UNIVERSITY OF TWENTE

The European Fight Against the Financing of Terrorism

A study of the European Union's Third AML/CFT Directive

Bachelor Thesis European Studies

Inca César Bloemkolk

(s0145807)

Faculty of Management and Governance

Department of Public Administration

Exam committee:

Supervisor: Dr. A.J.J. Meershoek

Second reader: Prof. dr. R.A. Wessel

Abstract

This thesis aims to study the EU's Third Directive on money laundering and terrorist financing and assess its adequacy for the purpose of combating the financing of terrorism. To carry out this research the thesis will center around the main research question: *To what extent is the Third AML/CFT Directive of the European Union adequate in dealing with the financing of terrorism?* In order to answer this question this thesis sheds light on the problem of terrorist financing and analysis the adequacy of the Third AML/CFT Directive through the scope of the Situational Crime Prevention approach. This approach argues that crime can be prevented through the usage of 'situational' measures aimed at decreasing the opportunities and increasing the efforts for criminals to commit crime. In this light, terrorist financing is seen as the crime, and the criminals are those individuals and organizations who gather and convey funds for terrorism purposes. By looking at the opportunities that enable terrorists to finance their activities an assessment is given on how adequately the Directive is aimed at preventing the process of terrorist financing.

This research finds that there are several areas in which the Third AML/CFT Directive is either lacking or inadequate for combating the financing of terrorism. The suitability of the anti-money laundering framework is questionable for the purpose of combating terrorist financing. Furthermore, private sector responsibilities in risk analyses have shown some fundamental flaws in achieving significant results and concerns over the violation of privacy, lack of transparency and accountability have been outlined.

Table of Contents

List of Abbreviations

AML – Anti-Money Laundering
CDD – Customer Due Diligence
CFSP – Common Foreign and Security Policy
CFT – Combating the Financing of Terrorism
CoC – Chamber of Commerce
CT – Counterterrorism
DoD – Department of Defense
EU – European Union
FARC – Revolutionary Armed Forces of Colombia
FATF – Financial Action Task Force
IRA – Irish Republican Army
JHA – Justice and Home Affairs
KYC – Know Your Customer
LTTE – Liberation Tigers of Tamil Eelam
ML – Money Laundering
PKK – Kurdistan Workers' Party
SCP – Situational Crime Prevention
STR – Suspicious Transaction Report
TF – Terrorist Financing
TFEU – Treaty on the Functioning of the European Union
UK – United Kingdom
UN – United Nations
US – United States

1. Introduction

This thesis will focus on the European Union's (EU) fight against the financing of terrorism. Terrorist organizations need money in order to carry out attacks, therefore preventing terrorists from acquiring funds to finance their activities is an essential part of the European fight against terrorism (Bures, 2010). This thesis investigates one specific instrument established by the EU in attempting to thwart terrorist financing. This instrument is known as Directive 2005/60/EC, or the *Third Directive on the prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing* (henceforth, the Third Directive) established by the European Parliament and the Council in 2005. The focus will lie on the problem at hand and on the implications and adequacy of the Third Directive and whether it has garnered any significant results for combating terrorist financing.

1.1 Background

The reasons for implementing policies regarding the combating of terrorist financing is that the EU is keen to conduct an "intelligence-led approach and improved information sharing within and between government and the private sector" (EU, 2005, p. 12). This approach has been adapted by the EU member states and remains a focal point of EU security policies, as attested by the Stockholm Program established in 2010 (European Council, 2010). The intelligence-led approach to combating the financing of terrorism can be characterized as "a proactive, preventative form of policing through the collection and analysis of massive sets of personal information with the help of smart technologies and in cooperation with private authorities" (Wesseling, 2013, p. 14). The Third Directive is the EU's "most important and comprehensive instrument for fighting terrorism financing" (Wesseling, 2013, p. 171). It is a tool for establishing cooperation with private authorities and it requires the storage and monitoring of data from clients in the banking and financial service sector, as well as the requirement for making 'risk assessments'.

Research conducted in the field of terrorist financing has for the most part been limited to describing which policies have been implemented and how they were implemented.

Literature on analyzing and evaluating these policies is scarce and sometimes lacking in validity (Wesseling, 2013). Therefore, this thesis will bring the described instrument under further analysis in order to investigate what this EU instrument has accomplished in the field of combating terrorist financing, how its composition matches the problem at hand, and what defects are apparent.

1.2 Problem definition & Research Questions

Terrorism attacks are regarded as a threat to European society and its democratic values. These attacks are carried out using products and means that require funding. This funding is what is known as the process of terrorist financing. Money could be seen as the 'lifeblood' of terrorist organizations since, without it, no significant attacks can be perpetrated. Preventing or detecting the flow of funds to terrorist organizations can disrupt their short-term operations and cripple their long-term aspirations. In today's world, where billions of daily financial transactions can easily mask those with terrorist intentions, detecting these transactions is not an easy task to say the least. Nevertheless, combating the financing of terrorism is considered to be an essential part of combating terrorism and therefore this thesis will focus on terrorist financing and the main EU policy that deals with this particular threat. Hence, the research question to be addressed in this thesis is the following:

To what extent is the Third AML/CFT Directive of the European Union adequate in dealing with the financing of terrorism?

In order to give a structured and clear answer to the research question, several sub-questions have been formulated, these are:

1. *How do terrorist organizations finance their activities?*
2. *How can opportunities that enable terrorists to finance their activities be diminished?*
3. *In what international legislative framework is the Third AML/CFT Directive embedded?*

4. *How is the Third AML/CFT Directive being used by the European Union to combat the financing of terrorism?*

1.3 Methodology

The following research will be descriptive and evaluative. It will be descriptive since I will be collecting and summarizing information on the Third Directive. The descriptive section essentially will introduce the problem(s) at hand and the instrument designed by the EU to counter it. First, the difficulties of defining terrorism and evaluating counterterrorism will be tackled, since it is crucial for this study to have an understanding of the concepts of terrorism and counterterrorism. Secondly, an overview of the specific problem will be given in chapter 3, showing the sources and methods that are used for funding terrorism. The theory of Situational Crime Prevention will briefly be discussed in chapter 4, which will give an insight into several opportunities that allow terrorism to be financed. The theory provides an analytical framework in which its preventive organized crime approach will be linked with terrorist financing. Chapter 5 and 6 will describe the efforts conducted in countering terrorist financing, both on the international and European level. Chapter 6 specifically, will describe and discuss the EU Third AML/CFT Directive. This will be done in order to shed light on its main features and intended results, and to relate them to what potential/theoretical impacts it may have regarding the combat against terrorist financing. The evaluative section will analyze the policy and will be outline its inadequacies, as well as making tentative recommendations for improvement.

As will be discussed in the literature review, evaluating counterterrorism policies does provide us with certain challenges to validity. As stated before, other factors, not including a certain CT-policy, may have affected the results from a policy outcome. Precisely guaranteeing that a certain result is derived from one particular policy is simply impossible to accomplish (Van Dongen, 2009). In order to minimize the threat to validity I will follow the recommendations discussed in the literature review, and not look at the counterterrorism policy effects as a whole in terms of the classical methods, but instead focus on very policy-specific outcomes, whose only possible source is the Third Directive.

As mentioned before, qualitative data will be used to conduct the necessary research for answering the research questions. This data will be collected by using document analysis (desk research), which implies using and examining already existing academic literature that comprises information about the topic. By utilizing primary sources such as documents from the EU official journal, and secondary sources, the document analysis will mainly provide the information needed to adequately describe the EU policy in question, and to critically analyze the aims of the policy in order to assess its adequacy for combating terrorist financing.

2. Literature Review

2.1 Defining terrorism

Although we hear the term 'terrorism' almost on a daily basis, there is no definitive, all-encompassing definition of terrorism. Before looking at measures being taken against the financing of terrorism, we must get a better understanding of what the concept of terrorism entails.

2.1.1 The difficulty of defining terrorism

What is it that constitutes terrorism? The term 'terror' has been used ever since the time of the French Revolution, during the so-called 'Reign of Terror' period from 1793 to 1794 (Giddens, 2006). During this excessively violent period the state used terrorizing methods against so-called 'enemies of the revolution'. Therefore, terror was associated with violence, oppression and torture conducted by the state (Hoffman, 2006). This phenomenon is now depicted as 'state terrorism' in academic literature. The meaning of terror – or terrorism – drastically changed during the 1880s when Russian revolutionary groups used violent tactics against the Russian state in an attempt to topple the czarist regime. This was the earliest form of terrorism directed against the state. During the rise of the totalitarian regimes in Italy and Germany in the 1920s and '30s, 'terror' became once again associated with violence perpetrated by the state (Hoffman, 2006). After the Second World War, the emergence of anti-colonialist, ethno-nationalist or separatist, or otherwise motivated groups, turned the tide as terrorism

was once again predominantly linked to violence perpetrated against the state. This 'yo-yo' effect of the concept of terrorism shows us that it is "a dynamic concept from the outset dependent to some degree on the political and historical context within which it has been employed" (Cronin, 2003, p. 34). Therefore, it is likely that the contemporary meaning and association with terrorism will be subjected to change in the future, adding to the complexity of finding a consistent, all-encompassing and universally accepted definition of terrorism.

Scholars have not yet been able to agree on certain aspects of what constitutes terrorism. One of the leading experts on the topic of terrorism, Bruce Hoffman (1998, p. 13) has stated it as follows: "Virtually any especially abhorrent act of violence that is perceived as directed against society – whether it involves the activities of anti-government dissidents or governments themselves, organized crime syndicates or common criminals, rioting mobs or persons engaged in militant protest, individual psychotics or lone extortionists – is often labeled 'terrorism'". This quote clearly illustrates how shrouded in controversy, emotion, inaccuracies and confusions surrounding the ongoing debate regarding the concept and phenomenon of terrorism is (Horgan, 2005). A fundamental problem is that according to Laqueur (1977) one being labeled a terrorist depends entirely upon the point of view of the definer. The phrase "one man's terrorist is another man's freedom fighter" (Laqueur, 1987, p. 7) perfectly illustrates this duality. One of the most recent examples of this are the pro-Russian separatist fighters in Eastern Ukraine. By the Ukrainian government in Kiev they are labeled as terrorists, whereas others call them freedom fighters. According to Hoffman (2006, p. 23), "[if] one identifies with the victim of the violence (…) then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not positive (…) light; and it is not terrorism". We can therefore say that apparently terrorism represents a different act to different people, meaning that an objective or value-free definition is further complicated (Laqueur, 1987). Equally biased are governments, as they too have differing views on what constitutes an act of terrorism or who or what a terrorist exactly is. As argued by Crenshaw (1995), states that sponsor terrorism will shape a definition that serves their own political ends. From this we can see that the concept of terrorism can suffer from bias as it is very much intertwined with sensitive issues that are emotionally and politically charged.

2.1.2 Characteristics of terrorism

It has become evident that establishing a universally accepted definition of terrorism has proven to be highly complicated. As its exact nature is still being debated, the search for an all-encompassing definition continues. Despite this, there is a growing consensus among scholars as to the core characteristics of terrorism regarding its motives and methods.

What are the core characteristics of terrorism? According to Deutch (1997, p. 12), "terrorism is best defined as acts of violence committed against innocent persons or non-combatants that are intended to achieve political ends through fear and intimidation". This definition contains some key elements of terrorism which are vital in answering the aforementioned question.

Regarding the first key element, it is safe to say that a terrorist primarily aims at achieving political objectives with the use of violence. In fact, in case of the "absence of a political aim, the activity in question will not be defined as terrorism" (Ganor, 2002, p. 294). Unfortunately, the political aims of terrorists vary greatly and are not always clear. Political objectives can be to coerce a change in the form of government, to amend certain social, political or economic policies, shifting state boundaries, or even compelling the withdrawal of military forces from what terrorists consider to be their homeland (Ganor, 2002; Primoratz, 2008). In this regard, terrorism is distinguishable from other forms of violence undertaken for non-political reasons.

A second key element of terrorism is the systematic and deliberate use of violence. Thus, "an activity that does not involve violence or a threat of violence will not be defined as terrorism" (Ganor, 2002, p. 294). Therefore, a protest with political objectives that strives to coerce change in a non-violent manner cannot be labeled as an act of terrorism. Here it should be noted that systematic and deliberate use of violence is not exclusively a characteristic of terrorism. In order for systematic and deliberate use of violence to be regarded as terrorism it must be linked with a political objective as mentioned above, as well as a third element.

The quote from Deutch mentioned at the beginning of this section contains that important third element. Fear can be used as a powerful tool in politics, or in achieving political objectives (Schmid, 2005). The term 'terrorism' is naturally intertwined with 'terror', a state of mind which is fed by fear. As Lenin once dryly stated, '[the] purpose of terrorism is to produce terror' (Schmid, 2005). A common characteristic of terrorism is the aim of targeting a wide audience, and instilling fear into the hearts and minds of a population (Bakker & Veldhuis, 2012). According to Kegley (2003, p. 22), "terrorism is aimed at the people watching, not at the actual victims. Terrorism is theater". The direct target of an attack oftentimes is not the main target, but rather serves as a tool to achieve whatever political objective the perpetrator wished to accomplish. In essence the terrorist is trying to create a 'theater of fear' in which the central idea is to 'kill one, frighten ten thousand'. We can witness this in the methods employed in the event of a terrorist attack. Placing a bomb on a public bus or densely populated train station, or flying planes into towers, are all ways to get a lot of people watching, and thus creating this environment of fear. As Jenkins (1975, p. 4) has stated: "Terrorists want a lot of people watching, not a lot of people dead".

2.2 Definitions of terrorism in practice

Now that we have highlighted the difficulty and problems associated with defining terrorism, and looked at its key characteristics, it is important to "conceptualize terrorism by determining where it fits within the study of politics" (Boulden & Weiss, 2004, p. 6). In doing so, this section will provide an overview of several operational definitions of terrorism used amongst governments and international organizations.

The *International Convention for the Suppression of the Financing of Terrorism* established by the UN General Assembly in 1999, refers to terrorism as an "act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act" (United Nations, 1999, p. 2). This definition contains the three key elements discussed in the previous section: violence, intimidation, and a political objective. This definition is somewhat

limited with the notion that intimidation can only be accomplished via an act of intentional bodily harm. In the EU, the Council makes a distinction between terrorist violence and political violent activism. In 2002, the Council Framework Decision on Combating Terrorism (Article 1) defined terrorism as "intentional acts (…) which given their nature and context, may seriously damage a country or an international organization where committed with the aim of seriously intimidating a population, unduly compelling a government or international organization to perform or abstain from performing an act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization" (Council, 2002, p. 4). Political violent activism differs from terrorism as the former is not targeting human lives or aiming to cause serious damage to social structures (Murphy, 2012). The United States Department of Defense (US DoD) defines terrorism as, "the unlawful use of violence or threat of violence, often motivated by religious, political or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political (US DoD, 2014, p. 251). This definition is slightly more encompassing as it includes the threat of violence. It also mentions fear as the tool of intimidation or in this case, coercion. A significant addition is the introduction of 'religious' and 'ideological' motives to the equation. Therefore, this definition may seem to be more encompassing than the previous definitions. However, 'political motives' should be considered in a broad sense. According to Ganor (2002, p. 294), "the motivation – whether ideological, religious, or something else – behind the political objective is irrelevant for the purpose of defining terrorism".

Even though differences in these three 'working' definitions are clearly visible, there is a common thread running through all of them. It is evident that definitions of terrorism used by governing entities agree on several core characteristics. Therefore, we can state that within the study of politics a certain act should only be labeled as terrorism when it constitutes; 1) an act of violence, 2) a political motive, and 3) with the intent to intimidate/cause fear.

2.3 Defining terrorist financing

As for the definition of 'terrorist financing' there is less debate over its context. In order to effectively prevent any financial influx for organizations or individuals motivated to carry out a terrorist offence, there must be a comprehensive definition of what encompasses the financing of terrorism. The EU gives such a definition in Article 1 of the Third Directive on money laundering and terrorist financing (ML/TF). It defines terrorist financing as "the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism" (EU, 2005, p. 20). The term 'funds' stands for any type of contribution, ranging from charity funds to state-sponsored funds. An exact description of the term is not included in the Council Directive. The International Convention for the Suppression of the Financing of Terrorism describes 'funds' as "assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, drafts, letters of credit" (UN, 1999, p. 2). The meanings of Articles 1 to 4 of the Council Framework on Combating Terrorism mentioned in the definition of terrorist financing constitute: "[1] Terrorist offences and fundamental rights and principles, [2] offences relating to a terrorist group, [3] offences linked to terrorist activities, and [4] inciting, aiding or abetting, and attempting [terrorism]" (Council, 2002, p. 4-5).

2.4 Evaluating counterterrorism policies

Assessing the effectiveness of counterterrorism policies would seem to be a logical component of the fight against terrorism. However, in contrast to the abundance of policies being implemented and academic articles being written on the topic of how terrorism should be fought, there is a significant gap in the literature regarding the effectiveness and adequacy of these measures. According to a study conducted by Lum, Kennedy and Sherley (2006, p. 33), "there has been a proliferation of anti-terrorism programs and policies as well as massive increases in expenditures toward combating

terrorism. Yet, we know almost nothing about the effectiveness of any of these programs". According to Van Um and Pisoiu (2011, p. 3), a major problem causing this knowledge deficiency is that "a generally accepted definition or framework of [CT] effectiveness does not exist in the literature to date". This lack of framework leads to various different approaches and indicators being utilized in order to study the effectiveness of counterterrorism measures. Popular measurements for success that have been utilized in the past generally focus on direct indicators such as the number of terrorist attacks that have been committed after a CT-policy was introduced, or the number of victims or material damage. Governmental actions have been monitored as well through the usage of the number of arrests as an indicator for success (Van Dongen, 2009).

Each one of these indicators has a specific set of problems regarding its validity of measuring success. However, in general, three key problems can be observed. Firstly, there is the so-called 'interpretation problem' as it is not clear whether the indicators mentioned above can be considered to be a success. There are many driving factors at work regarding the reasons for an increase in the number of attacks or in the number of arrests. Therefore, we must first know more about the driving factors and underlying causes of these fluctuations in the indicators before these indicators contain any real validity. Secondly, in case a certain indicator is indeed a good interpreter for success, there is what Van Dongen (2009) refers to as the 'attribution problem'. There are often a number of counterterrorism measures in place simultaneously. In effect this creates a problem for measuring effectiveness since it would be "unclear which instrument or measure or which combination of instruments or measures had brought about the desired effect" (Van Dongen, 2009, p. 8). The attribution problem and interpretation problem are strongly correlated since "gaining clarity about what caused a change in an indicator (…) will also shed light on whether that change is desirable or not" (Van Dongen, 2009, p. 8). The third key problem in measuring CT effectiveness is the "difference between operational and strategic success" (Van Dongen, 2009, p. 9). A mistake often made is regarding the fight against terrorism as a military dispute. In military disputes it is logical to think that the enemy is closer to 'winning' when the number and severity of attacks increase, or that it is 'losing' when the number of arrests increase. However, this belief comes from a logic of state-to-state warfare, and this often

"mistakenly applies (…) to a conflict between a state and a terrorist organization" (Van Dongen, 2009, p. 9). The key here is that the fight between a state and a terrorist organization is a political and not a military conflict.

This brief discussion shows how complicated it can be to evaluate the effectiveness and adequacy of counterterrorism policies. For this study we must take this into account and acknowledge that studying the effectiveness of combating terrorist financing policies is not an easy task since reliable and comprehensive data is not easily found (Bures, 2010; Van Um & Pisoiu, 2011). A solution proposed by Van Dongen (2009) is that instead of looking at the effects of counterterrorism measures as a whole, which is often the case in both scholars and policy makers alike, a more pinpoint approach should be considered. A tailor-made approach to every individual policy could lead to a more accurate evaluation of a particular policy and nullify some of the validity problems mentioned before. For the purpose of this thesis, such pinpoint indicators of success would be the number of Suspicious Transaction Reports (STRs) created by the regulatory entities that fall under the Third Directive. These STRs are sent to Financial Intelligence Units (FIU), where they are evaluated and can deem certain transactions as indeed being suspicious which can be used by intelligence agencies in order to conduct more thorough investigations. The purpose and significance of STRs will be discussed in more detail further on in this thesis.

3. The problem of terrorist financing

In order to study the way the EU combats the financing of terrorism, it is important that we look at the ways in which terrorism is financed and what measures have been taken against this on the global level of governance. This chapter will address the question: *how do terrorist organizations finance their activities*? Thus, giving us an in-depth look at the *modus operandi* of terrorist financing as well as providing an overview of the initiatives taken by the United Nations and the Financial Action Task Force (FATF).

3.1 Sources of terrorist financing

Terrorist organizations employ various ways of gathering the financial means necessary for carrying out their activities. As we know from our literature review, terrorism is a dynamic concept subjected to constant change. The financing of terrorism has a similar nature and is characterized by stemming from a diverse plethora of sources obtained via illegal as well as legitimate means (Clunan, 2013; Giovanna, 2009). We can roughly distinguish the following four sources of terrorist finances: state support, donations, legal economic activities, and illegal or criminal activities (Bakker & Donker, 2006).

Throughout history there have been many instances of state-sponsored terrorism, examples being the IRA, Hezbollah, and the Nicaraguan 'Contras'. These organizations could rely on support respectively from Libya, Iran and the United States (Bakker & Donker, 2006). In recent times the state support for terrorist organizations has diminished significantly under great international pressures. However, several states still provide direct or indirect support to organizations which are classifiable as terrorist (Clunan, 2013). Additionally, a state's lack of action in countering terrorism could be regarded as state support (Bakker & Donker, 2006). Many states have tolerated the presence of terrorist organizations within their borders and in some extreme cases the unhindered presence of terrorist training camps, as was the case with the Taliban regime in Afghanistan (Bantekas, 2003).

Donations are considered to be the primary source of income for ultra-nationalistic and Islamic terrorist organizations. In this instance internationally operating 'charity' organizations play an important role in gathering money through the financial donations of people both aware and unaware of their terrorist linkages (De Goede, 2007). The giving of alms ('Zakat' in Arabic), is the most important source of income for Islamic charity foundations. Zakat plays an important role in countries such as Saudi Arabia, in which income tax does not exist for religious reasons. Instead of income tax, individuals are expected to donate 2,5 percent of their income to a good cause. Unfortunately, some of these donations find their way to charity organizations financing terrorist activities (Bantekas, 2003; De Goede, 2007; Raphaeli, 2003).

A different form of terrorist financing is done through seemingly legal economic activities, which in turn can be divided in two kinds of activities. Firstly, by generating financial means through legal companies which are later employed for conducting terrorist acts. Reportedly, Al-Qaeda set up businesses in the construction and transport sector in various countries during the 1990s, whereas Hamas reportedly owns several companies in the textile industry (Bakker & Donker, 2006). Secondly, by investments and speculations done on the financial market by the organizations themselves. Allegedly, right before the 9/11 attacks specific speculations were done by terrorist organizations involved in the attacks, however, hard facts are lacking (Bakker & Donker, 2006). It is clear though that several terrorist organizations do possess expert knowledge about the workings and procedures of the financial sector.

The final source of terrorist finances comes from illegal or criminal activities. Financial means can be derived from cigarette smuggle, robbery, drug trade, arms deals, diamond trade, human trafficking, as well as through financial crimes such as fiscal fraud, credit card fraud, and extortion (Bantekas, 2003). Drug trade is a widely used method of generating income by terrorist organizations, especially in Colombia by the terrorist group FARC and by Islamic or separatist groups operating in Turkey (PKK) and Afghanistan (Taliban) (Bakker & Donker, 2006). These cases are also depicted as 'narco-terrorism' in literature and the media.

3.2 Methods of distribution

Similar to the variety of sources for terrorist finances, the distribution methods for moving capital from A to B are equally diverse. Both informal and formal channels are used for distribution, such as money transaction offices and 'underground banking' (Raphaeli, 2003; De Goede, 2007).

The legal and formal banking system is an often used channel for distributing financial means supporting terrorism. The majority of these transactions are inconspicuous as they get lost in a stream of international financial transactions, such as e.g. wire transfers of Saudi parents to their children studying abroad (Bakker & Donker, 2006). Also, so-called 'stored value cards', which are payment cards with a monetary value

stored on it, and 'prepaid debit cards', which are reloadable debit cards that do not require having a bank account, can be easily used for spending and distribution of terrorist money. It is possible to buy these with a false identity and can be easily distributed without requiring any digital data or personal information (Ridley, 2012).

Terrorist organizations go to great lengths to mask and erase their financial tracks in order to avoid detection. Often organizations will use a so-called 'feeder and operations accounts' framework, in which regular transfers from 'feeder' to 'operations' accounts are made via various suspense accounts in an attempt to mask terrorist financing (Raphaeli, 2003). These 'feeder' accounts can be administered by charity organizations and companies, and 'operations' accounts by anonymous or trustworthy individuals. The suspense accounts which are used in order to erase the direct links between 'feeder' and 'operations' accounts, can be administered by anonymous third parties, which further complicates its detection (Giovanna, 2009). It has been reported that some organizations make use of complicated financial constructions utilizing offshore companies which are portrayed as banking institutions in order to attract investors willing to invest in phony investment projects. The investments have been linked to terrorist organizations purchasing and trading in real estate (Delrue, 2014).

Besides the formal channels through which funds are distributed, a large amount of funding is conducted through informal channels. These channels, such as 'underground banking', are often favored as they manage to reach isolated areas without formal banking systems in place. The so-called 'Alternative Remittance System' (ARS), is an informal wire transfer system which is also known as 'Hawala' (De Goede, 2007; Delrue, 2014). The Hawala consists of the transfer of money from one party to another without the interference of any formal financial institution. Hawala is often used because it is perceived as faster, more reliable and further reaching than other methods of money transfer, and it is regarded as perhaps the foremost method of terrorist financing (De Goede, 2007).

4. Opportunities for terrorist financing: A Situational Crime Prevention approach

Now that we have a better understanding of what entails terrorist financing, this chapter will address the question: *How can opportunities that enable terrorists to finance their activities be diminished*? It aims to shed light on the *opportunities* in which terrorist financing can occur and so-often go undetected, and how these can be prevented. In order to do so, the following chapter will make use of a theory borrowed from criminology which is designed for preventing organized crime. Criminological theory can be applied to the topic of terrorism prevention since terrorism and organized crime, in many ways, are not so different from each other (Clarke & Newman, 2007). In essence, this chapter will serve to establish a link between organized crime and terrorism which will be used in order to analyze the problem of terrorist financing in light of the so-called *Situational Crime Prevention* (SCP) theory.

As we know from the literature review, the research into the origins and reasons for terrorism is extensive and many theories have been derived attempting to explain the phenomenon of terrorism. Many theories focus on psychological explanations for terrorism, e.g. 'Relative Deprivation', 'Social Distance', and 'Contagion' theories. In these psychological theories, violence is often seen as the end-product of their presumed psychological complications. However, other researchers have opted for different approaches in order to explain terrorism, e.g. 'instrumental approach', 'organizational approach', 'economic approach', in which violence is not seen as the end product of a terrorist, but merely as a tool to achieve its political aims. Therefore, terrorists do not simply violate for the sake of violating (Crenshaw, 1995). These theories and approaches all contribute to a better understanding of the phenomenon of terrorism. Unfortunately, terrorism as such is still underdeveloped in terms of our understanding and in terms of theorizing (Özdamar, 2008). Moreover, the scarcity of terrorism theory is eclipsed by the lack of theorization in the field of counterterrorism.

4.1 Organized crime and criminological theory

Criminology provides us with certain theories which are concerned with countering organized crime. Organized crime in itself bears many resemblances with terrorism. Similarly to terrorism, there is no common understanding of what entails organized crime as scholars and policy-makers differ from their views on what is prevalent in the area of organized crime. One view holds that organized crime is primarily concerned with 'crime' and as such represents a criminal activity. It distinguishes itself from ordinary crime in its level of sophistication, continuity and rationale (Von Lampe, 2008). In this view, organized crime can be characterized as 'rational criminal activity'. A different view argues that the emphasis lies on the word 'organized'. It is argued that organized crime can only occur with the existence of an organization or group participating in illicit activities. As such, organized crime refers to certain criminal organizations, and disregards lone offenders. A third and final view sees organized crime as neither primarily focused on 'crime' nor 'organization', but rather concerned with the concentration of power. This would manifest itself either in the form of an underworld network or even 'government', and/or as an alliance between criminals and corrupt political and economic elites (Von Lampe, 2008). As witnessed by these different dimensions, organized crime is similar to terrorism in the sense that they are both very dynamic concepts and are therefore challenging to deter.

Criminological theories offer us an insight into how law enforcement agencies deal with the problem of organized crime. Currently the majority of criminological theory focuses on social determinants or root causes of criminal behavior. These root causes are notoriously difficult to influence, therefore studies in crime prevention have been conducted which have established preventive theories of combating organized crime by manipulating the 'environment' (Van der Bunt & Van der Schoot, 2003). With 'environment' is meant, the places of (potential) crimes and spatial factors. This focus has created so-called 'environmental criminology' which studies crime and criminality in relation to particular places and the way in which individuals and organizations form their criminal activities spatially, which in turn is influenced by place-based or spatial factors (Brantingham & Faust, 1976). A popular theory from environmental criminology is 'Rational Choice' theory which provides the basic rationale for the importance of

'place', as it proposes that offenders will select targets and acquire means for achieving their goal in a manner that can be rationally explained (Cornish & Clarke, 2014). An additional theory of importance is the so-called 'Opportunity' theory which seeks to reduce opportunities for committing crime. Both these theories are the foundation of the 'Situational Crime Prevention' approach (Clarke, 1997).

4.2 Situational Crime Prevention

As the name implies, situational crime prevention aims at forestalling the occurrence of a crime, rather than on the sanctioning or punishing of perpetrators. It focuses on the settings for crime, rather than on those carrying out criminal acts. It deviates from other criminological theories in the sense that it does not focus on prevention by improving societal conditions or other factors leading to criminal behavior, but rather on making criminal acts less attractive to (potential) criminals. Essential to this approach is not the criminal justice system, but instead it relies on an array of public and private institutions and organizations[1] "whose products, services and operations spawn opportunities for a vast range of different crimes" (Clarke, 1997, p. 2). Situational crime prevention is comprised of so-called 'opportunity-reducing' techniques and measures that "1) are directed at highly specific forms of crime; 2) involve the management, design or manipulation of the immediate environment in as systematic and permanent way as possible; 3) make crime more difficult and risky, or less rewarding (…) as judged by a wide range of offenders" (Clarke, 1997, p. 4).

Situational measures are to be tailored to specific types of crime. The rationale behind this is that crime should not be looked upon from a broad perspective but rather with a very specific understanding of the details of a certain category of crime. A similar type of approach is drawn by Van Dongen (2009) in the area of evaluating counterterrorism measures, mentioned in the literature review. It is ineffective to view either terrorism or organized crime as homogeneous and/or one-dimensional. Much like the process of money laundering, the criminal act of financing terrorism can be carried out in many ways, with different sources, methods, and motives. Whether funding is provided with

[1] Examples given by Clarke (1997) include: schools, hospitals, shops and malls, transit systems, phone companies and manufacturing businesses, pubs and parking lots, local parks and entertainment facilities.

the giving of alms via *zakat* to charity organizations, or donations from terrorist sympathizers, through either the formal financial sector or Hawala-type systems, they all should be depicted as specific problems requiring tailor-made 'situational' counter measures. Altering the environment in which a certain crime can take place aims at affecting the risk assessments made by potential criminals in terms of benefits and costs or possible danger. Thus, reducing the opportunities for a crime to be committed could affect the modus operandi of criminal (terrorist) organizations reducing the number of incidences of a specific crime (Clarke, 1997). Situational crime prevention offers five principles to alter the environment for criminals and make crime less attractive. According to Clarke (1997) these are: 1) increase required efforts for crime to be committed, 2) increase the risk of criminal acts being detected, 3) make crime less rewarding, 4) remove excuses which offenders can use to justify their actions, 5) remove precipitating factors which could provoke criminal activities. The approach of situational crime prevention is deliberately general as it makes no distinction between any category or type of crime. This notion is what makes the situational prevention approach fitting for analyzing terrorist financing, since the assumption is made that situational prevention is "applicable to every kind of crime, not just to 'opportunistic' or acquisitive property offenses, but also to more calculated or deeply-motivated offenses (…) [w]hether offences are carefully planned or fueled by hate and rage, they are all heavily affected by situational contingencies" (Clarke, 1997, p. 5).

According to Van de Bunt and Van der Schoot (2003, p. 20), "criminal activities (…) have to be analyzed to reveal the facilitating role of situational factors". These situational factors can be used to intervene and obstruct the opportunities for criminal activities to take place. This is the crime prevention approach which is divided into five different steps: "1) Collection of data about the nature and dimensions of a specific crime phenomenon; 2) Analysis of the situational conditions which permit or facilitate the commission of the crime under construction; 3) Study of possible instruments aimed at blocking the opportunities for this kind of crime; 4) Implementation of the chosen measures; 5) Evaluation of the results and dissemination of the good practices" (Van de Bunt & Van der Schoot, 2003, p. 20-21). Central to this approach is the idea that "opportunity makes the terrorist [meaning that] the specific opportunities and

circumstances that each criminal or terrorist act requires will depend on the specific requirements of that particular crime" (Newman & Clarke, 2010, Brief 09)[2].

Utilizing a particular case example from the Netherlands, the remainder of this chapter will focus on applying the principles and approaches of situational crime prevention to the act of terrorist financing.

4.3 SCP in TF: Tamil Tigers in the Netherlands

The particular case discussed in this section shows what 'situational' measures can look like in practice and how they can be applied for the prevention of terrorist financing. In this case situational measures have been applied to an important source of terrorist finances; fundraising.

4.3.1 The Case

In 2010 Dutch law enforcement officials arrested 27 individuals suspected of gathering funds for the LTTE, the so-called 'Tamil Tigers', which had been placed on the European Union's list of terrorist organizations in 2006 (Weenink, 2011). The suspected criminals were presumably fundraising via door-to-door charity collections, yard sales, retail of DvDs and calenders and organizing illegal lotteries. The Tamil Tigers were known to retrieve funds worldwide, through similar sources and methods as used in the Netherlands (Human Rights Watch, 2006). Members of the LTTE allegedly pressured the Tamil community in the Netherlands to donate money for their cause (Weenink, 2011). With the help of these funds the LTTE conducted terrorist attacks in Sri Lanka over the course of several decades. However, it is impossible to know exactly which terrorist attacks were financed with the money raised in the Netherlands.

[2] The book *Policing Terrorism: An Executive's Guide,* written by Newman and Clarke (2010), is oriented towards policy makers and officials within law enforcement and does not include any page numbers. Instead it consists of 50 instructions or *briefs* which are numbered.

4.3.2 Situational measures against LTTE

The case of the LTTE in the Netherlands provides us with some views on what situational measures can be taken against the financing of terrorism. The criminal process of terrorist financing globally consists out of three steps: 1) the *gathering* of funds, 2) the *conveying* of funds, and 3) the *spending* of funds (Weenink, 2011). The final step does not fall under the scope of possible preventive measures being taken by law enforcement, whereas the first two steps do fall under that scope. The LTTE gathered funds through several ways, some of which were legal, such as charging entry fees at cultural and sportive events. The conveying of the created revenue to an organization with terrorist intent is what converted the funding from entry fees into a criminal act. Another legal way of fundraising was through the use of donations for the purpose of charity work. This was likely done on the basis of false promises and deceit on what the true purpose of the donations would be. Fully illegal was the collecting of money through extortion and threats to the Tamil diaspora in the Netherlands (HRW, 2006). Often the LTTE did not operate under its own name, but would set-up front organizations such as the *World Tamil Association, Tamil Coordinating Committee, Tamil Rehabilitation Organization,* and *Tamil Youth Organization* (Weenink, 2011; HRW, 2006). Dutch law enforcement officials arrested several of the leaders of these organizations, which led to their eventual downfall.

Ignorance among municipalities about the background of these front organizations has been the likely cause why these organizations were easily granted permits for organizing events. Education for municipalities conducted by the intelligence services or Ministry of Security and Justice representatives, could decrease the amount of permits being granted for organizing fundraising events by suspicious organizations (Weenink, 2011). A second measure could be to impede these type of organizations to be allowed to register at the Chamber of Commerce. This would obstruct the cloak of legality that these organizations use in order to acquire funds. These two measures would target the gathering of funds, whereas the measures already in place regarding anti-money laundering laws can be used to detect and prevent the conveying of funds to the terrorist organizations.

4.3.3 Conclusion

These situational-type measures show how the principles and steps of the situational crime prevention approach can alter the opportunities for terrorist financing. The steps of the crime prevention approach, discussed by Van de Bunt and Van der Schoot (2003), can be clearly seen. Four out of the five steps are being dealt with in this brief example case. Acquiring knowledge by law enforcement agencies about the nature of these (front) organizations in the Netherlands would be step one. The second step represents the facilitating opportunities these fundraising organizations had regarding the easy acquiring of permits and registration at the Chamber of Commerce (CoC). Steps three and four are represented in the blocking or altering of these opportunities through the denial of permits and hindrance of registration at the CoC. Increasing the required efforts for committing a crime is the first principle of situational crime prevention (Clarke, 1997). The way in which this example case shows how opportunities for terrorist fundraising can be obstructed and reduced, is a method of increasing the required efforts for committing that crime. The anti-money laundering regulation, which will be discussed extensively further on in this thesis, can increase the risk of terrorist financing being detected, thus ensuring the second principle of the SCP approach. The arrest of the 27 individuals involved in the gathering of funds for the LTTE can potentially make the financing of terrorism less rewarding, which upholds the third principle as mentioned by Clarke.

5. International CFT efforts

The continuously increasing cohesion of national, European and global law and order has led to the vision that when looking at how individuals, companies and other non-state actors are influenced by international decisions it is no longer adequate to only look at the European Union when investigating European political or legal issues (Wessel, 2006). This is even more the case with the problem of terrorist financing as this chapter will serve to portray the cohesion between European legislation and the international community decisions. In portraying this cohesion, this chapter will address

the question: *In what international legislative framework is the Third AML/CFT Directive embedded?*

The threats associated with the financing of terrorism are constantly evolving, which requires periodical actualizations of the measures in place to combat against this crime. Following the recommendations, resolutions and directives from international organizations such as the FATF, UN, and EU, the member states of these organizations have opted to follow two distinct approaches to combat the financing of terrorism (Johnson, 2008). Firstly, the preventative approach has led to the establishment of a series of obligations for the various financial entities, casinos, lawyers, notaries, etc., through which they must identify certain suspicious transactions. Secondly, the repressive approach has consisted of the blacklisting of individuals and organizations suspected of terrorist linkages or activities, on which sanctions have been imposed or assets have been frozen (Schneider & Caruso, 2011).

The EU policy combating the financing of terrorism is embedded in a larger global framework. This framework consists of multiple initiatives including UN resolutions and other international treaties. Relevant UN conventions and resolutions include the *International Convention for the Suppression of the Financing of Terrorism* (1999), the *UN Security Council Resolution 1267* (1999), and *1373* (2001). The International Convention for the Suppression of the Financing of Terrorism shows that terrorist financing was a global concern prior to the events of 9/11. Under this convention it has become illegal for any person to provide or acquire funds with the intention of using them - or with the knowledge that these funds will be used – for carrying out any acts of terrorism. Furthermore, in the same year as the convention, the Security Council adopted Resolution 1267, which was directly targeted at retrieving Osama Bin Laden from the Taliban and the freezing of all financial assets owned or controlled by the Taliban (UN, 1999). In the wake of the 9/11 attacks the Security Council Resolution 1373 was adopted in order to oblige its member states to refrain from any type of cooperation with any terrorist group, as well as urging for the immediate freezing of funds of anyone linked to acts of terrorism (UN, 2001). These resolutions formed the basis for the freezing and seizing of funds and assets in the EU with the adoption of Council Regulation (EC) No. 2580/2001. This required the blacklisting of persons and

organizations suspected of carrying out, or contributing to, acts of terrorism, in particular Osama Bin Laden and the Al Qaeda and Taliban networks. These economic sanctions were aimed at cutting off the flow of funds for terrorist organizations and to thwart their activities. A special committee of the UN was established for the development of lists containing names of individuals and organizations who were (supposedly) affiliated to terrorism, resulting in the freezing of their assets (Levi, 2010). However, the utilization of such 'blacklists' have raised controversy, as they were deemed to be incompatible with fundamental rights. Most prominently the *praesumptio innocentiae* is violated as proposals for additions to the blacklist have to describe the nature of the supporting evidence, but are not required to provide the actual evidence itself in case it could raise national security concerns (De Goede, 2011). Additionally, it remains unclear what the criteria are for blacklisted individuals or organizations to be scraped from that list (Levi, 2010).

These UN conventions and resolutions have been incorporated by the FATF into nine special recommendations on which the current EU CFT measures are largely based (Wesseling, 2013). The FATF is an intergovernmental policy-making body consisting of group of OECD member states. The nine special recommendations (see table 1) it has established are guidelines for regulating all types of financial transactions in order "to detect, prevent and suppress the financing of terrorism and terrorist acts" (FATF, 2001, p. 2).

Table 1: FATF's Nine Special Recommendations

1. *Ratification and implementation of UN instruments* – notably the 1999 Convention and Resolutions 1267 and 1373.
2. *Criminalizing the financing of terrorism and associated money laundering* – to give legal means and resources to investigating, prosecuting and punishing terrorist financing.
3. *Freezing and confiscating terrorist assets* – to prevent flows and punish terrorists.
4. *Reporting suspicious transactions related to terrorism* – to ensure the correct scope and timelines of suspicion reporting and action by those subject to a duty to report.
5. *International Cooperation* – to ensure mutual legal assistance and information exchange (civil, criminal and administrative) between countries relating to inquiries and proceedings.

6. *Alternative Remittance Systems* – to increase transparency and control over funds outside the conventional financial system and not subject to FATF standards.
7. *Wire transfers* – to make basic information available to the criminal justice system, intelligence and regulated entities.
8. *Non-profit organizations* – to prevent their abuse for TF purposes.
9. *Cash couriers* – to stop suspicious cross border flows and enable sanctions and confiscation where indicated.

Source: Howell et al., 2007, p. 13

The FATF does not possess binding powers to enforce these recommendations, however they are widely recognized as the international standard in combating the financing of terrorism. These recommendations do not extend directly to all EU member states as not all EU member states are members of the FATF. However, in the FATF's aim to extend its set standards to all areas, the European Commission has become a member of this intergovernmental body, and with that the FATF recommendations have been passed into Community law and apply to all EU member states. A comprehensive overview of how the FATF special recommendations have been implemented into EU law is given by Wesseling (2013):

Table 2: FATF Special Recommendations implemented into EU legislation

EU CFT Legislation	**FATF Special Recommendations to combat terrorism financing**
Regulation (EC) 2580/2001 freezing funds of suspected terrorists Common Position 2001/931/CFSP	SR 1: Ratification and implementation of UN instruments SR 3: Freezing and confiscating terrorist assets
Regulation (EC) 881/2002 implementing UN Al Qaeda and Taliban sanctions	SR 1: Ratification and implementation of UN instruments SR 3: Freezing and confiscating terrorist assets
Third Directive on the prevention of the use of the financial system against money laundering and combating the financing of terrorism (2005/60/EC)	SR 1: Ratification and implementation of UN instruments SR 2: Criminalizing the financing of terrorism SR 3: Freezing and confiscating terrorist assets SR 4: Reporting suspicious transactions related to terrorism SR 5: International co-operation SR 6: Alternative remittance SR 7: Wire transfers
Regulation Controlling Cash in the Community (EC) No 1889/2005	SR 9: Cash couriers

Regulation (EC) No 1781/2006 on information on the Payer Accompanying Transfers of Funds	SR 7: Wire transfers
Directive 2007/64/EC Payment Services Directive	SR 6: Alternative remittance

Source: Wesseling, 2013, p. 17

6. The EU Third AML/CFT Directive

With the knowledge in mind of the cohesion between international law and the EU Third Directive, this following chapter will address the question: *How is the Third AML/CFT Directive being used by the European Union to combat the financing of terrorism*?

The Third Directive is the most extensive EU instrument in fighting the financing of terrorism with a far-reaching impact on the daily financial transactions of ordinary citizens. It compels professionals of financial institutions and other regulated entities[3] to increase surveillance and vigilance on their clients and financial accounts. A central element in this surveillance is the 'Customer Due Diligence' requirement. According to those requirements regulated entities must acquire knowledge on the identity of their client, record and analyze the transactions made, and report any transaction that seems suspicious to a national Financial Intelligence Unit (FIU). These reports are known as 'Suspicious Transactions Reports' (SRT), and are a vital component in the tracking of terrorist transactions. The Third Directive relies on public-private security cooperation and is an example of the EU intelligence-led approach to fighting terrorism (Wesseling, 2013). The EU's increasing focus on the tracking of terrorist transactions is exemplified by this Directive which is a 'preventive effort' to combat the financing of terrorist activities (Allam & Gadzinowski, 2009). By posing monitoring and control duties on regulated entities, the Third Directive aims at:

- Identifying clients and monitor their transactions in order to preemptively detect terrorists and associated partners.

[3] Such entities are: insurance companies, auditors, credit institutions, notaries and independent legal professionals, real estate agents, casinos, dealers or legal persons trading in goods worth a minimum of EUR 15.000, trust or company service providers (EU, 2005).

- Disrupting terrorist activities by denying access for (alleged) terrorists to funding and access to money.
- Enhancing the prominence, confidence and security of the financial system by inhibiting the movement of legally or illegally acquired financial means for terrorist ends through the usage of the formal financial system (Wesseling, 2013).

With that being said, it is important to stress that the Third Directive does not directly compel the national regulatory entities to implement its requirements. Any Directive drawn-up by the EU compels the member states to implement its content by passing it into national legislation. However, the member states are able to chose in which way they are willing to implement the EU Directive. Article 288 TFEU provides as follows: "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods". Therefore, the Third Directive has been passed into national law by all the member states. In for instance, the Netherlands, this EU decree has led to the creation of the *Wet ter voorkoming van Witwassen en Terrorismefinanciering*. It is this national law that compels all the regulatory entities of the Netherlands to oblige and follow the requirements of the Third Directive, while utilizing the form and methods established by the Dutch legislator. This notion is important for our understanding of the implications of the Third Directive for European regulatory entities.

6.1 Risk-based approach

Replacing the so-called First and Second Anti-Money Laundering Directives (91/308/EEC and 2001/97/EC), the Third Directive represents a major shift in the composition of anti-money laundering legislation. The main differences are the addition of two key elements, which led to the fight against terrorist financing being mentioned explicitly and incorporated for the first time into the AML framework, as well as the introduction of a new type of approach; a risk-based approach.

The inclusion of 'terrorist financing' to the Directive was considered a logical step after the terrorist events that occurred in the US, Spain and the UK between 2001 and 2005.

The importance given to anti-money laundering legislation as a central element of combating terrorist financing is due to the fact that both phenomena share common characteristics. Both make use of the formal financial system to carry out international transactions and cash transfers of 'clean' or 'criminal' money, as well as service providers outside the formal financial sector (Wesseling, 2013).

The second major shift to occur was going from a rule-based approach in the First and Second Directives to a risk-based approach in the Third Directive. A rule-based approach calls for the utilization of a specific set of norms applied to every transaction. These norms are detailed and clear in order to properly assess a transaction, such as the explicit obligation to report every cash transfer exceeding the limit of €15.000,- (Van den Broek, 2011). This particular norm, along with multiple other norms, constitute a kind of 'check-the-box' list which financial officials (e.g. bank employees) use to 'score' a transaction based on a point system. If the transaction exceeds a certain amount or percentage of points it is deemed as suspicious and must be reported as such (Wesseling, 2013). Although clear and explicit in nature, financial institutions have considered the rule-based approach to be ineffective and disproportionally time consuming. Its rigid character meant that all transactions were approached similarly, without any reflection or assessment of the necessity of such actions. Moreover, it was believed that if criminals would be aware of the norms on these checklists they would adapt their transactions in order to seem non-suspicious (Van den Broek, 2011).

The surge of Jihadist terrorism in the West in the first lustrum of the 21st century, has led to 'risk assessment' and 'risk management' becoming crucial components in the so-called 'War on Terror' (Amoore & De Goede, 2005). Risk management aims at handling uncertainties in an organized way in which control over the financial sector can strengthen while allowing the mobility and flow of money to continue unhindered (Bergström et al., 2011). This implies that a risk-based approach is more flexible than a rule-based approach, as the former aims at differentiating high and low risk transactions and customers in order to allocate resources more precisely to those cases deemed suspicious. This efficiency is achieved by focusing on specific combinations of criteria instead of investigating all possible transactions. Combinations can consist of various kinds of risks such as "customer risk, product or services risk, and geographical risk"

(Wesseling, 2013, p. 183). These risks are evaluated according to the dynamics of terrorism and the changing terrorist financing trends that occur, and are adapted accordingly. Therefore, it is hard for terrorists to adopt a certain behavior that allows their transactions to go undetected (Amoore & De Goede, 2005). Increasing the difficulty for suspicious transactions to go unnoticed, and attesting to the intelligence-led approach, risk-based software is used in order to continuously monitor transactions whereby unusual or suspicious transactions can be 'red-flagged' almost instantly (Wesseling, 2013).

The risk-based approach implemented in the Third Directive thus addresses shortcomings of the rule-based approach. Regulated entities and their professionals have been given more flexibility and discretion regarding the procedures surrounding transaction monitoring. The goal in doing so is to design more cost-effective procedures and to reduce the administrative burden on the regulatory entities. According to Wesseling (2013, p. 183), "the risk-based approach brings great efficiency in the system in that it enables banks to dedicate their resources to those things which are of higher risk and those customers of lower risk cannot be burdened with undue due diligence". Therefore, this approach requires a more active and analytical behavior from banks and other financial entities. As stated in Article 34 of the Third Directive, these entities must produce reports that demonstrate "adequate and proportionate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication" (EU, 2005, p. 29). The Third Directive therefore entails a shift of authority and responsibility from the public to the private sector regarding matters of national security (Bergström et al, 2011; Van den Broek, 2011).

6.2 Customer Due Diligence

An essential part of the risk-based approach of the Third Directive is the principle of Customer Due Diligence (CDD). This principle requires the regulatory entities subjected under the Third Directive to gain information on the identity of their customers and related transactions. In the First and Second Directives this was referred to as the 'Know Your Customer' (KYC) element, and in the Third Directive this was modified into the

more detailed and flexible identification requirements of the customer due-diligence procedures. Originally, the notion of due diligence entails a practice "through which the parties to a merger spend time checking the balance sheets and legal histories of their potential partners before closing the deal" (Maurer, 2005, p. 476). Although this definition is tailored to corporate mergers and acquisitions, it can be used similarly for customer due-diligence in the field of CFT.

The way in which the Directive is structured there are two main requirements for an adequate customer due-diligence assessment; 'customer identification' and 'transaction monitoring' (EU, 2005). The former is the enhanced version of the KYC principle from the First and Second Directives which requires the regulatory entity to conduct a thorough background check on any new customer or business relationship. The second requirement requires said entities to carry out monitoring procedures on any transactions amounting to €15.000,- or more (EU, 2005). As stated in Article 8 of the Third Directive, customer due diligence measures include:

a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

c) obtaining information on the purpose and intended nature of the business relationship;

d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date (EU, 2005, p. 23).

In this decree we can identify the two main requirements of CDD, in which measures A, B, and C fall under the customer identification requirements, and D calls for the monitoring of transactions. The Third Directive set out these CDD requirements on three levels: 'regular CDD', 'simplified CDD', and 'enhanced CDD'. Regular CDD urges the regulatory entity to oblige to measure A to D mentioned above. Simplified CDD, the

regulatory entity is permitted to conduct reduced CDD measures for certain customers or businesses. This is specified under Article 11 which exemplifies cases that are entitled for simplified CDD.

Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;

(b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts;

(c) domestic public authorities (EU, 2005, p. 24).

In case of enhanced CDD, the regulatory entity must take a set of further steps on a risk-sensitive basis. An explanation of 'enhanced CDD' is given in Article 13 which occurs in matters in which a customer can "present a higher risk of money laundering or terrorist financing" (EU, 2005, p. 25) or in case the regulatory entity has not had a face-to-face meeting with the customer or business. In Article 13 the Third Directive describes this additional set of steps as follows:

a) ensuring that the customer's identity is established by additional documents, data or information;

b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by this Directive;

c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution (EU, 2005, p. 25).

In sum, the CDD procedures regulate how a customer must present itself in order to be admitted into the formal financial system. By way of risk assessments and scenarios, ideal types of ordinary financial conduct can be identified, which constitutes the vast majority of regular customers on the financial market, or suspicious transactions can be red-flagged. The assumptions of what can be regarded as potential terrorist financing is shaped by the FATF's special recommendations regarding this field, with the occasional

financial intelligence from FIUs (Wesseling, 2013). These assumptions have been implemented and formed into risk-analysis software and scenarios which outline the fight against terrorist financing.

6.3 Suspicious Transaction Reports and Financial Intelligence Units

6.3.1 STRs

When a financial institution or other regulatory entity has reason to believe that a transaction has been obtained through criminal activities, or are related to funding terrorism, they are obligated to report these suspicions to the Financial Intelligence Unit of their country. It is imperative that a financial institution does not notify their customers that a report of suspicious transaction has been sent to the relevant authorities (Schott, 2006).

A suspicious transaction can be defined as any transaction that deviates from the normal patterns of account activity, or 'script'. According to Schott (2006, p. 116), "any complex or unusually large transactions – in addition to any unusual patterns of transactions absent an apparent economic, commercial, or lawful purpose – are suspect and, therefore, merit further investigation by the financial institution and, if necessary, by the appropriate authorities". In order to spot these type of transactions the financial institutions should apply risk-based limits to monitor accounts which are seen as high-risk. Financial institutions are at all times required to be vigilant for any suspicious transactions. Indications of suspicious transactions are vast and the signs to look for are many, as can be seen in the overview given in the appendix of this thesis.

Basically, an STR is a tool for alerting authorities that a specific transaction could possibly be related to either money laundering or terrorist financing, and should be further investigated. Most often the financial institution will not have an exact knowledge nor evidence of the crime being committed, it simply is aware that a transaction is unusual and does not fit the normal patterns. Since the financial institution is unaware of the crime and cannot inquire the customer due to the risk of alerting said customer (Chatain et al., 2009). Therefore, the employee of the institution

should file a suspicious transaction report and leave the further investigation of the case to the appropriate authorities.

6.3.2 FIUs

The FIUs are the only agency that receive and process STRs in order to ensure centralization for an efficient preventive national and international framework against the misuse of the financial system for the purpose of money laundering and terrorist financing. Thus playing a vital role in the tracking and detecting of terrorist financing.

The primary goals of an FIU are "[1] to identify, trace, and document the movement of funds; [2] to identify and locate assets that are subject to law enforcement measures; [3] to support the prosecution of criminal activity" (Schott, 2006, p. 128). In order to achieve these goals, all FIUs in the world share three core functions: *receive, analyze* and *circulate* the information provided via the STRs to combat money laundering and terrorist financing (Chatain et al., 2009). The circulation of the financial information should be done both domestically and internationally. For this purpose the Egmont Group was created, which aims at providing a global forum comprised of 139 FIUs to date that stimulates international cooperation and information sharing in the fight against money laundering and terrorist financing.

Analyzing the information the FIU receives through the STRs is essential as often these transactions, though unusual, may appear innocent. However, even mundane-looking financial activities, such as cash withdrawals, ordinary deposits, transfer of funds, etc., can in fact be important pieces of information in detecting and prosecuting criminal activity (Chatain et al., 2009). Distinguishing between truly suspect transactions and those that are merely unusual, requires thorough examination and analysis on a well-informed basis.

7. Analysis

The following chapter will provide an overall analysis of the Third Directive in which the final sub-question of this thesis will be addressed by highlighting the competence/incompetence regarding the framework of the Third Directive in terms of adequacy for CFT. The second part of this analysis will link the Third Directive to the theory of Situational Crime Prevention and approach the competences and shortcomings in the fight against terrorist financing through the lens of criminology.

7.1 Introduction

So far this study has shown that combating the financing of terrorism is a tedious task requiring skill and resources. The complexity of the Third Directive is bound to create pitfalls which have been highlighted by academics and governing bodies alike. Such pitfalls are often made up of legal issues consisting of whether the Directive is compatible with the upholding of fundamental rights and civil liberties (Mitsilegas & Gilmore, 2007). A major concern that has become apparent, and is shared by many stakeholders in the field, are the meager results yielded by the Third Directive's outline regarding the combating of terrorist financing. As a report by the Commission (2012) shows, the compliance with the requirements outlined by the Third Directive is sufficient. Meaning that the regulatory entities subjected to the requirements show a satisfactory compliance regarding implementation and reporting. However, the effectiveness of the Directive is difficult to measure as there is a significant lack of quantitative data and only limited qualitative information (Bures, 2010). Moreover, it is argued that measuring the preventive effect of the FATF recommendations is practically impossible (Howell, 2007), which has implications for the Third Directive as this is based largely on those recommendations.

Observing these significant pitfalls, it is important to analyze the processes and mechanisms that drive and constitute the Third Directive.

7.2 The use of the Third Directive in the fight against terrorist financing

A primary objective of the Third Directive is to detect any possible transactions linked to terrorist financing and identify terrorists and their financers. The number of received STRs can be used as an indicator of the effectiveness and adequacy of the Third Directive in combating terrorist financing. However, a problematic feature of this indicator is that the FIUs responsible for processing the STRs do not always publish their data in standardized formats. A clear discrepancy can be seen in the fact that some FIUs indicate the number of STRs related specifically to terrorist financing, whereas others do not (Wesseling, 2013). This creates uncertainty since reports could be concerning either money laundering or terrorist financing. This may lead to a problem of validity when applying the statistics of FIUs to terrorist financing specifically. For instance, in the Netherlands the 2010 annual report of the Dutch FIU reported that it had received a total of 183.395 STRs, but they do not indicate which of these reports were specifically linked to terrorist financing, stating only that, regarding the financing of terrorism, several interesting cases had been shared with investigation agencies (FIU-NL, 2010). The reason for this vagueness in reporting comes from the fact that the Dutch Ministry of Finance decided that on the basis of reducing administrative burden, regulatory entities were exempted from indicating whether there was a suspicion of money laundering or terrorist financing (Wesseling, 2013). The FIU of the United Kingdom reported that in 2011, 247.601 STRs had been received, of which 662 were suspected of being transactions for terrorism, which amounts to 0.27% of the total number of received STRs (SOCA, 2012). It should be stressed that, due to the extremely low occurrence of terrorism, it is complicated to conclude that this low percentage of reported potential cases of terrorist financing, should be interpreted as a success or failure.

A similar lack of distinction between money laundering and terrorist financing in reporting can be noticed in the usage of discourse by the main EU institutions. In EU documents such as the 2012 Commission Report, money laundering and terrorist financing are either mentioned together or only references to money laundering are made. The sole mentioning of terrorist financing is extremely rare or altogether non-existent, and in the case of the Third Directive it is only mentioned on its own when the definition of terrorist financing is given. This notion can be an indication for the

unsuitability of the AML framework for CFT. Hence, a major point of criticism questions whether the AML framework constructed in the First and Second Directives is in fact suitable for combating terrorist financing. In the wake of the deadly terrorist attacks in the US and Europe, the concept of terrorist financing was added to the already existing anti-money laundering framework. Most notably after the 2004 Madrid attacks, a sense of urgency led to political leaders in Europe wanting to take swift action. Therefore, due to the sense of urgency and the overlapping characteristics that are shared by money laundering and terrorist finances, European leaders opted for using a legislative framework already established in 1991 with the enactment of the First AML Directive. However, this choice has been taken into question as it appears to have a number of downsides since the methods of combating money laundering do not necessarily apply to the financing of terrorism (Bures, 2010). Although sharing some similarities[4], their differences are more apparent. Money laundering is aimed at deriving profits from illegally obtained funds through criminal activities. In essence, money launderers try to wash or clean-up the tracks left by 'dirty money'. On the other hand, terrorist finances are often funds that have been obtained through legal means and before a crime has been committed, since terrorists have political aims, making profits is not their ultimate goal. Terrorist finances only become criminal after the transferring of funds to an individual or organization associated with terrorism. This process is also referred to as 'money dirtying' or 'reversed money laundering' which usually consists of small monetary amounts which are not necessarily derived through illegal methods (Delrue, 2014). Perhaps the most prominent issue is that by implementing terrorist financing into the AML legislative framework, the assumption is made that terrorism financiers to the same extent make use of the formal financial system as money launderers in organized crime (Wesseling, 2013). However, as mentioned in chapter 3, funding for terrorism often moves through informal systems, or alternative remittance systems, such as Hawala. These significant differences between money laundering and terrorist financing contribute to the high level of difficulty that surrounds the detection of terrorism-related money flows with the usage of AML instruments.

[4] These similarities occur most notably in the operational process upon entering the formal financial system in which both phenomena use the same methods of 'placement', 'layering', and 'integration' in order to erase tracks of either criminal origins (money laundering) or criminal purposes (terrorist financing). Placement refers to the money that is placed into the financial system; layering constitutes the masking of origins by moving the funds around different accounts and institutions; and integration refers to the purchase of legitimate assets, e.g. real estate, property, stock (Clunan, 2013).

In addition to the primary objective of the Third Directive, a more general objective can be seen as maintaining the stability and reputation of, and confidence in, the financial sector. This objective is virtually impossible to measure quantitatively and in terms of effectiveness. The numbers of received STRs and those transactions deemed as being related to terrorist financing, do not reveal the total amount of transactions being made for the financing of terrorism. The terrorism-related STRs merely show the transactions that have been detected, not those that have gone by undetected. As such it is impossible to give a percentage on how many of the terrorism-related transactions have in fact been intercepted. Moreover, with regard to stability, it should be questioned whether the funds that are transferred for terrorism purposes really pose any threat to the stability of the financial sector. The most expensive terrorist attack by far to ever have been recorded were the attacks of 9/11. The planning and execution of the attacks cost somewhere between $400.000 and $500.000 (NCTA, 2004). It is highly unlikely that such an amount could cause any damage to the financial sector specifically.

The Third Directive has altered the central approach of the previous two Directives from a rule-based approach to a risk-based approach. This shift has had major consequences for the responsibilities of national security as it shifted from the public to the private sector. The implications of this are that, as a result, a group of private actors consisting of detection software developers, legal experts and banking officers are in charge of identifying risky customers and monitor all suspicious transactions, whereas the public authorities are in charge of acting upon the information reported by the private actors and oversee the implementation of the Third Directive. Ultimately, the decisions made by the private sector structure the investigations conducted by FIUs and the possible prosecution of terrorists or their financers (Wesseling, 2013). Hence, the private sector has become a 'first line of defense' by making security decisions and paving the way for financial investigations carried out by the public authorities. This shift in public-private responsibilities has created an interest for regulatory entities (in particular banks) to be compliant with the legislation of the Third Directive, in order to not suffer any reputational damage and avoid being fined by the supervising authorities. A priority for banks and other regulatory entities to be compliant with the Third Directive, is not the same as actually combating the financing of terrorism. This would imply that finances for terrorism passing through the formal financial system can remain undetected, even

when the obliged entities fulfill all the CFT requirements of the Third Directive. This could be the case with terrorists having low risk profiles and only transferring small monetary amounts through low risk services in ways that fit normal patterns. Alternatively, this notion of compliance could suggest that individuals or organizations are wrongfully included into FIU databases, as bank employees may defensively report transactions to satisfy supervisory authorities and show their compliance with the CFT requirements.

The risk-based approach aims at being more flexible than its predecessor and thus reduces the administrative burden on the regulatory entities in charge of complying and better quality reporting of suspicious transactions. However, this approach does pose a number of challenges. As certain risks regarding customers, services, products or geographical areas are allowed to be prioritized in the risk-based analysis, monitoring practices and identification requirements are operationalized according to certain 'risk scores'. These scores are assigned to anything related to the transaction under scrutiny, ranging from the customer's profile, the financial product, or the countries involved. Customers labeled as high-risk are subjected to enhanced due diligence procedures, whereas others to regular or simplified due diligence procedures. The norms that are attached to this risk scores are intentionally flexible in order to respond to the dynamic nature of terrorist financing methods. A down-side to this is that decision-making procedures are plagued by the lack of transparency, legal certainty and accountability (Bures, 2010). It remains unclear when and on the basis of what information decisions are made regarding suspicions for certain transactions. Since the monitoring and reporting of suspicious transactions must remain entirely hidden to customers it is not possible for them to complain or appeal against such a report. Furthermore, there is evidence to believe that "defensive reporting of fictive suspicious transactions takes place" (Wesseling, 2013, p. 210) due to the previously discussed compliance interests. This may lead to individuals being wrongfully added to police databases which "makes the case for accountability all the more urgent" (Wesseling, 2013, p. 210). Moreover, it is important to stress that the risk-based approach in risk-analysis software is not an objective mathematical approach, but rather an approximate set of assumptions on the sources and methods of terrorist financing. The flagged transactions deemed as suspicious by the risk-based software are always assessed by humans on their

significance and they decide what further actions are taken. This assessment requirement by a private professional can potentially lead to racial profiling and discrimination as certain individuals can be picked out based on their names (e.g. Arabic names) or behaviors (e.g. frequent money transfers to or from Arabic countries) (Mitsilegas & Gilmore, 2007).

Furthermore, the obligation to report all suspicious transactions has raised privacy concerns amongst predominantly legal professionals (i.e. lawyers and notaries), that the obligation is breaching their lawyer-client relationship and confidentiality. Moreover, the right to a fair trial and respect for private life was said to be breached according to these legal actors. However, in 2007 a court ruling from the European Court of Justice (ECJ) regarding the Second Directive which was the first instance that lawyer reporting was obligated, ruled in case C-305/05 that the right to fair trial was not breached by the Second Directive (Bergström et al., 2011), which carried on into the following Third Directive. The allocation of maximum powers to the FIUs granting them almost unlimited access to any financial, administrative, and law enforcement data that they require for conducting proper research, can cause conflicts with data protection regulation resulting in privacy issues for the regulatory entities reporting the data (Allam & Gadzianowski, 2009). Lastly, concerns over privacy rights have been voiced on the process of matching customer identification information with various blacklists as a requirement for the customer due diligence procedures. These lists could potentially lead to unjustified reputational and financial damage as they not only contain names of convicted individuals and organizations, but also of suspected persons and entities (Wesseling, 2013).

7.3 Applying Situational Crime Prevention theory to the Third AML/CFT Directive

The techniques, steps and principles of Situational Crime Prevention theory which have been discussed in Chapter 4, can be applied to the Third Directive in order to see whether preventive measures for organized crime can shed light on the mechanisms of the Third Directive. Furthermore, the analytical tools that are provided by Situational Crime Prevention theory can be used to uncover the areas of the Third Directive which

can be improved in terms of adequacy for fighting crime in the form of terrorist financing.

For the purpose of analytical clarity it is useful to recall the principles of SCP theory. The first two principles of SCP theory regard the increased efforts for criminals, and the increased risk of detection. The third principle deals with removing the reward for crime and making it less lucrative. The fourth and fifth principles deal with removing excuses for offenders to justify their actions, and removing any precipitating factors which could lead to criminal activity. For the case of terrorist financing, the first, second and third principles seem to be most applicable and relevant as an approach towards combating these criminal acts.

The primary principle of the Third Directive is in line with SCP theory in the sense that it alters the environment in which terrorists and their associates are capable of transferring funds. This deterrent effect for terrorist financing in the formal financial system cannot be measured easily, as it implies the need for counting terrorism-related transactions that did not occur. The possibility exists that the deterrent effects of the Third Directive have caused a shift towards different means of transferring funds that lie outside of the formal financial system, and thus outside the scope of the Third Directive. In this case, the policy will have fulfilled the first two principles of SCP theory in that it has increased the efforts required for terrorist transactions and the risk of being detected, by denying terrorists access to the formal financial sector. However, two side notes to this potential claim should be made. Firstly, the possible exclusion of terrorists from the formal financial system can lead them to make increased use of alternative financial systems, such as Hawala-type systems. Secondly, it is not unlikely that terrorist financiers continue using the services provided in the formal financial system but avoid being detected by utilizing false identities and conducting transactions in ways that are not regarded as suspicious.

According to the second ‘opportunity-reducing’ technique of SCP theory, the management, design and manipulation of the environment should be dealt with in as systematic and stable way as possible. With respect to the risk-based approach introduced in the Third Directive, the distortion that exists between regulatory entities

falling under its scope, has been discussed in the previous section of this analysis. Drawing from SCP theory, it is important that supervisory authorities within and amongst jurisdictions develop common guidelines and practices for regulatory entities regarding the risk-based approach. Based on the principle of subsidiarity, common and standardized set of guidelines and practices can most effectively be established by the EU in order to improve the risk-based reporting of suspicious transactions. Additionally, this technique should be applied to the standardization of reporting for all FIUs in order to avoid such discrepancies as can be seen between different European FIUs.

Perhaps the most powerful tool of the Third Directive in terms of SCP theory, is the requirement of customer due diligence procedures to be conducted on every customer or client. The CDD procedure attributes greatly to the Third Directive's capacity in increasing the effort that is required to conduct a financial transaction on the formal financial system. Moreover, it satisfies the second principle by increasing the risk of a customer being detected as being a financier for a terrorist organization. In order to increase the scope of the CDD procedure, the threshold for monitoring procedures required with every transaction of €15.000,- or more can be lowered in order to fortify the first and second principle of SCP theory. This in turn could alter the environment for financial transactions and increase the risk of detection when transferring smaller amounts of money as is often the case with terrorist financing.

8. Conclusion

This final conclusion will serve as the answer to the main research question: *To what extent is the Third AML/CFT Directive of the European Union adequate in dealing with the financing of terrorism?*

This study of the EU's Third Directive for combating money laundering and terrorist financing has shown that the field in which this policy impacts consists of both private and public actors. Private actors, identify high-risk customers and monitor their transactions. In turn, the public authorities receive the reports sent by the private actors and act upon this information and supervise the correct implementation of the Third

Directive. This division of roles means that a wide array of private entities and actors are responsible for detecting and pre-selecting profiles which they see as being suspicious and potentially high-risk. This is done through the process of individual and subjective decisions, albeit on a risk-sensitive basis. Subsequently, these decisions are implemented by public authorities for structuring the further investigations into these profiles. By charging regulatory entities otherwise not involved in combating terrorism, a shift has taken place as these entities are now fully involved in the terrorism prevention measures. In a sense they have become unpaid criminal investigators, which in practice leads to compliance with the regulations rather than actively seeking to combat terrorist financing.

Furthermore, the risk-based approach has been designed in accordance with the intelligence-led approach to counterterrorism. This is done in order for the future to seem manageable by calculating risk scores and monitoring transactions with the help of risk-sensitive software, and matching profiles against blacklists. However, the analysis of this assumption has shown that in practice risk analysis depends on the risk reports produced by regulatory entities that have been produced by gathering client and transaction information or by specific compliance software. This denounces the assumption that the standards for risk analysis are neutral and objective. In fact, it is derived from information that is deemed suitable for calculation, and more importantly from shared subjective assumptions about who are most likely to finance terrorism, and where this is likely to happen. Moreover, the eventual STRs which are sent to the FIUs are always made by humans, leading easily to subjective reporting. Thus, reports about suspicion and potential risk are essentially based on ethical and social standards and beliefs rather than mathematical and technological standards. This can lead to security decisions amongst similar entities being distorted, for instance when similar cases are treated in a way that varies from bank to bank.

Another vital characteristic of the risk-based approach is its flexibility. The dynamic changes in modus operandi of terrorists can be used to justify this flexibility, however a downside to this approach is the creation of legal uncertainty and lack of transparency. The fact that every bank can draw its own compliance strategy and create its own risk assessments leaves much room for subjectivity, rogue-like behavior in terms of

discrimination, privacy violations, and a general lack of insight into the thinking processes leading up to these reported suspicions.

The short-comings of the Third Directive are not at all surprising given the fact that detecting terrorist finances through the monitoring of customers and transactions is a very complicated task. A complicating factor lies in the fact that the costs of terrorist acts are relatively low and do not require abnormal financial behavior which can be detected. Furthermore, the occurrence of terrorism is rare and the methods of financing it are diverse, which makes it extremely complicated to establish meaning risk scenarios.

In the search for an appropriate answer to the question whether the Third Directive can be deemed adequate in combating the financing of terrorism, this research has shown that the Third Directive encounters many shortcomings and has been unable to garner any significant results with respect to the detection of suspected terrorists. In light of the meager outcomes and apparent inadequacies of the Third Directive, perhaps the focus should not lie on whether or not this instrument garners significant statistical data and prevents terrorist financing, but rather on its power to change the environment of the financial sector. In line with the principles of SCP theory, the ultimate goal is to make life harder for terrorists. By reducing the opportunities they have for committing financial crimes and making sure they have to be on their guard when conducting any financial transactions, the Third Directive may have garnered results which unfortunately are virtually impossible to measure empirically. Instead they venture in the realm of those individuals that had contemplated making a terrorist finance transaction but ultimately abstained and refrained from executing their plan.

References

Allam, M., Gadzinowski, D. (2009). Combating the Financing of Terrorism: EU Policies, Polity and Politics. *EIPASCOPE, 2*(1), 37-43.

Amoore, L., De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law & Social Change, 45*(1), 149-173.

Bakker, E., Donker, T.J. (2006). Bestrijding van Terrorismefinanciering: Succes en Falen in beleid. *Atlantisch Perspectief, 30*(3), 12-20.

Bakker, E., Veldhuis, T. (2012). A Fear Management Approach to Counter-Terrorism (ICCT Discussion Paper February 2012). Retrieved from: http://www.icct.nl/download/file/ICCT-Veldhuis-Bakker-Fear-Management-February-2012.pdf

Bantekas, I. (2003). The International Law of Terrorist Financing. *The American Journal of International Law, 97*(2), 315-333.

Bergström, M., Svedberg Helgesson, K., Mörth, U. (2011). A New Role for For-Profit Actors?: The Case of Anti-Money Laundering and Risk Management. *Journal of Common Market Studies, 9*(5), 1043-1064.

Boulden, J., Weiss, T. (2004). *Terrorism and the UN: Before and After September 11*. Bloomington: Indiana University Press.

Brantingham, P.J., Faust, F.L. (1976). A Conceptual Model of Crime Prevention. *Crime & Delinquency, 22*(1), 284-296.

Bures, O. (2010). EU's Fight against Terrorist Finances: Internal Shortcomings and Unsuitable External Models. *Terrorism and Political Violence, 22*(3), 418-437.

Chatain, P.L., et al. (2009). *Preventing Money Laundering and Terrorist Financing: A Practical Guide for Bank Supervisors.* Washington D.C.: The World Bank.

Clarke, R.V. (1997). *Situational Crime Prevention: Successful Case Studies*. Albany: Harrow and Heston Publishers.

Clarke, R.V., Newman, G.R. (2007). Police and the Prevention of Terrorism. *Policing*, *1*(1), 9-20.

Clunan, A.L. (2013). The Fight against Terrorist Financing. *Political Science Quarterly, 121*(4), 569-596.

Cornish, D.B., Clarke, R.V. (Eds.). (2014). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New Brunswick: Transaction Publishers.

Council of the European Union. (2002). Council Framework Decision of 13 June 2002 on combating terrorism. *Official Journal of the European Union*, 2002/475/JHA.

Crenshaw, M. (1995). *Terrorism in context*. University Park: Pennsylvania State University Press.

Cronin, A.K. (2003). Behind the Curve: Globalization and International Terrorism. *International Security, 27*(3), 30-58.

Cronin, A. K., & Ludes, J. L. (Eds.). (2004). *Attacking Terrorism: Elements of a Grand Strategy.* Washington D.C.: Georgetown University Press.

De Goede, M. (2007). Underground money. *Cultural Critique, 65*(3), 140-163.

De Goede, M. (2011). Blacklisting and the ban: Contesting targeted sanctions in Europe. *Security Dialogue, 42*(6), 499-515.

Delrue, G. (2014). *Witwassen en Financiering van Terrorisme* (3rd edition). Antwerpen: Maklu Uitgevers N.V.

Deutch, J. (1997). Terrorism. *Foreign Policy, 108*(3), 10-22.

European Commission. (2012). Report from the Commission to the European Parliament and the Council of 11 April 2012 on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Retrieved, 5 January, 2015, from http://www.eurofinas.org/uploads/documents/policies/AML/20120411_report_en.pdf

European Council. (2010). The Stockholm Programme – an open and secure Europe serving and protecting citizens. *Official Journal of the European Union*, 2010/C 115/01.

European Union. (2005). Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Retrieved, 15 November, 2014, from http://eur-ulex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:en:PDF

FATF. (2001). *FATF IX Special Recommendations*, FATF Standards (October 2001). Retrieved 24 December, 2014, from http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/9specialrec/fatf-9specialrec.pdf

FIU Nederland. (2010). *Jaaroverzicht 2010*. Zoetermeer: FIU Nederland. Retrieved 15 January, 2015, from http://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/u3/FIU%20Jaaroverzicht%202010.pdf

Ganor, B. (2002). Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? *Police Practice and Research, 3*(4), 287-304.

Giddens, A. (2006). *Sociology* (5th edition). Oxford: Blackwell Publishers.

Giovanna, M.D. (2009, April). *The EU and the fight against terrorist financing after 9/11: institutionalizing cooperation beyond pillars.* Paper presented at ECPR Joint Sessions Workshop 28, Lisbon, Portugal.

Hoffman, B. (1998). *Inside Terrorism*. London: Victor Gollancz.

Hoffman, B. (2006). *Inside Terrorism* (Revised and expanded ed.). New York: Columbia University Press.

House of Lords. (2009). Minutes of Evidence Taken Before The Select Committee on the European Union (Sub-Committee F) on Money Laundering and the Financing of Terrorism, 4 March 2009. Retrieved, 7 January, 2015, from http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/132ii.pdf

Horgan, J. (2005). *The Psychology of Terrorism*. New York: Routledge.

Howell, J., & Co. (2007). The EU's efforts in the fight against terrorist financing. *European Commission,* Retrieved 14 December, 2014, from http://www.statewatch.org/news/2007/sep/eu-terr-finance-report-2007.pdf

Human Rights Watch. (2006). Funding the "Final War": LTTE Intimidation and Extortion in the Tamil Diaspora. *Human Rights Watch, 18*(1), 1-47.

Jenkins, B.M. (1975). International Terrorism: A New Mode of Conflict. In D. Carlton & C. Schaerf (Eds.), *International Terrorism and World Security.* London.

Johnson, J. (2008). Is the global financial system AML/CFT prepared?. *Journal of Financial Crime, 15*(1), 7-21.

Kaunert, C., Giovanna, M.D. (2010). Post-9/11 EU counter-terrorist financing cooperation: differentiating supranational policy entrepreneurship by the Commission and the Council Secretariat. *European Security, 19*(2), 275-295.

Kegley, C.W. (2003). *The New Global Terrorism: Characteristics, Causes, Controls.* Upper Saddle River: Prentice Hall.

Kingdon, J.W. (1995). *Agendas, alternatives, and public policies: Second edition.* New York: Harper Collins College Publishers.

Laqueur, W. (1977). *Terrorism*. Boston: Little, Brown and Company.

Laqueur, W. (1987). *The Age of Terrorism*. Boston: Little, Brown and Company.

Levi, M. (2010). Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance'. *British Journal of Criminology Special Issue Terrorism: Criminological Perspectives, 50*(4), 650–669.

Lum, C., Kennedy, L., & Sherley, A. (2006). *The Effectiveness of Counter-Terrorism Strategies-A Campbell Systematic Review.* Oslo: The Campbell Collaboration.

Maurer, B. (2005). Due Diligence and "Reasonable Man," Offshore. *Cultural Anthropology, 20*(4), 474-505.

Mitsilegas, V., Gilmore, B. (2007). The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards. *International Comparative Law Quarterly, 56*(1), 119-141.

Murphy, C.C. (2012). EU Counter-Terrorism Law. Oxford: Hart Publishing.

National Commission on Terrorist Attacks. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: W.W. Norton & Company.

Newman, G.R., Clarke, R.V. (2010). *Policing Terrorism: An Executives Guide*. Washington D.C.: U.S. Department of Justice.

Özdamar, Ö. (2008). Theorizing Terrorist Behavior: Major Approaches and Their Characteristics. *Defense Against Terrorism Review, 1*(2), 89-101.

Primoratz, I. (2008). A Philosopher looks at Contemporary Terrorism. *Cardozo Law Review, 29*(1), 33-51.

Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism and Political Violence, 15*(4), 59-82.

Ridley, N. (2012). *Terrorist Financing: The Failure of Counter Measures.* Cheltenham: Edward Elgar Publishing Limited.

Schmid, A. (2005). Terrorism as Psychological Warfare. *Democracy and Security, 1*(2), 137-146.

Schneider, F., Caruso, R. (2011). The (Hidden) Financial Flows of Terrorist and Transnational Crime Organizations: A Literature Review and Some Preliminary Empirical Results. *Economics of Security Working Paper 52,* Berlin: Economics of Security. Retrieved 14 December, 2014, from http://www.diw.de/documents/publikationen/73/diw_01.c.386645.de/diw_econsec0052.pdf

Schott, P.A. (2006). *Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism.* Washington D.C.: The World Bank.

Serious Organized Crime Agency. (2012). *Annual Report and Accounts 2011/2012*. London: The Stationary Office. Retrieved 15 January, 2015, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229080/0291.pdf

United Nations. (1999). *International Convention for the Suppression of the Financing of Terrorism*, English version, Retrieved 22 November, 2014, from http://www.un.org/law/cod/finterr.htm

United Nations. (2001). *Resolution 1373,* Retrieved 23 December, 2014, from http://unscr.com/en/resolutions/1373

United States Department of Defense (2014). *Department of Defense Dictionary of Military and Associated Terms,* 8 November 2010 (as amended through 15 November 2014). Retrieved 28 November, 2014, from www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Van Um, E., & Pisoiu, D. (2011). *Effective counterterrorism: What have we learned so far?* Economics of Security Working Paper 55, Economics of Security, Berlin.

Van den Broek, M. (2011). The EU's preventive AML/CFT policy: asymmetrical harmonization. *Journal of Money laundering Control, 14*(2), 170-182.

Van der Bunt, H., Van der Schoot, C. (Eds.). (2003). *Prevention of Organised Crime.* Meppel: Boom Juridische Uitgevers.

Van Dongen, T. (2009). *Break it Down: An Alternative Approach to Measuring Effectiveness in Counterterrorism.* Economics of Security Working Paper 23, Economics of Security, Berlin.

Von Lampe, K. (2008). Organized Crime in Europe: Conceptions and Realities. *Policing, 2*(1), 7-17.

Weenink, A.W. (2011). De rol van de recherche bij terrorismepreventie. *Justitiële verkenningen, 37*(2), 87-107.

Wessel, R.A. (2006). *The Invasion by International Organizations: De toenemende samenhang tussen de mondiale, Europese en nationale rechtsorde.* University of Twente: oration.

Wesseling, M. (2013). *The European Fight against Terrorism Financing: Professional Fields and New Governing Practices*. Den Bosch: Uitgeverij BOXPress.

Appendix

Overview of indications of suspicious transactions:

General signs:
- Assets withdrawn immediately after they are credited to an account.
- A dormant account suddenly becomes active without any plausible reason.
- The high asset value of a client is not compatible with either the information concerning the client or the relevant business.
- A client provides false or doctored information or refuses to communicate required information to the bank.
- The arrangement of a transaction either insinuates an unlawful purpose, is economically illogical or unidentifiable.

Signs regarding cash transactions:
- Frequent deposit of cash incompatible with either the information concerning the client or his business.
- Deposit of cash immediately followed by the issuance of checks or transfers towards accounts opened in other banks located in the same country or abroad.
- Frequent cash withdrawal without any obvious connection with the client's business.
- Frequent exchange of notes of high denomination for smaller denominations or against another currency.
- Cashing checks, including travelers' checks, for large amounts.
- Frequent cash transactions for amounts just below the level where identification or reporting by the financial institution is required.

Signs regarding transactions on deposit accounts:
- Closing of an account followed by the opening of new accounts in the same name or by members of the client's family.
- Purchase of stocks and shares with funds that have been transferred from abroad or just after cash deposit on the account.
- Illogical structures (numerous accounts, frequent transfers between accounts, etc.).
- Granting of guarantees (pledge, bonds) without any obvious reason.
- Transfers in favor of other banks without any indication of the beneficiary.
- Unexpected repayment, without a convincing explanation, of a delinquent loan.
- Deposit of checks of large amounts incompatible with either the information concerning the client or the relevant business.

Source: Schott, 2006, p. 117-118