Economics of Security Working Paper Series

economics-of-security.eu

Stefan D. Haigner, Friedrich Schneider and
Florian Wakolbinger

Combating money laundering and the financing of terrorism: A survey

April 2012

Economics of Security Working Paper 65

This publication is an output of EUSECON, a research project supported by the European Commission's Seventh Framework Programme.

European Security Economics
EUSECON
www.economics-of-security.eu

Economics of Security is an initiative managed by DIW Berlin

Correct citation: Haigner, S.D., Schneider, F. and Wakolbinger, F. (2012). "Combating money laundering and the financing of terrorism: A survey". Economics of Security Working Paper 65, Berlin: Economics of Security.

First published in 2012

ISSN: 1868-0488

For further information, please contact:

Economics of Security, c/o Department of Development and Security, DIW Berlin – German Institute for Economic Research, Mohrenstr. 58, 10117 Berlin, Germany.

Tel: +49 (0)30 89 789-277

Email: eusecon@diw.de

Website: www.economics-of-security.eu

Combating money laundering and the financing of terrorism: A survey*

Stefan D. Haigner[#], Friedrich Schneider[#, §] and Florian Wakolbinger[#]

[#] University of Linz

This version: April 13, 2012

Abstract:

Policy programs on anti-money laundering and combating the financing of terrorism (AML/CFT) have largely called for preventive measures like keeping record of financial transactions and reporting suspicious ones. In this survey study, we analyze the extent of global money laundering and terrorist financing and discuss the preventive policies and their evaluations. Moreover, we investigate whether more effective tax information exchange would bolster AML/CFT policies in that it reduced tax evasion, thus the volume of transnational financial flows (i.e. to and from offshore financial centres) and thus in turn cover given to money laundering and terrorist financing. We conclude that such a strategy can reduce financial flows, yet due to a "weakest link problem" even a few countries not participating can greatly undo what others have achieved.

JEL classification: K42, H26, H56

Keywords: money laundering, terrorist financing, tax information exchange

---

* We thank participants of the EUSECON Final Workshop in Brussels for helpful comments. Funding from the European Union Seventh Framework Programme under grant agreement n°218105 (EUSECON) is gratefully acknowledged.

§ Corresponding author: Prof. Dr. Dr.h.c.mult. Friedrich Schneider, Department of Economics, Johannes Kepler University, Altenbergerstrasse 69, 4040 Linz, Austria, Phone: +43 (0)732 2468-8210, Fax: +43 (0)732 2468-8902, E-mail: friedrich.schneider@jku.at, http://www.econ.jku.at/schneider

1 Introduction

In the recent decades the transaction volume on financial markets has tremendously increased and now accounts for trillions of US dollars per day. However, the same international financial systems that allow commerce, assets and money to flow freely between nations also provide criminals and terrorists with a way to move money around the globe within seconds. Transnational terrorism and organized crime thus have become a global problem threatening society by decreasing the stability of transnational economic activity, infiltrating legal structures and fostering the dependence of "weak states" on organized crime.

Thus, money laundering has been high on the agenda of governments and law enforcement authorities for already about 20 years, while it has been linked to terrorist financing in the aftermath of the airplane attacks on the New York World Trade Centre on September 11, 2001. Since then, the regulations imposed on countries' financial systems intended to thwart money laundering have been viewed as key components also in the fight against terrorist financing. What have initially been strategies to destroy the laundering of money, predominantly stemming from illicit drug trafficking, are now also used to curb the financing of terrorism. As such, the anti-money laundering (AML) focus of transnational bodies like the Financial Action Task Force (FATF) has been extended to combating terrorist financing (CFT). This has been prominently witnessed by the issuance of the FATF's nine special recommendations on terrorist financing, in addition to the previously existing 40 recommendations on money laundering (Jayasuriya, 2009).

In the light of the large political support they are provided with, these strategies must be evaluated with respect to their effectiveness by both social scientists and security practitioners. In doing so, it is necessary to uncover the sources of transnational criminal and terrorist funds, their volume, to gain knowledge on the various methods used to launder money and to finance terrorism as well as to investigate compliance among jurisdictions and financial institutions with the international standards and recommendations issued in the course of the fight against criminal and terrorist financing.

We are analyzing these issues by surveying the abundant literature on the topic. Moreover, we explore the possibility to supplement "traditional" AML/CFT strategies by increasing efforts to curb tax evasion. The logic behind this "new" strategy is that tax evasion, in particular by placing assets offshore instead of in the home country, produces large capital flows in offshore financial centres, which provide cover to criminal/terrorist funds which are also partly routed through those centres. Thus, if financial flows resulting from tax evasion (and tax avoidance) were reduced, the transactions involving money laundering and terrorist financing would be easier to detect.

In Section 2 of this study, we will provide some facts and figures on money laundering and terrorist financing and extensively review the literature on the sources of criminal/terrorist funds and the methods of laundering and transfer. By doing so, we intend to widen the knowledge of this subject and the understanding of the main issues under debate. The body of literature on terrorist and organized crime financing is diverse and quite often very descriptive, which is why we only summarize some important contributions. Our selection is subjective, however, we strongly belief to have covered the most important issues. Not surprisingly, the recent literature is heavily influenced by al-Qaeda´s recent attacks, in particular the airplane attack on the New York World Trade Centre on September 11, 2001.

We will present some channels of funding for terrorist organizations with related sources in the literature and will make a distinction between (initially) legal and illegal sources. In this context, we must generally assert that it is very difficult to identify the extent of money laundering and terrorist financing, because such activities can be neither observed nor recorded in statistics[1]. Moreover, we will analyze the methods of money laundering and the transfer of illegal money. In particular, we will focus on mispricing, a considerably underestimated method of money laundering, and alternative remittance systems, which allow criminals and terrorists to avoid the official sector and thus the scrutiny of law enforcement.

In Section 3, we discuss the standards and recommendations set forth in the international fight against money laundering and terrorist financing and their implementation in countries' legal systems and enforcement mechanisms. In the past years AML/CFT policies have largely been carried out by using a "twin-track-approach" (Stessens, 2000) consisting of i) preventive measures (i.e. implementing the "know your customer prin-

---

[1] Compare i.e. Bierstecker (2002), Costa (2005), Pieth (2005) and Schneider (2008a, 2008b).

ciple" and requiring institutions to report suspicious transactions) and ii) repressive measures (i.e. criminalizing money laundering and imposing severe fines). In this context, it has been argued that the intelligence process to fight against terrorist financing should combine expertise from different fields to detect the various indicators and trends (Giraldo and Trinkunas, 2007, Wilton Park Report, 2007). In particular, properly examining financial transactions will require law enforcement agents to cooperate with accountants and banking experts, recognition of the necessity to analyze reports on suspicious activities as well as to transnationally share information among Financial Intelligence Units (FIUs) and cooperation of governments among each other and with multilateral institutions. Another issue we address in Section 3 is the compliance of countries and their institutions with the standards set forth by the (OECD-based) Financial Transaction Task Force (FATF). We will also provide quantitative measures of the compliance rates, based on the FATF's evaluations.

In Section 4, we eventually explore whether intensifying measures against offshore tax evasion could invoke support for AML/CFT strategies. Criminal and terrorist financial flows might be difficult to detect because there is a large financial asset trading volume in offshore financial centres, resulting from the fact that individuals and corporations place money and assets there to avoid or evade taxes[2]. Thus, it could be useful to increase tax information exchange and establish agreements on it, because this should reduce the trading and asset volume in offshore financial centres, and thus cover given to criminal money flows should be reduced. The ultimate question thus is whether and to what extent increased tax information exchange can reduce tax avoidance and tax evasion such that less money is routed through offshore financial centres. We approach this question by surveying both the theoretical as well as empirical results that help to give an answer. Afterwards, we will discuss whether increased tax information exchange can be useful even if many countries do not participate in it. In Section 5, we summarize and draw conclusions.

[2] The tax rates in offshore financial centres appearing on the list of top 20 destinations for money laundering (Table 3) are: Cayman Islands (Income tax: 0%, Corporate tax: 0%, VAT: 0%), Bahamas (0%, 0%, 0%), Bermuda (0%, 0%, 0%), Luxembourg (38.95%, 21.84%, 15%), Hong Kong (15%, 15%, 0%), Switzerland (22.4%, 13%, 8%).

2 Facts and figures on criminal/terrorist funds

This section focuses on the financing of terrorism as well as transnational crime, since both forms of illicit activity pose severe threats to society and its institutions. Moreover, the analyses of the financing of crime and terrorism cannot be properly disentangled due to the following two reasons. First, definitions are unclear. Already in the 1980s, more than 100 definitions of terrorism existed, sometimes overlapping with the definitions of political violence or further forms of criminal activity (Sanchez-Cuenca and de la Calle, 2009)[3]. Second, some syndicates typically considered as being “criminal” (i.e. the Mafia or Mexican/Colombian drug cartels) often use methods typically defined as being “terroristic”, like bombing or taking hostages (Schneider et al., 2010), and vice versa. While, for example, some environmentalist groups should be regarded as “criminal”, they are sometimes termed “terroristic” (Nagtzaam and Lentini, 2008).

2.1 Terrorist financing versus transnational crime turnover

Before detailing the financing of transnational crime and terrorism, we briefly sketch some common aspects of as well as differences between the two notions. In general, criminals and terrorists are comparable in that i) both are typically “rational” actors, ii) both use extreme violence like kidnapping, murder or blackmailing, and threaten with retaliation, iii) both operate secretly, although also openly when being in friendly territory, and iv) both defy public institutions and the state (Schneider, 2011)[4].

Concerning the financing and transfer of funds, criminals and terrorists have the following things in common. First, both use electronic payment systems and wire transfers to move money internationally. Second, both engage in a wide variety of illicit activities. On the one hand, terrorists use crime and cooperate with criminals in generating

---

[3] A widely accepted definition of terrorism defines it as “the premediated use or threat of use of extranormal violence or brutality by sub-national groups to obtain a political, religious, or ideological objective through intimidation of a huge audience, usually not directly involved with the policymaking that the terrorists seek to influence” (Enders and Sandler, 2002). While this definition focuses on the actions (i.e. attacks) other definitions focus on the individuals who carry out terrorist attacks.

[4] See, i.e., Schneider (2008a, 2008b, 2009), Sanderson (2004); Gilmore (2004), Shelley (2005); Wilkinson (2005); Makarenko (2003a, 2003b), Schneider et al., (2010), Bell (2003) or Koh (2006) for a more detailed discussion on the similarities, differences and boundaries of terrorism and transnational crime.

funds and obtaining weaponry. In particular, they most frequently resort to drug trade (Makarenko, 2003a), while they also use trading in arms and precious stones, smuggling of cash, cigarettes and other addictive substances or kidnapping. On the other hand, criminals sometimes are using terror in raising revenue (see Masciandaro, 2004, 2005, 2006, Picarelli, 2006, Shelley, 2005 or Yepes, 2008 for a thorough discussion).

In addition to the above mentioned similarities, there are also some notable differences between terrorists and transnational criminals. Terrorists, for example, i) yield tremendous destruction (in terms of human lives, nations as well as economies) by making use of fairly cheap and simple technology, and ii) are often organized in flexible networks with decentralized decisions, while criminal syndicates typically have a more rigorous hierarchy. The most important differences with respect to the financing of activities, however, are that iii) terrorists have indiscriminate targets and ideological goals apart from making profits, while raising profits is key to transnational criminals. In addition, terrorists iv) need financial means to execute attacks, but hiding assets is seldom necessary, and v) they typically use different sources of money, depending on their motivations, the available sources of money and the resistance they face from law enforcement. Money from both legal (donations, or charitable contributions) as well as illegal sources (typically in cooperation with criminals) is used. Often, the financing means are “clean” until they are used to make possible terrorist attacks (Napoleoni, 2005, Krueger, 2008, Yepes, 2008).

2.2 Criminals’/terrorists’ funding requirements

2.2.1 Funding required by terrorists

As noted above, raising funds is typically not the ultimate aim of terrorists, and funding is merely necessary to pursue the ideological goals. While obviously, funding is needed for carrying out the terrorist attacks (direct costs), there are also indirect costs which are used to develop and maintain a terrorist organization and to foster its ideology. Thus, funding is also required for, for example, training new terrorists, forging documents, paying bribes, weapons as well as the terrorists and their families themselves, and seeking public support (i.e. making use of propaganda in the media). Typically, the type of funding for both direct and indirect costs will, as a matter of fact, vary by the specific nature of the attacks and the organizational structure of the terror syndicate (FATF, 2008).

2.2.1.1 Direct costs

Direct costs of terrorist attacks refer to the material and products used in the attacks, i.e. vehicles, bomb-making components, maps or surveillance material. As Table 1 below suggests, those direct costs are astonishingly low, especially when being compared to the destruction of infrastructure, human lives as well as even societies the attacks yield (FATF, 2008).

Table 1: Estimated direct costs of selected terrorist attacks

Attack	Date	Estimated cost
London Subway	July 7, 2005	~ GBP 8,000[§]
Madrid Railways	March 11, 2004	~ USD 10,000[&]
Istanbul Trucks	November 15/20, 2003	< USD 40,000[&]
Jakarta Marriot Hotel	August 5, 2003	~ USD 30,000[&]
Bali	October 12, 2002	< USD 50,000[&]
WTC New York	September 11, 2001	~ USD 300,000 - 500,000[+]
USS Cole	October 12, 2000	< USD 10,000[&]
US Embassies Kenya/Tanzania	August 7, 1998	< USD 50,000[&]

Sources: [§] UKHO (2006), [&] UN (2004), [+] Kiser (2005)

While only for the most significant terrorist attack on the World Trade Centre in New York, the direct costs reach the six-digit domain, the costs for other huge attacks like the 2004 Madrid Railway bombings or the attacks on the US embassies in Kenya and Tanzania in 1998 are well below USD 50,000. Thus, in raising and moving money to cover the direct cost of terrorist attacks, employing sophisticated means of concealment and covering the tracks is often not necessary.

2.2.1.2 Indirect costs

Apart from the direct costs of executing attacks, running and maintaining a terrorist organization also involves substantial indirect costs. They typically exceed the direct costs by far and can be categorized in the following way (FATF, 2008).

Salaries/subsistence and communications

The expenses of the operative personnel as well as their family members have to be covered. Moreover, members of terrorist cells have to communicate with each other and also with the parent network if there is one. This component of indirect costs is especially important if planning and executing attacks is the only source of income for the operative personnel.

Training, travel, and logistics

Both ideological as well as practical training of the operative personnel is a key investment for terrorist organizations. Thus, permitting and financing training and the associated travel is important, and it can require substantial financial means. According to FATF (2008), even terrorists operating independently without connection to a larger network, who recently carried out attacks, have travelled to receive training or other forms of “indoctrination” prior to the attacks.

Shared funding

Terrorist syndicates who are part of a larger network and share common ideological or religious goals with it might be inclined to provide funding for other members of this network. Thus, costs might also be incurred for supporting fellow terrorist groups.

Advertising and recruiting

While maintaining a terrorist network or a specific syndicate in terms providing subsistence, training, travel and supply of material accounts for the most substantial fraction of total cost of terrorism (FATF, 2008), funding is also required for developing a supportive environment, recruiting new members and fostering the intended ideology among larger groups of the population. In this context, terrorist organizations might provide funding for supportive ***charities*** or ***media*** who provide favourable coverage in return.

Some terrorist groups have connections to charities in high-risk areas or underdeveloped parts of the world, where public social welfare systems do not exist. In those areas, terrorist organizations can attain public support by providing funding for charities which support the population. On the other hand, terrorist groups might also use financial means from other sources given to existing and affiliated charities for terroristic purposes. This latter practice is advantageous to terrorists because it provides a "veil of legitimacy" for their funding (Kohlmann, 2006).

In addition to the public- and social welfare involvement of terrorist organisations, mass media outlets are often used to promote a certain ideology. Terrorist groups such as al-Qaeda, for example, have frequently been manipulating television by releasing videos. Moreover, virtually all terrorist organisations have a websites for recruitment, fostering their ideology and justifying the violent approach they use, like suicide bombing or killing innocent civilians.[5]

2.2.1.3 Total costs

The above discussed variety of funding requirements documents that the low direct costs of executing attacks are not sufficient as an indicator for the funding needs of terrorists. Rather, the costs of maintaining a terrorist organization have also to be taken into account, since substantial infrastructure, recruitment and provision of public support is necessary to sustain terrorist networks.

Al-Qaeda, for example, is therefore believed to have spent some USD 30 mn. per year prior to the attacks on September 11, 2001 on the items discussed above, like funding operations, maintaining, training, military devices, but also contributions to the Taliban, their high-level officials as well as fellow terrorist groups (US National Commission, 2004). According to FATF (2008), those funding requirements have not substantially changed since then, although al-Qaeda may have continually downshifted its hierarchical command-like organization and changed to a more fragmented and decentralized structure in the recent years.

The al-Qaeda funding requirements reported by US National Commission (2004) are in line with the estimations by Schneider and Caruso (2011), who employ a MIMIC-Approach[6] to estimate the financial flows of al-Qaeda and other Arab Islamist terror organisations. As can be seen from Table 2, al-Qaeda's annual financial flows are estimated to be between USD 20 mn. and USD 50 mn. The biggest syndicate in terms of

---

[5] Weimann (2004) discusses al-Qaeda's use of the internet in depths, while Jorisch (2004) provides research on Al-Manar TV.

[6] Detailed explanations of this estimation procedure are relegated to Appendix A.

members, Hezbollah, is estimated to have about the same funding requirements as al-Qaeda (USD 50 mn.), while the other mentioned organisations like Hamas or Front Islamique du Salut have smaller budgets.

The figures in Table 2 document that the funding requirements of terrorist syndicates substantially outnumber the direct costs associated to a terrorist attack, which are typically lower than USD 50,000 (see Table 1). However, as will be documented below, the total funding requirements of terror organizations are quite small when being compared to the turnover of transnational crime.

Table 2: Preliminary overview of financial flows of Arabic islamist terror organisations

Name	**Members (worldwide)**	**Annual financial flows (annual budget)**
	Average over 1999-2006	
Al-Qaeda	1500-3000	~ USD 20-50 mn.
Front Islamique du Salut (Algeria)	~ 400	~ USD 5 mn.
Hamas	~ 2000	~ USD 10 mn.
Hezbollah	~ 10.000	~ USD 50 mn.
Arabic Mujahedin (terror) organisations:		
- Iraq	~ 800	~ USD 5 mn.
- Iran	~ 600	~ USD 5 mn.
- Libya	~ 600	~ USD 10 mn.
- Egypt (Egyptian Islamic Jihad; most likely united with Al-Qaeda; Islam./Arab.)	~ 600	~ USD 8 mn.

Source: Schneider and Caruso (2011)

2.2.2 Transnational crime turnover

Unlike terrorist syndicates, who do not specifically aim at making profits, but at pursuing ideological and political goals, raising revenue must be considered as a major purpose of organized transnational crime. Thus, unlike in the case of terrorists, it is somewhat inappropriate to speak of “criminals’ funding requirements”, since raising funds is not a requirement, but a goal itself.

Profits raised by pursuing illicit activities like, for example, drug, weapon or human trafficking are typically denoted as “dirty money”, and, as shall be discussed below, criminals undertake considerable effort in “laundering” dirty money such that it can be officially used for procurement, investment, development and enlargement of criminal syndicates and also for engaging in an preparing further criminal activity. Impeding fundraising by criminal groups and money laundering is thus of paramount importance to states and jurisdictions. This section analyzes the extent of present money laundering[7], before proceeding with a description of money laundering techniques and possible strategies of impediment.

Baker (2005) estimates that worldwide, in total between USD 1.0 and 1.6 trillion are raised by criminal activity in various forms per year[8]. About half of it, i.e. USD 500 to 800 per year is estimated to come from developing and transitional economies (Baker, 2005). Those countries typically have the weakest legal and administrative structures, the largest criminal gangs of drug dealers, and, far too often, economic and political elites who want to bring their money out of the country by any possible means.

2.2.2.1 Development of money laundering over time

In order to investigate the development of such criminal flows over time, Schneider (2008a, 2008b) employs a MIMIC-procedure[9] and estimates money laundering from organized transnational crime to have increased from USD 273 bn. in 1995 (1.33% of official GDP) to USD 603 bn. (or 1.74% of the official GDP) in 2006. The estimations are undertaken for 20 OECD countries[10]. On a worldwide basis, however, the amount of money raised and laundered only by criminals involved in the drug business is estimated to be USD 600 bn. in 2006.

2.2.2.2 Distribution of money laundering over countries

For efficiently combating money laundering, it is of paramount importance to know where it takes place and to what extent the different countries and financial mar-

---

[7] For a detailed analysis see Schneider (2008a, 2008b and 2009), Schneider and Windischbauer (2008), Schneider, Dreer and Riegler (2006), and Takats (2007).

[8] This estimate has been adopted by the World Bank.

[9] Appendix A explains this procedure in detail using the example of the financial flows to and among Islamist terrorist organizations.

[10] Data used in those estimations were on Australia, Austria, Belgium, Canada, Denmark, Germany, Finland, France, Greece, Great Britain, Ireland, Italy, Japan, Netherlands, New Zealand, Norway, Portugal, Switzerland, Spain and the United States.

kets are involved in it. Unger (2007) estimates the distribution of laundered money over the 20 “top destinations of money laundering” over three years, from 1997 to 2000. The results are shown in Table 3. Two estimates are presented, one by Walker (2000, 2007) and one by the IMF. Note that Walker’s estimate of total worldwide money laundering (USD 2.85 trillion) is much larger than the IMF figure (USD 1.50 trillion USD), although both figures refer to the year 2005[11].

Interestingly, Table 3 shows that two thirds of worldwide money laundering was routed through the 20 countries listed. In contrast to an intuition one might have, it has to be noted that most of these countries are to be considered as being established and well developed, and have quite sizeable legal/official economies. However, among the top 20 destinations of money laundering are also four microstate offshore countries (OFCS). Those countries, typically denoted as “tax havens”, are the Cayman Islands, Vatican City, Bermuda and Liechtenstein[12].

One might, however, have suspected a higher fraction of criminal money to be routed through those tax havens. But Table 3 clearly indicates that the majority of countries which attract money laundering flows are fairly big and well-established rather than tiny. The United States has the largest worldwide share of money laundering of almost 19%. However, the second-largest share is attributed to the Cayman Islands (4,9%), a “tax haven”. Russia (4,2% of worldwide money laundering), Italy (3,7%), but also smaller countries like Switzerland (2,1%), Liechtenstein (1,7%) and Austria (1,7%) seem to be quite attractive places for money laundering.

Note that according to the IMF estimations, the total amount of money laundered in Austria, Switzerland and the United Kingdom accounts for roughly 5.5 % of the total worldwide amount of money laundering, which comes quite close to the share of world GDP of those three countries, which is roughly 10%.

Importantly however, it must be noted that it is not clear from the estimations presented here whether money from criminal sources stays in the countries on the list or

---

[11] Walker’s figures have been criticized as being far too high, which is one reason why IMF figures have also been chosen to be presented.

[12] Compare also Masciandaro (2005, 2006), Masciandaro and Portolano (2004), Zdanowicz (2009), Truman and Reuter (2004), and Walker and Unger (2009):

whether it is only laundered there. To sum up, Table 3 demonstrates that the total amount of laundered money clearly exceeds the respective figure on terrorist financing and that it must be considered as substantial. Moreover, it is noticeable that about two thirds of total money laundering is routed through 20 out of about 200 countries in total.

Table 3: Distribution and absolute amounts of money laundering in the top 20 destinations

Rank	Destination	% of worldwide money laundering	Walker estimate	IMF estimate
			USD bn.	USD bn.
1	United States	18.90%	538.1	283.5
2	Cayman Islands	4.90%	138.3	73.5
3	Russia	4.20%	120.5	63.0
4	Italy	3.70%	105.7	55.5
5	China	3.30%	94.7	49.5
6	Romania	3.10%	89.6	46.5
7	Canada	3.00%	85.4	45.0
8	Vatican City	2.80%	80.6	42.0
9	Luxembourg	2.80%	78.5	42.0
10	France	2.40%	68.5	36.0
11	Bahamas	2.30%	66.4	34.5
12	Germany	2.20%	61.3	33.0
13	Switzerland	2.10%	59.0	31.5
14	Bermuda	1.90%	52.9	28.5
15	Netherlands	1.70%	49.6	25.5
16	Liechtenstein	1.70%	48.9	25.5
17	Austria	1.70%	48.4	25.5
18	Hong Kong	1.60%	44.5	24.0
19	United Kingdom	1.60%	44.5	24.0
20	Spain	1.20%	35.5	18.0
	Sum over Top 20	**67.10%**	**1,910.9**	**1,006.5**
	Worldwide total	**100.00%**	**2,850.0**	**1,500.0**

Source: Unger (2007)

2.2.2.3 A macro-perspective on money laundering

Depending on which estimate of Table 3 is used, the total worldwide amount of money laundered accounts for 3.28 to 6.23 percent of world GDP[13]. This is consistent with IMF (2002, 2007) as well as World Bank estimates according to which 2 - 4% of the world gross domestic product (GDP) stem from illicit (criminal) sources. Moreover, Agarwal and Agarwal (2006) estimate from economic intelligence units that global money laundering amounts to more than 2.0 to 2.5 trillion US$ annually or about five percent of World GDP in 2006[14] and thus yield similar results. The same authors (2004), however, observe a figure of USD 500 bn. to USD 1 trillion in 2004.

Recent IMF estimates on money laundering by drug traffickers who "introduce" the proceeds gained through the selling of drugs into the legal financial market, amount to USD 600 bn. annually. Finally, IDB (2004) concludes that a rough estimate for Latin America appears to between 2.5 and 6.3 % of annual GDP of Latin American countries.

While the figures presented above are truly alarming in that they document that the share of worldwide money laundering, which can be viewed as a lower bound estimate for total criminal turnover in world GDP is quite substantial, other studies yield even higher such shares. Simulations by Bagella et al. (2009)[15], for example, show that money laundering accounts for as much as 19 percent of the GDP measured for the EU-15 countries, while it accounts for 13 percent on the US economy. The authors have simulated money laundering between 2000 and 2007. In addition, simulated money laundering appears to be less volatile than the corresponding GDP. For the EU-15 area, the simulated statistics suggest that money laundering volatility accounts for only about one third of the GDP volatility. Applied to the US economy, the same procedure yields a fraction of two fifths. Clearly, those figures are very high, and Bagella et al. (2009)

---

[13] According to IMF data, world GDP in 2005 was USD 45.7 trillion (IMF, 2012).

[14] According to IMF data, world GDP in 2006 was USD 49.3 trillion (IMF, 2012).

[15] The authors use a theoretical two-sector dynamic general equilibrium model to measure money laundering for the United States and the EU-15 macro areas over a quarterly sample between the years 2000 and 2007. Their series are generated through a fully micro-founded dynamic model, which is appropriately calibrated to replicate selected stochastic properties of the two economies. Their model (and the analysis) has a short run perspective. For this reason, the paper also discusses the stochastic properties of the Hodrick-Prescott filtered series.

have unfortunately not reported consistency checks to determine whether such figures are plausible in the end.

Comparable measures to the ones presented above are yielded by simulations using a gravity model[16] (Walker and Unger, 2009). Gravity models have recently become popular in international trade theory and as such make possible estimating the flows of illicit funds from and to each of the plenty jurisdictions in the world. Using triangulation, the authors demonstrate that the estimates produced by this "Walker Model"[17] are consistent with recent findings on money laundering. With the procedure employed, once the scale of money laundering is known, its macroeconomic effects and the impact of crime prevention, regulation as well as law enforcement effects on money laundering and transnational crime can also be measured.

Walker and Unger (2009) conclude that their model seems to be the most reliable and robust method to estimate global money laundering as well as the important effects of transnational crime on economic, social and political institutions. However, they also note that the attractiveness and distance indicator in the "Walker-model" are still quite ad hoc, though a valid first approximation. Thus, a better micro-foundation for the Walker Model will be needed in the future. In implementing such micro-foundation, being able to appropriately describe the behaviour of money launderers, and in particular the decision-making that determines to which specific country money to launder is sent, is of paramount importance. Thus, similar to new trade theory modelling, appropriate behavioural assumptions about money launderers' decisions are necessary in a well-defined "money-laundering gravity model". Such a gravity model must be the (reduced form) outcome of money launderers' rational calculus of sending their money to another country and possibly getting caught, but potentially making large profits.

[16] Walker and Unger (2009) criticize that "conventional" methods such as case studies, proxy variables, or models for measuring the shadow economy all tend to under- or overestimate money laundering and thus use a different approach employing a gravity model.

[17] This model was first presented in 1994 and has been used and updated recently.

2.3 Sources of criminal/terrorist funds

While transnational criminal syndicates make profits by carrying out illicit activities and the funding of criminal groups thus by definition stems from those illicit activities, terrorists receive funding from both illegal (i.e. by cooperating with criminal syndicates) as well as legal sources (i.e. state sponsors or charities). In the latter case, as noted above, “clean” money is used to prepare or carry out terrorist attacks, and the money turns “dirty” just when being used for terrorist purposes. As shall be discussed below, this way of financing frequently happens. This section first gives an overview over the wide variety of terrorist financing sources and then briefly discusses the sources of criminal funds (i.e. the various criminal activities and their contributions to worldwide criminal turnover). Yet, again we must note that criminal and terrorist funding sources cannot be fully disentangled, since, as discussed earlier already, it might well be that terrorists resort to criminal activities in order raise funds, as criminals might use operations typically considered as “terroristic” in order to achieve their (financial) goals.

2.3.1 Legal sources of terrorist financing

As noted above, not all the financing received by terrorist syndicates does necessarily stem from illegal activities. Rather, there are completely legal activities conducted by charities, Diaspora, and firms, which are used to finance terrorism (Yepes, 2008) Moreover, the “9/11 commission” pointed out that a core number of financial facilitators involved in raising, moving, and storing the money al-Qaeda used where in fact donors, primarily residing the Gulf Region, but also in other countries around the world. According to Comras (2007) these persons and groups used legal charities and businesses as covers to develop a substantial financial network to foster terroristic activities. In the following, we will present those legal sources of terrorist financing in more detail.

2.3.1.1 State Sponsors

According to Yepes (2008), Afghanistan and Sudan have been sponsoring terrorist groups. In this context, it was possible to prove that the majority of companies and banks used by, for example, Osama Bin Laden, were located in Khartoum (Sudan) such as Faisal Islamic Bank, Ladin International, Taba investment Co. Ltd, Al Themar Al

Mubaraka, Al Qudarat, Islamic Bank Al Shama. Furthermore, al-Qaeda´s controlled companies in Africa included the holding company Wasi al AQuq, a Sudanese construction firm, Al-Hiraj, an ostrich farm, and shrimp boats in Kenya (Yepes, 2008). It must be assumed that Afghanistan and Sudan have been providing support, including financial means, in the acquisition and holding of the mentioned companies and holdings by Osama Bin Laden and other al-Qaeda members.

2.3.1.2 Private individual and corporate Donors

that among the most important cases of the private donors involved in terrorist financing, is Saleh Al Rajhi and his family members (Kohlmann, 2006, and Simpson 2007a, 2007b). According to CIA reports and federal court filing by the US Justice Department, “they have been major donors to Islamic charities that are suspected by Western intelligence agencies of funding terrorism”.

An endowment holding describing much of Al Rajhi´s wealth gives an indication of the scale of his support. His webpage details nearly USD 50 mn. of direct donations within Saudi-Arabia and at least USD 12 mn. of donations being transferred to other countries. The overseas money went to aid embattled Muslims in Kosovo, Chechnya and the Palestinian territories and to finance “Islamic instruction”.

Moreover, the US Justice Department has been investigating possible criminal tax-law violations by a Boston private-equity firm that manages hundreds of millions of dollars for Muslim investors in Europe and the Middle East and is affiliated with a Swiss investment group that U.S. authorities suspect of financing Islamist extremists (Simpson, 2007b). Furthermore, some private corporate donors have been cited by Morigi (2004), and finally, Fried et al. (1975) conclude that private individual and corporate donors could be related to those individuals or enterprises that have recycled Petrodollars in 1974.

2.3.1.3 Ethnic Communities and Religious Financing

According to Comras (2007), religious financing plays an important role in the Muslim world. In particular, it there is a “Coranic Tax”, typically consisting of support offered by the rich to the poor, which wealthy people are virtually obliged to pay within the Islamic community. Furthermore, charities are a very important part of Muslim law and tradition.

It is argued that al-Qaeda took advantage of these conventions and raised funds through, for example, collection boxes at mosques and Islamic centres (Comras, 2007). Similarly, Mosque Network seems to provide financial support for the Jihad (Napoleoni, 2005). In this context, Napoleoni (2005) states “The Mosque Network is as efficient as ever and continues to be the main vehicle through which Islamist organizations, countries, state-shells, armed groups and their sponsors link up and do business with each other”.

2.3.1.4 Charities

Donations to NGOs and charities are perfectly legal in most countries: As a matter of fact, however, problems arise if some objectives of NGOs are not legal or linked to a diversion of some of the legally received funds legally to illegal activities. Kohlmann (2006) as well as Raphaeli (2003) have highlighted how terrorist organizations have resorted to a variety of charitable as well as front and fraudulent organizations to mobilize financial resources in order to carry out their actions.

Raphaeli (2003), for example, demonstrates the linkage between charity and terrorism in the case of Enaam Arnaout. Arnaout served in the office of an organization known as Maktab al Khidamat. This organization has been run by Sheikh Abdullah Azzam and Osama Bin Laden for the principal purpose of providing logistical support to the Mujahideen (holy warriors) fighting the Soviet Union in Afghanistan.

Furthermore, Croissant and Barlow (2007) report in details the role of several charities in Southeast Asia, which were linked to the brother-in-law of Osama Bin Laden, Mohammed Jamal Khalifa. In particular, Khalifa has directed a Saudi-Arabian charity known as the “International Islamic Relief Organization” (IIRO). Yet, intelligence reports indicate that IIRO has been used to support local terrorist operations throughout Southeast Asia. In addition, Khalifa has also established a charity labelled as the “International Relations and Information Centre” (IRIC).

While, according to Abuza (2008), most operations of Islamic charities in South Asia go to legal social work, it is undeniable that much of the Jemaah Islamiyah’s funding comes from charities. In particular, an estimated 15 to 20 percent of Islamic charity funds in Indonesia are diverted to Islamist activities.

Finally, a note must be made on the interdependencies between charities and state-support of terrorism, which we discuss above. It must be stressed that the role of charities cannot be completely disentangled from other phenomena of state-support. In this respect, we underline the role of the "Muslim World League" (MWL) founded by Saudi Arabia in 1962 in order to support the propagation of Wahhabism (a branch of Islam). According to Looney (2006), MWL supported institutions outside of Saudi Arabia, especially in Afghanistan, Pakistan, Southeast Asia and the Middle East. In this context, Saudi public and private support has been estimated at over $75 bn. during the last four decades. Many experts have drawn a link between this monetary effort whose ultimate goal was the spread of Wahhabi Islam and the rise of al-Qaeda's appeal in the Muslim world (see, for example, Levitt, 2002 or Basile, 2004). The latter, in particular, also highlights the role of two other well-established charities, the "Benevolence International Foundation", and the "Qatar Charitable Society" (QCS) in financing terroristic activities.

2.3.1.5 Legal business

In many cases, terrorist groups establish legal businesses, but do not primarily intend to raise legal revenues. Rather, those businesses are to cover illegal activities or to provide employment for terrorist groups' members[18]. For the example of al-Qaeda the literature shows that the truly transnational financial engine of this terrorist group and its sympathizers continue to raise money through their own business activities. In particular, the al-Qaeda group consists of the following companies, among others. In Africa, the holding company "Wadi al Aqiq", a Sudanese construction firm, "Al Hiraj", an ostrich farm and shrimp boats in Kenya. In the Middle East, al-Qaeda holds shares in the As-Shamir Islamic Bank, large tracks of forests in Turkey as well as agricultural holdings in Tajikistan. In Europe and the United States, al-Qaeda terrorists have holding companies, venture capital firms, banks and import-export companies (Napoleoni, 2005, and Mintz ,1998). Further, the portfolio includes real estate in London, Paris and French

---

[18] The legal business support to terrorist activities are noted by, among others, Napoleoni (2005), Ehrenfeld R., (2007), Gunaratna (2003), Schneider (2004, 2008a, 2008b), Millard (2006) and Comras (2007)

Riviera; dairy business in Denmark; wood and paper industries in Norway; and hospital equipment in Sweden.

Networks of companies and shell companies, shell banks, and offshore trusts must be assumed to be used to raise money, hide assets, and protect the identity of other financial contributors. Consider again the example of al-Qaeda. The importance of the network in terms of correspondent banking can be seen by examining the case of the "Al Shamal Islamic Bank" in Khartoum, in which foreign currency accounts were set up for a number of companies belonging to Bin Laden. Shamal sustained banking relationships with a variety of reputable banks such as CityBank and others, which is why Al-Qaeda was able to move money rapidly and without impediments around the world.

Some scholars like Comras (2007) investigate the use of trusts by terrorist groups. Raphaeli (2003), for example, reports a USD 3.7 mn. investment in New Jersey undertaken by an investment company known as "BMI". One of the biggest investors in BMI was Yasin al-Qadi, a Saudi businessman from Jeddah considered by US authorities as a leading member of a global network that finances Islamic work (i.e. "true" charitable giving, religious education etc.), but also terrorism. Another major investor was one of the leaders of Hamas, Moussa abu Marzuq.

2.3.2 Illegal sources of terrorist financing

2.3.2.1 Drug Trafficking

Undoubtedly, a fundamental source of funding for terrorist groups is the narcotic industry. In particular, as pointed out by Makarenko (2003a), illicit drug trafficking had always been the most common criminal activity terrorist groups have been involved in. Since the 1970s groups such as "Fuerzas Armadas Revolucionarias de Colombia" (FARC), "Euzkadi Ta Askatasuna" (ETA – Basque Fatherland and Liberty), "Partiya Karkaren Kurdistan" (PKK – Kurdistan Workers Party) or "Sendero Luminoso" have all been involved in drug trafficking. This is well-documented, as it is documented that nowadays Islamist groups engage in drug trafficking as well[19]. The recent account by

[19] According to Yepes (2008), in May 2002 a report called "Global Overview of Narcotics-Funded Terrorist and Other extremist groups" was launched. It has before been prepared by the Federal Research Division of the Library of Congress and the US Department of Defence. This report has examined con-

Peters (2009), for example, documents in details the strong ties between drug-trafficking and Al Qaeda in Afghanistan and Pakistan. Furthermore, Paoli et al. (2007) report on opium and heroin trafficking in Tajikistan in detail. According to Hardouin and Weichhardt (2006), the "Islamic Movement of Uzbekistan" (IMU), has reportedly profited from the drugs smuggling out of Afghanistan and trafficking through Central Asia to both Russia and Europe. Moreover, several Islamist groups in Central Asia are reported to have strong ties and involvement with drug trafficking (Cornell, 2005, 2006).

2.3.2.2 Oil Smuggling

Oil smuggling is another business where terrorists and criminals interact with one another, but also with legal institutions (Johnson, 2011, Napoleoni, 2005). Countries having a significant problem with oil smuggling are in particular Thailand, China, Russia, Cambodia, Iran and Tanzania. In all these countries, oil smugglers earn significant profits, a substantial portion of which enters the money laundering cycle. Oil smuggling is also related to arms trade.

2.3.2.3 Arms/Diamonds Trafficking

In addition to the narcotic business, arms trafficking and illegal diamonds trade are among the most important illegal sources of terrorist funding (Levi and Gilmore, 2002, Schneider, 2004, 2008a, 2008b, 2009, Yepes, 2008).

Illegal diamonds trade

More specifically, Raphaeli (2003) reports the activity of some Liberia-based al-Qaeda operatives in the African gem-business. Furthermore, Passas and Jones (2006) highlight the role of commodities, foremost among these diamonds, in the financing of terrorist groups by covering many areas of legal and illicit trade.

---

nections between extremist groups and narcotics trafficking in the following regions. In Latin America, the Triborder Region (Argentina, Brazil, and Paraguay), Colombia, and Peru; in the Middle East, Lebanon; in Southern Europe, Albania and Macedonia; in Central Asia, Kyrgyzstan, Tajikistan, and Uzbekistan; and in East Asia, the Philippines.

Also, the linkage between al-Qaeda and the illicit diamond market is analyzed by some studies. In particular, journalistic inquiries uncovered the links between al-Qaeda and the illicit trade in so-called "blood diamonds" bought from rebel groups in Africa in the recent years[20]. Moreover, Hübschle (2007) reports also about al-Qaeda interest in Tanzanite trading.

Arms trafficking

The illicit arms trade demonstrates how comparatively easy it is to obtain false documentation accompanying arms shipments, like especially end-user certificates. Inconsistent documentation requirements across countries and inefficient control in customs and port authorities in many states have created an environment in which concealing the transfer of illicit arms does not require considerable efforts. In particular, such illicit arms transfer frequently comes in one of the following three forms.

1) When a state is involved in supplying arms to an embargoed state, payments often come in the form of commercial payments, such as an “oil for arms” deal to avoid bank involvement.
2) When an arms broker supplies an insurgent/terrorist group in an embargoed state, banks are often used because shipments are usually paid for by making use of letters of credit or by the direct transfer of hard-currency funds. In the latter case, money laundering becomes an important factor to ensure that the final arms destination is disguised. It is at this point that offshore banks play an important role because their facilities can ensure that any deposit or transfer is routed via several intermediary institutions. Moreover, they allow deposits or transfers to be conducted in the name of a series of shell companies. Both of these techniques are used to hide the financial trail behind multiple administrative layers.
3) In situations where access to normal banking channels is difficult (for example, as with most non-state actors), the financing of arms deals frequently takes a different form, most often through commodity exchanges. According to Smillie et

[20] See, for example, the account by Lucy Jones on the BBC news website http://news.bbc.co.uk/2/hi/2775763.stm

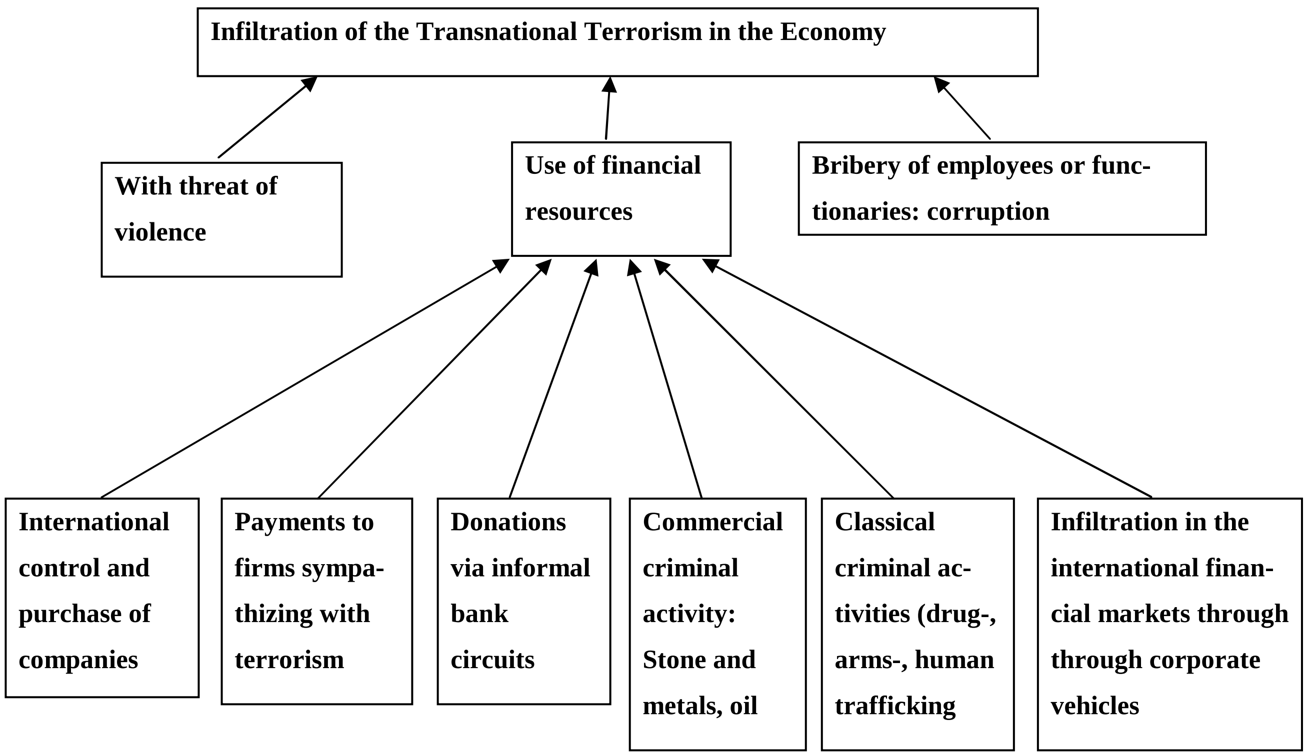
al. (2000), for example, illicit arms transfers to Liberia and Sierra Leone were often financed with diamonds and timber concessions.

2.3.3 An overview on the sources of terrorist financing

To conclude the discussion on the sources of terrorist financing, we graphically show the various channels of infiltration with transnational terrorist networks which appear in economies and institutions (Figure 1) Moreover, we shed light on the relative importance of the various sources of terrorist financing using the example of al-Qaeda.

In this context, Figure 1 concentrates on the use of financial resources and clearly demonstrates that the financial means/flows to and from terrorists stand on the six pillars "Control and purchase of companies", "sympathising firms", "donations with informal circuits", "commercial criminal activity", "classical criminal activity" and "infiltration of international financial markets".

Figure 1: Infiltration of the transnational terrorism in the economy



Source: Yepes (2008)

Table 4, in turn, documents the relative importance of financing sources for terrorist organizations using the example of al-Qaeda. The values have been estimated by making use of the MIMIC-approach (see Schneider, 2008a, 2008b, 2009 for details or Appendix A for a short description). As can be seen, the drug business is the most important financing source for al-Qaeda, accounting for some 30 – 35 percent of the annual budget of USD 20 – 50 mn. Donations from governments, wealthy individuals or religious groups are almost as important and in total contribute 20 – 30 percent of the budget. Tribute payments account for 15 – 20 percent, while active members and supporters provide (including engagement in criminal activities) 10 – 15 percent of the annual budget.

Table 4: The financial flows and financing sources of al-Qaeda

Annual financial flows (budget) of Al-Qaeda (Average 1999-2006)	USD 20 - 50 mn.
Ways of financing of terror organisations (using the example of Al-Qaeda)	
- Drug business (mainly transporting drugs)	30 - 35%
- Donations from governments, wealthy individuals or religious groups	20 - 30%
- Tribute payments from Islamic countries	15 - 20%
- Active members and supporters (including classical criminal activities like kidnapping, blackmailing, etc.)	10 - 15%
Total	**75 – 100%**

Source: Schneider and Caruso (2011)

2.3.4 Sources of transnational criminal turnover

After the extensive discussion of financial flows to and from terrorist syndicates, we will now briefly turn to describing the sources of transnational crime turnover. Again, however, we stress that the sources of financing of transnational crime and terrorism cannot be entirely disentangled, since some terrorists use criminal methods to raise funds, and some criminals operate with methods typically denoted as “terroristic”. Furthermore, we note that we will restrain from going into too much detail here, since many of the criminal activities used to raise funds for criminal/terrorist purposes have already been discussed. Rather, we take a global perspective here and give a broad overview on the importance of various forms of crime and their contribution to world-wide criminal turnover in this subsection.

In Table 5, the global flows from illicit activities worldwide are shown. As can be seen, the proceeds of forging money, illegally trading arms, Human trafficking as well as corruption each account for only small fractions of the criminal money turnover. Funds generated by such "crmininal activity" account for some 30 to 35 percent of the global total, while illicit funds generated abusive transfer pricing, faked transactions as well as mispricing in commercial activity which is not illegal per se, is by far the largest component. It accounts for some 60 to 65 percent of the global total.

Table 5: Global flows from illicit activities, years 2000/01

Global Flows	**Low (USD bn.)**	**%**	**High (USD bn.)**	**%**
Drugs	120	11.00%	200	12.50%
Counterfeit goods	80	7.50%	120	7.50%
Counterfeit currency	3	0.20%	3	0.20%
Human trafficking	12	1.10%	15	0.90%
Illegal arms trade	6	2.00%	10	0.60%
Smuggling	60	5.60%	100	6.30%
Racketeering	50	4.70%	100	6.30%
Crime subtotal	**331**	**31.20%**	**549**	**34.30%**
Mispricing	200	18.90%	250	15.60%
Abusive transfer pricing	300	28.30%	500	31.20%
Fake transactions	200	18.90%	250	15.60%
Commercial subtotal	**700**	**66.00%**	**1,000**	**62.50%**
Corruption	30	2.80%	50	5.10%
Total	**1,061**	**100.00%**	**1,599**	**100.00%**

Source: Baker (2005)

2.4 Moving criminal/terrorist funds across nations and jurisdictions

As a matter of fact, internationally operating criminals and terrorists must in course of their illegal activities move their funds across nations and jurisdictions. As will turn out later within this study, it is precisely the moving of criminal/terrorist funds where authorities are able to most effectively detect illegal and terroristic activity, and have yielded substantial success in doing so in the past.

The issue of moving criminal/terrorist funds is tightly interlinked with the issue of money laundering, since money laundering frequently takes place by moving money from illegal sources between countries, often indirectly via a substantial number of intermediate stations. In this study, it is necessary to shed light on both the ways by which criminals and terrorists move funds across countries, as well as, more specifically, on the methods and techniques of money laundering. We will discuss the former in this, and the latter in the next subsection.

Basically, there are four ways criminals and terrorists can make use of in order to move illegal money across countries. The first is through the (official) financial system (i.e. transferring money or assets by making use of financial intermediaries like banks), the second is physical movement by cash couriers, the third is by making use of the international trade system, and the fourth is by using so-called "informal value transfer systems" or "alternative remittance systems" (i.e. Hawala), or, as discussed above already, charities (FATF, 2008). While terrorists and criminals make extensive use of all four mentioned possibilities of money movement, it is due to the "multiplicity of organisational structures employed by terror networks, the continuing evolution of techniques in response to international counter-terrorist measures and the opportunistic nature[21] of terrorist financing", however, difficult, if not impossible to determine a most commonly used method of transmission (FATF, 2008). As a matter of fact, disruption of terrorist financing is the harder the more informal the ways of transmission used are. Yet, a challenge common to the detection of all methods of illegal money transmission is that identifying the connections between funds and terroristic activities can be "extremely difficult" (FATF, 2008), if the terroristic activity is taking place not in the country where the funding originates, but elsewhere, as it is frequently the case.

2.4.1 Transmission in the official financial sector

The official financial sector is represented by ordinary financial institutions like, for example, banks, as well as other regulated financial service providers. Those institutions are the primary gateway through which retail and commercial transactions flow, and are thus offer terrorists and criminals the opportunity to most efficiently transfer

[21] See, for example, Williams (2005) or US National Commission (2004).

their funds. Moreover, the speed with which funds can be transmitted through official financial intermediaries, and the fact that transmissions can often be carried out without detection (i.e. if transaction are routed through offshore financial centres and in combinations with offshore corporate entities), makes the official financial sector an attractive means of money transfer for criminals and terrorists (FATF, 2008).

When operating in the official financial sector, criminals and terrorists have been proven to make extensive use of so-called “Money and value Transfer” (MVT) mechanisms within the network of officially registered and internationally operating money transfer companies. The specific means terrorists and criminals have been found to use range from large-scale regulated funds transfer devices to relatively small-scale electronic means of money transmission (FATF, 2008).

In this context, it is important to stress that the recent diffusion of electronic payment devices has had a twofold impact on terrorist financing and its detection. On the one hand, electronic systems facilitate tracing individual payment and transfer records and thus detect suspicious transactions. On the other hand although, if consistent standards for recording important information (such as identities of transmitters and addressees of transactions) are lacking, transactions can only hardly be traced due to the increased volume and speed of transactions, which electronic means make possible.

2.4.2 Physical transmission by cash couriers

In case terrorists need to escape the “Anti Money Laundering/Combating the financing of terrorism (AML/CFT) standards which are widely applied in financial institutions, physical transmission of cash is an attractive option.

In this context, it has been found that often, prior to transmission, cash is converted into high-value goods such as gold or precious stones, in order to decrease the probability of detection in the process of transmission (FATF, 2006). Furthermore, reports show that physical fund transfer is most widely used within the Middle East and South Asia as well as Africa. In those regions, cash-based societies are still widespread, and electronic banking systems are not popular. However, even within Europe, money couriers are active, as analyses of terrorism cases have shown (FATF, 2008). In general, physical transfer is made use of if funds generated outside of the official financial system are intended to be kept out of the system in order to avoid detection. Typically, direct flight routes are used for simple transfers, but indirect flight routings with frequent changes of couriers as well as currencies have also been detected in the past (FATF, 2008).

While physical movement of money is typically more expensive in comparison with electronic transfer, it has become an attractive method among criminals and terrorists because detection is more unlikely since due-diligence practices (which will be discussed at length in the next section) in official financial institutions are spreading.

2.4.3 Transmission via the trade sector

In addition to using the official financial systems to transfer money (i.e. trading cash or other financial assets), trade in commodity goods is also used by criminals and terrorists in order to transfer illegal money. In this context, we stress that in the course of the last decades, international trade has undergone significant growth. According to the World Trade Organization WTO (2012a, 2012b), global merchandise trade exceeded USD 14 trillion in 2010, while trade in services accounted for USD 3.6 trillion in the same year. These figures highlight that detection of suspicious money transfers is difficult, due to the mere number of transaction that have to be checked.

As will be discussed below, the transmission of illegal money via the trade system is a frequently used method of money laundering. However, also terrorists make use of it in order to transfer funds.

2.4.4 Transmission by informal value transfer systems (IVTS)

Informal value transfer systems (IVTS) or “Alternative Remittance Systems” (ARS) are, according to FATF (2008), used by terrorist organizations for convenience and easy access. Moreover, they are attractive due to weaker record-keeping and less stringent regulatory surveillance in many regions. The high level of anonymity, as well as cultural reasons might also contribute to the attractiveness of informal remittance transfer.

Typically, IVTS come in many different forms and names and show specific regional characteristics. A widely used name denoting a specific variant of those systems is **“Hawala (door to door)”**. Due to the reasons outlined above, especially during the 1990s international concern grew over the IVTS and their abuse by transnational criminals and terrorists. Some academic works by Williams (2007), Passas (2004), and El-Quorchi and Maimbo (2003) have explained how informal systems operate, including their risks. In this context, it has been argued that Hawala is vulnerable to criminal abuse, and there is evidence that money derived from drug trafficking, illegal arms sales, body part trade, corruption, tax evasion, and all kinds of fraud have indeed moved through Hawala networks (Williams, 2007, El-Quorchi and Maimbo, 2003).

Some literature (Passas, 2004, Bunt, 2007) thus stresses the need for a regulation of the Hawala system. According to Bunt (2007), for example, Hawala bankers[22] are financial service providers who carry out financial transactions without a license and therefore without government control. They accept cash, cheques or other valuable goods (diamonds, gold) at one location and pay a corresponding sum in cash or other remuneration at another location. Unlike official banks, Hawala bankers disregard the obligations concerning the identification of clients, record keeping, and the disclosure of unusual transactions, to which these official financial institutions are subject.

To sum up, through Hawala, which forms an integral part of the informal black market economy, underground bankers ensure the transfer of money without having to move it physically or electronically. When a payment needs to be made overseas, the underground banker will get in touch with a courier (by personal conversation, email, fax or phone) in the destination country informing him of the details. To enable the recipient to obtain the money, a code referring to the underground banker in the country of origin is given to him. Such a system is almost untraceable since it leaves little if any paper trail. Transaction records are, if they are kept at all, being kept only until the money is delivered, at which time they are destroyed. Even if paper or electronic records are available, they are often in written in dialects or languages that serve as “de facto encryption system”.

To the best of our knowledge, there is no comprehensive study on the global flows of money related to Hawala systems. Rather, the literature stresses the difficulty

[22] Several traditional terms, like Hundi (India) and Fei-ch’ein (China) remind one of the fact that Hawala banking systems were developed independently from one another in different parts of the world. At present, a range of other terms is used to refer to the same phenomenon, such as “informal banking”, “underground banking”, “ethnic banking” or “informal value transfer system”.

to produce a quantitative assessment of such transfers (Wilson, 2002). In order to nevertheless capture the magnitude of the phenomenon, it is necessary to refer to different sources. Table 6 below presents some guesstimates and estimates of different studies. According to Fischer (2002) the annual turnover of the Hawala banking system already in the early 1970s in Arab states was as much as USD 60 bn. Six million foreign labourers in Saudi Arabia, who have been sending USD 40 bn. per year to their families and relatives in their home countries, made substantial use of the "ethnic" Hawala system. Fletcher and Baldrin (2002) estimate that USD 2.5 bn. have been transferred to Pakistan via Hawala-remittances in 2001. The amount of money in India´s Hindi system was USD 50 bn. in 1971.

Despite the growing competition by official remittance services, the use of Hawala banking has probably not declined. While according to a recent IMF-estimate, (especially Asian) migrants transfer USD 100 bn. dollars per year to family members and relations in their country of origin through the official financial system, an about equal amount of money is transferred in the form of goods, cash, and through "underground banking facilities" (IMF 2007). For Somalia, estimations range between USD 500 mn. and USD 1 bn. (Viles, 2008). In Afghanistan, in the city of Herat, the total of funds processed by Hawaladars is about USD 2.3 mn. per month. Thereof, USD 0.7 mn. must be directly linked to drug trade, whereas USD 1.3 mn. can be attributed to trade in legal goods (Thompson, 2006).

Table 6: Hawala guesstimates and estimates

Author/Source	country/area	year/period	estimated amount of informal money flows
Thompson (2006)	Afghanistan, city of Herat	unknown	USD 2.3 mn. per month
Fischer (2002)	Saudi Arabia	unknown	USD 40 bn. per year
Fletcher and Baldrin (2002)	Pakistan	2001	USD 2.5 bn.
Viles (2008)	Somalia		USD 0.5-1 bn.
Page and Plaza (2006)	global	2004	USD 57.53 bn.
Omer (2004)	Somalia		
Omer and El Koury (2004)	Somalia	2004	USD 0.7-1 bn. per year
Syed Manzar Abbas Zaidi (2010)	Pakistan	unknown	USD 2.5-3 bn. per year

ICG (2002)	Pakistan and Afghanistan	unknown	USD 2-5 bn. per year
Jessee (2006)	Pakistan	unknown	USD 2-3 bn. per year

An obvious question the above discussion yields is on adequate policy measures to curb the disadvantages of Hawala. An immediate strategy to treat the abuse of Hawala by criminals and terrorists would be to put the system under regulation, i.e. enforcing to take records of its users, just as within the formal financial sector. However, subjecting Hawala to the same rules as formal banks is likely to cause additional problems.

Hawala banking is regarded as a centuries-old institution which has not yet outlived its usefulness (Bunt, 2007). Low-income workers and migrant workers in particular supposedly put more trust in Hawala bankers than in formal banks. Thus, regulation either through registration or licensing is seen as ineffective because it will simply push the system further into the underground, further complicating the already problematic task of controlling Hawala transactions (Razavy, 2005, Perkel, 2004).

Nonetheless, as Bunt (2007) concedes, Hawala is frequently denoted “underground banking” and is thus a system that flies under the radar of modern supervision of financial transactions. “Underground banking” must be considered a threat to the effectiveness of anti-money laundering measures and the fight against terrorist financing. To prevent underground bankers from becoming a safe haven for criminals and terrorists, they should be subject to the standard regulations regarding record keeping, disclosure of unusual transactions and identification of clients[23].

However, in contrast to the disadvantages just discussed, Hawala undoubtedly also brings about major advantages, which we think should also be put forward. Among all remittance systems, it might come closest to “true” free market banking without government regulation, and it functioned well for centuries. Moreover, as already said, it is widely used by low-income workers and migrants, who supposedly have only limited, if any access to official financial intermediaries.

[23] Compare also Richard (2005) and Rider (2004).

2.5 Money laundering

While due to the relatedness of money laundering and international fund transmission we have already touched some aspects of money laundering in the section above, we will specifically concentrate on money laundering techniques here. As a matter of fact, the ultimate purpose of money laundering is to make illegal money appear legal (compare Walker, 2000, 2004, 2007). Hence, it comes with no surprise that it is frequently carried out by transnational criminals as well as terrorists and that both draw substantial benefits from money laundering. Note in this context that money laundering is frequently carried out by making use of shell companies and offshore bank facilities.

A frequently adopted technique is known as “starburst”[24]. A deposit of dirty money is made in a bank with standing instructions to wire it in small, random fragments to hundreds of other bank accounts around the world, in both onshore and offshore financial centres. Tracking down the money becomes very difficult, since getting legal permission to pursue bank accounts in multiple jurisdictions can take years. According to Napoleoni (2005), “you build a long chain of representative offices at the end of which there is a shell company registered offshore, and you are lucky, if you get to the end of the chain. Financial investigations often run into a blind alley always through, somewhere, in a tiny offshore office”. Below, we will now discuss further money laundering techniques.

2.5.1 Money laundering techniques

There are numerous methods of money laundering and Table 7 shows the twelve most important ones according to Unger (2007). Which of these methods is most frequently adopted depends on the type of criminal activity and on the specific institutional arrangements present in the country where the illegal money is “earned”. For example, in the drug business, the method of “business ownership” is quite often used. Drug dealers in big cities, for example, typically earn smaller amounts of cash in a lot of different places, which they infiltrate into cash intensive operations such as restaurants which are especially well suited for money laundering purposes. However, also cash deposits (the so-called “smurfing method”) or illegal gambling are quite often used.

[24] See Koh (2006), Schneider (2004, 2008a, 2008b, 2009) or Masciandaro (2004) for further details.

Table 7 obviously shows that there are a number of ways to launder money. It could thus be more efficient to put efforts in curbing criminal activities than to fight against money laundering.

Table 7: Money laundering techniques

1	**Wire transfers or electronic banking**	The primary tool of money launderers to move funds in the banking system. These moves can conceal the illicit origins of the funds or just place the money where the launderers need them. Often the funds go through several banks and even different jurisdictions.
2	**Cash deposits**	Money launderers need to deposit cash advances to bank accounts prior to wire transfers. Due to anti-money-laundering regulations they often "structure" the payments, i.e. break down large amounts to smaller ones. This is called "smurfing".
3	**Informal value transfer systems (IVTS)**	Money launderers need not rely on the banking sector, other transfer providers, such as Hawala or Hindi are readily available to undertake fund transfers. These systems consist of shops (mainly selling groceries, phone cards or other similar) being also involved in transfer services. IVTSs allow international fund transfers, as the shops taking part are present in several jurisdictions.
4	**Cash smuggling**	Money launderers might mail, Fedex or simply carry cash with them from one region to another, or even to different jurisdictions.
5	**Gambling**	Casinos, horse-races and lotteries are ways of legalizing funds. The money launderer can buy winning tickets for "dirty" cash – or, in the case of casinos, chips – and redeem the tickets or chips in a "clean" bank check. Afterwards, the check can be easily deposited in the banking sector.
6	**Insurance policies**	Money launderers purchase single premium insurance (with dirty cash), redeem early (and pay some penalty) in order to receive clean checks to deposit. Longer term premium payments might make laundering even harder to detect.
7	**Securities**	Usually used to facilitate fund transfers, where underlying security deals provide cover (and legitimate looking reason) for transfers.
8	**Business ownership**	Money might be laundered through legitimate businesses, where laundering funds can be added to legitimate revenues. Cash-intensive operations, such as restaurants, are especially well suited for laundering.
9	**Shell corporations**	Money launderers might exclusively create companies to provide cover for fund moves without legitimate business activities.
10	**Purchases**	Real estate or any durable goods purchases can be used to launder money. Typically, items are bought for cash and resold for clean money, like bank checks.
11	**Credit card advance payment**	Money launderers pay money in advance with dirty money, and receive clean checks on the balance from the bank.

12	**ATM operations**	Banks might allow other firms to operate their ATMs, i.e. to maintain and fill them with cash. Money launderers fill ATMs with dirty cash, and receive clean checks (for the cash withdrawn) from the bank.

Source: Unger (2007)

2.5.2 Mispricing or "money laundering through the back door"

In the subsection above we have discussed twelve according to Unger (2007) most important money laundering techniques. Many of those techniques have been denoted "money laundering through the front door" (Zdankowicz, 2004) since they make use of the official financial sector, although putting, as a matter of fact, considerable efforts into concealment too. However, according to Zdankovicz (2004), money laundering happens also "through the back door" by the mispricing of internationally traded goods. In that context, the author notes that "intelligence agencies are generally doing an adequate job curtailing the former (front door money laundering) but have largely ignored the latter (back door money laundering).

There are two principal ways of money laundering through the back door. Either are imports overvalued or exports undervalued. While this would normally not be profitable and thus not feasible to either the importer or exporter, it can be rational to undertake such activity if importer and exporter collude and intend to launder money[25].

2.5.2.1 Overvaluing imports

To be more specific, we describe in the following how money laundering by overvaluing imports works using an example noted in Zdankowicz (2004). Assume a foreign exporter exports 10,000 items of a certain product (say, razor blades) purchased for USD 1,000 (USD 0.1 per blade) in total to a domestic importer and charges USD 1 mn. (USD 100 per blade). Then, the domestic importer has moved USD 1 mn. less "transaction cost" of USD 1,000 (the "true" price of the blades") to the foreign country and by doing so laundered the money.

By evaluating US import and export transaction data (USDC, 2001), Zdankowicz (2004) detected some exceptionally high-priced US imports from al-Qaeda watch coun-

[25] This method is also applicable if colluding firms intend to evade taxes (Zdankowicz, 2004).

tries. They are reported in Table 8. Unfortunately however, the author does not say how frequently such transactions with exceptionally high import prices appear, apart from noting that apparently “thousands of such transactions have been detected”. Thus we are not able to determine whether they are the exception or the rule, nor are we able to infer the extent of money laundering or terrorist financing from these figures.

Table 8: Exceptionally high import prices from al-Qaeda watch countries

Product	**Country of origin**	**Price**
Toilet/Facial Tissue	China	USD 4,121.81/kg
Threaded Nuts	Belgium	USD 2,426.70/kg
Tweezers – Base Metal	Japan	USD 4,896.00/unit
Lawnmower Blades	Australia	USD 2,326.75/unit
Razors	U.K.	USD 113.20/unit
Cotton Dishtowels	Pakistan	USD 153.72/unit
Glass Mirror (less t. 929 sq. cm.)	Indonesia	USD 164.54/sq.cm.
Razors	Egypt	USD 22.89/unit
Air Pumps (hand/foot operated)	Malaysia	USD 5,000.00/unit
Camshafts and Crankshafts	Saudi Arabia	USD 15,200.00/unit

Source: Zdankovicz (2004)

2.5.2.2 Undervaluing exports

In order to launder money, undervaluing exports is more frequently adopted and preferred over overvaluing exports since exports are apparently less strictly monitored than imports, at least by US authorities (Zdankowicz, 2004). In the course of using the method of undervaluing exports, money from illegal sources is used to buy products at the domestic market (say, gold watches) for cash. ‘Those products are then exported below the market price. The foreign importer pays the low price and resells the products at the foreign official market, at their “true” value.

Table 9 presents some of the detected underpriced US-Exports (Zdankowicz, 2004, USDC, 2001). However, as with undervalued imports, we have to note that from those figures we are not able to draw conclusions on the frequency with which this method of money laundering and terrorist financing has been adopted. Again, the data do not include information on how frequently such transactions have been found.

Table 9: Exceptionally low export prices to al-Qaeda watch countries

Product	Destination country	Price
Diamonds – Not Industrial	India	USD 13.45/carat
Forklifts, Self-Propelled	Jamaica	USD 384.14/unit
Bulldozers – Self-Propelled	Colombia	USD1,741.92/unit
Video Projectors – Colour	Brazil	USD 33.95/unit
Missile and Rocket Launchers	Israel	USD 52.03/unit
Colour Video Monitors	Indonesia	USD 22.43/unit
Colour Video Monitors	Pakistan	USD 21.90/unit
Sports Footwear (Athletic Shoes)	Jordan	USD 0.40/pair
Radioactive Elements, Isotopes	Egypt	USD 0.01/mbq

Source: Zdankovicz (2004)

3 Organizations, standards and achievements in combating money laundering and terrorist financing

Obviously, governments, authorities and the international community take considerable efforts in combating the money laundering and terrorist financing described in the previous chapter since both of these offences are, according to Ertl (2004) likely to

- Decrease stability of the international economic activity, i.e. by distorting capital markets
- Triggering or amplifying financial crises
- Infiltrating legal economic structures
- Fostering the dependence of "weak states" on organized crime

The following chapter features a comprehensive description of i) the organizations and authorities involved in the fight against money laundering and terrorist financing, ii) the standards and recommendations those organizations call for, iii) some (preliminary) evaluations of the commitment of countries to those standards and the extent to which they have been implemented in the recent years and iv) the shift from a rule- to a risk based strategy intended to be undertaken in combating money laundering and terrorist financing.

It is fair to note that the fight against money laundering and terrorist financing has developed into a “central issue” in the realm of the international community and its organizations (i.e. the United Nations, OECD or regional bodies such as the EU).

Moreover, it is important to note that by the increasing globalization and international integration of the financial markets and a continuously increasing velocity of the circulation of money, the possibilities to launder money have increased and the methods changed. While in the 1980s, money laundering has typically been linked to drug trafficking and the “Mafia”; it is today one of the most important and also most efficient economic crimes (Ertl, 2004). As discussed in the chapter above, money laundering accounts for about 2-4 percent of world GDP according to IMF (2002, 2007) and world bank estimates, while it is estimated to be considerably higher (13 percent of EU-15 GDP and 19 percent of US GDP) according to other studies (see, i.e. Bagella et al., 2009).

While money laundering is in the focus of the international community since about the end of the 1980s (see the discussion on the founding of the FATF below), fighting terrorist financing has been spurred in particular after the airplane attacks on the New York World Trade Centre on September 11, 2001 (Ertl, 2004). In this context, it is noteworthy that less than two weeks after these attacks (on September 24, 2001), the US administration issued an Executive Order imposing extraterritorial financial sanctions on banks, financial institutions, legal and natural persons as well as US and foreign business entity that provide support for international terrorist groups. Moreover, on October 26, 2001, the US Congress expanded the predicate offence of money laundering to also include terrorist attacks and any activity that provides material support for individuals, groups or entities involved in terrorism by issuing a law entitled “the uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism”. This legislation became also known as the “Patriot Act 2001” (Kern, 2002). Thus, the first efforts in the “War on Terrorism” of the US Government at that time were in impeding terrorist financing rather than military intervening in countries suspected to foster terrorism. And these first efforts have in the past been numerously denoted as a success story (see, i.e. Biersteker and Eckert, 2008, Clunan, 2006 or

Taylor, 2007). Indeed, by investigating the financial flows preceding the September 11, 2001 attacks, connections could be brought to light and intelligence on the planning gained.

However, certain points in the Executive Order allowing unilateral blacklisting of both groups and individuals suspected of terrorist financing have since then been ruled unconstitutional, since they have limited individual constitutional rights too far (The Guardian, 2006). Moreover, as discussed above, in contrast to money laundering, the financial flows being linked to international terrorism are low, which as a matter of fact significantly complicates their disclosure (Ertl, 2004).

Thus, in tackling terrorist financing, multi-level cooperative and regulatory measures are called for (Heng and McDonagh, 2008), which in the following will be discussed at length. In particular, the discussion on organizations, standards and achievements in the fight of money laundering and terrorist financing will reveal that the common viewpoint is that institutions involved in financial transactions must act preventively and proactively against potential money launderers. The so-called “Know your customer” principle, meaning to determine the identity of customers, to continuously survey his or her accounts and transactions and to report suspicious transactions to the authorities, is of paramount importance and central to all standards intended to tackle money laundering. Also, governments and authorities are requested to take efforts and international cooperation is called for since in most so far detected incidents of money laundering, international transactions have been carried out (Ertl, 2004).

3.1 Organizations involved in combating money laundering and terrorist financing

As discussed above, the years after the airplane attack on the New York World Trade Centre on September 11, 2001 have not only witnessed the creation of international political and military coalitions, but collective actions tackling the financial sector and its vulnerability to money laundering and terrorist financing. The most notably of those actions was the establishment of the Financial Action Task Force (FATF) and its satellite organizations.

In the following paragraphs we will give information on the most important such regional, superregional as well as international bodies.

3.1.1 The Financial Action Task Force (FATF)

The Financial Acton Task Force (FATF) was founded in 1989 at the summit of the G7-countries in Paris on proposal of the General Assembly of the United Nations (UN) which pledged first in 1988 to stop money laundering. At that time, as discussed above, money laundering was prevalent predominantly in drug trafficking (Johnson, 2008). The FATF is located at the headquarters of the Organization for Economic Cooperation and Development (OECD) in Paris, however, it views itself as an independent institution wanting to sustain its “task-force character” (Ertl, 2004). Currently, the FATF comprises 34 member countries[26] as well as two regional organizations[27] and represents most major financial centres of the world (FATF, 2012).

The first and foremost purpose of the FATF is and was to develop appropriate means for combating money laundering. In doing so, the organization issued a set of 40 recommendations (FATF/OECD, 2010a) in 1990 intended to set forth a comprehensive strategy for the fight against money laundering[28]. Those recommendations cover the law and its enforcement, provide guidelines for financial institutions and non-financial businesses, cover the regulation of the financial sector and include matters relating to international cooperation. The 40 recommendations have been revised and substantially updated in the aftermaths of the airplane attacks on the New York World Trade Centre on September 11, 2001. In particular, they have been supplemented by a set of nine special recommendations[29] specifically dwelling on the issue of terrorist financing.

FATF member countries have been evaluated against commitment to the 40 recommendations as well as the nine special recommendations by making use of self-assessment and mutual assessment procedures. While self assessment is carried out on

[26] The member countries are Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, Finland, France, Germany, Greece, Hong Kong (China), Iceland, India, Ireland, Italy, Japan, Kingdom of the Netherlands (including Aruba, Curacao and Saint Marteen), Luxembourg, Mexico, New Zealand, Norway, Protugal, Republic of Korea, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

[27] The member regional organisations are the European Commission and the Gulf Cooperation Council with member states Bahrein, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

[28] The 40 recommendations are listed in Appendix B.

[29] The nine special recommendations are also listed in Appendix B.

the basis of a yearly questionnaire, mutual evaluation is done by experts on law, financial regulation, law enforcement and international cooperation from other countries and takes place on-site (Johnson, 2008). In such evaluations, countries are assessed as being non-compliant, partially compliant, largely compliant or fully compliant with each of the 40 plus nine recommendations. The mutual assessment reports for each country are made publicly available at the website of the organization (www.fatf-gafi.org).

The aim of the FATF is a worldwide implementation of unique standards and to stimulate member countries as well as non-members to increase efforts in the fight against money laundering and terrorist financing. In order to tie in non-member states, so called FATF-style regional bodies (FSRB) have been established. Those are introduced and discussed in the following section.

3.1.2 FATF-style regional bodies (FSRB)

In the following we will describe eight FATF-style regional bodies (FSRB), established in order to spread the FATF recommendations (FATF/OECD, 2010a) and standards among countries which are not member of the FATF.

3.1.2.1 The Caribbean Financial Action Task Force (CFATF)

The Caribbean Financial Action Task Force was founded in the early 1990s and represents 30 countries[30] within the Caribbean region. They agreed to a common approach in fighting money laundering and formulated 19 anti-money-laundering recommendations which address issues specifically relevant to the region (Johnson, 2008).

3.1.2.2 The Eurasian Group

The Eurasian Group (EAG) was established in 2004 and has now eight members[31]. The primary objective is cooperation throughout the Eurasian region in issues on

---

[30] Member countries are Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Island, Cayman Islands, Curacao, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, Nicaragua, St. Kitts and Nevis, St. Lucia, St. Maarten, St. Vincent and the Grenadines, Suriname, Trinidad and Tobago, Turks and Caicos Islands and Venezuela.

[31] Those are Belarus, China, Kazakhstan, Kyrgystan, Russian Federation, Tajikistan, Turkmenistan and Uzbekistan.

the fight against money laundering and terrorist financing. Moreover, it promotes the FATF 40 plus 9 recommendations (FATF/OECD, 2010a, 2010b) and carries out mutual evaluations according to FATF standards.

3.1.2.3 The Eastern and Southern Africa Anti-Money Laundering Group

The Eastern and Southern Africa Anti-Money Laundering Group currently has 15 member countries[32] and has been established in 1999. It has also implemented the FATF's 40 recommendations (FATF/OECD, 2010a), taking into account regional factors. Moreover, it includes the FATF nine special recommendations (FATF/OECD, 2010b) in its brief. Members, however, typically carry out self-assessment rather than mutual evaluations (Johnson, 2008).

3.1.2.4 The intergovernmental action group against money-laundering in Africa (GIABA)

The intergovernmental action group against money-laundering in Africa was founded in 1999 by a joint decision of the Economic Community of West African States[33]. GIABA members recognize the need to take action against money laundering and the financing of terrorism and stress that those issues are of global importance. The aim of GIABA is to protect the member countries' economies and financial institutions from criminal abuse (Johnson, 2008).

3.1.2.5 The Asia/Pacific group on Money laundering (APG)

The Asia/Pacific group on Money laundering (APG) is an autonomous regional body whose member countries[34] collaborate in the fight against money laundering and

---

[32] Those are Botswana, Comoros, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Seychelles, Tanzania, Uganda, Zambia as well as Zimbabwe.

[33] Member countries are Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, Gambia, Ghana, Guinea Bissau, Guinea Conakry, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, Togo.

[34] Those are Afghanistan, Australia, Bangladesh, Brunei Darussalam, Cambodia, Canada, China, Cook Islands, Fiji, Hong Kong (China), India, Indonesia, Republic of Korea, Japan, Laos, Macao, Malaysia, Maldives, The Marshall Islands, Mongolia, Myanmar, Nauru, Nepal, New Zealand, Niue, Pakistan, Palau, Papua New Guinea, The Philippines, Samoa, Singapore, Solomon Islands, Sri Lanka, Taiwan, Thailand, Timor Este, Tonga, USA, Vanuatu, Vietnam.

the financing of terrorism. The group aims at adopting the internationally accepted AML/CFT standards.

3.1.2.6 The Financial Action Task Force on Money Laundering in South America (GAFISUD)

GAFISUD is a regional South American body established in 2000[35]. It has adopted the 40 plus nine recommendations (FATF/OECD 2010a, 2010b) and aims at further developing them to increase efficiency of national anti-money laundering and terrorist financing policies.

3.1.2.7 The Middle East and North Africa Financial Action Task Force (MENAFATF)

The Middle East and North Africa Financial Action Task Force was founded in 2004[36] and aims at fostering cooperation in the fight against money laundering and terrorist financing in the Middle East and North Africa. It has adopted the 40 plus nine recommendations (FATF/OECD, 2010a, 2010b) as well as relevant UN treaties (Johnson, 2008).

3.1.2.8 The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

MONEYVAL was established in 1997 and has currently 29 member countries[37] from Central and Eastern Europe. It aims to ensure that the member countries comply with the FATF 40 plus nine recommendations (FATF/OECD, 2010a, 2010b) and other international standards in the fight against money laundering and terrorist financing.

---

[35] Members are Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, Mexico, Panama, Paraguay, Peru and Uruguay.

[36] Member countreis are Algeria, Bahrain, Egypt, Mauritania, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Republc of Iraq, Saudi-Arabia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.

[37] Those are Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Israel, Latvia, Liechenstein, Lithuania, Macedonia, Malta, Moldova, Monaco, Montenegro, Poland, Romania, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, Ukraine.

MONEYVAL uses mutual evaluation to the extent of compliance with the standards among member countries.

The above listed groups encompass, together with the “core-FATF” the most important world financial centres and a majority of countries. The groups have been set up to take action against money laundering and terrorist financing and typically amend the FATF 40 plus nine recommendations (FATF/OECD, 2010a, and 2010b) in order to suit to their local environment and specifics. Since many of the FATF style regional bodies make use of the same assessment criteria in evaluating member countries’ compliance, and reports are made publicly available, comparing evaluation reports across groups is possible. The available assessments will be discussed in the next sections.

3.2 Standards in combating money laundering and terrorist financing

3.2.1 The FATF’s 40 recommendations on tackling money laundering

As discussed above, the Financial Action Task Force (FATF) is the most important body in the international fight against money laundering and terrorist financing. It has issued its widely known and applied “Set of 40 recommendations” on money laundering in April 1990 (note that at that time, terrorist financing was not a big issue). This set has been revised in 1996 as well as 2003 and is since many years recognized as the international standard in the combat against money laundering (Gardner, 2007). They define the principles by which countries, financial institutions as well as some designated non-financial businesses, should act, but are also intended to leave flexibility such that they can be implemented in the various different constitutions and institutional frameworks (Johnson, 2008). The recommendations are not legally binding, however, a majority of countries have made a political commitment to apply them (Gardner, 2007).

In terms of contents, the FATF’s 40 recommendations[38] cover the following:

- Legal measures
- Institutional measures
- Measures to be taken by financial institutions
- Measures to be taken by non-financial businesses

[38] See Appendix B for a complete listing oft he FATF’s 40 recommendations

- Measures to be taken with respect to the informal sector
- Entity transparency
- International cooperation

The central issue of the FATF's 40 recommendations is "customer due diligence" or the "know your customer" principle. In the course of applying it, anonymous accounts are to be eliminated, customers to be identified, records of transactions for at least five years to be kept and to be made available to the competent authorities upon request, and authorities are to be notified if suspicious transactions occur.

In addition, the FATF recommends that countries criminalize money laundering as well as "wilful blindness", and that punishment for such crimes should be one year of imprisonment or higher (Gardner, 2007). Moreover, the FATF calls for endowing the authorities with the legal power to identifying, tracing and confiscating laundered money, and it calls for increasing international cooperation and making information on cross-border financial flows available to central banks and multilateral financial institutions (FATF/OECD 2010a).

3.2.2 The FATF's nine special recommendations on tackling terrorist financing

After the airplane attacks on the New York World Trade Centre on September 11, 2001, the FATF has issued its nine special recommendations on countering terrorist financing[39]. They list the actions which are according to the FATF necessary in the fight against terrorist financing and the FATF calls for their implementation in conjunction with the 40 recommendations on money laundering discussed above (Johnson, 2008). In particular, the nine special recommendations on tackling terrorist financing urge countries to

1) ratify all relevant UN resolutions
2) criminalise terrorist organisations, activities and financing
3) allow for the freezing and confiscation of terrorist assets
4) report suspicious transactions related to terrorism

---

[39] See Appendix B for a complete listing oft he FATF's nine special recommendations, including some detailed explanations.

5) provide international co-operation in matters related to terrorism
6) subject alternative remittance systems to the same oversight as the banking sector
7) strengthen customer identification requirements on wire transfers
8) make sure non-profit organisations cannot be used to launder terrorist funds
9) put in place a system to record and detect cross border transportation of currency and bearer instruments

Note that these special recommendations, in particular Recommendation 6 are calling for licensing and registrations of all remittance systems, including the alternative ones like Hawala or Hindi (see the discussion in Section 2.4.4). In an extensive survey Wang (2011) compares the approach of registering (undertaken i.e. in the UK and Sweden) and the stricter approach of licensing (undertaken in i.e. Germany and Norway). The conclusion of this comparison is that with respect to alternative remittance systems, thresholds for requirements the operators of such systems have to obey have to be held low. If they are too high, operation is likely to be driven into the underground sector.

3.2.3 The EU directives on prevention of money laundering

The European Union (EU) took action in the treatment of money laundering by issuing its "Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering" in 1991 (European Union, 1991). This document is henceforth denoted the "first directive" since two more such directives have followed so far. The second directive of 2001 (European Union, 2004) broadened the scope of the first directive in including non-financial institutions such as, for example, real estate agents, casinos, lawyers and notaries as entities subject to the issued rules. In 2005, the third directive replaced the second one (European Union, 2005).

In general, it can be said that the EU directives carry forth the FATF's 40 recommendations on money laundering and its nine special recommendations on terrorist financing into European Law and that they provide an EU-wide basis for the implementation of the recommendations. Note in this context that the second and the third directive have been responses to amendments of the FATF's recommendations (van den Broek, 2011).

3.3 Evaluations of the actions against money laundering and terrorist financing

As noted earlier already, a number of member countries of the FATF or the FATF-style regional bodies have been evaluated against commitment to the 40 recommendations as well as the nine special recommendations. Evaluation was done by either self-assessment or mutual investigation. While self assessment is carried out on the basis of a yearly questionnaire, mutual evaluation is done by experts on law, financial regulation, law enforcement and international cooperation from other countries and takes place on-site (Johnson, 2008). In such evaluations, countries are assessed with respect to each single recommendation or special recommendation and categorized as being either

- Non-Compliant (NC)
- Partially Compliant (PC)
- Largely Compliant (LC) or
- Fully compliant (C)

with the 40 plus nine recommendations. As also noted above, the mutual assessment reports for each country are made publicly available at the website of the organization (www.fatf-gafi.org).

3.3.1 Results of mutual evaluations according to IMF (2011)

An extensive overview and discussion of the results of the mutual evaluations of 162 countries can be found in IMF (2011). In the following we will descriptively compare the assessments of the 27 EU-countries as well as 43 countries from an IMF-list of offshore financial centres (IMF, 2000). We compare those two types of states because i) as discussed in Section 2, a considerable fraction of money laundering and terrorist financing is routed through such offshore centres, and ii) in Section 4 we will be investigating whether increasing tax information exchange with the authorities of such centres could bolster the fight against money laundering and terrorist financing by reducing tax avoidance and thus international financial flows, which are assumed to provide cover for illegal flows and money laundering. We will compare the EU-countries' and offshore centres' evaluations on i) the total of the 40 and nine recommendations on money laundering and terrorist financing, ii) the recommendations on legal and institutional measures, iii) the recommendations on the duties of financial and non-financial businesses as well as the informal sector, and iv) the recommendations on entity transparency and international cooperation.

3.3.1.1 Scores on total "AML" (anti-money laundering) and "CFT" (combating the financing of terrorism)

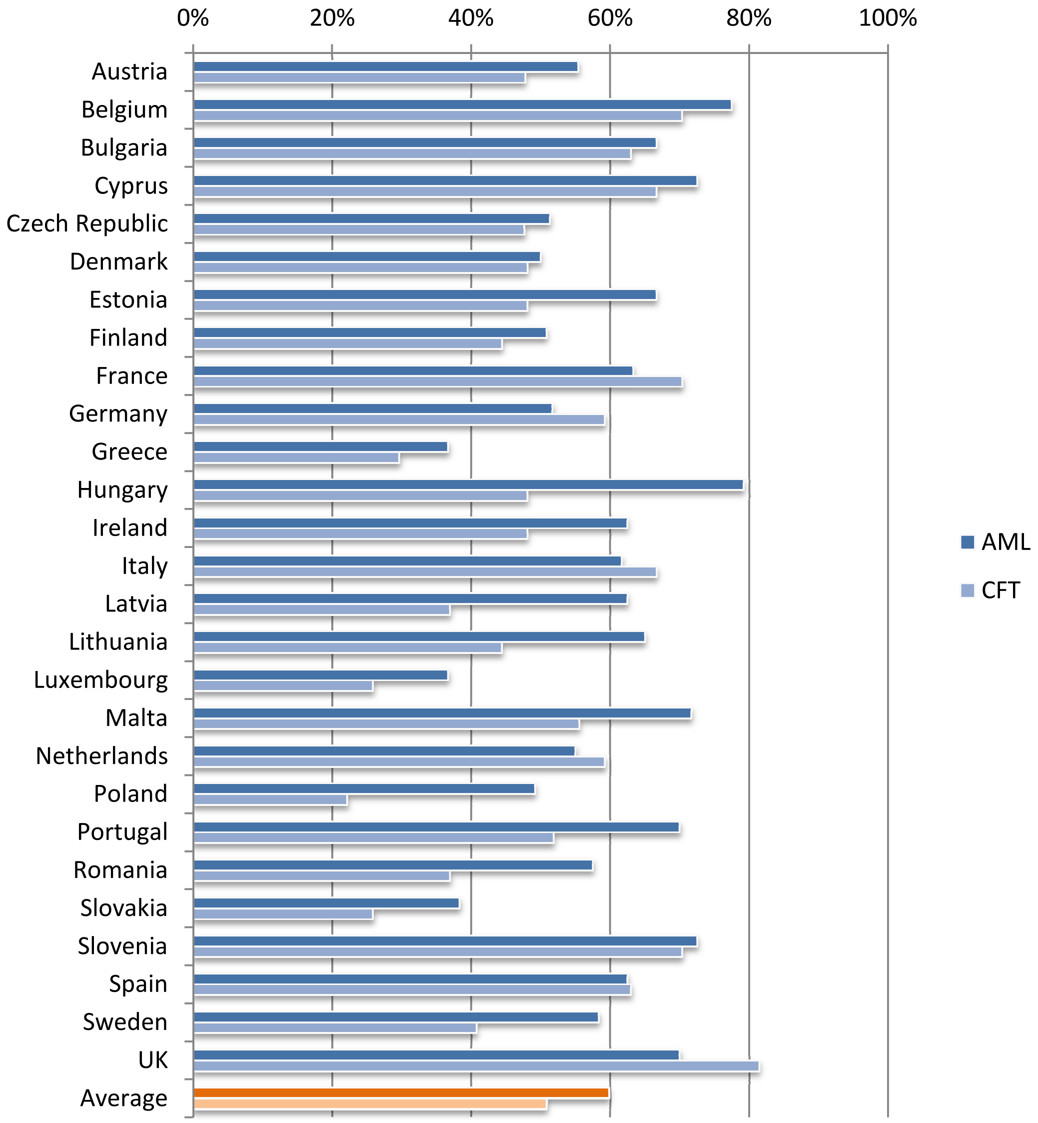
Figure 2 shows "the extent of compliance"[40] with the recommendations on anti-money laundering (AML) and combating the financing of terrorism (CFT) for the 27 EU member countries. Figure 3 does the same for 43 countries appearing on an IMF (2000) list of offshore financial centres. As can be seen, there is quite considerable variation in the scores both among the EU countries as well as among the offshore financial centres. Moreover, it is remarkable that 100 percent compliance never appears. Not surprisingly, average compliance with the recommendations is higher among the EU countries than among the offshore financial centres, however, three EU countries have compliance levels of less than 40 percent for both AML as well as CFT recommendations. On the other hand, for 15 member countries, compliance with either AML or CFT recommendations or both exceeds 60 percent.

Interestingly, while some of the designated offshore financial centres (IMF, 2000) show quite high compliance, more than one in four has compliance levels below 40 percent.

---

[40] The percentages indicated in the tables are based on the ratings assigned in course of the mutual evaluations. There, each country has been rated with respect to each recommendation or special recommendation whether it is „compliant" (C), „largely compliant" (LC), „partially compliant" (PC) or „non-compliant" (NC). For calculating the percentages, the ratings have been replaced with 1 (C), 0.66 (LC), 0.33 (PC) or 0 (NC). Then, the scores of each country over the considered recommendations have been summed up and divided by the total number of considered recommendations.

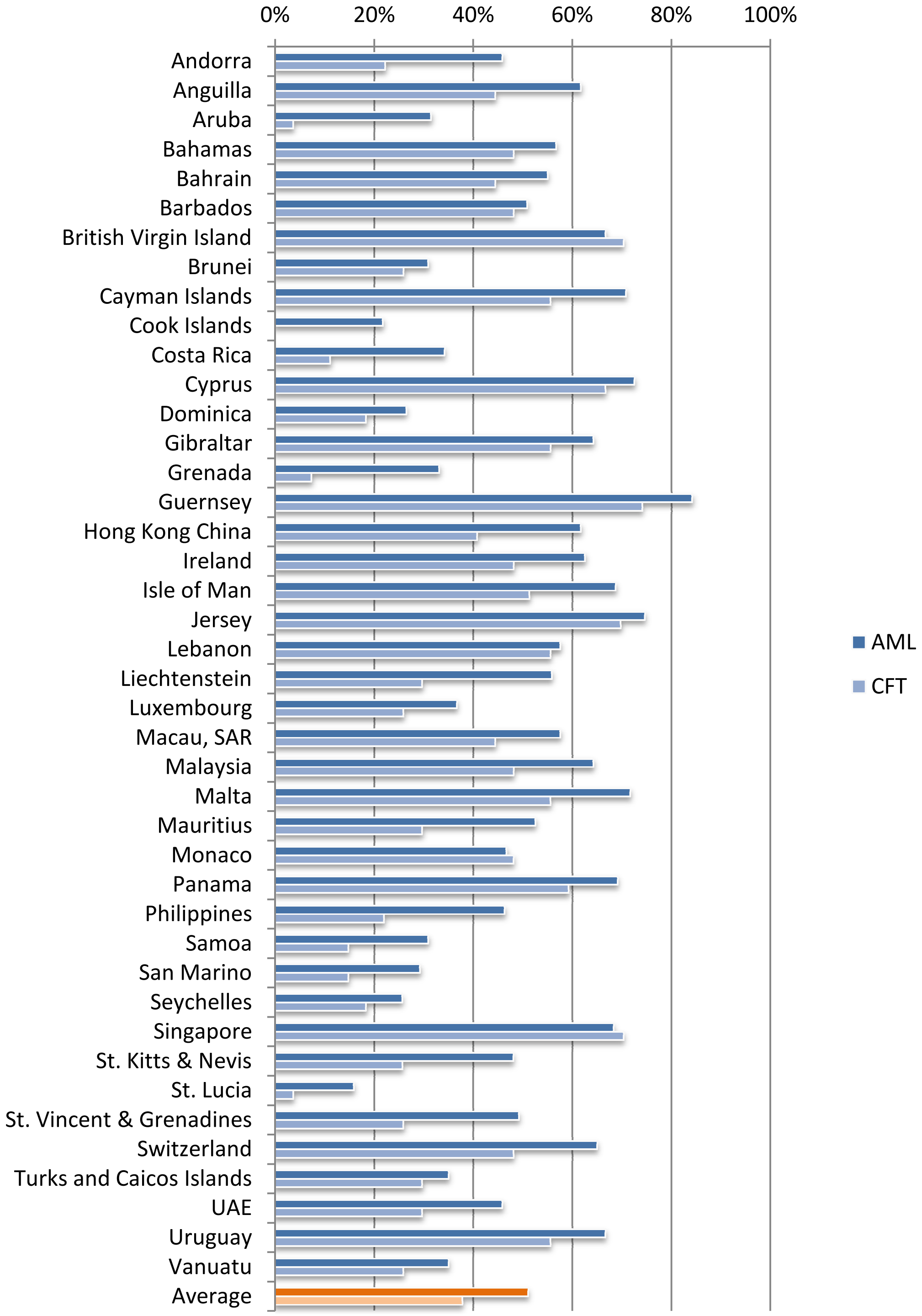
Figure 2: Extent of compliance with AML (anti money laundering) and CFT (combating the financing of terrorism) recommendations – EU-countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered. For AML (anti-money laundering), all 40 recommendations have been considered, for CFT (combating the financing of terrorism all 9 special recommendations.

Figure 3: Extent of compliance with AML (anti money laundering) and CFT (combating the financing of terrorism) recommendations – offshore financial centres



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered. For AML (anti-money laundering), all 40 recommendations have been considered, for CFT (combating the financing of terrorism all 9 special recommendations.

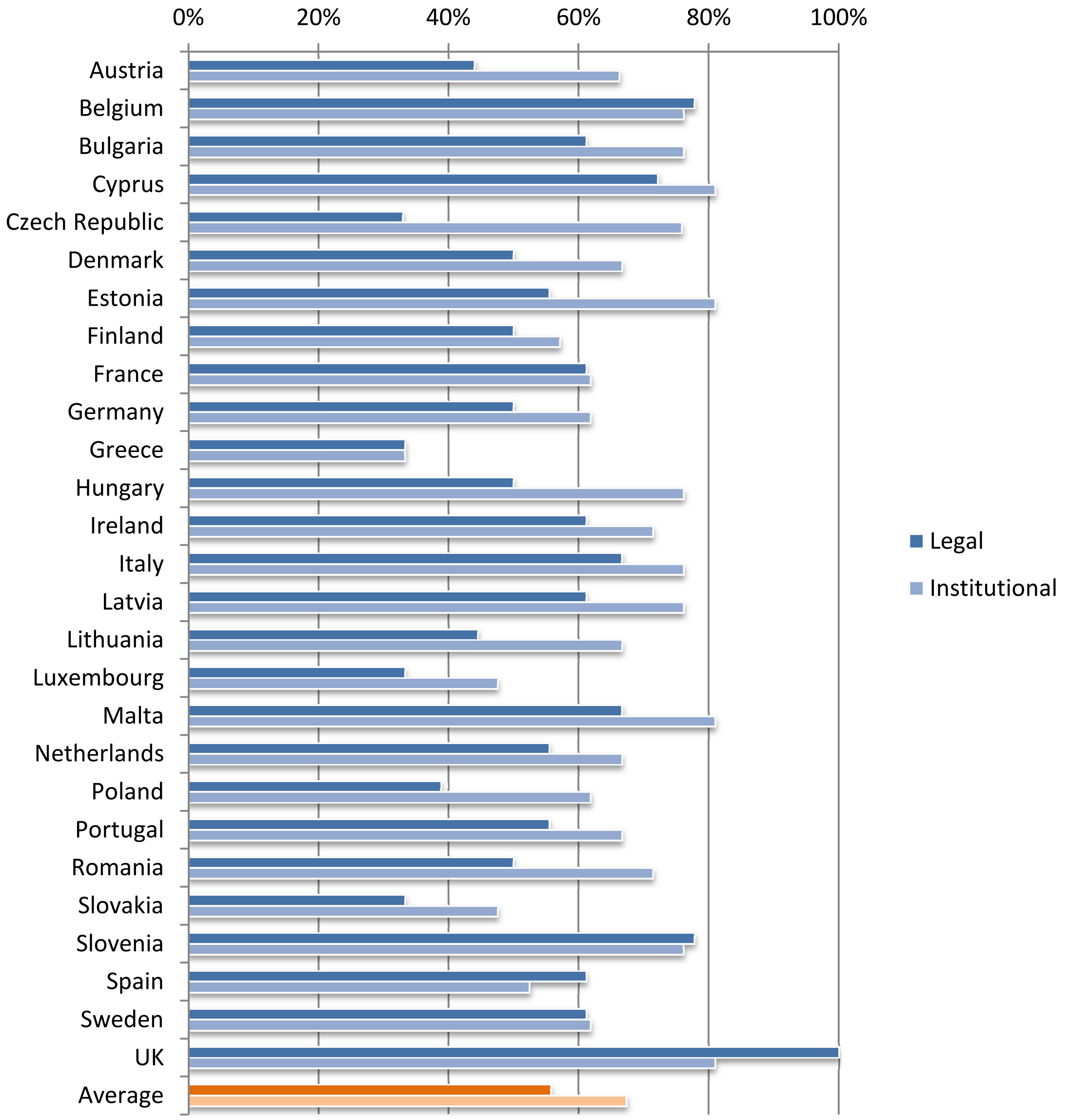
3.3.1.2 Scores on recommendations addressing legal and institutional issues

Legal issues in the fight against money laundering and terrorist financing are addressed by the recommendations 1, 2 and 3 as well as special recommendations 1, 2 and three. Institutional issues, in turn, are addressed by recommendations 26 – 32[41]. Basically, the legal recommendations call for criminalizing money laundering and imposing substantial punishment, while the institutional recommendations require endowing financial intelligence units and other investigators with all available information, technical equipment as well as enough financial resources in order to carry out their work.

As can be seen from Figure 4 (EU countries) and Figure 5 (offshore financial centres), compliance with legal and institutional standards is generally above average (compare Figure 2 and Figure 3 with the scores taking into account all recommendations). Among the EU countries, there is only one yielding a compliance rate of less than 40 percent, while the average rate is around 60 percent of compliance. Among the offshore financial centres, some have high compliance rates exceeding 80 percent, while again one in four is below 40 percent of compliance.

[41] A list of all recommendations including detailed explanations is available in Appendix B.

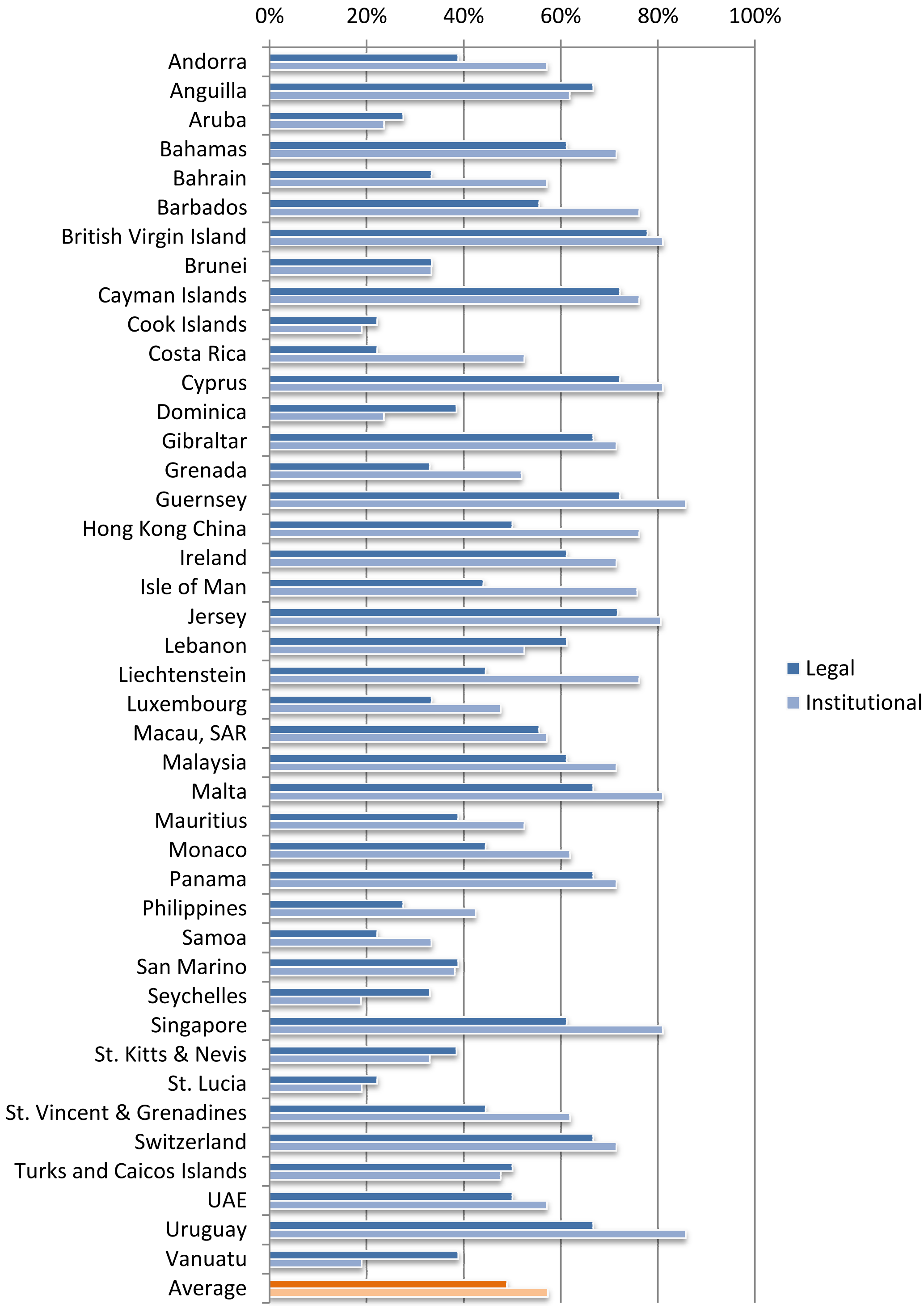
Figure 4: Extent of compliance with recommendations addressing legal and institutional issues – EU countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings “Compliant” (C), “largely compliant” (LC), “partially compliant” (PC) and “non-compliant” (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered. For “Legal”, recommendations 1, 2, 3 and special recommendations 1, 2 and 3 are considered, while for “Institutional”, recommendations 26 – 32 apply.

Figure 5: Extent of compliance with recommendations addressing legal and institutional issues – offshore financial centres



Source: IMF (2011) and own calculations

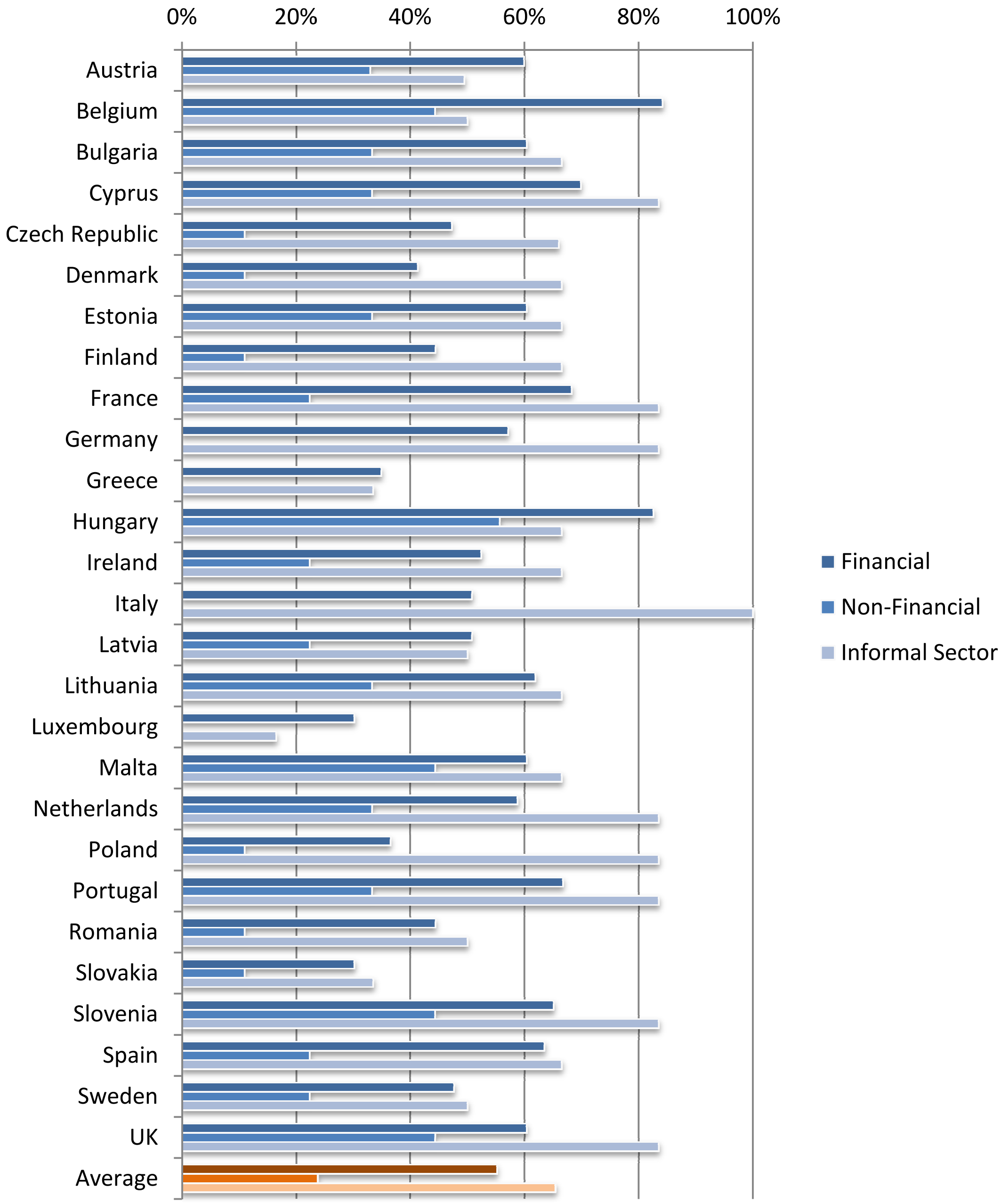
The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered. For "Legal", recommendations 1, 2, 3 and special recommendations 1, 2 and 3 are considered, while for "Institutional", recommendations 26 – 32 apply.

3.3.1.3 Scores on recommendations addressing the financial, non-financial and informal sector

FATF-recommendation 4 – 11, 13 – 15, 17 – 19, 21 – 23 and 25 as well as special recommendations 4, 6 and 7 are addressing the regulation of the financial sector. Designated non-financial businesses (i.e. casinos, real-estate agents, lawyers, notaries etc.) are treated with recommendations 12, 16 and 24, while measures intended at preventing the abuse of the informal sector are dealt with in recommendation 20 and special recommendation 9. The recommendations mentioned above in general call for application of the “know your customer principle”, saying that businesses should keep record of their customers’ transactions, determine and record their identity and report suspicious transactions.

Figure 6 shows the level of compliance for the 27 EU countries, while Figure 7 does so for the 43 offshore financial centres analyzed in this context. As can be seen, there are notable differences in the compliance rates across sectors. Compliance with recommendations addressing the informal sector is generally very high and exceeding 80 percent for nine EU countries as well as five offshore financial centres. Moreover, compliance with recommendations addressing the financial sector is lower in turn, but the by far lowest compliance rates are with the recommendations addressing the non-financial businesses like casinos, real-estate agents or notaries etc. Here, average compliance is slightly higher than 20 percent for EU countries and slightly lower than 20 percent for the offshore financial centres. It is also noteworthy that compliance with recommendations for treating the financial sector is lower than 40 percent for as much as 15 offshore financial centres.

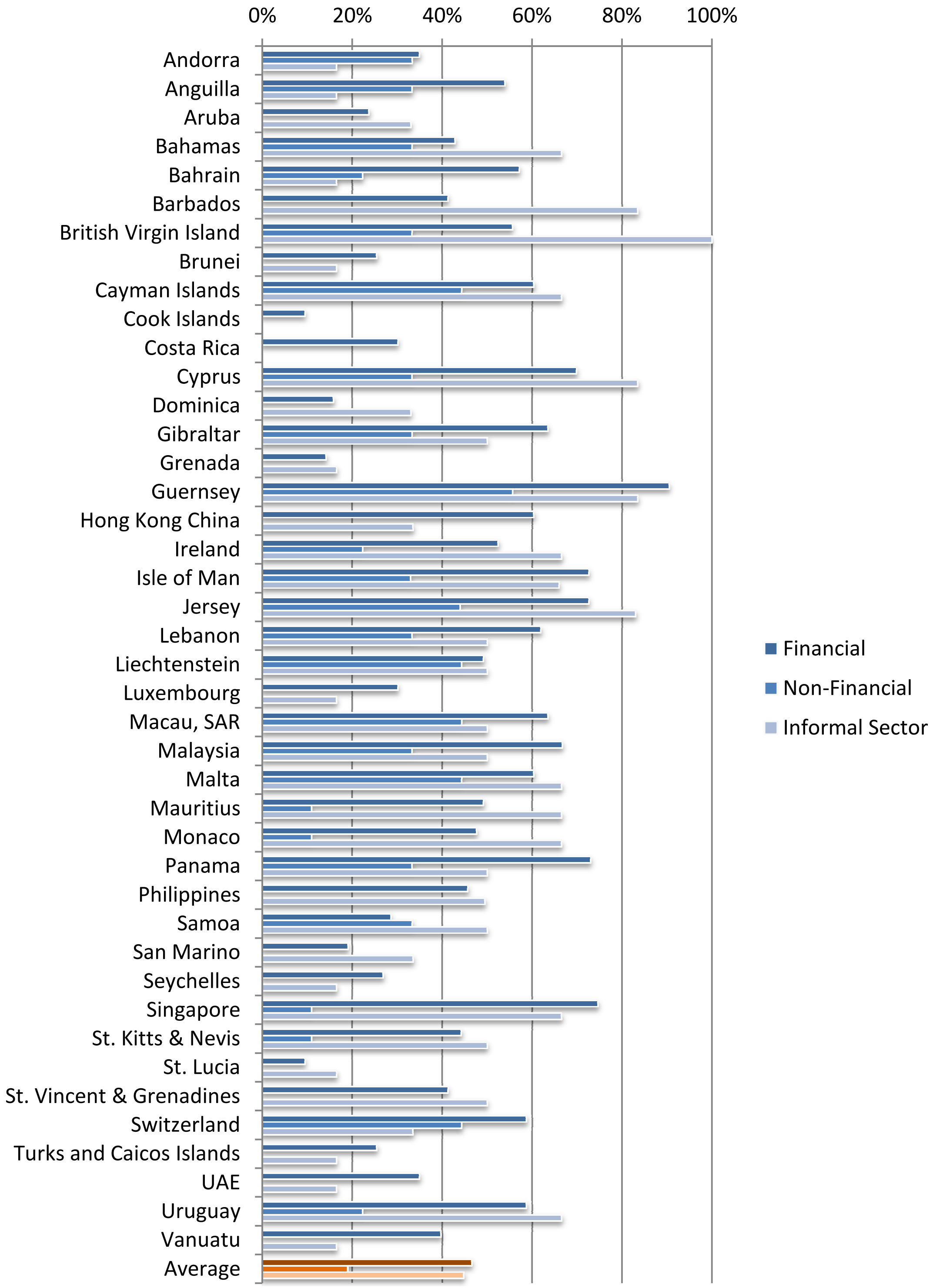
Figure 6: Extent of compliance with recommendations addressing the financial, non-financial and informal sector – EU countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered.

Figure 7: Extent of compliance with recommendations addressing the financial, non-financial and informal sector – EU countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings “Compliant” (C), “largely compliant” (LC), “partially compliant” (PC) and “non-compliant” (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered.

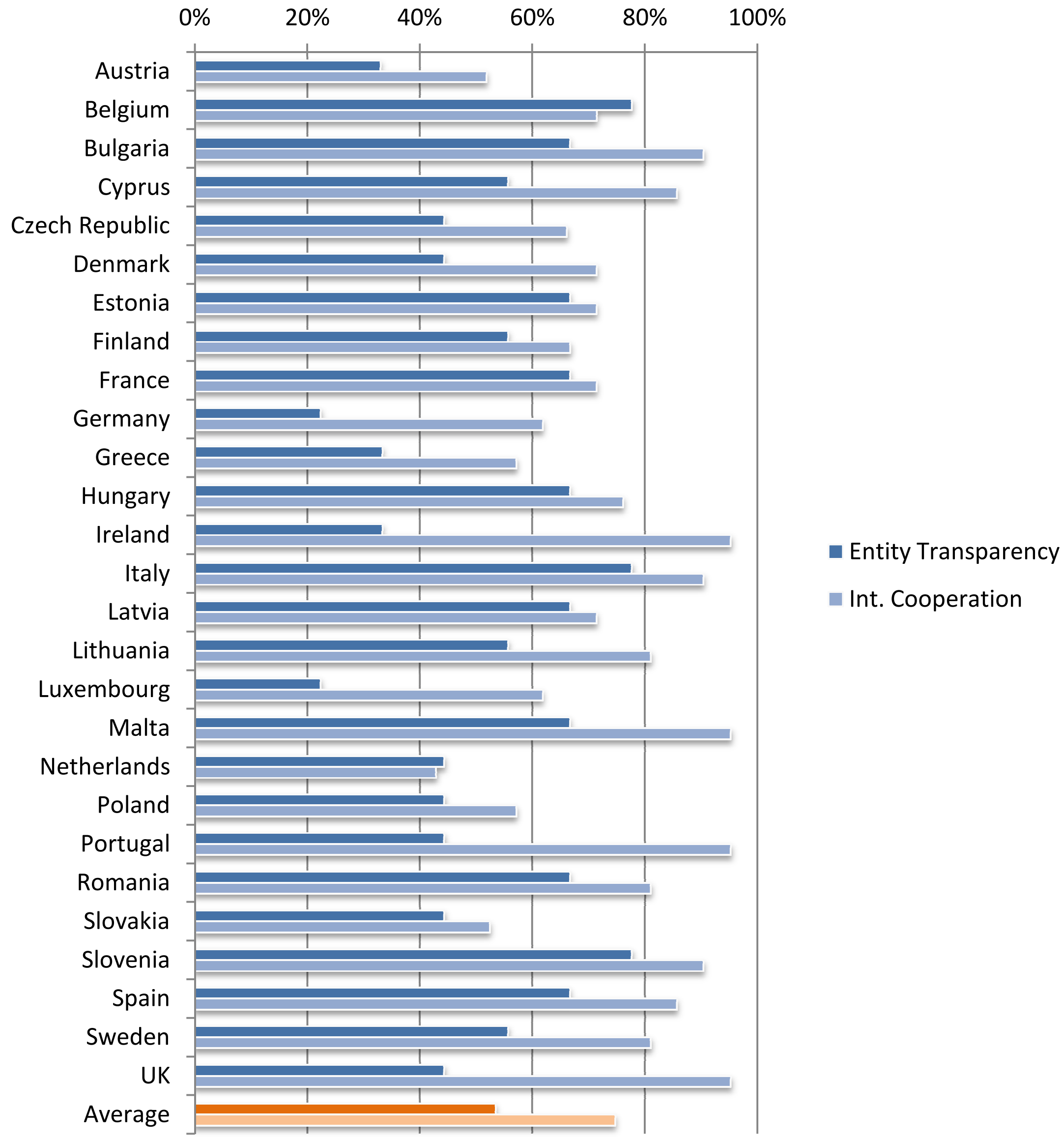
3.3.1.4 Scores on recommendations addressing entity transparency and international cooperation

In addition to calling for rigorous treatment of financial institutions, some non-financial businesses and the informal sector as well as severe punishment for money launderers, the FATF also requests entity transparency (by recommendation 33, 34 and special recommendation 8) and international cooperation across jurisdictions (recommendations 35 – 40 and special recommendation 5. By calling for entity transparency, the FATF requires that information on financial institutions and their customers etc. should be made available to the authorities and financial intelligence units. By calling for international cooperation, the FATF urges to share this information with other countries' authorities and not to deny information sharing on grounds of bank-secrecy laws etc.

As can be seen from Figure 8 (EU countries) and Figure 9 (offshore financial centres), compliance with the recommendations addressing international cooperation is quite high among EU countries (the average is slightly lower than 80 percent), although some countries like for example Austria, the Netherlands or Slovakia show considerably lower compliance levels. Across the offshore financial centres, the variation in compliance is high. For many it is around 40 percent or lower, while others yield levels close to 100 percent.

Most striking are, however, the results on entity transparency. For six of the listed offshore financial centres, compliance is around 10 percent, and the average over all offshore financial centres is only 40 percent. This is, as will turn out in Section 3.3.2 below, the reason why tax information exchange agreements (TIEAs) are often inefficient, although being in place. The authorities of offshore financial centres agree to share information with other countries, but they have simply no information available because entity transparency is so low.

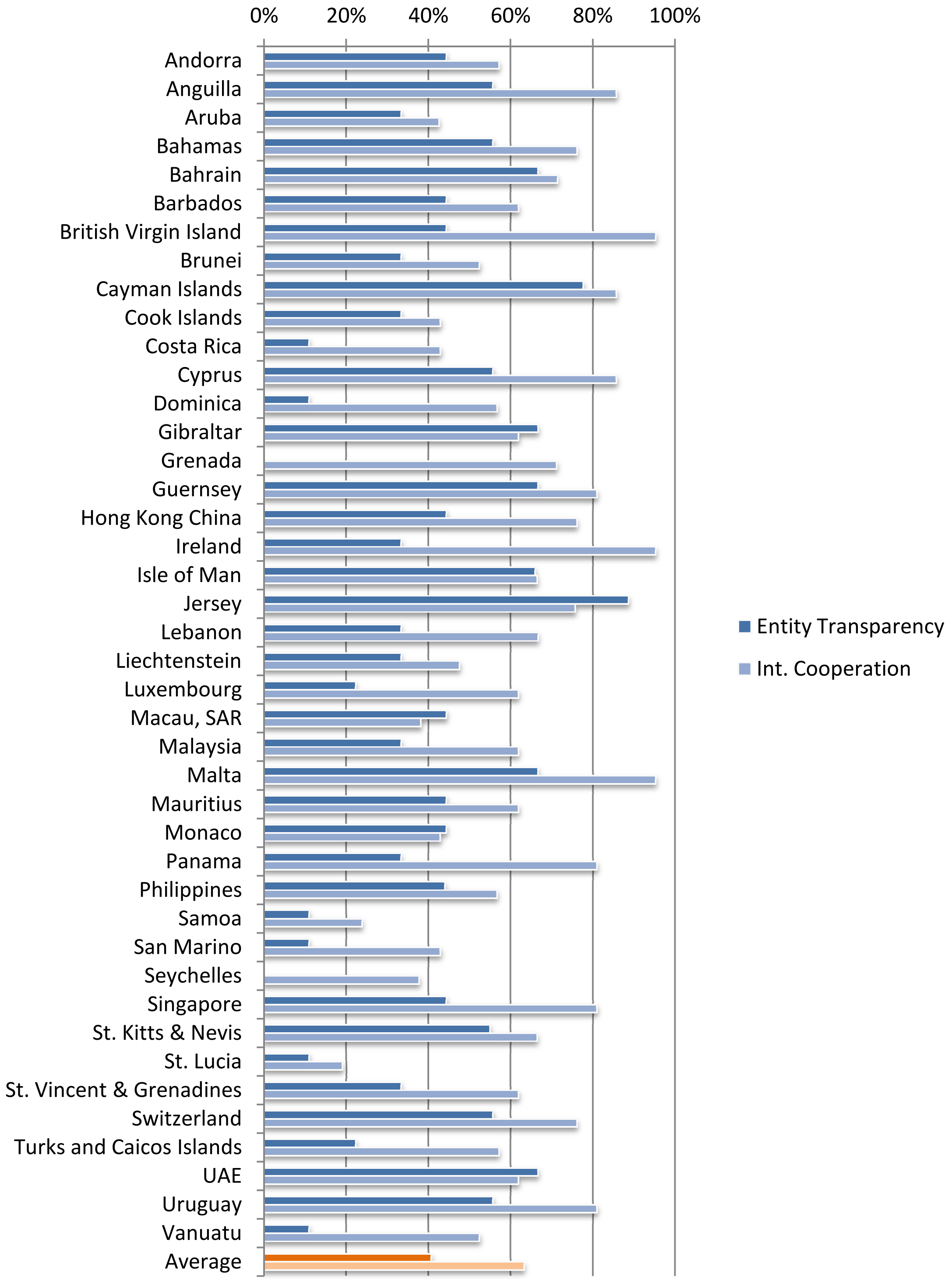
Figure 8: Extent of compliance with recommendations addressing entity transparency and international cooperation – EU countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered.

Figure 9: Extent of compliance with recommendations addressing entity transparency and international cooperation – EU countries



Source: IMF (2011) and own calculations

The displayed percentages have been calculated as follows: First the recommendation-wise ratings "Compliant" (C), "largely compliant" (LC), "partially compliant" (PC) and "non-compliant" (NC) have been replaced by the numbers 1, 0.66, 0.33 and 0. Then, for each country, the numbers for the rating of each recommendation have been summed up, and divided by the total number of recommendations considered.

3.3.1.5 Econometric analysis of countries' compliance

An econometric analysis explaining countries' compliance by a set of macroeconomic, institutional and financial variables produces the following insightful results. First, countries with higher economic development appear to show higher compliance levels. The IMF (2011) sample includes 46 advanced economies with an average compliance level (over all AML/CFT recommendations) of 56.8 percent. The 115 emerging economies, on the contrary, score 37 percent on average. GDP per capita (expressed in Purchasing Power Parity) is a significant explanatory variable with a positive coefficient, as expected. Second, stronger domestic governance (i.e. a better regulatory framework) has a statistically significant positive impact on compliance. Furthermore, countries with lower control over corruption tend to have lower compliance scores. Third, countries with efficient banking sectors (measured by the net interest margins)[42] are estimated to have, on average, significantly higher levels of compliance with the FATF recommendations. Fourth, however, compliance levels do not correlate with a country's involvement in the global drug business. If, as is frequently done, the involvement in the global drug business (measured by, i.e., UINODC's index of contribution to the global drug problem) is interpreted as a proxy for money laundering (ML) and terrorist financing (TF) risk, this means that there are countries with high levels of compliance, but still high risk of ML/TF, and vice versa. This raises the question whether focusing (exclusively) on compliance with the FATF recommendations brings about advancements in thwarting ML/TF risk (IMF, 2011). Indeed, some caveats to the results of the evaluations of compliance apply, which will be discussed in the next subsection.

3.3.1.6 Caveats

To sum up, we must conclude that compliance with the FATFs recommendations on treating money laundering and terrorist financing is low. This conclusion is also drawn by other studies (i.e. Johnson, 2008, see the discussion below). Not surprisingly,

[42] In this context, large net interest margins indicate inefficient banking operations, high risks in lending, and monopoly power of banks. Likewise, lower margins would correspond to more efficient banking sectors (IMF, 2011). A comparable and widely used indicator of financial market efficiency is the "bid and ask spread".

it is lower among offshore financial centres than among EU-countries, but even among the latter set of countries, variation in compliance is high (i.e. a considerable fraction of countries has shows only low levels of compliance).

However, in a discussion of the evaluation results it must also be stated that an evaluation where complex systems like countries' legal and institutional structures are rated in four different categories is not likely to be capable of processing all relevant information, nor is it likely to be fully objective. On the contrary, international bodies like the FATF and its regional counterparts might have an incentive to produce evaluation results at the "lower margin" of the possible spectrum rather than the higher, such that more efforts are taken in order to improve compliance and thus advance in the fight against money laundering and terrorist financing.

It is thus also fair to note that the standards requested by the FATF and its regional bodies are high[43] and their establishment requires considerable amounts of financial as well as human resources and might in our opinion, depending on the laws in place before implementation, also considerably restrict privacy rights. With the advantage of higher probabilities to detect money laundering and terrorist financing comes the disadvantage that surveillance of the population, including the recording of financial data increases, and determination of an appropriate and bearable extent of surveillance is to be made in a political process. Thus, recommending, against the background of the just discussed evaluation results, to "increase compliance" with the measures suggested by the FATF is, although obvious, a too simple conclusion. Rather, the costs and benefits of implementing the FATF-recommendations must be taken into account.

3.3.2 Assessment by another study (Johnson, 2008)

While the study by IMF (2011) on the mutual evaluations of compliance with the FATF's recommendations and special recommendations is the most encompassing one, Johnson (2008) uses a similar approach to provide interesting results.

The author uses the mutual evaluations of 16 FATF and 21 non-FATF member countries (the number of countries where evaluations were available at the time of re-

---

[43] According to Wang (2011), the FATF requirements are denoted the „gold standard" in AML/CFT policies.

search) to find that “AML/CFT systems of FATF members and non-FATF countries are poor”. Moreover, she asserts that “the lack of compliance with global AML/CFT standards leaves so many holes in these countries’ regulatory, financial and legal systems that money laundering with or without any relationship to the financing of terrorism, would be relatively easy to achieve”.

In addition, Johnson (2008) carries out non-parametric tests to show that compliance with the FATF’s recommendations is significantly higher among FATF member countries than among non-members, and finds that the variance of compliance levels is higher among non-FATF members than among members.

3.4 The shift from a rule- to a risk based approach in AML/CFT policies

In general, in issuing the 40 recommendations on money laundering and the nine special recommendations on terrorist financing, the FATF applied a so-called rule-based approach, implying that legislators and policymakers are called for adopting detailed rules on what institutions, businesses as well as private persons have to do in specific incidences. For example, one such rule could be that financial institutions have to gather data on their customers and report any suspicious money transfer, even if the suspicion is not well founded. Afterwards, the competent authority will decide how to proceed and whether to further pursue the case. Another frequently applied such rule is that institutions must report every cash transaction exceeding the amount of € 15,000 to the competent authorities (van den Broek, 2011).

This rule-based approach has been criticised as being static, passive (see, i.e. dalla Pellegrina and Masciandaro, 2009, or Ross and Hannan, 2007) and producing a large volume of low-quality reports and thus being inefficient (Takáts, 2007, Ross and Hannan, 2007). Thus, the FATF as well as also the European Union now intend to shift from a rule- to a risk-based approach. The major difference between the two approaches is that the risk-based approach leaves some discretion to the supervised financial and non-financial institutions. They must first assess the probability that customers are involved in money laundering and terrorist financing, and then apply the auditing and detection procedures based on the determined risk. The result is that low-risk transactions are audited less frequently and less intensive than high-risk transactions. To our knowledge, the shift from the rule- to the risk based approach is the most significant amendment of AML/CFT measures of the recent years.

van den Broek (2011) nicely reviews the advantages and disadvantages of both the rule- as well as the risk based approach and asserts that the major advantages of the risk based approach are i) that it is more flexible (see also Muller et al., 2009, Unger and van Waarden, 2009 or dalla Pellegrina and Masciandaro, 2009), ii) that due to leaving more discretion to the financial entities, less reporting of suspicious transaction will be done and the quality of the reports could increase (see also Ross and Hannan, 2007, FATF, 2007), and iii) because financial entities are better in assessing risks than the competent authorities, AML/CFT policies are likely to become more effective.

On another note, van den Broek (2011) shows that in reviewing the three EU directives on AML/CMT policy measures (European Union, 1991, 2004, 2005) a shift from a rule- to a risk-based approach can already be seen. For example, the third directive (European Union, 2005) puts more weight on enforcement rules than the previous two, which can be put down to a shift to the risk based approach since leaving higher discretion to financial entities requires also tighter and better defined enforcement rules. Another example is that the third EU directive allows not only the financial entities, but also the supervising authorities to apply risk-based auditing.

While as said above, the third EU directive dwells more on enforcement of AML/CFT measures than the previous two directives, van den Broek (2011) concludes that still a lot of efforts have to be taken in harmonizing enforcement measures among the EU-countries, since "if only the material norms are harmonised but not the enforcement thereof, there remains a lot to wonder whether this harmonization really takes place. This leaves us with the question: why only do half the job?" (van den Broek, 2011).

4 Can increased tax information exchange help in thwarting money laundering and terrorist financing?

As discussed above, in the past years AML/CFT policies have largely been carried out by using a "twin-track-approach" (Stessens, 2000) consisting of i) preventive measures (i.e. implementing the "know your customer principle" and requiring institutions to report suspicious transactions) and ii) repressive measures (i.e. criminalizing money laundering and imposing severe fines).

In this section, we explore whether the following supplementary strategy in the realm of preventive measures could be successful. Since criminal funds intended to launder money or finance terrorist activities are often routed through offshore financial centres (compare Table 3), increased tax information exchange with such offshore financial centres (IMF, 2000) could supplement AML/CFT policies due to the following reason. Criminal money flows might be difficult to detect because there is a large financial asset trading volume in such offshore financial centres, resulting from the fact that individuals and corporations place money and assets there to avoid or evade taxes[44]. Thus, it could be useful to increase tax information exchange and establish agreements on it, because this should reduce the trading and asset volume in offshore financial centres, and thus cover given to criminal money flows should be reduced. The ultimate question thus is whether and to what extent increased tax information exchange can reduce tax avoidance and tax evasion such that less money is routed through offshore financial centres. We approach this question by surveying both the theoretical as well as empirical results that help to give an answer. Afterwards, we will discuss whether increased tax information exchange can be useful even if many countries do not participate in it.

4.1 Theories on offshore tax evasion

Theoretical models of tax evasion are useful in predicting the response of tax evasion to an increase or decrease in institutional parameters like i) the tax rate, ii) the fines or iii) the probability of detection. While most theoretical work[45] analyzes tax evasion within a country (i.e. within the models the fraction of income to be hidden from the tax administration is determined), it is perfectly applicable to the question we analyze here: Transferring assets to offshore financial centres in order to avoid or evade taxes. In con-

[44] The tax rates in offshore financial centres appearing on the list of top 20 destinations for money laundering (Table 3) are: Cayman Islands (Income tax: 0%, Corporate tax: 0%, VAT: 0%), Bahamas (0%, 0%, 0%), Bermuda (0%, 0%, 0%), Luxembourg (38.95%, 21.84%, 15%), Hong Kong (15%, 15%, 0%), Switzerland (22.4%, 13%, 8%).

[45] see for example Andreoni et al. (1998) for an extensive survey.

text of this question, increasing tax information exchange would simply increase the probability of detection[46] and its impact can thus be analyzed within conventional models.

In the seminal model on tax evasion, Allingham and Sandmo (1972) assume taxpayer i to maximize her expected utility $E(U_i)$, which is essentially a weighted average of the respective utility the taxpayer will incur in two different states. This model assumes utility to be concave, i.e. $U_i'(\cdot) > 0$ and $U_i''(\cdot) < 0$, such that the incremental gain in utility of additional income decreases with initial income. Moreover absolute risk aversion is assumed to decrease in income.

With probability $(1 - \mathrm{p})$ taxpayer i is not detected at evading taxes and thus yields net income[47]

$$\mathrm{Y_i = W_i - tX_i} \tag{1}$$

where $\mathrm{W_i}$ is taxpayer i's gross income which is assumed to be exogenous, $\mathrm{X_i}$ the amount of income she places in the home country (and thus pays taxes for it) and t a constant marginal tax rate. Taxpayer i's utility in this state is thus $\mathrm{U_i(W_i - tX_i)}$.

With probability p, she is audited and punished in case authorities find out that she has evaded taxes by moving parts of her income offshore. Thus, in this state her income is

[46] There is a noteworthy discussion evolving about the effectiveness of tax information exchange agreements (TIEAs). Some authors doubt that they would have large effects on i.e. the probability of detecting tax evasion, because i) information sharing only takes place upon request (i.e. the authority requiring information must have an ex-ante suspicion), ii) typically some bank secrecy laws are unaffected by TIEAs, and iii) authorities in offshore centers frequently do not require gathering information on asset-holders, such that they have no relevant information to share (Hanlon et al., 2011). Others, however, point to the deterrent effect of TIEAs (i.e. they work even without having to execute tax information because assets are withdrawn even before a TIEA takes action) (Barber, 2007).

[47] In this simplified model, we do not have room to distiguish between i) the case where already taxed income is placed in an offshore financial centre in order to avoid capital gains taxes etc. and ii) the case where income is moved offshore before income taxation.

$$Z_i = W_i - tX_i - \pi(W_i - X_i) \tag{2}$$

where $\pi(W_i - X_i)$ is the fine to be issued in case of non-compliance to the domestic tax law[48]. The utility of taxpayer i in this alternative state is $U_i\big(W_i - tX_i - \pi(W_i - X_i)\big)$. Thus the optimal amount of income to be declared in this model is determined by maximizing taxpayer i's expected utility function

$$E(U_i) = (1 - p)U_i(Y_i) + pU_i(Z_i) \tag{3}$$

Utility maximization involves differentiating Equation (3) with respect to the amount of income placed at home, X_i, which yields

$$(1 - p)U'_i(Y_i) \cdot -t + pU'_i(Z_i) \cdot (-t + \pi) = 0 \tag{4}$$

or

$$\frac{U'_i(Y_i)}{U'_i(Z_i)} = \frac{p\cdot(-t+\pi)}{(1-p)\cdot -t} \tag{5}$$

where $U'_i(\cdot)$ is the first derivative of $U_i(\cdot)$. Differentiating Equation 4 (note that implicit differentiation is necessary) with respect to the probability of detection, p, or the punishment rate π shows what the model predicts to happen with the amount of income placed at home, X_i if p or π increase (i.e. tax information agreements with offshore financial centres are signed). Not surprisingly, X_i increases (i.e. tax evasion decreases) with increasing probability of detection or increasing fines. Note that this can intuitively be seen from Equation 5 by considering that an increase in p or π will in-

[48] As can be seen, the fine is proportional to the income which has been placed offshore. Yitzhaki (1974) offers another prominent formulation where the fine is proportional to the amount of evaded taxes. Out of two reasons however, we chose to present the former layout. First, basing the fines on the evaded taxes could yield the somewhat counterintuitive result that taxpayers will choose to declare more income as marginal tax rates rise, and second, the definition we present keeps the model slightly more parsimonious, which will prove advantageous as extensions are introduced.

crease the value of the fraction on the right hand side. Thus, the relation between $U'_i(Y_i)$ and $U'_i(Z_i)$ must also increase, which happens (by the assumption of diminishing marginal utility or risk aversion) if Y_i decreases relative to Z_i, i.e. more income is placed at home instead of offshore and thus taxed.

Thus, it can be shown that with increasing probability of detection and increasing fines (i.e. by signing tax information exchange agreements with offshore financial centres), less income will be concealed (i.e. placed offshore) from the domestic tax authorities.

Introducing moral costs of tax evasion, i.e. that people face some disutility when evading taxes, is an obvious and easily applicable extension of Allingham and Sandmo's (1972) or Yitzhaki's (1974) model implemented by Gordon (1989). His model leaves the comparative static effects unchanged, since moral costs are assumed to be linear and enter the model simply as additional costs of tax evasion, next to the expected fine. If one, however, relaxes the assumption of linearity and assumes those costs to increase in the non-declared income, one receives some peculiar insights. While an increase in the audit and punishment rates will still decrease tax evasion, the effectiveness of the penalty will decrease. To see this, consider an increasing punishment rate. It will decrease tax evasion, but because of this decrease, moral costs will decrease too, which will partially crowd out the effect of punishment (Sandmo, 2005). To put it differently, given these assumptions, higher punishment makes taxpayers see it as less necessary to commit to common moral behaviour. While this might be true and intuitively appealing, disentangling the effects of incentives and morale when observing taxpayers will prove difficult.

More recently, Haigner et al. (2010) have extended the seminal model (Allingham and Sandmo, 1972) by introducing social preferences according to Charness and Rabin (2002) as well as institutional satisfaction. They find that punishment is less effective if institutions are inefficient, because then, the costs of tax evasion are low since taxpayers receive little from state production of public goods in return to their tax payments. Moreover, altruistic taxpayers react stronger to punishment than competitive taxpayers do. However, the comparative static effects with respect to probability of detection and punishment rates already shown by Allingham and Sandmo (1972) remain.

To sum up, we note that it is theoretically easy to show that with increasing tax information exchange with offshore financial centres, less income and financial assets will be placed there and cover for flows involving money laundering and terrorist financing should be reduced.

4.2 Empirical evidence on offshore tax evasion

While there are some theoretical models that can usefully be applied to determine the likely impact of increased tax information exchange with offshore financial centres on tax evasion (i.e. asset placing), empirical evidence is very scarce. This is most likely due to the fact that tax evasion is an illegal activity and considerable efforts are undergone to conceal it. Moreover, the defining conditions of offshore financial centres (i.e. strict bank secrecy laws, lack of information-gathering and record-keeping) make it very difficult to find appropriate data.

4.2.1 Sensitivity of offshore asset volume to the risk of being caught

To our knowledge, the studies fitting best to the question of interest within this study are Hanlon et al. (2011) and Kudrle (2008). Unfortunately, the evidence they produce points in two different directions.

Hanlon et al.'s (2011) study bolsters optimism on the capability of increased tax information exchange in thwarting money laundering and terrorist financing routed through offshore financial centres. These authors use time series data on portfolio investment flows provided by the US Federal reserve board to investigate what they call round-tripping. Applying this method, an onshore citizen sends money to an offshore account registered under the name of some foreign entity, although controlled by the citizen. The money is then invested in US securities. Doing so, the capital gains are exempt of taxes in the US such that it is beneficial to US citizens to pretend to be a foreign investor. Hanlon et al. (2011) employ data on US inbound portfolio investment to see whether it changes if i) US tax rates are altered and ii) tax information exchange agreements (TIEAs) come into effect. Note that US inbound investment might also origin from "true" foreigners, but this "lawful" investment should not be sensitive to changes in US tax rules and agreements. If data thus reveals that US inbound investment is sensitive to changes in the taxes US citizens are exposed to, tax evasion is indicated.

To measure such sensitivities, Hanlon et al. (2011) employ the enactment of bilateral tax information exchange agreements (TIEAs) between US and certain offshore financial centres[49] as well as the announcement of increased OECD efforts to curb tax evasion and run regressions indicating the effects of such incidents. The magnitude of the estimated effects is striking and documented in Table 10 below.

Table 10: Changes in US inbound portfolio investment (PI) from offshore relative to inbound PI from onshore

Incident	Equity	Debt
Tax information agreement signed	-0.072*	-0.309***
Tax information agreement in effect	-0.259***	-0.168**
Increased OECD efforts 1998	-0.096***	-0.161***
Increased OECD efforts 2001	-0.042*	-0.217***

Source: Hanlon et al. (2011)
* significant at 10%, ** significant at 5%, *** significant at 1%

US equity inbound portfolio investment from offshore financial centres is estimated to decrease, relative to inbound portfolio investment from onshore countries, by more than one fourth, while debt inbound portfolio investment from offshore (relative to onshore) is estimated to decrease by 17 percent. Moreover, Hanlon et al. (2011) interestingly run separate regressions treating i) the date where the TIEAs have been signed and announced and ii) the date where they came into effect. As documented in Table 10, inbound portfolio investment is already significantly reduced after signing a TIEA, it does not even have to be in effect. An analysis of increased OECD efforts to curb tax evasion yields similar results.

While these results are strongly supporting the assumption that increasing tax information exchange with offshore financial centres would substantially reduce the asset volume placed there (because of tax evasion) and thus cover given to transactions involving money laundering and terrorist financing, generalizing the results might be restricted to the following reason:

Hanlon et al. (2011) study a specific group of investors; those US citizens who invest in US assets, pretending to be a non-US citizen and therefore exempt of paying

[49] For example, the United States have signed TIEAs with Bermuda in 1998 or the Netherland Antilles in 2007.

taxes. Nothing can be asserted about the behaviour of tax evaders who place their money offshore and invest in foreign assets. Since the two groups of investors (those investing in the US and abroad) differ in some aspects of behaviour, it is difficult to infer from results on investors buying domestic assets to all investors.

Kudrle's (2008) helps to increase understanding of the behaviour of all offshore investors. He investigates the amount of assets placed in "tax havens"[50] and how it changed after the OECD-Publication "Harmful Tax Competition" (1998), which essentially issued an ultimatum to the tax havens to share investor information with other countries (i.e. the US and European Union member countries), and its amendments (OECD, 2001, 2004)[51]. Remarkably, his ARIMA-Regressions detected no effect of the OECD initiatives on the asset volume placed in tax havens, although many tax haven (including the Cayman Islands, which are in terms of asset volume outnumbering other havens by far), were eager to cooperate with other countries in information sharing in order to avoid to be condemned by OECD and other bodies like the European Union. For example, in the OECD Progress Report of 2004, only five tax havens have been listed as not cooperative: Andorra, Liechtenstein, Liberia, Monaco and the Marshall Islands, while all others have agreed to "high standards of transparency and effective exchange of information in both civil and criminal taxation matters" (Kudrle, 2008).

Why is it then that the asset volume (and thus tax evasion by making use of tax havens) did not decline? First, Kudrle (2008) asserts that one specific form of tax evasion, registering a corporate entity in an offshore centre, although entrepreneurial activities are carried out onshore, has not been well addressed by OECD (1998, 2001, 2004) such that tax havens may still host such entities. Admittedly however, it is difficult to determine and investigate if entrepreneurial activities are predominantly undertaken onshore or offshore.

---

[50] According to a definition by the US Government accountability office, a country is considered as a tax haven if it among other things, promotes itself as an "offshore financial centre". Thus the two notions "tax haven" and "offshore financial centre" have much in common.

[51] While according to Kudrle (2008) the tone of the 1998 publication was quite aggressive, the language of the amendments (i.e. OECD Progress Report of 2001) shifted from confrontation to cooperation.

Secondly, however, although tax havens have agreed to gather information on account holders in their territory, this potential "threat to tax evaders" can easily be neutralized by making use of shell companies or foreign trusts. An onshore country's citizen can transfer his money to the shell company registered offshore, which acts as the official owner of the money, while not revealing the identity of the "true" owner. Third, tax havens typically share information on asset holders' identities, if they have, only upon request. Thus onshore authorities must first have a suspicion in order to be able to gather information capable of proving tax evasion.

Kudrle (2008) thus calls for automatic information exchange, based on consistent international identifying numbers. He points to the "EU Saving Directive" which covers (by enforcing depositor identity information exchange) a "sufficient range of financial instruments" to thwart tax evasion (within the EU).

To sum up the discussion of the impact of tax information exchange agreements (TIEAs) with offshore financial centres on tax evasion by placing assets offshore (and thus providing cover for criminal money flows), we must assert that the empirical evidence is mixed. While some studies (i.e. Manlon et al.) point to the deterrent effect of TIEAs and indicate that they reduce tax evasion, others (Kudrle, 2008) conclude that in the existing form, TIEAs do not produce any effects because they are easy to circumvent. According to the latter study, more stringent depositor identity information exchange (i.e. automatic information sharing) would be necessary to effectively curb tax evasion.

4.2.2 Sensitivity of offshore asset volume to transaction costs

Another useful approach to determine the effect of increased tax information exchange with offshore financial centres on the asset volume placed there (which provides cover to criminal funds) is to investigate the impact of transaction costs (i.e. transaction taxes, agency costs, commission) on the trading volume. Economically, increased tax information exchange by signing TIEAs with offshore financial centres can simply be interpreted as increased costs of placing assets offshore, since TIEAs increase the likelihood of being punished for tax evasion and thus increase its expected costs. We will deal this issue rather shortly and present some estimated elasticities of the trading volume with respect to trading costs in Table 11 below.

Table 11: Estimated elasticities of the trading volume with respect to transaction costs

Source	Country	Market	Elasticity	Measure
Schmidt (2007)	Multinational	Foreign Exchange	-0.4	BAS
Baltagi et al. (2006)	China	Stock Market	-1	TTC
	China	Stock Market	-0.5	STT
Chou and Wang (2006)	Taiwan	Futures Market	-1	STT
	Taiwan	Futures Market	-0.6 to -0.8	BAS
Wang and Yau (2000)	United States	S&P 500 Index Futures	-0.8 (-1.23)*	BAS
	United States	DM Futures	-1.3 (2.1)	BAS
	United States	Silver Futures	-0.9 (1.6)	BAS
	United States	Gold Futures	-1.3 (1.9)	BAS
Hu (1998)	Multinational	Stock Market	0	STT
Wang et al. (1997)	United States	S&P 500 Index Futures	-2	BAS
	United States	T-bond Futures	-1.2	BAS
	United States	DM Futures	-2.7	BAS
	United States	Wheat Futures	-0.1	BAS
	United States	Soybean Futures	-0.2	BAS
	United States	Copper Futures	-2.3	BAS
	United States	Gold Futures	-2.6	BAS
Lindgren and Westlund (1990)	Sweden	Stock Market	-0.9 to -1.4	TTC
Jackson and O'Donnell (1985)	United Kingdom	Stock Market	-0.5 (-1.7)*	TTC

Source: Matheson (2011)
TTC: Total Transaction Costs
SST: Security Transaction Taxes
BAS: Bid and Ask spread

As can be seen, the studies named in Table 11 measure the impact of transaction costs on the trading volume either by investigating i) variations in the total transaction costs reported, ii) the introduction or change of security transaction taxes or iii) shifts in the bid and ask spread. Note that the bid and ask spreads can be perfectly interpreted as transaction costs since they account for the flow of money kept by the trading institutions. As expected, the measured elasticities are negative, indicating that increased transaction costs reduce the trading volume. Applied to the AML/CFT issue, raising the transaction costs of placing assets offshore (i.e. by increasing the probability of being punished for tax evasion) could be useful because the high trading volume offshore provides cover to financial flows involving money laundering and terrorist financing.

4.3 The weakest-link problem

An important caveat against the (at least partly) promising findings discussed above, however, must be stated since it is not clear whether higher transaction costs reduce the trading volume i) at all (i.e. in total, less trading is carried out) or ii) simply shift the trading to other locations with still lower costs. If the latter was the case, then AML/CFT policies could only be bolstered by increasing transaction costs in virtually all offshore financial centres and tax havens. If not all of these havens participated, trading would simply be shifted to non-participant havens and cover to criminal money flows would be provided there.

This is the so-called "weakest link problem", to be discussed in this section. It refers to the fact that in such a situation, the "global" efforts against money laundering and terrorist financing can only be as strong as its weakest link (i.e. institutions so weak as to provide cover to criminal money flows). The problem arises because of a trade-off faced by offshore as well as onshore countries between (monetary) gains from having assets placed within the country and potential (monetary as well as societal) gains from preventing terrorism and/or tax evasion. As a matter of fact, imposing restrictions such that, amongst others, tax evaders, criminals and terrorists will incur higher costs and a higher probability of detection will reduce gains from having assets placed, while it will increase the gains from having prevented crime.

Thus, it is the relation between losses and potential gains that drives the decisions whether to cooperate or not in preventing money laundering and terrorist financing (i.e. by engaging in tax information exchange).

At best, the situation is as modelled by Sandler (2005) and depicted in Figure 10. Here, the decision is modelled as a two country stag-hunt game between a (big) onshore and a (small) offshore country. The strategies of both countries can be to comply with AML/CFT measures or not. The payoffs are as follows. If both countries comply with AML/CFT measures (i.e. agreeing to exchange tax information to prevent tax evasion, money laundering and terrorist financing), both receive payoff A, the highest possible payoff arising because of the prevention of crime. If however, both countries do not comply with AML/CFT measures, they will receive the second highest payoff B (arising from the fact that high financial gains are incurred, but crime is not prevented. If however, one country complies, while the other doesn't, then the complying country will have the lowest possible payoff C (no financial gains, no crime prevented), while the non-compliant country will have payoff B (financial gains, no crime prevented). The relation between the different payoffs is thus A > B > C.

This game obviously has no dominant strategies (i.e. strategies that maximize own payoffs whatever the other country does), but two pure strategy Nash-Equilibria (both comply and both do not comply). Thus, in this situation, a coordination problem arises, in which each country must estimate the probability that the other country will comply and act accordingly. The outcome is a mixed strategy Nash-Equilibrium which by its nature does not guarantee compliance and thus the prevention of money laundering and terrorist financing (by reducing tax evasion). At least, however, both countries have incentives to coordinate at joint compliance.

Figure 10: Joint payoff relations from complying or not complying with AML/CFT strategies – stag hunt game

		Offshore	
		comply with AML/CFT	not comply with AML/CFT
Onshore	comply with AML/CFT	A, A	C, B
	not comply with AML/CFT	B, C	B, B

Source: Sandler (2005)

Unfortunately, it is not likely that the situation in the decision problem involving the prevention of money laundering and terrorist financing between offshore and onshore countries is as depicted by Figure 10 above. Rather, in our opinion, we must assume that offshore financial centres are not threatened by money laundering and terrorist financing such that they do not profit from preventing it. This alters the payoff structure in the following way. Onshore yields the highest possible payoffs if both countries comply with AML/CFT measures (crime and tax evasion prevented), however, in case of compliance, Offshore yields only the second highest payoff since it could do better with non-compliance (i.e. luring assets from onshore) at no further cost (crime is no threat). If Onshore, however, complies, but Offshore doesn't, then the former will yield lowest possible payoffs (crime is not prevented, gains from asset placing are gone).

If Onshore does not comply, the best strategy for Offshore is again non-compliance, since in case of compliance not as many assets can be lured. The situation is depicted in Figure 11, with a payoff relation of A > B > C > D. As can be seen, non-compliance is a dominant strategy for Offshore, while for Onshore, compliance is favourable only if Offshore complies (which it won't do).

Figure 11: Joint payoff relations from complying or not complying with AML/CFT strategies in case money laundering and terrorism is no threat for offshore countries

		Offshore	
		comply with AML/CFT	not comply with AML/CFT
Onshore	comply with AML/CFT	A, B	D, A
	not comply with AML/CFT	C, C	C, B

The bad news is that if no enforcement mechanisms bringing about compliance of the offshore country are found, the likely outcome in such a situation is non-compliance by both Offshore as well as Onshore[52]. Since we believe that the assumptions we have made in constructing this decision problem are appropriate, we are left with the conclusion that a so-called "weakest link problem" in the fight against money laundering and terrorist financing is likely to occur. Offshore jurisdictions simply have only little incentive to comply with international tax-, money laundering- and terrorist financing standards as issued by OECD or FATF.

5 Summary and conclusions

In this survey study we have i) investigated the extent of worldwide money laundering and terrorist financing in terms of (transnational) financial flows ii) discussed the sources of criminal and terrorist funds and the methods which are applied to launder them, iii) provided a lengthy description of the international approach against money

[52] Note that we have assumed that in case of non-compliance of Offshore, Onshore does not benefit from compliance because crime cannot be prevented at all. If this assumption is relaxed, the outcome of the game could be compliance (Onshore) and non-compliance (Offshore).

laundering and terrorist financing, including the organizations and standards involved in it, iv) investigated the extent of compliance among countries and (financial as well as non-financial businesses) with those standards, and v) both theoretically as well as empirically explored whether intensifying tax information exchange between onshore and offshore countries could, by reducing offshore tax evasion, help thwarting money laundering and terrorist financing (by reducing cover provided to criminal transactions due to less wealth placed and less trading volume in offshore financial centres).

The analysis shows that worldwide financial flows involving money laundering account for about USD 1.5 – 3 trillion, based on different estimates (Unger, 2007) which is about 3 – 6 percent of world GDP or about 0.1 – 0.2 percent of worldwide currency trading at foreign exchange markets. Financial flows to be attributed to terrorism are much lower, with, for example, al-Qaeda financial flows of about USD 20 – 50 mn. per year (Schneider and Caruso, 2011). Among the top 20 destinations of money laundering fund flows are some offshore financial centres (according to IMF, 2000) like the Cayman Islands (accounting for an estimated 4.9 percent of worldwide flows), Luxembourg (2.8 percent), the Bahamas (2.3 percent) or Switzerland (2.1 percent) as well as major “onshore countries” like the USA (account for the highest share with 18.9 percent), Russia (4.2 percent) Italy (3.7 percent) or China (3.3 percent).

Moreover, the analysis shows that compliance with international standards against money laundering, which are set forth predominantly by the Financial Action Task Force (FATF) and its 40 recommendations on the treatment of money laundering and nine special recommendations on the treatment of terrorist financing, is low (compare also IMF, 2011, Johnson, 2008). For example, average compliance with recommendations addressed at financial institutions, which are basically calling for implementation of the “know your customer principle” and the reporting of suspicious transactions, is 55 percent among EU countries and 47 percent among offshore financial centres. However, in the evaluations of compliance, complex legal and institutional systems are rated in a four-category ordinal scale; a procedure unlikely to being able to capture all information and being fully objective. The evaluating organization might also face the incentive to rate compliance low rather than high, in order to stimulate efforts in thwarting money laundering and terrorist financing. Such efforts must therefore be carefully evaluated against costs and benefits, since increasing compliance can bring about significant costs, both in term of required (human and financial) resources as well as in terms of i.e. reduced privacy rights of citizens.

Finally, our exploratory analysis of the likely impact of intensified measures against offshore tax evasion on trading volume in those centres shows mixed evidence. While it is theoretically easy to show that, for example, intensified tax information exchange, will reduce offshore trading volume and thus cover provided to criminal money flows, empirical evidence on the recent OECD initiatives against tax evasion (OECD, 1998, 2001, 2004) finds no or very little effect on the total volume of assets placed offshore (Kudrle, 2008, Hanlon et al., 2011). This is remarkable since many offshore centres have been keen on signing tax information exchange agreements with onshore bodies like the US or the European Union in order to avoid to be condemned by the OECD. Most likely, however, those information exchange agreements to not produce enough threat to potential tax evaders, since they can i) easily be circumvented by making use of shell companies and ii) provide information on personal and corporate identifies not automatically, but only upon request.

Based on those findings, we draw the following conclusions and suggest the following measures to bolster the international fight against money laundering and terrorist financing.

First, the shift from the traditional rule-based to the risk based approach (leaving the institutions subject to anti-money laundering and combating the financing of terrorism (AML/CFT) more discretion) should be further pursued since it tends to be more efficient (compare van den Broek, 2011).

Second, in doing so, policy makers should clearly define the main information and data requirements authorities need to effectively thwart money laundering and terrorist financing. Then, they need to advice financial and non-financial businesses on how to detect these data and how to determine suspicious transactions. The complexity of terrorist financing requires cooperation of law enforcement and the private sector.

Third, more and better information exchange is key to making AML/CFT strategies more efficient and mandatory for their success. Still, legal barriers remain when information is to be exchanged across jurisdictions, but gathering information in one country is prohibited by data privacy and bank secrecy laws still in place. This is one of the reasons why compliance with the FATF's standards is so low, and poses many restrictions on which institutions can disclose data in their possession (compare e.g. SWIFT "case").

Fourth, since next to the official financial sector, alternative remittance systems (i.e. Hawala) are widely used to transmit criminal and terrorist funds, those systems should be put under regulation and surveillance too. However, care is to be taken since imposing too strict rules would drive those systems further underground, while reducing the volume of transactions is not feasible since so many people (i.e. migrants) do not have access to official banks and must therefore rely on it. Thus, gradually integrating the alternative remittance systems into the "official economy", including training of operators, should be preferred over allowing only licensed operators to engage in this business (compare Wang, 2008).

Fifth, in order to invoke, with respect to money laundering and terrorist financing, a positive side-effect of strategies to curb offshore tax evasion, the respective tax information agreements signed in the recent years must be meliorated. In particular, switching from upon-request to automatic information exchange would considerably increase the probability detection. Moreover, destroying the possibilities to circumvent information exchange by making use of shell companies hiding the identity of potential tax evaders will be necessary. Finally, such a strategy will lead to success only if virtually all offshore financial centres participate. Otherwise, criminal and terrorist funds are likely to find enough cover by routing transactions through non-participant jurisdictions. Enforcing compliance, although the incentives for offshore countries are weak, is possible, i.e. by imposing withholding taxes on capital gains flowing to non-cooperative jurisdictions.

6 References

Allingham, M., Sandmo, A. (1972) "Income tax evasion: A theoretical analysis", *Journal of Public Economics* 1, 323-338.

Abuza Z. (2008) "The Social Organization of terror in Southeast Asia: the Case of Jemaah Islamiyah", in *Biersteker and Eckert, (2008) (eds.) "Countering the financing of terrorism"*.

Agarwal, J., Agarwal, A. (2004) "Globalization and International Capital Flows", *Finance India*, 19(1), 65-99.

Agarwal, J., Agarwal, A. (2006) "Money Laundering: New Forms of Crime, and Victimization", Paper presented at the *National Workshop on New Forms of Crime, Victimization, Department of Criminology, University of Madras, India*.

Andreoni, J., Erard, B. and Feinstein, J. (1998) "Tax compliance", *Journal of Economic Literature* XXXVI, 818-860.

Bagella, M., Busato, F., Argentiero, A. (2009) "Money Laundering in a Microfounded Dynamic Model: Simulations for the U.S. and the EU-15 Economies", *Review of Law and Economics*, 5(2), 879-902.

Baker, R. (2005) "Capitalism´s Achilles Heel – Dirty Money and How to Renew the Free-Market System", *John Wiley and Sons*, Hobokken (NY).

Baltagi, B, Li, D., Li, Q. (2006) "Transaction Tax and Stock Market Behaviour: Evidence from an Emerging Market" *Empirical Economics* 31, 393–408.

Barber, H. (2007) "Tax havens today: The benefits and pitfalls of banking and investing offshore", *John Wiley and Sons*, New Jersey.

Basile, M. (2004) "Going to the Source: Why Al Qaeda's Financial Network Is Likely to Withstand the Current War on Terrorist Financing", *Studies in Conflict & Terrorism* 27, 169–185.

Bell, R. (2003) "The confiscation, forfeiture and Disruption of Terrorist finances", *Journal of Money Laundering Control* 7(2), 105-126.

Biersteker, T. (2002) "Targeting Terrorist Finances: The New Challenges of Financial Market Globalisation", in *"Worlds in collision. Terror and the Future of Global Order", Palgrave and Macmillan*, 74-85.

Biersteker, T., Eckert, S. (2008) "The politics of numbers in the financial "war" on terrorism", Paper prepared for the *International Studies Association Meeting, San Francisco*.

Bunt, H. (2007) "The Relation between Organized Crime and Informal Markets: The Role of Hawala Bankers in the Transfer of Proceeds from Organized Crime", *CRIMPREV Discussion Paper*, Gant University, Belgium.

Charness, G., Rabin, M. (2002) "Understanding social preferences with simple tests", *Quarterly Journal of Economics* 117, 817-869.

Chou, R., Wang, G. (2006) “Transaction Tax and Market Quality of the Taiwan Stock Index Futures”, *Journal of Futures Markets* 26(12), 1195–1216.

Clunan, A. (2006) “The fight against terrorist financing”, *Political Science Quarterly* 121(4).

Comras, V. (2007) “Al Qaeda Finances and Funding to Affiliated Groups”, *Terrorism Financing and State Responses*, Stanford, 115-133.

Cornell S. (2005) “Narcotics, Radicalism and Armed Conflict in Central Asia: The Islamic Movement of Uzbekistan”, *Terrorism and Political Violence* 17(4), 619-639.

Cornell, S. (2006) “The Narcotics Threat in Greater Central Asia: from Crime-Terror Nexus to state infiltration”, *China and Eurasia Forum Quarterly* 4(1), 37-67.

Costa, A. M. (2005) “Drugs, Crime and Terrorism Financing: Breaking the links”, *Conference on Combating Terrorist Financing*, Vienna, UNODC, 1-7.

Croissant A., Barlow D. (2007) “Following the Money Trail: Terrorist Financing, and Government Responses in Southeast Asia”, *Studies in Conflict & Terrorism* 30, 131–156.

dalla Pellegrina, L., Masciandaro, D. (2009) “The risk-based approach in the new European anti-money laundering legislation: a law and economics view”, *Review of Law and Economics* 5(2), 931-952.

Ehrenfeld, R. (2007) “Funding Evil: How Terrorism is Financed and the Nexus of Terrorist Organizations”, in Costigan S., Gold D. (2007) (eds.) *“Terrornomics”*, Ashgate Publishing.

El Quorchi, M., Maimbo, S., Wilson, J. (2003) “Informal Funds Transfer Systems: An Analysis of the Informal Hawala System”, *International Monetary Fund*, Washington, DC, 1-53.

Enders, W., Sandler, T. (2002) “Patterns of Transnational Terrorism, 1970-1999: Alternative Time-Series Estimates”, *International Studies Quarterly*, 46(2), 145-165.

Ertl, B. (2004) “Der Kampf gegen Geldwäscherei und Terrorismusfinanzierung”, *Working Paper 4/2004*, Bundesministerium für Finanzen, Vienna.

European Union (1991) “Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering”, OJ L 166, June, page 77.

European Union (2004) “Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering”, OJ L 344, December, page 76.

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”, OJ L 309, November, page 15.

FATF (2006) “Trade Based Money Laundering: Typologies Report”, Financial Action Task Force, Paris, www.fatf-gafi.org

FATF(2007) “Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures”, Financial Action Task Force, Paris, www.fatf-gafi.org

FATF (2008) “Terrorist financing”. Financial Action Task Force, Paris, www.fatf-gafi.org

FATF (2012) “FATF Members and Observers”. Financial Action Task Force, Paris, www.fatf-gafi.org

FATF/OECD (2010a) “FATF 40 recommendations, October 2003, incorporating all subsequent amendments until October 2004”, Financial Action Task Force, Paris, www.fatf-gafi.org

FATF/OECD (2010b) “FATF IX Special recommendations on terrorist financing, October 2001, incorporating all subsequent amendments until February 2008”, Financial Action Task Force, Paris, www.fatf-gafi.org

Fischer, H. (2002) “Hawala – What is it and How to Emasculate it”, *Study*, California, Beverly Hills.

Fletcher, N. Baldwin, J. (2002) “Money Laundry Counter Measures with Primary Focus upon Terrorism and the U.S. Patriot Act 2001”, *Journal of Money Laundering Control*, 6(2), 105-136.

Fried, E., C., Schultze, C. (1975) “Higher Oil Prices and the World Economy: The Adjustment Problem”, Brookings Institution, Washington D.C., 197-226.

Gardner, K. (2007) “Fighting terrorism the FATF way”, Global Governance 13, 325-345.

Gilmore, W. (2004) “Dirty money: the Evolution of International Measures to Counter Money Laundering and the Financing of Terrorism”, *Council of Europe Pub.*, Strasbourg

Giraldo, J., Trinkunas, H. (2007) “Terrorism financing and state responses: A comparative perspective”, Stanford University Press 1(20), 282-296.

Gordon, J. (1989) “Individual morality and reputation costs as deterrence to tax evasion”, European Economic Review 33, 797-805.

Guardinan, The (2006) “Judge strikes down Bush on terror groups”, www.guardian.co.uk

Gunaratna, R. (2003) “Inside Al Qaeda: Global Network of Terror”, Hurst & Company, London.

Haigner, S., Jenewein, S., Schneider, F., Wakolbinger, F. (2010) “Institutional satisfaction and social preferences as determinants of the shadow economy”, *GAW Research Project*.

Hanlon, M., Maydew, E., Thornock, J. (2011) “Taking the long way home: Offshore investments in US equity and debt markets and US tax evasion”, *SSRN working paper* 1915429.

Hardouin P., Weichhardt, R. (2006) “Terrorist fund raising through criminal activities”, *Journal of Money Laundering Control*, 9(3), 303-308.

Heng, Y., McDonagh, K. (2008) “The other war on terror revealed: Global governmentality and the Financial Action Task Force’s campaign against terrorist financing”, *Review of International Studies* 34, 553-573.

Hu, S. (1998) “The Effects of the Stock Transaction Tax on the Stock Market—Experience from Asian Markets”, *Pacific Basin Finance Journal* 6, 347–64.

Hübschle A. (2007) “Terrorist Financing in Southern Africa: Are we making a mountain out of a molehill”, *ISS paper* 132.

ICG (2002) "Somalia: Countering terrorism in a failed state", International Crisis Group, Nairobi and Brussels.

IDB (2004) "Unlocking Credit: The Quest for deep and stable bank landing", Economic and Social Progress Report, Washington D. C: *Inter-American Development Bank and Jones Hopkins*, Hopkins University Press.

IMF (2000) "Offshore financial centres", IMF Background Paper, prepared by the Monetary and Exchange Affairs Department, International Monetary Fund, www.imf.org

IMF (2002) "Money Laundering: New Facts", International Monetary Fund, www.imf.org

IMF (2007) "Financial System Abuse, Financial Crime and Money Laundering", Monetary and Exchange Affairs and Policy Development, International Monetary Fund, www.imf.org

IMF (2011) "Anti-money laundering and combating the financing of terrorism (AML/CFT) – Report on the review of the effectiveness of the program", Prepared by the Legal Department (in consultation with other departments), International Monetary Fund, www.imf.org

IMF (2012) "World Economic and Financial Surveys - World Economic Outlook Database", WEO Data, September 2011 Edition, International Monetary Fund, www.imf.org

Jackson, P., O'Donnell, A. (1985) "The effects of stamp duty on equity transactions and prices in the UK Stock Exchange", Bank of England, London (UK).

Jayasuriya, D. (2009) "Anti-money laundering efforts, stock market operations and good governance", *Qualitative Research in Financial Markets* 1(1), 46-58.

Jessee D. (2006) "Tactical Means, Strategic Ends: Al Qaeda's Use of denial and Deception", *Terrorism and Political Violence* 18, 367-388.

Johnson, J. (2001) "In Pursuit of Dirty Money: Identifying Weaknesses in the Global Financial System", *Journal of Money Laundering Control*, 5(2), 122-133.

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

Jorisch, A. (2004) “Beacon of Hatred: Inside Hezbollah’s Al-Manar Television”, The Washington Institute for Near East Policy, Washington DC.

Kern, A. (2002) “Extraterritorial US banking regulation and international terrorism: The patriot act and the international response”, *Journal of International Banking Regulation* 3(4), 306-326.

Kiser, S. (2005) “Financing Terror: An analysis and simulation for affecting Al Qaeda’s financial infrastructure”, *Pardee RAND Graduate School (PRGS) Dissertation Series*.

Koh, J.-M. (2006) “Suppressing terrorist financing and money laundering, *Springer*, Berlin.

Kohlmann, E. (2006) “The role of Islamic charities in international terrorist recruitment and financing”, *DIIS Working Paper No. 2006/7*, Danish Institute for International Studies, Copenhagen, www.diis.dk

Krueger, A. (2008) “What makes a home-grown terrorist: Human Capital and participation in domestic Islamic terrorist groups in the U.S.A.”, *Economic Letters* 101/3, 293-296.

Kudrle, R. (2008) “The OECD’s Harmful tax competition initiative and the tax havens: From bombshell to damp squib, Global Economy Journal 8(1), Berkeley Electronic Press.

Levi, M., Gilmore, W. (2002) “Terrorist Finance, Money Laundering and the Rise and Rise of Mutual Evaluation: A New Paradigm for Crime Control”, in: *Financing Terrorism*, Netherlands, Kluwer Academic Publishers, 87-115.

Levitt, M. (2002) “The Political economy of Middle East Terrorism”, *Middle East Review of International Affairs*, 6(4), 48-65.

Lindgren, R., Westlund, A. (1990) “How did the transaction costs on the Stockholm Stock Exchange influence trading volume and price volatility?”, *Skandinaviska Enskilda Banken Quarterly Review* 2/1990, 30-35.

Looney R. (2007) “The Mirage of Terrorist Financing: The Case of Islamic Charities”, *Strategic Insights*, 5(3).

Makarenko, T. (2003a) “Tracing the dynamics of the illicit arms trade”, *Jane’s Intelligence Review*.

Makarenko, T. (2003b) “A model of terrorist-criminal relations”, *Janes´s Intelligence Review*.

Matheson, T. (2011) “Taxing financial transactions: Issues and evidence”, *IMF Working Paper* 11/54.

Masciandaro, D. (2004) “Global Financial Crime: Terrorism, Money Laundering and Off Shore Centres”, Aldershot (England), Burlington, Ashgate.

Masciandaro, D. (2005) “Financial Supervisory Unification and Financial Intelligence Units”, *Journal of Money Laundering Control*, 8(4), 354-371.

Masciandaro, D. (2006) “Offshore Financial Centres and International Soft Laws: Explaining the Regulation Gap”, *Second Annual Conference*, Società Italiana di Diritto ed Economia, Roma, 1-49.

Millard, G. (2006) “Business of Crime: the Enterprise of Crime and Terror – the Implications for Good Business”, *Journal of Financial Crime*, 13(3), 277-282.

Mintz, J. (1998) “Bin Laden’s Finances are Moving Target”, *The Washington Post*, 28 August, A01.

Morigi, A. (2004) “Multinazionali del terrore”, Alessandria, Piemme, Italy.

Muller, W., Kalin, C., Goldsworth, J. (2007) “Anti-money Laundering”, *International Law and Practice*, Wiley, New York.

Nagtzaam, G., Lentini, P. (2008) “Vigilantes on the High Seas? The Sea Shepherds and Political Violence”, *Terrorism and Political Violence* 20(1), 110-33.

Napoleoni, L. (2005) “Terror Incorporated: Tracing the Dollars behind the Terror Networks”, *Seven Stories Press*, New York.

OECD (1998) “Harmful tax competition: An emerging global issue”, OECD, Paris.

OECD (2001) “Project on Harmful Tax Practices: The 2001 Progress Report”, Centre for Tax Policy and Administration, OECD, Paris.

OECD (2004) “Project on Harmful Tax Practices: The 2004 Progress Report”, Centre for Tax Policy and Administration, OECD, Paris.

Omer, A. (2002) “A report on Supporting Systems and Procedures for the effective regulation and monitoring of Somali remittance companies (Hawala)”, UNDP.

Omer, A., El Koury, G. (2004) “Regulation and supervision in a vacuum: The story of the Somali remittance sector”, *Small Enterprise Development* 15(1), 44-52.

Page J., Plaza S. (2006) “Migration Remittances and Development: A review of Global evidence”, *Journal of African Economies* 15(2), 245-336.

Paoli L., Rabkov I., Greenfield V., Reuter P. (2007) “Tajikistan: The Rise of a Narco-State”, *Journal of Drug Issues*.

Passas, N. (2004) “Law Enforcement Challenges in Hawala-related Investigations”, *Journal of Financial Crime* 12(2).

Perkel, W. (2004) “Money Laundering and Terrorism: Informal Value Transfer Systems”, *American Criminal Law Review* 41(2), 183-211.

Peters, G. (2009) “How Opium Profits the Taliban”, Peaceworks n.626, United States Institute of Peace.

Picarelli, J. (2006) “The Turbulent Nexus of Transnational Organised Crime and Terrorism: A Theory of Malevolent International Relations”, *Global Crime,* 7(1), 1-24.

Pieth, M. (2002) “Financing terrorism” Kluwer Academic Publishers, Dordrecht, Boston.

Raphaeli, N. (2003) “Financing of Terrorism: Sources, Methods and Channels”, *Journal of Terrorism and Political Violence* 15(4), 59-82.

Razavy, M. (2005) “Hawala: An Underground Haven for Terrorist of Social Phenomenon?”, *Crime, Law and Social Change* 44(2), 277-299.

Richard, A. (2005) “Fighting Terrorist Financing: Transatlantic Cooperation and International Institutions”, Centre for Transatlantic Relations, Johns Hopkins University.

Rider, B. (2004) “The War on Terror and Crime and the Offshore Centres”, in: Global Financial Crime: Terrorism, Money Laundering and Offshore Centres, Aldershot, 61-95.

Ross, S., Hannan, M. (2007) “Money laundering regulation and risk-based decision making”, *Journal of Money Laundering Control* 10(1), 106-15.

Sanchez-Cuenca, I., de la Calle, L. (2009) “Domestic Terrorism: The hidden side of political violence”, *Annual Review of Political Science* 12, 31-49.

Sanderson, T. (2004) “Transnational Terror and Organized Crime: Blurring the Lines”, *Sais Review* XXIV(1), 49-61.

Sandler, T. (2005) “Collective versus unilateral responses to terrorism”, *Public Choice* 124, 75-93.

Sandmo, A. (2005) “The theory of tax evasion: A retrospective view”, *National Tax Journal* 58, 643-663.

Schmidt, R., 2007, “The Currency Transaction Tax: Rate and Revenue Estimates” North-South Institute, Ottawa.

Schneider, F. (2004) “The financial flows of Islamic Terrorism”, in: Masciandaro, D. (ed.) *“Global Financial Crime: Terrorism, Money Laundering and Offshore Centres”*, Ashgate, 97-126.

Schneider, F. (2005) “Shadow Economies Around the World: What do we Really Know?”, *European Journal of Political Economy* 21(3), 598-642.

Schneider, F. (2008a) “Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings”, *Discussion Paper*, Department of Economics, University of Linz.

Schneider, F. (2008b) “Money Laundering from Revenues from Organized Crime: Some Preliminary Empirical Findings”, Revised version of a paper which was presented at the Conference *„Illicit Trade and Globalization“*, CES-ifo Venice Summer Workshop, Venice National University, San Servolo, July 14-15.

Schneider, F. (2009) “Die Finanzströme von Organisierter Kriminalität und Terrorismus: Was wissen wir (nicht)?”, *Vierteljahreshefte zur Wirtschaftsforschung*, DIW Berlin, 78(4), 73-87.

Schneider, F. (2011) “The financial flows of the transnational crime: Some preliminary empirical results”, *Economics of Security Working Paper* 53.

Schneider, F., Brück, T., Meierrieks, D. (2010) “The economics of terrorism and counter-terrorism: A survey”, *CESifo Working Paper Series* No. 3012.

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.

Schneider, F., Dreer, E., Riegler, W. (2006) “Geldwäsche: Formen, Akteure, Größenordnung – Warum die Politik machtlos ist”, *Gabler-Verlag*, Wiesbaden.

Schneider, F., Enste, D. (2000) “Shadow Economy: Causes, Size and Consequences”, *Journal of Economic Literature* XXXVIII(1), 77-114.

Schneider, F., Windischbauer, U. (2008) “Money Laundering: Some Facts”, European *Journal of Law and Economics*, 26(4), 387-404.

Shahar, Y. (2001) “Tracing Bin Laden’s money: Easier said than done”, www.ict.org

Shelley, L. (2005) “The Nexus between Terrorism and Organized Crime”, in: Confronting Terrorism Financing, Lanham, MD (etc.), *University Press of America*, 29-33.

Simpson, G. (2007a) “U.S. Tracks Saudi Bank Favoured by Extremists”, *The Wall Street Journal*, 26 July, New York, A10.

Simpson, G. (2007b): “U.S. Investigating Firm Tied to Muslim Investors”, *The Wall Street Journal*, January 31, 1-2.

Smillie, I., Gberie, L., Hazleton, R. (2000) “The Heart of the Matter: Sierra Leone, Diamonds and Human Security”, Ontario, Canada.

Takats, I. (2007) “A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement”, Paper presented at the Conference *"Tackling Money Laundering"*, University of Utrecht, Utrecht, November 2-3.

Taylor, J. (2007) “Global financial warriors: The untold story of international finance in the post 9/11 world”, Norton, New York.

Thompson, E. (2006) “The nexus of drug trafficking and hawala in Afghanistan, Afghanistan’s drug industry: Structure, functioning, dynamics and implications for counter-narcotics policy”, *United Nations Office on Drugs and Crime* and *The World Bank*, 155-188.

UKHO (2006) “Report of the Official Account of the Bombings in London on 7th July 2005”, *United Kingdom Home Office*, London, www.homeoffice.gov.uk/documents/7-july-report?version=1

UN (2004), “First Report of the [UN] Monitoring Team pursuant to resolution 1526 Report on al-Qaeda and the Taliban”, S/2004/679, UN Security Council Committee established pursuant to Resolution 1267 (1999), *United Nations*, New York, www.un.org/Docs/sc/committees/1267/1267mg.htm

Unger, B. (2007) “The scale and impacts of money laundering”. *Edward Elgar Publishing Company*, Cheltenham (UK).

Unger, B., van Waarden, F. (2009) “Attempts to dodge drowning in data: rule- and risk-based anti money laundering policies compared”, *TKI Working Paper* No. 09-19, Tjalling Koopmans Institute, Utrecht School of Economics, Utrecht.

USDC (2001) “CDIM (US Imports of merchandise)”, “CDEX (US Exports of merchandise)”, *US Department of Commerce*, Bureau of Census, www.census.gov/foreign-trade/guide/

US National Commission (2004) “Monograph on Terrorist Financing”, Staff Report to the Commission, Washington DC, National Commission on Terrorist Attacks Upon the United States, www.9-11commission.gov/staff_statements/index.htm

van den Broek, M. (2011) “The EU’s preventive AML/CFT policy: asymmetrical harmonization”, *Journal of Money Laundering Control* 14(2), 170-182.

Viles T. (2008) “Hawala, Hysteria and Hegemony”, *Journal of Money Laundering Control* 11(1), 25-33.

Walker, J. (2000) “Money Laundering: Quantifying International Patterns”, *Australian Social Monitor* 2(6), 139-147.

Walker, J. (2004) “A Very Tentative Exploration of the Relationship between Shadow Economy and the Production and Transit of Illicit Drugs”, *UNODC Document*, New York.

Walker, J. (2007) “Measuring Global Money Laundering”, Paper presented at the conference *“Tackling Money Laundering”*, University of Utrecht, Netherlands.

Walker, J., Unger, B. (2009) “Measuring Global Money Laundering: The Walker Gravity Model”, *Review of Law and Economics*, 5(2), p. 821-853.

Wang, J. (2011) “Regulating Hawala: a comparison of five national approaches”, *Journal of Money Laundering Control* 14(3), 210-231.

Wang, G., Yau, J. (2000) “Trading Volume, Bid-Ask Spread, and Price Volatility in Futures Markets” *Journal of Futures Markets* 20(10), 943–70.

Wang, G., Yau, J., Baptiste, T. (1997) “Trading Volume and Transaction Costs in Futures Markets, *Journal of Futures Markets* 17(7), 757–80.

Weimann, G. (2004) "www.terror.net: How Modern Terrorism Uses the Internet", United States Institute of Peace, Washington DC, www.usip.org/pubs/specialreports/sr116.pdf

Wilkinson, P. (2005) "International Terrorism: The Changing Threat and the EU's Response", *Cahier de Chaillot* 84.

Williams, P. (2005) "Warning Indicators, Terrorist Finances, and Terrorist Adaptation," Strategic Insights IV(1), US Naval Postgraduate School, Monterey, California; www.ccc.nps.navy.mil/si/2005/Jan/williamsJan05.asp

Williams, P. (2007) "Warming Indicators and Terrorist Finances, Terrorism financing and state responses: A comparative perspective", *Stanford University Press*, 72-92.

Wilson J.F., (2002) "Hawala and other Informal Payments Systems: An Economic Perspective", *International Monetary Fund*.

Wilton Park Report (2007) "Combating Financing of Terrorism", Conference WP852.

WTO (2011a) "International Trade Statistics 2011, World merchandise exports by major product group", *World Trade Organization*, www.wto.org

WTO (2011b) "International Trade Statistics 2011, World trade in commercial services by category", *World Trade Organization*, www.wto.org

Yepes, V. (2008) "International Cooperation in the Fight against Terrorist Financing", *Universitat de Barcelona Dissertation*.

Yitzhaki, S. (1974) "A note on income tax evasion: A theoretical analysis", *Journal of Public Economics* 3, 201-202.

Zaidi, M., (2010) "Understanding the Appeal of Taliban in Pakistan", *Journal of Strategic Security*, 3(3), 1-14.

Zdankowicz, J. (2004) "Detecting money laundering and terrorist financing via data mining", *Communications of the ACM* 47(5), 53-55.

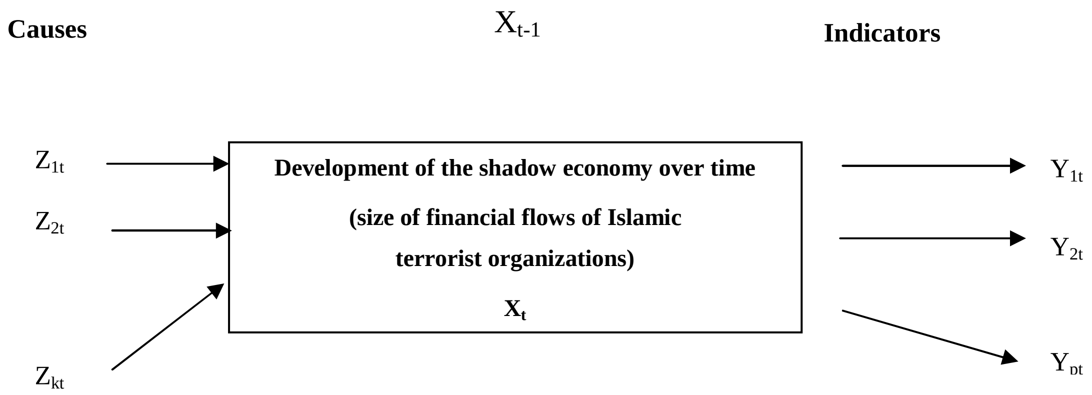
7 Appendix A: The MIMIC-approach (estimation procedure used to estimate the financial flows of Islamist terrorist groups

As the size of financial flows of Islamist terrorist groups is an unknown (hidden) figure, a latent estimator approach using a MIMIC (i.e. **m**ultiple **i**ndicators, **m**ultiple **c**auses estimation) procedure is applied[53]. As the name suggests, the procedure explicitly considers the multiple causes as well as the multiple indicators of the hidden variable and is called the "model-approach". The method is based on the statistical theory of unobserved variables, which consider multiple causes and multiple indicators of the variable to be analyzed (in this case, the size of the financial flows of Islamist terror-organizations). A factor-analytic approach is used to measure the hidden and unobserved variable over time, and the unknown coefficients are estimated in a set of structural equations.

In general, the MIMIC model consists of two parts. The *measurement model* links the unobserved variables to observed indicators, while the *structural equations model* specifies causal relationships among the unobserved variables. In this case, the unobserved variable (size of the financial flows of Islamist terror-organizations) is assumed to be influenced by a set of indicators for these financial flows, thus capturing the structural dependence of these financial flows on variables that may be useful in predicting its movement and size. The interaction over time between the causes Z_{it} (i = 1, 2, ..., k), the size of the financial flows X_t, and the indicators Y_{jt} (j = 1, 2, ..., p) is shown in Figure 12.

[53] For a detailed discussion see Schneider and Enste (2000) and Schneider (2005).

Figure 12: Development of the size of financial flows of Islamist terrorist organisations over time



Source: Schneider and Caruso (2011)

As *causes* and *indicators* for the estimation of the size of the financial flows of the Islamist terrorist group, the following variables have been used.

Causes

1) number of active members and active supporters (positive sign expected)
2) tribute payments from Islamist countries (positive sign expected)
3) financial flows from wealthy people and from Islamist religious organizations in Islamic countries (positive sign expected)
4) illegal amount of diamond trading (positive sign expected)
5) illegal amount of drug trading (positive sign expected)
6) GDP per capita in Islamic countries (negative sign expected)

Indicators

1) cash flows in Islamic countries (positive sign expected)
2) rate of GDP adjusted for the means of all Islamic countries (negative sign expected)
3) amount of currency trading (positive sign expected)

Figure 13 shows the estimation (MIMIC approach) of the financial flows (unobserved/latent variable) of over 8 terrorist organizations and over the period 1999 to 2006.

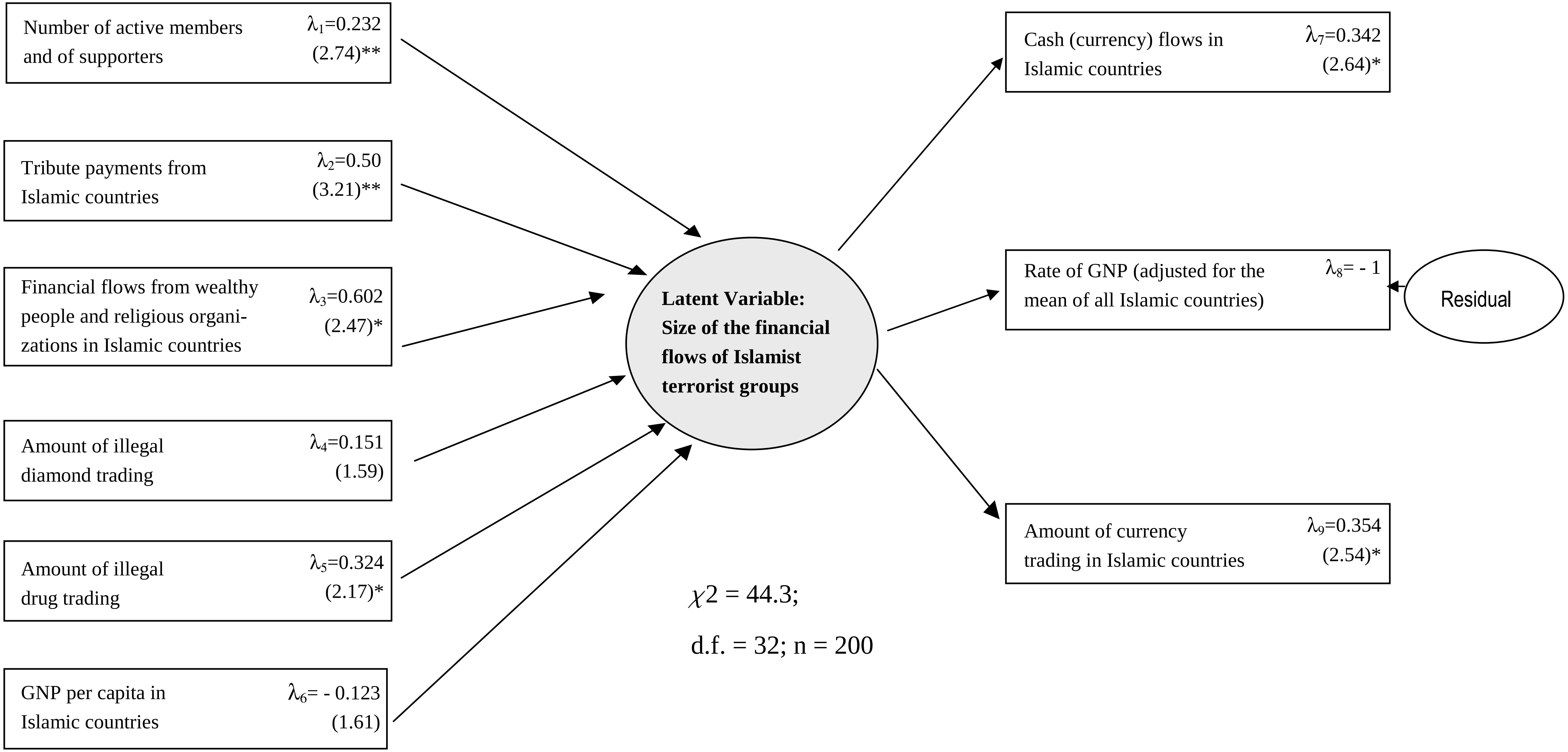
As can be seen, the causal variables "number of active members and number of supporters", "tribute payments from Islamist countries", "financial flows from wealthy people and from Islamic religious organizations" have the expected sign and the estimated coefficients are highly statistically significant. This is also true for the causal variable "amount of illegal drug trading", which has the expected sign and is statistically significant. The variables "amount of illegal diamond trading" and "GDP per capita in Islamic countries" have the expected signs, but are not statistically significant using the usual confidence intervals. Hence, out of the 6 variables 4 turn out to be highly statistically significant.

Further, all three indicator variables, "cash currency flows in Islamic countries", "amount of currency trading" as well as "rate of GDP (adjusted for the mean of all Islamic countries)" have the expected signs and are statistically significant. The estimation thus shows that there is systematic relationship between the major causes (financial sources for the financing of Islamist terrorist groups) and important indicator variables.

While the MIMIC-approach makes possible estimating unobserved variables like financial flows of terrorist organizations, it has the disadvantage that it produces relative rather than absolute estimations. Hence, one has to calculate the absolute values of interest with the help of other estimations out of the relative ones. Doing this[54] we achieve the results documented in Table 2 and

[54] See Schneider (2008a, 2008b, 2009) for details.

Figure 13: Estimation (latent estimator approach) of the financial flows (budget) of Islamist terrorist groups using causes (determinants) and traces (indicators), MIMIC estimation procedure, combined cross section and time series over eight Islamist terrorist organizations and over 1999 to 2006



* significant at 5%, ** significant at 1%

Source: Schneider and Caruso (2011)

8 Appendix B: The FATF 40 recommendations on money laundering and the FATF 9 special recommendations on terrorist financing

Table 12: The 40 FATF-recommendations on money laundering

A: LEGAL SYSTEMS	
Scope of the criminal offence of money laundering	
1	Countries should criminalize money laundering and consider it as a "predicate offence", punishable with at least one year of imprisonment.
2	Countries should ensure that the intent and knowledge required to proving the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions. Criminal liability should apply to legal persons.
Provisional measures and confiscation	
3	Countries should enable their authorities to confiscate property laundered and proceeds from money laundering. Moreover, authorities should be enabled to engage in a) identifying and tracing property, b) freezing and seizing of property if applicable, c) preventive measures and d) appropriate investigative measures.
B: MEASURES TO BE TAKEN BY FINANCIAL AND NON-FINANCIAL INSTITUTIONS	
4	Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF recommendations.
Customer due diligence and record-keeping	
5	Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. Rather, the identities of customers should be identified and verified in case of establishing business relations, carrying out occasional transaction as well as in case of suspicion of money laundering (Customer due diligence).
6	Financial institutions should, in addition to the due diligence measures, have appropriate risk management systems to determine whether a customer is a politically exposed person. If so, they should enhance monitoring and take establish the sources of wealth and funds.
7	Financial institutions should, in case of cross border banking relationships, gather sufficient information on the respondents business, his institution's anti-money laundering controls and his reputation. Furthermore, they should increase monitoring and documentation in such cases.
8	Financial institutions should pay special attention to money laundering threats that arise from new technologies that might favour anonymity and prevent their use in money laundering schemes. Moreover, they should implement procedures addressing the specific risks of non face-to-face business relationships.

continued on the next page

Table 12 continued

9	Countries may permit financial institutions to mandate third parties with carrying out the customer due diligence process, if the third party is regulated itself and provides sufficient information and documentation relating to the customer due diligence process without delay.
10	Financial institutions should keep, for at least five years, all records on both national as well as international transactions, including customer information, and should make available this information to authorities.
11	Financial institutions should pay special attention to complex and unusually large transactions if they have no apparent economic or lawful purpose. The background of such transactions should be examined as far as possible.
12	The customer due diligence and record keeping requirements set out in recommendations 5, 6 and 8 to 11 should also apply to a) casinos, b) real estate agents, c) dealers in metals and precious stones, d) lawyers and notaries and e) trust providers.
Reporting of suspicious transactions and compliance	
13	If a financial institution suspects that funds are the proceeds of criminal activity, it should be required to report its suspicions promptly to the financial intelligence unit (FIU)
14	Financial institutions as well as their employees should be protected from criminal or civil liability if they report their suspicions in good faith to the FIU, even if they do not know precisely what the underlying criminal activity was.
15	Financial institutions should develop programs against money laundering, including the development of internal procedures, adequate screening, employee training and auditing.
16	The requirements set out in recommendations 13 to 15 and 21 apply also to non-financial businesses, like casinos, real-estate agents, dealers in precious stones and metals, lawyers or notaries, provided they carry out suspicious transactions for customers.
Other measures to deter money laundering and terrorist financing	
17	Countries should ensure that effective sanctions are available to treat natural and legal persons covered by the recommendations, who do not comply.
18	Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse banking relationships with shell banks.
19	Countries should consider the feasibility and utility of a system where financial institutions would report all domestic and international currency transactions above a fixed amount to a national central agency.

continued on the next page

Table 12 continued

20	Countries should consider applying the FATF recommendations also to non-financial businesses which pose a money laundering or terrorist financing risk. Moreover, they should encourage developing modern and secure money management techniques which are less vulnerable to money laundering.
Measures to be taken with respect to non-compliant countries	
21	Financial institutions should give special attention to business relationships and transactions with persons and companies from countries with do not sufficiently apply the FATF recommendations. If countries continue not to apply the FATF recommendations, countries should be enabled to set countermeasures.
22	Financial institutions should ensure that the principles applicable to financial institutions outlined above are also applicable to foreign branches and subsidiaries, especially in countries which do not sufficiently comply with the FATF recommendations.
Regulation and supervision	
23	Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF recommendations. Moreover, criminals and their associates should be prevented from becoming owners of significant amounts of shares of financial institutions.
24	Designated non-financial businesses and professions should be subject to the following regulatory devices. Casinos should be licensed, and all other non-financial businesses should be monitored on a risk-sensitive basis.
25	The authorities should establish guidelines and give feedback to assist financial and non-financial institutions in applying measures to combat money laundering and terrorist financing.
C: INSTITUTIONAL AND OTHER MEASURES NECESSARY TO COMBAT MONEY LAUNDERING	
Competent authorities, their powers and resources	
26	Countries should establish a Financial Intelligence Unit (FIU) that serves as a centre for receiving analysis and disseminating information on money laundering and terrorist financing. It should have access to financial, administrative and law enforcement information required to undertake its functions.
27	Countries should ensure that designated law enforcement authorities have responsibility for AML/CFT investigations and that special investigative technique, such as controlled delivery or undercover operations are supported and developed.
28	When conduction investigations, competent authorities should be able to obtain all necessary documentation and information, including powers to use compulsory measures for the production of records, the search of persons as well as the seizure of evidence.

continued on the next page

Table 12 continued

29	Supervisors should have adequate powers to monitor and ensure compliance by financial institutions, including the authority to conduct inspections and to impose sanctions in case of non-compliance.
30	Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources.
31	Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to cooperate and coordinate the implementation of policies to combat money laundering and terrorist financing.
32	Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems.
Transparency of legal persons and arrangements	
33	Countries should take measures to prevent the unlawful use of legal persons by money launderers. In doing so, countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons and that this information is timely accessible by the competent authorities.
34	Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, they should ensure that there is adequate and accurate information on express trusts, including information on the settler, trustee and beneficiaries, and that this information is timely accessible by the competent authorities.
D: INTERNATIONAL COOPERATION	
35	Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.
Mutual legal assistance and extradition	
36	Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions and related proceedings. In particular, countries should not refuse to execute a request for mutual legal assistance on the grounds of laws that require financial institutions to maintain secrecy or confidentiality.
37	Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.
38	There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered or proceeds from money laundering.

continued on the next page

Table 12 continued

39	Countries should recognize money laundering as an extraditable offence.
Other forms of cooperation	
40	Countries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts. In particular, competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters, and they should not require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide cooperation.
Source: FATF/OECD (2010a)	

Table 13: The 9 FATF special recommendations on terrorist financing

I	Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.
II	Each country should criminalise the financing of terrorism, terrorist acts and terrorist organizations. Countries should ensure that such offences are designated as money laundering predicate offences.
III	Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions on prevention and suppression of the financing of terrorist acts.
IV	If financial institutions suspect or have reasonable grounds to suspect that funds are linked to terrorism, they should be required to report promptly their suspicions to the competent authorities.
V	Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the highest possible extent of mutual assistance in connection with inquiries and proceedings related to terrorism.
VI	Each country should take measures to ensure that persons or legal entities that provide a service for the transmission of money ore value should be licensed and registered and subject to all FATF recommendations that apply to banks and non-bank financial institutions.
VII	Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information on funds transfers and related messages that are sent.
VIII	Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused.
IX	Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.
Source: FATF/OECD (2010b)	

9 Appendix C: Jurisdictions' compliance with groupings of FATF anti-money laundering/combating terrorist financing (AML/CFT) recommendations

Table 14: Jurisdictions' compliance with groupings of AML/CFT recommendations – Advanced Economies

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Transparency	International Cooperation	AML	CFT	Total AML/CFT
Andorra	2007	38.8%	57.1%	34.9%	33.3%	16.5%	44.3%	57.1%	45.8%	22.2%	41.5%
Austria	2008	44.0%	66.3%	59.9%	33.0%	49.5%	33.0%	51.9%	55.4%	47.8%	54.0%
Australia	2005	72.2%	71.4%	33.3%	11.0%	66.5%	44.3%	90.4%	53.3%	48.1%	52.4%
Belgium	2005	77.8%	76.1%	84.1%	44.3%	50.0%	77.7%	71.4%	77.5%	70.3%	76.2%
Bermuda	2007	50.0%	52.4%	27.0%	0.0%	50.0%	77.7%	76.1%	44.2%	37.0%	42.9%
British Virgin Island	2008	77.8%	81.0%	55.6%	33.3%	100.0%	44.3%	95.3%	66.7%	70.3%	67.3%
Canada	2007	66.7%	61.9%	41.3%	0.0%	100.0%	33.3%	71.4%	50.0%	55.6%	51.0%
Cayman Islands	2007	72.2%	76.1%	60.3%	44.3%	66.5%	77.7%	85.7%	70.8%	55.6%	68.0%
Cyprus	2005	72.2%	81.0%	69.9%	33.3%	83.5%	55.7%	85.7%	72.5%	66.7%	71.4%
Czech Republic	2005	33.0%	75.9%	47.2%	11.0%	66.0%	44.3%	66.1%	51.3%	47.7%	50.7%
Denmark	2006	50.0%	66.7%	41.3%	11.0%	66.5%	44.3%	71.4%	50.0%	48.1%	49.7%
Estonia	2008	55.5%	81.0%	60.3%	33.3%	66.5%	66.7%	71.4%	66.7%	48.1%	63.3%
Finland	2007	50.0%	57.1%	44.4%	11.0%	66.5%	55.7%	66.7%	50.8%	44.4%	49.7%
France	2010	61.2%	61.9%	68.2%	22.3%	83.5%	66.7%	71.4%	63.3%	70.3%	64.6%
Germany	2009	50.0%	61.9%	57.1%	0.0%	83.5%	22.3%	61.9%	51.7%	59.2%	53.1%
Gibraltar	2006	66.7%	71.4%	63.5%	33.3%	50.0%	66.7%	61.9%	64.2%	55.6%	62.6%
Greece	2006	33.3%	33.3%	34.9%	0.0%	33.5%	33.3%	57.1%	36.7%	29.7%	35.4%
Guernsey	2010	72.2%	85.7%	90.5%	55.7%	83.5%	66.7%	81.0%	84.2%	74.1%	82.3%
Hong Kong China	2007	50.0%	76.1%	60.3%	0.0%	33.5%	44.3%	76.1%	61.7%	40.8%	57.8%
Iceland	2006	44.5%	57.1%	49.2%	22.3%	66.5%	44.3%	57.1%	54.2%	29.7%	49.7%
Ireland	2005	61.2%	71.4%	52.4%	22.3%	66.5%	33.3%	95.3%	62.5%	48.1%	59.9%
Isle of Man	2008	44.0%	75.7%	72.6%	33.0%	66.0%	66.0%	66.4%	68.8%	51.3%	65.6%

to be continued on next page

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Israel	2007	66.7%	81.0%	55.6%	0.0%	50.0%	44.3%	81.0%	60.0%	59.2%	59.9%
Italy	2005	66.7%	76.1%	50.8%	0.0%	100.0%	77.7%	90.4%	61.7%	66.7%	62.6%
Japan	2008	50.0%	71.4%	46.0%	22.3%	50.0%	11.0%	42.9%	48.3%	37.0%	46.3%
Jersey	2008	71.7%	80.6%	72.6%	44.0%	83.0%	88.7%	75.7%	74.6%	69.8%	73.7%
Korea	2008	27.8%	52.4%	38.1%	0.0%	83.5%	11.0%	66.7%	43.3%	29.7%	40.8%
Liechtenstein	2007	44.5%	76.1%	49.2%	44.3%	50.0%	33.3%	47.6%	55.8%	29.7%	51.0%
Luxembourg	2009	33.3%	47.6%	30.1%	0.0%	16.5%	22.3%	61.9%	36.7%	25.9%	34.7%
Macau, SAR	2006	55.5%	57.1%	63.5%	44.3%	50.0%	44.3%	38.1%	57.5%	44.4%	55.1%
Malta	2005	66.7%	81.0%	60.3%	44.3%	66.5%	66.7%	95.3%	71.7%	55.6%	68.7%
Monaco	2006	44.5%	61.9%	47.6%	11.0%	66.5%	44.3%	42.9%	46.7%	48.1%	46.9%
Netherlands	2010	55.5%	66.7%	58.7%	33.3%	83.5%	44.3%	42.9%	55.0%	59.2%	55.8%
New Zealand	2009	72.2%	66.7%	27.0%	0.0%	66.5%	11.0%	71.4%	42.5%	48.1%	43.5%
Norway	2005	66.7%	61.9%	63.5%	55.7%	66.5%	55.7%	66.7%	69.2%	37.0%	63.3%
Portugal	2006	55.5%	66.7%	66.7%	33.3%	83.5%	44.3%	95.3%	70.0%	51.9%	66.7%
San Marino	2007	38.8%	38.1%	19.0%	0.0%	33.5%	11.0%	42.9%	29.2%	14.8%	26.5%
Singapore	2007	61.2%	81.0%	74.6%	11.0%	66.5%	44.3%	81.0%	68.3%	70.3%	68.7%
Slovakia	2005	33.3%	47.6%	30.1%	11.0%	33.5%	44.3%	52.4%	38.3%	25.9%	36.1%
Slovenia	2005	77.8%	76.1%	65.1%	44.3%	83.5%	77.7%	90.4%	72.5%	70.3%	72.1%
Spain	2005	61.2%	52.4%	63.5%	22.3%	66.5%	66.7%	85.7%	62.5%	63.0%	62.6%
Sweden	2005	61.2%	61.9%	47.6%	22.3%	50.0%	55.7%	81.0%	58.3%	40.8%	55.1%
Switzerland	2005	66.7%	71.4%	58.7%	44.3%	33.5%	55.7%	76.1%	65.0%	48.1%	61.9%
Taiwan, POC	2007	22.2%	76.1%	54.0%	0.0%	16.5%	44.3%	52.4%	52.5%	25.9%	47.6%
UK	2006	100.0%	81.0%	60.3%	44.3%	83.5%	44.3%	95.3%	70.0%	81.4%	72.1%
USA	2005	77.8%	81.0%	73.0%	11.0%	100.0%	33.3%	76.1%	68.3%	77.8%	70.1%
No. of Recommendations		6	7	21	3	2	3	7	40	9	49
Total countries		46	46	46	46	46	46	46	46	46	46
Theoretical Compliance		276.0	322.0	966.0	138.0	92.0	138.0	322.0	1840.0	414.0	2254.0
Real Compliance		157.2	217.9	521.7	30.9	58.0	66.6	226.9	1072.1	207.1	1279.2

Degree of Compliance	57.0	67.7	54.0	22.4	63.0	48.2	70.5	58.3	50.0	56.8
Average Compliance	3.4	4.7	11.3	0.7	1.3	1.4	4.9	23.3	4.5	27.8

Source: IMF (2011) and own calculations

Note: The table is not meant to describe a jurisdiction‘s current level of compliance with the AML/CFT standard, but rather the level of compliance at the time of its most recent evaluation, indicated in the column “Year of Assessment”. IMF (2011) used the original compliance rating data, where the measure of compliance was defined as C, “Compliant”, LC, “Largely Compliant”, PC, “Partially Compliant” NC, “Non-Compliant” and NA, “Not Applicable”. In order to provide a quantitative measure of AML/CFT compliance, IMF (2011) replaced existing ratings with the following numbers: C-“1”, LC-“0.66”, PC-“0.33” and NC-“0”, NA-“1.”

Concerning the measurement of components of the AML/CFT regime:

The **legal** measures include Recommendations 1, 2, 3, as well as Special Recommendations I, II, and III (i.e. six items in total).

Institutional measures are evaluated through the scores on Recommendations 26, 27, 28, 29, 30, 31, and 32 (i.e. seven items in total).

Preventive financial sector measures are evaluated through scores for Recommendations 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 22, 23 and 25 as well as Special Recommendations IV, VI, and VII (i.e. 21 items in total).

For **preventive designated non-financial business measures**: Recommendations 12, 16, and 24 (i.e. three items in total).

Measures intended at preventing the abuse of the **informal sector** concern Recommendation 20 as well as Special Recommendation IX (i.e. two items in total).

Entity transparency measures consist of Recommendations 33, 34, and Special Recommendation VIII (i.e. three items in total).

International cooperation measures cover Recommendations 35, 36, 37, 38, 39, 40, and Special Recommendation V (i.e. seven items in total).

AML-specific compliance is measured by the scores on FATF Recommendations 1 to 40 while CFT-specific compliance is measured through those on FATF Special Recommendations I to IX.

For each country, the level of compliance presented in the cells of the table is the sum of numbers assigned to the ratings for the Recommendations referenced in that cell divided by the total number of recommendations considered in that cell (i.e. for the subset related to the informal sector, which includes Recommendation 20 and Special Recommendation IX, if both recommendations are rated PC, the level of compliance would be 0.66/2 = 33%. The maximum level of compliance would be 100% if both recommendations are rated C).

Table 15: Jurisdictions' compliance with groupings of AML/CFT recommendations – Emerging and developing economies

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Albania	2011	44.5%	42.9%	42.9%	33.3%	33.5%	44.3%	52.4%	46.7%	29.7%	43.5%
Anguilla	2009	66.7%	61.9%	54.0%	33.3%	16.5%	55.7%	85.7%	61.7%	44.4%	58.5%
Antigua & Barbuda	2007	38.8%	52.4%	14.3%	11.0%	66.5%	11.0%	81.0%	37.5%	18.6%	34.0%
Argentina	2009	27.8%	23.9%	22.2%	0.0%	33.5%	0.0%	38.1%	24.2%	18.6%	23.1%
Armenia	2009	44.5%	47.6%	65.1%	11.0%	33.5%	55.7%	52.4%	56.7%	37.0%	53.1%
Aruba	2008	27.5%	23.6%	23.7%	0.0%	33.0%	33.3%	42.6%	31.5%	3.7%	26.3%
Azerbaijan	2008	22.2%	28.6%	23.8%	0.0%	33.5%	44.3%	47.6%	29.2%	22.2%	27.9%
Bahamas	2006	61.2%	71.4%	42.9%	33.3%	66.5%	55.7%	76.1%	56.7%	48.1%	55.1%
Bahrain	2005	33.3%	57.1%	57.1%	22.3%	16.5%	66.7%	71.4%	55.0%	44.4%	53.1%
Bangladesh	2008	27.5%	33.0%	29.9%	0.0%	49.5%	11.0%	33.0%	29.7%	22.0%	28.3%
Barbados	2006	55.5%	76.1%	41.3%	0.0%	83.5%	44.3%	61.9%	50.8%	48.1%	50.3%
Belarus	2008	55.5%	52.4%	42.9%	11.0%	50.0%	77.7%	61.9%	51.7%	37.0%	49.0%
Benin	2009	27.8%	33.3%	20.6%	0.0%	0.0%	33.3%	42.9%	30.8%	0.0%	25.2%
Bolivia	2006	33.3%	28.6%	25.4%	0.0%	0.0%	11.0%	42.9%	30.8%	3.7%	25.9%
Bosnia and Herze-govina	2009	33.3%	33.3%	41.3%	0.0%	33.5%	44.3%	61.9%	41.7%	29.7%	39.4%
Botswana	2007	16.7%	33.3%	27.0%	0.0%	16.5%	0.0%	42.9%	30.8%	0.0%	25.2%
Brazil	2009	16.7%	52.4%	61.9%	0.0%	50.0%	44.3%	61.9%	54.2%	29.7%	49.7%
Brunei	2010	33.3%	33.3%	25.4%	0.0%	16.5%	33.3%	52.4%	30.8%	25.9%	29.9%
Bulgaria	2007	61.2%	76.1%	60.3%	33.3%	66.5%	66.7%	90.4%	66.7%	63.0%	66.0%
Burkina Faso	2009	22.0%	18.9%	9.4%	0.0%	0.0%	33.3%	42.4%	21.5%	0.0%	17.5%
Cambodia	2007	0.0%	14.3%	15.9%	11.0%	0.0%	55.7%	14.3%	17.5%	3.7%	15.0%
Cape Verde	2007	27.8%	23.9%	8.0%	0.0%	16.5%	55.7%	23.9%	20.8%	3.7%	17.7%
Chile	2010	49.5%	70.9%	53.6%	22.0%	49.5%	11.0%	61.6%	57.9%	25.7%	52.0%
China	2006	33.3%	71.4%	44.4%	0.0%	66.5%	33.3%	76.1%	50.8%	40.8%	49.0%
Colombia	2008	72.2%	85.7%	73.0%	33.3%	83.5%	44.3%	85.7%	75.8%	59.2%	72.8%
Comoros	2009	27.8%	23.9%	9.5%	0.0%	16.5%	0.0%	33.3%	17.5%	11.1%	16.3%

to be continued on next page

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Cook Islands	2009	22.2%	19.0%	9.5%	0.0%	0.0%	33.3%	42.9%	21.7%	0.0%	17.7%
Costa Rica	2006	22.2%	52.4%	30.1%	0.0%	0.0%	11.0%	42.9%	34.2%	11.1%	29.9%
Croatia	2006	33.3%	71.4%	28.6%	0.0%	33.5%	44.3%	57.1%	43.3%	18.6%	38.8%
Djibouti	2007	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Dominica	2008	38.5%	23.6%	15.8%	0.0%	33.0%	11.0%	56.7%	26.5%	18.3%	25.0%
Dominican Republic	2005	22.2%	38.1%	34.9%	0.0%	50.0%	11.0%	38.1%	33.3%	22.2%	31.3%
Ecuador	2005	16.7%	33.3%	11.1%	0.0%	0.0%	22.3%	23.9%	20.0%	0.0%	16.3%
Egypt	2008	50.0%	61.9%	49.2%	22.3%	50.0%	77.7%	71.4%	55.8%	48.1%	54.4%
El Salvador	2009	77.8%	42.9%	46.0%	0.0%	66.5%	44.3%	66.7%	50.8%	48.1%	50.3%
Fiji	2006	33.3%	52.4%	47.6%	33.3%	66.5%	33.3%	52.4%	50.8%	25.9%	46.3%
Gambia	2008	50.0%	23.9%	33.3%	0.0%	0.0%	33.3%	42.9%	33.3%	25.9%	32.0%
Georgia	2006	33.3%	57.1%	31.8%	22.3%	33.5%	55.7%	61.9%	45.0%	22.2%	40.8%
Ghana	2008	27.5%	33.0%	22.0%	0.0%	16.5%	11.0%	33.0%	24.0%	22.0%	23.6%
Grenada	2008	33.0%	51.9%	14.2%	0.0%	16.5%	0.0%	71.1%	33.1%	7.3%	28.4%
Guatemala	2009	50.0%	52.4%	63.5%	0.0%	66.5%	33.3%	71.4%	56.7%	51.9%	55.8%
Guinea Bissau	2008	22.0%	14.3%	11.0%	0.0%	16.5%	33.3%	33.0%	19.9%	3.7%	16.9%
Haiti	2007	11.2%	23.9%	19.0%	0.0%	16.5%	33.3%	33.3%	24.2%	3.7%	20.4%
Honduras	2007	44.0%	37.9%	31.7%	0.0%	16.5%	0.0%	37.7%	31.5%	25.8%	30.4%
Hungary	2010	50.0%	76.1%	82.5%	55.7%	66.5%	66.7%	76.1%	79.2%	48.1%	73.5%
India	2009	44.5%	71.4%	61.9%	0.0%	50.0%	22.3%	61.9%	56.7%	44.4%	54.4%
Indonesia	2007	22.2%	47.6%	36.5%	0.0%	66.5%	33.3%	42.9%	40.8%	14.8%	36.1%
Jamaica	2005	66.7%	66.7%	52.4%	0.0%	50.0%	55.7%	57.1%	53.3%	55.6%	53.7%
Jordan	2008	27.8%	47.6%	44.4%	11.0%	0.0%	55.7%	38.1%	44.2%	14.8%	38.8%
Kyrgyz Republic	2007	11.2%	42.9%	44.4%	0.0%	66.5%	44.3%	47.6%	44.2%	14.8%	38.8%
Latvia	2006	61.2%	76.1%	50.8%	22.3%	50.0%	66.7%	71.4%	62.5%	37.0%	57.8%
Lebanon	2009	61.2%	52.4%	61.9%	33.3%	50.0%	33.3%	66.7%	57.5%	55.6%	57.1%
Lithuania	2006	44.5%	66.7%	61.9%	33.3%	66.5%	55.7%	81.0%	65.0%	44.4%	61.2%
Macedonia	2007	38.8%	52.4%	30.1%	0.0%	50.0%	44.3%	52.4%	40.8%	22.2%	37.4%

to be continued on next page

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Malawi	2008	44.5%	38.1%	46.0%	0.0%	50.0%	22.3%	57.1%	45.0%	29.7%	42.2%
Malaysia	2007	61.2%	71.4%	66.7%	33.3%	50.0%	33.3%	61.9%	64.2%	48.1%	61.2%
Mali	2008	22.2%	9.6%	8.0%	0.0%	0.0%	33.3%	23.9%	15.0%	3.7%	12.9%
Mauritania	2005	27.8%	28.6%	27.0%	0.0%	33.5%	55.7%	57.1%	31.7%	33.3%	32.0%
Mauritius	2007	38.8%	52.4%	49.2%	11.0%	66.5%	44.3%	61.9%	52.5%	29.7%	48.3%
Mexico	2008	38.8%	61.9%	58.7%	0.0%	16.5%	33.3%	61.9%	55.0%	29.7%	50.3%
Moldova	2005	33.3%	42.9%	30.1%	0.0%	50.0%	55.7%	61.9%	39.2%	29.7%	37.4%
Mongolia	2006	16.7%	33.3%	28.6%	0.0%	66.5%	33.3%	52.4%	35.8%	11.1%	31.3%
Montenegro	2008	44.5%	71.4%	57.1%	22.3%	50.0%	44.3%	71.4%	62.5%	29.7%	56.5%
Morocco	2007	33.3%	19.0%	22.2%	0.0%	0.0%	55.7%	61.9%	30.8%	18.6%	28.6%
Myanmar	2008	22.2%	42.9%	28.6%	11.0%	33.5%	55.7%	23.9%	34.2%	11.1%	29.9%
Namibia	2005	16.7%	28.6%	15.9%	0.0%	50.0%	11.0%	42.9%	24.2%	11.1%	21.8%
Nepal	2005	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Nicaragua	2008	44.0%	28.3%	39.4%	0.0%	49.5%	44.3%	61.6%	42.2%	29.3%	39.8%
Niger	2008	22.0%	19.0%	12.6%	0.0%	16.5%	44.3%	56.7%	25.7%	7.3%	22.3%
Nigeria	2007	22.2%	47.6%	22.2%	11.0%	33.5%	33.3%	38.1%	33.3%	7.4%	28.6%
Pakistan	2009	0.0%	23.9%	11.1%	0.0%	50.0%	0.0%	23.9%	16.7%	0.0%	13.6%
Palau	2008	44.5%	42.9%	22.2%	0.0%	66.5%	33.3%	52.4%	34.2%	29.7%	33.3%
Panama	2005	66.7%	71.4%	73.0%	33.3%	50.0%	33.3%	81.0%	69.2%	59.2%	67.3%
Paraguay	2008	16.7%	19.0%	19.0%	0.0%	0.0%	0.0%	28.6%	20.8%	0.0%	17.0%
Peru	2008	61.2%	71.4%	46.0%	33.3%	50.0%	66.7%	71.4%	59.2%	40.8%	55.8%
Philippines	2008	27.5%	42.4%	45.7%	0.0%	49.5%	44.0%	56.7%	46.3%	22.0%	41.8%
Poland	2006	38.8%	61.9%	36.5%	11.0%	83.5%	44.3%	57.1%	49.2%	22.2%	44.2%
Qatar	2007	33.3%	47.6%	27.0%	11.0%	16.5%	55.7%	38.1%	36.7%	14.8%	32.7%
Romania	2007	50.0%	71.4%	44.4%	11.0%	50.0%	66.7%	81.0%	57.5%	37.0%	53.7%
Russian Federation	2007	66.7%	66.7%	46.0%	33.3%	50.0%	55.7%	81.0%	60.8%	37.0%	56.5%
Rwanda	2005	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Samoa	2006	22.2%	33.3%	28.6%	33.3%	50.0%	11.0%	23.9%	30.8%	14.8%	27.9%

to be continued on next page

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Saudi Arabia	2009	38.8%	61.9%	61.9%	0.0%	66.5%	66.7%	47.6%	56.7%	40.8%	53.7%
Senegal	2007	49.5%	66.1%	31.6%	11.0%	49.5%	44.3%	71.1%	49.7%	22.0%	44.6%
Serbia	2009	38.8%	52.4%	52.4%	11.0%	50.0%	44.3%	52.4%	50.8%	33.3%	47.6%
Seychelles	2006	33.0%	18.9%	26.8%	0.0%	16.5%	0.0%	37.7%	25.6%	18.3%	24.3%
Sierra Leone	2006	16.7%	14.3%	15.9%	0.0%	16.5%	11.0%	9.6%	16.7%	0.0%	13.6%
Solomon Islands	2009	55.5%	57.1%	42.9%	0.0%	16.5%	11.0%	61.9%	45.0%	37.0%	43.5%
South Africa	2008	66.7%	66.7%	38.1%	22.3%	66.5%	22.3%	76.1%	50.8%	48.1%	50.3%
Sri Lanka	2006	33.3%	33.3%	22.2%	0.0%	16.5%	33.3%	47.6%	30.0%	18.6%	27.9%
St. Kitts & Nevis	2008	38.5%	33.0%	44.2%	11.0%	50.0%	55.0%	66.4%	48.1%	25.7%	43.9%
St. Lucia	2008	22.2%	19.0%	9.5%	0.0%	16.5%	11.0%	19.0%	15.8%	3.7%	13.6%
St. Vincent & Grenadines	2009	44.5%	61.9%	41.3%	0.0%	50.0%	33.3%	61.9%	49.2%	25.9%	44.9%
Sudan	2004	33.3%	4.7%	15.9%	0.0%	50.0%	44.3%	33.3%	21.7%	18.6%	21.1%
Suriname	2009	22.2%	38.1%	8.0%	0.0%	16.5%	33.3%	42.9%	25.0%	0.0%	20.4%
Syria	2006	38.8%	47.6%	44.4%	22.3%	33.5%	55.7%	42.9%	47.5%	22.2%	42.9%
Tajikistan	2007	11.2%	19.0%	14.3%	0.0%	0.0%	33.3%	0.0%	15.0%	0.0%	12.2%
Tanzania	2009	0.0%	23.9%	11.1%	0.0%	50.0%	0.0%	23.9%	16.7%	0.0%	13.6%
Thailand	2007	44.5%	38.1%	27.0%	0.0%	16.5%	44.3%	38.1%	33.3%	22.2%	31.3%
Tonga	2009	16.7%	47.6%	25.4%	0.0%	0.0%	11.0%	33.3%	27.5%	14.8%	25.2%
Trinidad and Tobago	2005	11.2%	38.1%	9.5%	0.0%	83.5%	11.0%	42.9%	23.3%	11.1%	21.1%
Tunisia	2006	55.5%	57.1%	38.1%	22.3%	66.5%	89.0%	61.9%	50.0%	48.1%	49.7%
Turkey	2006	44.5%	47.6%	30.1%	0.0%	83.5%	55.7%	52.4%	40.8%	33.3%	39.4%
Turks and Caicos Islands	2007	50.0%	47.6%	25.4%	0.0%	16.5%	22.3%	57.1%	35.0%	29.7%	34.0%
UAE	2007	50.0%	57.1%	34.9%	0.0%	16.5%	66.7%	61.9%	45.8%	29.7%	42.9%
Uganda	2005	11.2%	9.6%	17.5%	0.0%	0.0%	11.0%	14.3%	12.5%	14.8%	12.9%
Ukraine	2008	27.8%	52.4%	44.4%	0.0%	50.0%	55.7%	52.4%	45.8%	29.7%	42.9%
Uruguay	2009	66.7%	85.7%	58.7%	22.3%	66.5%	55.7%	81.0%	66.7%	55.6%	64.6%
Uzbekistan	2009	55.5%	61.9%	54.0%	33.3%	66.5%	55.7%	71.4%	59.2%	48.1%	57.1%

to be continued on next page

Country	Year of assessment	Legal	Institutional	Preventing financial institutions	Preventing designated non-financial businesses	Informal Sector	Entity Transparency	International Cooperation	AML	CFT	Total AML/CFT
Vanuatu	2006	38.8%	19.0%	39.7%	0.0%	16.5%	11.0%	52.4%	35.0%	25.9%	33.3%
Venezuela	2008	38.5%	42.6%	42.6%	0.0%	0.0%	11.0%	71.0%	43.9%	22.0%	39.9%
Vietnam	2008	16.5%	37.7%	28.4%	0.0%	49.5%	22.0%	28.3%	31.4%	7.3%	27.0%
Yemen	2007	16.7%	23.9%	15.9%	11.0%	33.5%	55.7%	28.6%	25.8%	3.7%	21.8%
Zambia	2007	11.0%	28.3%	14.1%	0.0%	0.0%	11.0%	23.6%	18.2%	3.7%	15.5%
Zimbabwe	2006	16.7%	38.1%	42.9%	22.3%	33.5%	22.3%	23.9%	38.3%	11.1%	33.3%
No. of Recommen-dations		6	7	21	3	2	3	7	40	9	49
Total countries		115	115	115	115	115	115	115	115	115	115
Theoretical Compliance		690	805	2415	345	230	345	805	4600	1035	5635
Real Compliance		243.3	352.6	839.9	28.0	85.2	126.9	407.6	1833.2	250.3	2083.5
Degree of Compliance		35.3	43.8	34.8	8.1	37.0	36.8	50.6	39.9	24.2	37.0
Average Compliance		2.1	3.1	7.3	0.2	0.7	1.1	3.5	15.9	2.2	18.1

Source: Staff calculations.

Note: The table is not meant to describe a jurisdiction‘s current level of compliance with the AML/CFT standard, but rather the level of compliance at the time of its most recent evaluation, indicated in the column “Year of Assessment”. IMF (2011) used the original compliance rating data, where the measure of compliance was defined as C, “Compliant”, LC, “Largely Compliant”, PC, “Partially Compliant” NC, “Non-Compliant” and NA, “Not Applicable”. In order to provide a quantitative measure of AML/CFT compliance, IMF (2011) replaced existing ratings with the following numbers: C-“1”, LC-“0.66”, PC-“0.33” and NC-“0”, NA-“1.”

Concerning the measurement of components of the AML/CFT regime:

The **legal** measures include Recommendations 1, 2, 3, as well as Special Recommendations I, II, and III (i.e. six items in total).

Institutional measures are evaluated through the scores on Recommendations 26, 27, 28, 29, 30, 31, and 32 (i.e. seven items in total).

Preventive financial sector measures are evaluated through scores for Recommendations 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 22, 23 and 25 as well as Special Recommendations IV, VI, and VII (i.e. 21 items in total).

For **preventive designated non-financial business measures**: Recommendations 12, 16, and 24 (i.e. three items in total).

Measures intended at preventing the abuse of the **informal sector** concern Recommendation 20 as well as Special Recommendation IX (i.e. two items in total).

Entity transparency measures consist of Recommendations 33, 34, and Special Recommendation VIII (i.e. three items in total).

International cooperation measures cover Recommendations 35, 36, 37, 38, 39, 40, and Special Recommendation V (i.e. seven items in total).

AML-specific compliance is measured by the scores on FATF Recommendations 1 to 40 while CFT-specific compliance is measured through those on FATF Special Recommendations I to IX.

For each country, the level of compliance presented in the cells of the table is the sum of numbers assigned to the ratings for the Recommendations referenced in that cell divided by the total number of recommendations considered in that cell (i.e. for the subset related to the informal sector, which includes Recommendation 20 and Special Recommendation IX, if both recommendations are rated PC, the level of compliance would be 0.66/2 = 33%. The maximum level of compliance would be 100% if both recommendations are rated C).