. This article paid specific attention to how dark networks thrive in ‘failed states’. Demiroz et al. (2012) expand on this by linking failed states to brokers between several dark networks due to extremely low social control. Thereby, referring to links between organized crime, terrorist organizations and even dictatorships.

Raab and Milward made a new publication in 2007 in which they deepened the concept of dark networks. They started with restating their views on the ‘need for a failed state’, which is now no longer a necessity since some successful dark networks emerged in areas where there were no failed states. Yet, they stayed with the notion that a dark network thrives in non pressurized areas, for instance due to low social control. The additions that this paper made to the definition of dark networks lie mostly in the newly introduced nuances and conditions. The foundation of almost all ties within a dark network are built on trust, as there are no formal contracts or legal parties binding members of these networks together. In the specific context of terrorism, the needed trust is often outsourced to a shared extremist ideology (Raab et al. 2007). Transnational terrorist organizations may be enabled to use jurisdictional arbitrage to their advantage, as different countries may have different policies. The

organizations may simply choose the country with the most favorable policies and laws to operate from (Raab et al. 2007). In this publication there is also an argument as to why studying dark networks is considered scientifically valuable. The argument that Raab et al. make is that there is enough understanding of the functioning of organizations and that it becomes possible to make theoretically sound inferences on dark networks. Even if the sources of information on these dark networks are non-scientific at times.

However, another paper (Morris et al. 2013) claims that this is untrue. Due to the impact that the findings of studies on dark networks can have, the source of information is to be held in the highest regard. If due to incorrect information, scientific publications are made that are considered true, then there will be policy adaptations that are detrimental to the public safety. This is why Morris et al. argue that it is best to not study the dark networks, unless it is one hundred percent certain that the information is actually true. Apart from the sources of information, Morris et al. also point to the weaknesses of social network analysis in this context. Social network analysis tends to have hard borders on a network, whereas these borders are not always felt as concrete in the real world. This makes that some nodes may be given a discredited position or even left out of the network entirely. In turn this can lead to wrong conclusions on how the network may have functioned. In opposition to that argument Raab et al. argue that it is essential to study dark networks as it is still a theory that needs to be proven in full.

The term resilience is given extra attention by Raab et al. it is now defined as: the avoidance of disintegration under stress. For instance if a node is removed from the network then the network should still be able to function. The specific name given to this attribute is connectivity robustness. Raab et al. also make the proposition that dark networks should minimalize the amount of ties present in a network, as it harms the networks ability to stay covert. That finding is in line with the paper of Helfstein et al. (2011) as they also argue that tie minimalization may be used by criminals to avoid detection from law enforcement. The final paper in this literature review gives a good summarizing perspective on dark networks. Kelly et al. (2019) state that the strength of the concept of dark networks lies in its capacity to conceptualize the organizational structure of a network through the identification of key nodes that could be represented through either familial ties or a combination of personal, professional, religious or ideological associations. The value of applying this analytical framework to the case studies in this thesis allows for the data to be organized by forming a visual representation of the two networks. The literature also provides the prediction that the

two networks under study are likely to be structured in a way that allows for a resilient dark network.

It is expected that the concept of dark networks will not be able to accurately describe all aspects of terrorist networks and other illicit networks under one definition without becoming unspecific. Thereby, it is expected that most facets of the terrorist networks under study will be accurately described by the theory of dark networks, while some aspects will not be captured within the context of dark networks. These uncaptured aspects can be considered oddities or perhaps used to expand the concept of dark networks. The networks of both terrorist networks under analysis are expected to be centralized, to avoid nodes at the edges of the network to know the details of their operation, while showing some parameters of being decentralized to keep some nodes expendable. The expected shape of the network is a hub and spoke network, as these networks are best described by having a couple of key nodes in a centralized network, which act as key players, connecting the centralized network to smaller networks on the outside. The context of dark networks is particularly efficient at defining these key players. It is likely that the network takes on the shape of hub and spoke because it is unlikely that all nodes are interconnected. Having a network that is shaped like a chain, however, is difficult as it becomes more susceptible to falling apart if one of the key players is removed from the network (Helfstein et al. 2011).

For the first subquestion the following hypothesis goes: It is expected that dark networks are significantly different from ‘regular’ networks as the respective organizational structure has to be able to remain undetected. Therefore, it is very likely that the structure of a dark network is more capable of adapting to change, as well as being able to function when some parts of the network are removed. This means that the network is likely to display its resilience in a structure that is able to deal with external pressure. Thereby, the structure predicted by the theory of dark networks is a hub and spoke network.

Hypothesis 1. The networks will display features of resilience in the form of a hub and spoke network.

The second subquestion is: what were the network structures of both terrorist networks and what did these structures mean? As stated earlier, the expected network structure for both the 9/11 network and the Paris/Brussels network are expected to operate via a hub and spoke network, since these networks allow for a good combination between network resilience and centralization. Resilience is important as it allows the network to remain productive when it

adapts and centralization is given its appropriate role as secrecy is paramount. Centralization is important as information flow has to be efficient throughout a network, especially in planning illicit activities.

Hypothesis 2. The expected network structure for both the 9/11 network and the Paris/Brussels network is a hub and spoke network.

The third subquestion is followed by the expectation that the two networks under study can be empirically characterized as dark networks, as their structures will follow the predicted morphological structures as well as meeting the requirements for being called a dark network.

Hypothesis 3. The structural network characteristics of terrorist networks are similar to those associated with dark networks.

3. Research design and conceptualization

3.1 Case study design

In order to derive appropriate inferences in the field of terrorism and dark networks this thesis relies on the use of a comparative case study analysis. A selection was made on two prominent terrorist organizations to research the concept of dark networks. The two selected case studies will be subjected social network analysis. By using social network analysis, key parameters will be identified. Using these parameters, inferences can be made on the network structure. These network structures can then be put into comparison to see how the networks are different from one another. Apart from using parameters, the analysis will also use network visualizations which are provided by the social network analysis software as well. These visualizations can then be used to compare network structures directly. For the social network analysis the UCINET software and the Social Network Visualizer tool are utilized. Some of the subquestions can be answered using existing knowledge via a literature review as not all subquestions are reliant on the use of a social network analysis.

3.2 Social Network Analysis

The use of social network analysis relies on a couple of premises (Wasserman et al. 2012). These premises have to be taken into account before the social network analysis is performed, as these premises affect the findings. The first premise is that nodes/actors are interdependent rather than independent (Wasserman et al. 2012), meaning that the actors are depending on one another, which is necessary to form a network. The second premise is that the links between the nodes are information and resource bridges which are used to exchange these commodities (Wasserman et al. 2012). The third premise is that network models that are aimed specifically on one actor are inherent to viewing the network as a means of providing or constricting this single actor (Wasserman et al. 2012). The final premise is that the network is a visualization of relationship patterns between actors over a prolonged period of time (Wasserman et al. 2012). Note that these networks and the output values that they produce are based on models which are derived from reality, therefore, the networks and their respective outputs are reflections of reality. This is why the morphological structure and the functional structure are not identical (Spagna 2018). The morphological network structure under study

can be used to make inferences on how the functional structure has operated. Whether the inferences were correct can be verified using the news reports, police reports and statements from the incarcerated members of the network.

In this thesis, the method to test for the differences in social network structure is central. This, however, poses an issue as there is not one standardized parameter for social network analysis in a comparative fashion (Pimentel 2015). That means that other parameters are going to be necessary to identify network similarity and significant network differences. The following parameters will be used in this thesis to identify key characteristics as well as similarity, of which some were used by Spagna (2018): density, degree centrality, betweenness centrality, and closeness centrality. This study relied on these degree-based methods to make inferences on the local centrality. These local inferences allowed them to draw conclusions on individual actors. Pimentel (2015) argued that the best way to analyze networks for similar structure is to take complexity parameters, as similar complexity often means similar structure. Some of these complexity parameters are: density and average distance. The used parameters and how they compare to the topic of dark networks are listed down below in the operationalization.

3.3 Compatibility of the cases

The two selected case studies in this thesis are the 9/11 network and the Paris/Brussels network. These two terrorist networks were selected on the basis of two criteria; information availability and similarity. Both groups have, as stated before, similar origins and similar ideologies. By controlling these two variables it becomes easier to emphasize the differences in network structure and as to how these organizations may have functioned.

Both networks meet the definitions of dark networks, as they can clearly be defined as dark networks with illicit goals. Both networks also required a physical base for planning. In the case of Al Qaeda, this was Afghanistan and for the Paris Brussels network, this was the Molenbeek area in Brussels. The network flexibility is to be analyzed in the coming section. Both networks have also avoided institutionalization. The final condition is also met, both networks have definitely thrived in non pressurized environments.

In terms of ideology both networks can be considered similar. The exact ideologies in religious perspective may be different but both strive towards a similar goal. That goal in this instance is causing damage to Western societies. The level of complexity in which they were

able to plan and conduct their operations is similar but not of the same order. The attacks in Brussels and Paris were carefully planned, yet the level of complexity required to execute the 9/11 attacks was larger. The Al Qaeda network also counted more attackers than the Paris Brussels network, as the amount of perpetrators in their network was 19 and in the Paris Brussels network it was 11. The largest problem with comparing these two groups is that the time period in which they operated was completely different. Due to the 9/11 attacks, Western society became better prepared by taking measures to limit the damage that could be done by terrorists (Jervis 2013). This meant that the Paris Brussels attackers may have been more constrained during their planning than the 9/11 attackers were. The 9/11 attackers are also a very well studied and recorded group in todays day and age, whereas the Paris Brussels group may not have received as much scientific attention yet.

3.4 The case studies

9/11 Network

On the 9th of September in 2001, the world was shook by a terror attack on the United States of America. A terror group associated with Al Qaeda hijacked 4 commercial airliners with the purpose of using these as immense explosives to target key icons of American society, namely the World Trade Center, the Pentagon and presumably the White House. The first group of hijackers captured American Airlines flight 11 and flew into the North Tower of the World Trade Center. A second group captured United Airlines flight 175 and hit the South Tower a mere seventeen minutes later. The third group of hijackers managed to capture American Airlines flight 77 which they used to attack the Pentagon. The fourth and final group of hijackers captured United Airlines flight 93 with which they attempted to attack either the White House or the Capitol. However, the passengers managed to recapture the plane and crashed before the hijackers could reach the final destination. The total death count is estimated to be around 2977 and the wounded beyond 25,000. A terror attack of such scale and complexity had not been seen before. With these attacks Al Qaeda aimed to make a statement towards the world. This statement would later be clarified in the “Letter to America”. The message that this letter contained is that Al Qaeda wanted the American military presence and influence in the Islamic countries in the Middle East and Asia reduced (MetaTempo 2001). It is very likely that the people in the selection pool from Al Qaeda were specifically recruited and selected for this particular attack (MetaTempo 2001). The recruits

may have been specifically chosen based on their discipline and intrinsic motivation, as the execution of this attack required remaining undercover for prolonged periods of time as well as conducting complex tasks, such as following flight training (MetaTempo 2001). Al Qaeda had a unique structure as was described in the theory section of this thesis. Since it was capable of conducting such complex operations it is key to study how it was able to do so (MetaTempo 2001). The network of the 9/11 hijackers was first mapped to a large extent by Krebs (2002). Krebs argued that this network was shaped like a chain, and that it had a significant coherence within. At first, it was argued that the hijackers did not know the other hijackers in their groups. This was questioned by Krebs in his paper on the structure of the network of this terrorist network (2002). Due to the complexity, effectiveness and available literature of this network it is a particularly suitable case study for the research of high-functioning Islamic extremist terror organizations. The data for this research was retrieved from the UCINET database (Borgatti et al. 2006). The page of this dataset on the database explains that the Krebs (2002) dataset that was used to map the connections between the attackers and the people could be of relevance. It is important to note that these networks are approximations of how real life relations may have been. Especially since some of the actors in the network are no longer alive and their relations with other actors may have ben speculated. Due to the nature of a command and control structure, with the pilots leading different cells within the network, identified by Krebs (2002), it is hypothesized that the structure of the 9/11 hijacker network will be a hub and spoke.

The Brussels & Paris Network

In 2015 an 2016, France and Belgium were shook by a multitude of terror attacks of which some were conducted by ISIS based terror cells (Van Ostaeyen 2019). It started in 2015 with the attacks on Charlie Hebdo and a Jewish supermarket in Paris. However, these attacks were likely not affiliated with ISIS but Al Qaeda (Britannica 2018). In November 2015, Paris was shocked by terror attacks again, this time on a much larger scale. The Bataclan and neighboring bars were attacked along with the State de France. This attack was claimed by ISIS. The attackers used assault rifles to shoot people and in some instances the attackers blew themselves up using bomb vests. In the aftermath of the attacks, a 130 people died and over 400 were wounded. A couple months later, in March 2016, two well coordinated suicide bombers blew themselves up at the Zaventem Airport and metro station. These attacks were once again claimed by ISIS and had perpetrators from the same network as the previously

mentioned attacks (EUROJUST 2018). The two attackers were Khalid el Bakraoui and Ibrahim el Bakraoui, whom are also incorporated in the later listed model. Many people were involved in the planning and execution of the attacks. The data of how the network is composed can be found in the appendix (Appendix 1, Appendix 2 & Appendix 3). The dataset was made by myself to replicate the data that was used by the Spagna (2018), as their dataset was not made publicly available. It is important to note that these networks are approximations of how real life relations may have been. Especially since some of the actors in the network are no longer alive and their relations with other actors may have ben speculated. I hypothesize that the network of the Paris/Brussels network will also have the structure of a hub and spoke network as they have central members which are deemed responsible for the planning (BBC News 2016).

3.5 Conceptualization & operationalization

Conceptualization:
Understanding terrorist organizations through social network analysis requires interpretations of how the numerical values that are generated by the analysis are given their appropriate definitions. In the operationalization, several social network analysis parameters that are relevant for the research are discussed. These parameters are important on two different levels. One being the individual level, where inferences are made about a single actor within the network. The other being the macro level, here inferences are made about the entire network which can then be used to compare both networks on relevant criterion. The criterion for the parameters of both actor level data and network level data are specified in the operationalization. The outcomes can lead to the following conclusions for one of the actors: an actor can be considered a key player if he or she is placed centrally within the network (Spagna 2018). An actor can be seen as a broker if they are displaying a high betweenness centrality value. An actor can be considered a planner if they are displaying a high degree centrality value (Spagna 2018). An actor can be considered an information accessor if they are displaying a high closeness centrality value (Spagna 2018). An actor can be considered a coordinator if they are in a position that allows them to be in contact with the majority of the network, similar to a planner (Spagna 2018). An actor can be considered a gatekeeper if they are displaying a high betweenness centrality but not a particularly high degree centrality, which means that they manage information and resource flows (Spagna 2018). An actor is

likely to be a leader or supporter if they are displaying a high degree centrality but not a particularly high betweenness centrality (Spagna 2018).

This means that their position is not always of importance within the network even though they have ties with multiple network members. These nodes should be judged case by case. Note that these labels are on a spectrum which is relative and values can vary between datasets. The outcomes can lead to the following conclusions for the entire network structure: if there is a high density that means that there are a lot of connections between the actors in the network (Spagna 2018). The high density then means that the network is likely to be an all connected network in which almost every actor has a tie to almost every other actor. Using the outcomes of these parameters, it is clear that a basic understanding of the functioning and structures of both networks becomes available. By using these findings the research question and its respective sub questions can be answered. Taking a look at the morphological structure will be done by using network visualizations as well. This allows for a quick overview as to what the network structure looks like.

Operationalization

Density

Density is calculated by dividing the amount of links of nodes by the possible total amount of links. This parameter is used to express the coherence and interconnectedness of a network.

Degree centrality

The degree is a parameter that refers to the amount of ties that a node has. There are several ways to express the degree: highest degree, average degree or the degree for the size of the individual nodes. In the specific context of dark networks that are related to terrorism, a high degree is associated with tactical planning (Spagna 2018). However, not all nodes with a high degree are key players. Centrality is an important tool in Social Network Analysis to identify the key players within a network.

Betweenness Centrality

Betweenness is calculated as the proportion of shortest paths that travel through an actor. (Spagna 2018). It is used to express how a node can influence the information flow throughout the network. Therefore, a high betweenness is considered as a sign of being a broker, since these nodes can link one part of a network to another part in a relatively short distance. Such brokers can function in many different ways. They can be arms dealers but also secure links to avoid one part of the network knowing another.

Closeness Centrality

Closeness is defined as nodes that are enabled to let information flow efficiently through a network. Closeness centrality is calculated as the lowest distance from one node to each other node, or as the article puts it: “closeness centrality is the reciprocal of farness which for a node is the sum of the lengths of the geodesics distances to every other node” (Spagna 2018). A high value for closeness means that the node is associated with the ability to access information both inside and outside the network (Spagna 2018). These nodes have access to sources that are outside of the network because they are relatively close to all other actors within the network.

Network complexity

There are several programs that enable a topological test of network complexity (Pimentel 2015). By testing for a complexity using these programs, the topological structure of both networks can be directly compared using the output values, as similar complexity insinuates similar structure. The following indicator was used by the program to conduct the social network complexity analysis. It used an activity on the node project scheduling network, which means that it used a set of nodes that are connected by arcs (ties) to analyze the network. Three complexity tests are recommended. The first test is for the coefficient of network complexity (Vanhoucke et al. 2008), which is calculated by taking the total amount of ties and by dividing this number by nodes. In some instances this parameter is referred to as density. The second test is the complexity index (Vanhoucke et al. 2008). The final test originates from the paper of Spagna (2018) which recognizes the fragmentation centrality as a method to test for the topographical structure of a network. This is calculated by giving the proportion of all node pairs which are not interconnected. Comparing these different fragmentation centralities is a valuable tool to see how the networks are differently structured.

Network variations

There are many variations in how social networks can be shaped, but in the field of terrorism, there are three distinctive structures. The first is the all channel network. In an all channel network almost all nodes are interconnected. Such a network is also a clear example of a grassroots structure rather than a hierarchical structure as the people that make up the network are connected in ways that are equal in ranking (Kelly et al. 2019). The second structure that a network can take on is the chain network. In a chain network, all nodes are linked in a sequential fashion which makes up a chain. In one of his visualizations Krebs (2002) argued that the 9/11 network was a chain. The third network is the hub and spoke network. In a hub and spoke network there are a few central nodes with other smaller networks that spread to

the edges. All of these structures have the ability to quickly respond to changes, which, according to Raab et al. (2003), is a key characteristic of dark networks.

3.4 Analysis

The analysis for both datasets is conducted using the UCINET software. This software was created by Borgatti Everett and Freeman in 2002 (Borgatti et al. 2006). The software was made to analyze social networks from several datasets. The datasets that were used were also retrieved from the UCINET database.

The Al Qaeda dataset was specifically made after the scientific papers from Krebs (2002). The files were made by Steve Borgatti. The coding of the dataset and the dataset itself are included in the appendix (Appendix 1). The ties that are visualized are the relational ties. This can vary from going to the same school to being in the same airplane while conducting the attack. There are two types of contacts; the trusted prior contacts and the other associates. The groups can also be split into several groups based on the targets that each smaller cell had.

The Paris Brussels dataset was created by me, made specifically to replicate all the ties that existed in the model of Spagna (2018). The ties that are visualized are relational ties. In this case it is based on affiliation and association. The groups can also be split into two parts; the attackers and the people that are associated with them or have helped them. The files for both datasets can be found in the appendix (Appendix 2 & Appendix 3).

As explained in the operationalization, the network will be tested for several local centralities and network complexity parameters. UCINET has the tools that are readily available to conduct these analyses. Social Network Visualizer also displays the wanted values when a network is added to the system.

4. Results

9/11 Network

Using the earlier mentioned combination of betweenness centrality and the degree centrality, it becomes clear that Mohammed Atta was likely the leader of the 9/11 attacks, as he displays both a large degree centrality and betweenness centrality, making him a key player.

The model has also identified Ramzi Bin al-Shibh, Lotfi Raissi and Nawaf Alhazmi as key players. Alhazmi was one of the members of the cell that targeted the Pentagon. Ramzi Bin al-Shibh was known as a key facilitator for the attacks. This is logical according to the visualization above as he displays a relatively median degree centrality while he is identified because of his high betweenness centrality. As became clear during research, a high betweenness centrality is associated with being a broker. This is proven in the case of Ramzi Bin al-Shibh, as seen in figure 1. Lotfi Raissi is also taken up in the model and is identified as an actor with a high betweenness centrality as he connects large parts of the networks to one another. However, Raissi was not part of the cell or network itself, he just happened to be know some of the hijackers via flight school or university (MetaTempo 2001). If Raissi had been a part of the network it is clear that he would have been vital, however, it is best to leave him out of the equation as it became clear via lawsuits that Raissi had no real connection to the hijackers or even more the attacks on 9/11.

The nodes that are identified because of their high degree centrality are: Mohammed Atta, Marwan Al-Shehhi and Essid Sami Ben Khemail. As stated before, Mohammed Atta was most likely the leader so the high degree centrality was expected. He also has the highest degree centrality of the entire network. Marwan Al-Shehhi was the pilot of the South Tower group. His degree centrality is high due to his ties to the fellow pilots as well as the group of the South Tower. This makes it likely that Al-Shehhi was also involved in the planning and that he was the leader of his group. The final node that stands out because of a high degree centrality is Essid Sami Ben Khemail. Sami Essid was arrested in Milan for running a terror cell in that region. His exact role in this organization is not clear, however, he could have attended the training camp at the same time as some members of the 9/11 network, thereby being affiliated with a large number of them which has generated a high degree centrality.

The complexity of the 9/11 network is in this case expressed in density, as mentioned earlier. The density of the full network is 0.054 or alternatively, 5.4%. This means that 5.4% of all possible ties actually exist within the network. The average distance of the full network is 3.41. Note that the full network is included. The numbers are different when the nodes at the edges of the network are excluded. Due to the low significance of some of the exterior nodes to the network and the functioning of the terrorist network, they can be excluded. This selection was made on the basis of a conviction that was related to the actions of this specific terrorist network, thus including: active affiliation, supplying intelligence and active participation.

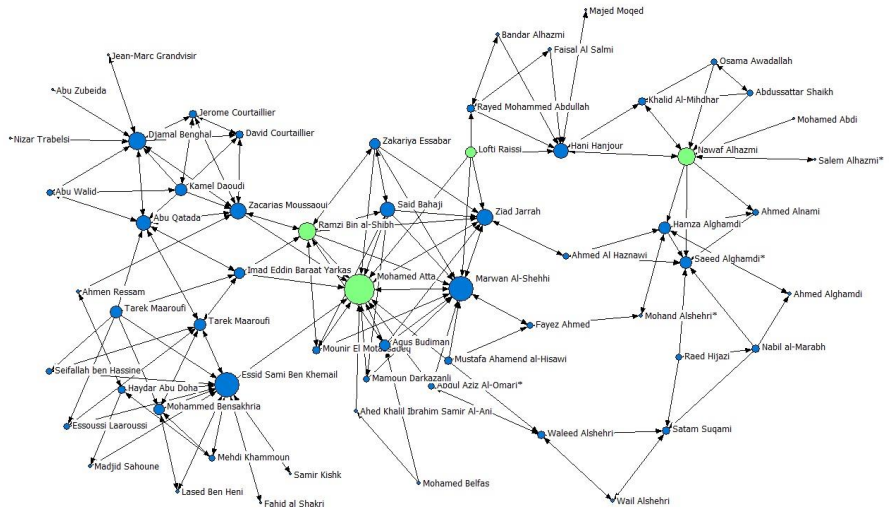

Figure 1 - [9/11 Network] (Based on Krebs 2002, UCINET)

In the network visualization seen in figure 1, the key players are identified using the betweenness centrality. The nodes of the actors are sized based on the degree centrality. This allows for a quick multilevel analysis. The ties between the nodes are all visualized. The key players are depicted in green and the size of the nodes is determined by the degree centrality. This network seems to be a hub and spoke as predicted in hypothesis 1, as it has a central network which connects multiple separate sections.

The Brussels & Paris Network

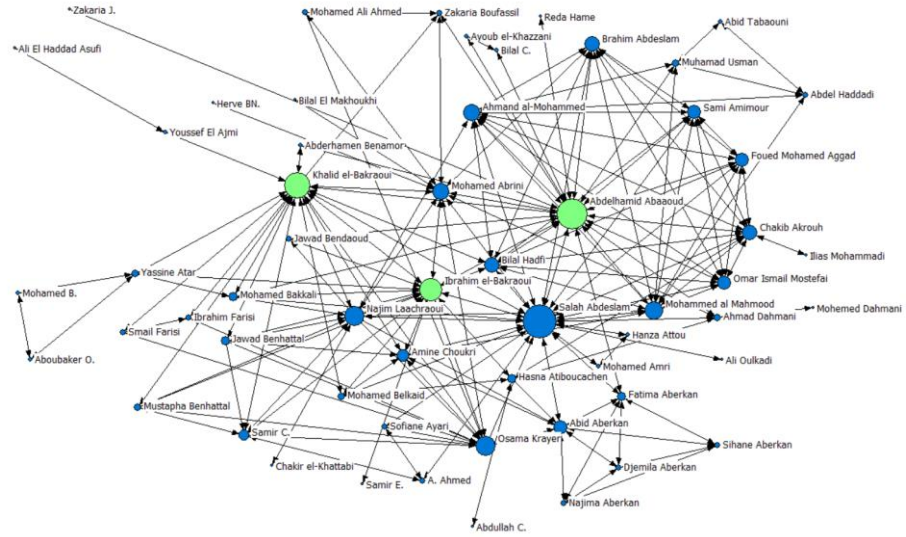

Figure 2 – [Paris/Brussels network] (Self made using Excel, data extracted from Spagna 2018)

The same method of degree centrality and betweenness centrality was used on the Paris Brussels network, which can be seen in the model in figure 2. This led to the believe that Abdelhamid Abaaoud was the leader of the network. This assumption is supported by what law enforcement found so far (Hallday et al. 2021). This network is clearly not a hub and spoke which contradicts hypothesis 1 and 2 as now not both networks are hub and spoke networks

Other key players that the model identified were Ibrahim el Bakraoui and Khalid el Bakraoui. These brothers were two of the attackers on the Zaventem Airport and the Brussels metro station. Their identification as key players can be explained because they have direct links to other people in the network (depicted as the circle surrounding Abaaoud), as well as links to people that other network members do not have links to.

Salah Abdeslam has the second highest degree, which leads to the believe that he was a very active member of the attacker group. He might have been a coordinator. In his particular context, it is difficult to assess what he has done exactly at the night of the attacks. It is clear that he drove some attackers to the sites which they had to attack, but whether or not he took

part in some of the attacks is still unclear. The model did not identify him as a key player due to him having connections that other network members may share.

In figure 2, it can clearly be seen that the network surrounding Abaaoud is a very dense network, whereas the rest of the network is less densely connected. The network is more of an all spoke network than it is a hub and spoke or a chain. The group of attackers clearly form a densely connected web while the other nodes generally have a low degree centrality. The In terms of complexity, this network is notably different from the 9/11 network as the density of the full network stands at 0.010 or alternatively, 10%. This means that there is a 10% saturation of all possible nodes. However, when the network is distilled down to just the more prolific actors that partook in the attacks, this value changes dramatically. The new density value is 0.42 or 42%. This means that of all connections possible 42% actually exist.

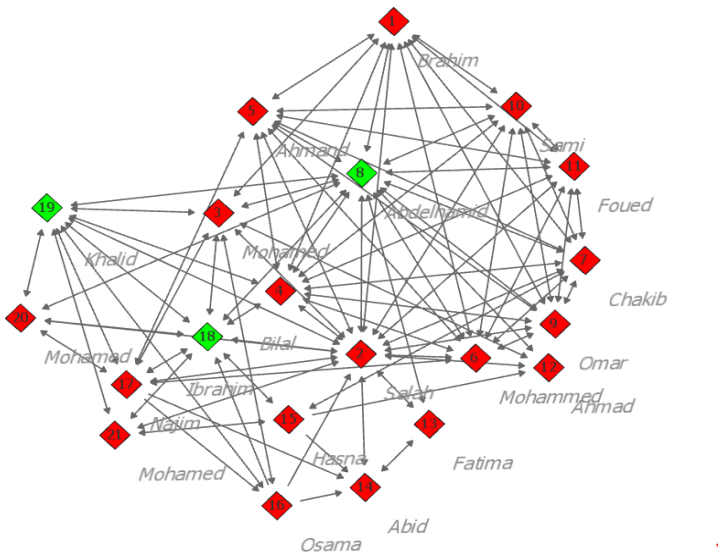

Figure 3: the Paris/Brussels network with the outer nodes removed, made using Social Network Visualizer.

The thesis will now make a comparison of the two models in relation to dark networks. At first glance, it becomes quite clear that the networks are very different. The network of the 9/11 attackers is a clear display of a hub and spoke network, whereas the Paris/Brussels network is a clear depiction of an all spoke network. The reason why these networks are so different can likely be attributed to planning. In the case of the 9/11 attackers, the operation was set up beforehand and after that, the right people were picked for the job. In the case of

the Brussels Paris network, a large proportion of the people already knew each other from the Molenbeek area and some people may have met in Syria.

The first striking difference between the two networks is their density. The network components of both networks are not comparable due to the large differences in interconnectedness. The 9/11 network components are clearly less connected to one another which may imply that the network was actually designed beforehand to avoid suspicion from law enforcement agencies (Helfstein et al. 2011). Another explanation could be that the actors did not get to know one another due to having different tasks within the attack, but that can be an externality of a designed network. The Paris/Brussels network on the other hand shows a very high density throughout the network component of the network. This leads to the believe that the network was more of a spontaneous formation rather than a designed network.

When looking at the overall structure, it also becomes clear that the way in which these networks functioned was different. The 9/11 network was a more hierarchical network that had several smaller networks that may have served their own purpose, along with a more central network which may have served as a command network. Note that the visual links are not just formal links, they are can also be informal connection, thus making it harder to distinct how some people related to one another. The Paris/Brussels network has a structure that is more in the trend of an all spoke network, with a more horizontal command structure. As every member was connected to almost every other member, it is likely that the connections were also highly personal. In this respect, the 9/11 network resembles an organized crime network more than it represents a ‘typical’ terror cell, whereas the Paris/Brussels network is more a typical depiction of a ‘regular’ terrorist network. This means that the results are not in line with hypothesis 1 as the 9/11 network is a hub and spoke network but the Paris/Brussels network is not. Therefore, hypothesis 2 can be rejected as not both networks are hub and spoke networks and their values are significantly different. Hypothesis 3 is still up for debate as both networks replicate different elements of a dark network. The 9/11 network has the tailored network structure while the Paris/Brussels network has many connections that are based on trust, which are both highly important factors (Raab et al. 2003).

Social network analysis	9/11 Network	Paris/Brussels Network
Density	0.054	0.010
Group degree centrality	0.131	0.327
Group betweenness centralization	0.102	0.257
Group closeness centrality	0.000	0.411

Figure 4: the outcomes of the social network analyses using Social Network Visualizer

5. Conclusion and discussion

Met opmerkingen [MH1]: Morris et al. gebruiken bij de discussie, zodat ke de resultaten iets kunt relativeren.

Zorg in 4 results dat je terugkoppelt naar de hypothesen.

The first sub-question was posed to find the key characteristics of dark networks were and how they relate to terrorist networks. This question was followed by hypothesis 1: The networks will display features of resilience in the form of a hub and spoke network.

The key characteristics of dark networks in general can be distilled down to four criteria (Raab et al. 2003). Firstly, dark networks strive for illicit or illegal goals. Secondly, they are covert and try to avoid unwanted attention. Thirdly, dark networks deal can not be institutionalized. Lastly, they thrive in unpressurized areas. The relation between dark networks and terrorist networks lies in the distinction that terrorist networks meet all four criteria of dark networks. Terrorist networks are similar to criminal networks in some respects, yet in most respects the parameters of their networks are different. The key characteristic which links these terrorist networks to dark networks is the high degree of resilience which their network structures display. In the results it was seen that the 9/11 network was a hub and spoke network to ensure a high degree of resilience. In the case of the Paris/Brussels network there was an all spoke network which is less resilient and easier to detect.

The second question aims to delve deeper into the morphological structure of the networks. It was followed by hypothesis 2: The expected network structure for both the 9/11 network and the Paris/Brussels network is a hub and spoke network.

The 9/11 network has a morphological structure which resembles a hub and spoke network. It has one central hub which splits to multiple smaller networks towards the edges. This structure implies that there may be a strong hierarchy along with a careful planning of the organization, as well as the existence of one central network responsible for the planning. It is also more likely that the hub and spoke network is able to keep itself hidden from law enforcement due to limited interactions. The network of the Paris/Brussels network is an all spoke network. In this network, many of the attackers are connected to one another. Yet, if one of the key members would disappear the rest of the network might still be able to function. The numbers found in figure 4 clearly indicate that the Paris/Brussels network is much more interconnected than the 9/11 network.

The third subquestion aims to get a better grip on how the networks under study compare to the concept of dark networks using an empirical characterization. It was followed by

hypothesis 3: The structural network characteristics of terrorist networks are similar to those associated with dark networks.

The networks under study can be empirically characterized as highly functioning dark networks. The 9/11 network can be identified as an optimized hierarchical network which has been structured not too dissimilar to a regular legal organization, unlike the Paris Brussels network, which is more of a network of friends and acquaintances rather than a structured social network. However, both networks were very capable of conducting highly complex attacks that were carefully planned. The 9/11 network from Al Qaeda was carefully put together, thereby it is likely a designed network. The network was designed to complete an objective and each member was handpicked out of a group of loyalists to the Al Qaeda ideology. The Paris Brussels network is the polar opposite. The Paris/Brussels network started as a group of individuals with similar ideologies that knew each other from either their time as a foreign fighter in Syria or as someone from their Islamic radical friend group. It was only after this network already existed that the preparations for a terror attack began. However, despite the inherent different natures of the networks, both were still very capable of avoiding law enforcement and successfully conduct their attacks.

The research question is: to what extent does the literature of dark networks accurately predict the structure of Islamic extremist terrorist networks and how comparable are the network structures of the Islamic extremist terrorist networks to one another? This thesis finds that the theory of dark networks does not always accurately predict the structure of Islamic extremist terrorist networks. The literature of dark networks clearly aims at hub and spoke networks to define resilience, which is in line with the characteristics of organized crime and the 9/11 network. The Paris/Brussels network, however, had a completely different structure, namely an all spoke network. This leads to believe that the theory is not fully capable of grasping all possible network structures of terrorist networks that meet the same requirements as dark networks.

As explained earlier, the 9/11 network and the Paris/Brussels network are both considered dark networks based on the requirements, but they are not both hub and spoke networks as the theory on dark networks would suggest. This leads to believe that the concept of dark networks is not yet complete. It can be explained how the theory of dark networks has missed the possibility of an all spoke network. In the particular case of the Paris Brussels network,

the network came into existence spontaneously, it was not designed. Raab and Milward (2006) unknowingly made the assumption that all dark networks had some sort of assigned structure to them. This is not true for the Paris Brussels network as they do not follow the hub and spoke structure. This is likely because they did not set out to be a formal organization. The key assumption of Raab and Milward (2006) is that dark networks are always organizations, this is not always true as networks can be much broader. That is why I argue that it is essential to distinguish between these two forms of dark networks. First, there is designed dark networks, networks with a purposeful structure, often expressed as a hierarchy. The other would be called emergent dark networks. These networks come into existence more spontaneously and do not have a set structure. However, a designed network may emerge from an emergent network, as members from an organization can start operations for which they will design a network, such as the leaders from Al Qaeda did in constructing the 9/11 network. It is also important to note that the use of social network analysis is an approximation of reality and not always a flawless description. To improve the definition of dark networks, more types of case studies should be compared to the framework of dark networks. Studying dark networks to a larger degree will lead to a better understanding of the covert and illegal networks that threaten society.

The findings of this thesis are subject to limitations as studying dark networks through social network analysis has its problems (Morris et al. 2013). They state that the information sources on which the datasets of the dark networks are based, are often subject to incomplete or corrupted data entries. This leads to sometimes partially incorrect social networks, which in turn can lead to incorrect conclusions. An example of an incorrect conclusion could be the involvement of Lotfi Raissi. Apart from data entries, studying dark networks poses its problems due to their covert nature (Raab et al. 2003) as these types of organizations are not eager to discuss their organizational structure. Due to these factors can the thesis be used as an approximation of reality as many sciences attempt when using models.

Reference list

Alhajjar, E., Fameli, R., & Warren, S. (2021). Are Terrorist Networks Just Glorified Criminal Cells? *Northeast Journal of Complex Systems*, *3*(1). https://doi.org/10.22191/nejcs/vol3/iss1/1

BBC News. (2016, April 27). *Paris attacks: Who were the attackers?* https://www.bbc.com/news/world-europe-34832512

Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). *UCINet* (6.748 [64-bit]) [Social Network Analysis Software]. Harvard MA Analytic Technologies. https://sites.google.com/site/ucinetsoftware/home

Brinton Milward, H., & Raab, J. (2006). Dark Networks as Organizational Problems: Elements of a Theory[1]. *International Public Management Journal*, *9*(3), 333–360. https://doi.org/10.1080/10967490600899747

Charlie Hebdo shooting | Facts, Victims, & Response. (2018). Encyclopedia Britannica. Retrieved August 23, 2021, from https://www.britannica.com/event/Charlie-Hebdo-shooting

Demiroz, F., & Kapucu, N. (2012). Anatomy of a dark network: the case of the Turkish Ergenekon terrorist organization. *Trends in Organized Crime*, *15*(4), 271–295. https://doi.org/10.1007/s12117-012-9151-7

DISHMAN, C. (2005). The Leaderless Nexus: When Crime and Terror Converge. *Studies in Conflict & Terrorism*, *28*(3), 237–252. https://doi.org/10.1080/10576100590928124

Erickson, B. H. (1981). Secret Societies and Social Structure. *Social Forces*, *60*(1), 188–210. https://doi.org/10.1093/sf/60.1.188

EUROJUST. (2018). *Brussels Terrorist Attacks of March 2016*. https://www.eurojust.europa.eu/sites/default/files/2018-06/2016-03_Brussels-terrorist-attack.pdf

European Union. (2021). *European Union Terrorism Situation and Trend Report*. Publications Office of the European Union, Luxembourg. https://doi.org/10.2813/677724QL-AJ-21-001-EN-N

The fall-out from the Brussels terrorist attacks. (2016, June 15). European Policy Centre. https://www.epc.eu/en/Publications/The-fall-out-from-the-Brussels%7E1d2eb4

Federal Bureau of Investigation. (2022, May 9). *World Trade Center Bombing 1993*. https://www.fbi.gov/history/famous-cases/world-trade-center-bombing-1993

Gunaratna, R. (2004). The post-madrid face of Al Qaeda. *The Washington Quarterly*, *27*(3), 91–100. https://doi.org/10.1162/016366004323090278

Halliday, J., & Bucks, J. (2021, August 31). *Abdelhamid Abaaoud: what we know about the Paris attacks "mastermind."* The Guardian. https://www.theguardian.com/world/2015/nov/16/abdelhamid-abaaoud-suspected-mastermind-of-paris-terror-attacks

Hanneman, R. A., & Riddle, M. (2005). *Introduction to social network methods*. University of California. http://faculty.ucr.edu/~hanneman/nettext/

Hegghammer, T. (2010). The Rise of Muslim Foreign Fighters: Islam and the Globalization of Jihad. *International Security*, *35*(3), 53–94. https://doi.org/10.1162/isec_a_00023

Helfstein, S., & Wright, D. (2011). Covert or Convenient? Evolution of Terror Attack Networks. *Journal of Conflict Resolution*, *55*(5), 785–813. https://doi.org/10.1177/0022002710393919

Jackson, B. P. (2006). Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda. *Studies in Conflict & Terrorism*, *29*(3), 241–262. https://doi.org/10.1080/10576100600564042

Jervis, R. (2013). American Foreign Policy in a New Era. *Taylor and Francis Group*. https://doi.org/10.4324/9780203956298

Kelly, M., & McCarthy-Jones, A. (2019). Mapping Connections: A Dark Network Analysis of Neojihadism in Australia. *Terrorism and Political Violence*, *33*(4), 743–765. https://doi.org/10.1080/09546553.2019.1586675

Krebs, V. E. (2002). Mapping networks of terrorist cells. *CONNECTIONS*. https://www.aclu.org/sites/default/files/field_document/ACLURM002810.pdf

MetaTempo. (2001). *Hunting the sleepers*. Waybackmachine. Retrieved August 6, 2022, from https://web.archive.org/web/20071128125328/http://www.metatempo.com/huntingthesleepers.pdf

Morris, J. F., & Deckro, R. F. (2013). SNA data difficulties with dark networks. *Behavioral Sciences of Terrorism and Political Aggression*, *5*(2), 70–93. https://doi.org/10.1080/19434472.2012.731696

Pimentel, Fernando. (2015). Re: How can I measure similarity between two networks?. Retrieved from: https://www.researchgate.net/post/How-can-I-measure-similarity-between-two-networks/56333e015e9d97abcd8b45be/citation/download.

Pourhabibi, T., Ong, K. L., Boo, Y. L., & Kam, B. H. (2021). Detecting covert communities in multi-layer networks: A network embedding approach. *Future Generation Computer Systems*, *124*, 467–479. https://doi.org/10.1016/j.future.2021.06.027

Raab, J. (2003). Dark Networks as Problems. *Journal of Public Administration Research and Theory*, *13*(4), 413–439. https://doi.org/10.1093/jopart/mug029

Santifort, C., Sandler, T., & Brandt, P. T. (2012). Terrorist attack and target diversity. *Journal of Peace Research*, *50*(1), 75–90. https://doi.org/10.1177/0022343312445651

Shamieh, L., & Szenes, Z. (2015). The Rise of Islamic State of Iraq and Syria (ISIS). *Academic and Applied Research in Military and Public Management Science*, *14*(4), 363–378. https://doi.org/10.32565/aarms.2015.4.10

Simmel, G. (1906). The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology*, *11*, 441 - 498.

Spagna, N. (2018). Understanding the Command and Control through the Social Network Analysis: the case studies of the Paris-Brussels attacks. *Security Terrorism Society*. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/05/Understanding-the-Command-and-Control-C2-through-the-Social-Network-Analysis_-the-case-studies-of-Paris-Brussels-terrorist-attacks.pdf

Terrorism. (2023, March 27). Federal Bureau of Investigation. https://www.fbi.gov/investigate/terrorism

van Ostaeyen, P. (2019, April). *The History and Influence of the Belgian ISIS Contingent*. EUROPOL. https://www.europol.europa.eu/publications-events/publications/history-and-influence-of-belgian-isis-contingent

Vanhoucke, M., Coelho, J., Debels, D., Maenhout, B., & Tavares, L. V. (2008). An evaluation of the adequacy of project network generators with systematically sampled networks. *European Journal of Operational Research*, *187*(2), 511–524. https://doi.org/10.1016/j.ejor.2007.03.032

Wasserman, S., & Faust, K. (2012). *Social Network Analysis: Methods and Applications (Structural Analysis in the Social Sciences)*. Cambridge University Press. https://doi.org/10.1017/CBO9780511815478

Wu, P., & Li, S. (2011). Social Network Analysis Layout Algorithm under Ontology Model. *Journal of Software*, *6*(7). https://doi.org/10.4304/jsw.6.7.1321-1328

Xu, J., & Chen, H. (2008). The topology of dark networks. *Communications of the ACM*, *51*(10), 58–65. https://doi.org/10.1145/1400181.1400198

Appendix 1: 9/11 Hijackers Krebs V.E. (2002)

Appendix 2: Paris/Brussels network, network made in excel based on Spagna N. (2018)

Appendix 3: Paris/Brussels network, network made using Appendix 2 by removing non-attackers from network.

Software:

Social Network Visualizer v3.04

UCINET 6 v6.748 V S. Borgatti (2002)