

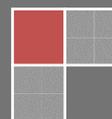


**REPUBLIC OF CROATIA  
MINISTRY OF FINANCE**

**ANY-MONEY LAUNDERING OFFICE  
(FINANCIAL-INTELLIGENCE UNIT)**

**FINANCING OF TERRORISM  
TYPOLOGY REPORT  
(CASES FROM INTERNATIONAL PRACTICE)**

**Zagreb, November 2012**



C O N T E N T :			page
1.	<b>INTRODUCTION</b>		3
2.	<b>PREVENTION OF TERRORIST FINANCING</b>		4
	2.1.	<b>International legal framework</b>	5
	2.2.	<b>Building the national system for suppression of terrorist financing</b>	6
	2.2.1.	Legal framework with review of the role of Anti-Money Laundering Office	6
	2.2.2.	Role of the Anti-Money Laundering Office	9
	2.3.	<b>The terrorist/terrorist organizations requirements for funds</b>	10
+	2.3.1.	Financing of terrorist operations	11
	2.3.2.	Financing of broad organizational requirements	12
	2.4.	<b>Raising financial funds for terrorist / terrorist organizations</b>	13
	2.5.	<b>Moving terrorist funds</b>	14
	2.6.	<b>Key Findings</b>	15
3.	<b>CASE STUDIES OF TERRORIST FINANCING TYPOLOGIES FROM INTERNATIONAL PRACTICE</b>		16
	3.1.	<b>Using of charities</b>	16
		Example 1	16
		Example 2	16
	3.2.	<b>Abuse of legitimate business</b>	17
		Example 1	17
		Example 2	17
	3.3.	<b>SELF-FUNDING</b>	18
		Example 1	18
	3.4.	<b>Using criminal proceeds</b>	19
	3.4.1.	<b>Raising funds through drug trafficking</b>	19
		Example 1	19
		Example 2	19
		Example 3	20
	3.4.2.	<b>Raising funds by credit card fraud</b>	20
		Example 1	20
		Example 2	21
	3.4.3.	<b>Raising funds by cheque fraud</b>	21
		Example 1	21
	3.5.	<b>Using of safe havens, failed states and state sponsors</b>	22
		Example 1	22
	3.6.	<b>Use of formal financial sector</b>	23
		Example 1	23
	3.7.	<b>Use of trade sector</b>	23
		Example 1	23
	3.8.	<b>Use of cash couriers</b>	24
		Example 1	24
		Bibliography	25

## 1. INTRODUCTION

Under Art. 66(4) of the Anti-Money Laundering and Counter Terrorism Financing Act (Official Gazette No. 87/08) (hereinafter: the Act), the Anti-Money Laundering Office (hereinafter: the AMLO) disseminates or discloses to the reporting entities listed in Art. 4(2) of the Act who have an obligation to implement the anti-money laundering and counter terrorism financing measures (hereinafter: the reporting entities) any information regarding the current money laundering and terrorism financing techniques, methods, trends and typologies.

Generally, in the context of anti-money laundering and counter terrorism financing, typology is defined as a systematic classification or breakdown methods, techniques and trends observed over a given period of time, which share multiple common characteristics or features.

This document draws attention to the terrorist financing typologies from international practice and it is intended for all reporting entities, the supervisory authorities under Article 83 of the Law and all other state bodies in Article 58 of the Law.

The purpose of this document on typologies and cases is to assist the Reporting Entities and supervisory authorities in their respective roles, as stipulated by law, in connection with the implementation of measures and activities aimed at prevention and detection of terrorism financing, to the law enforcement authorities and other relevant state bodies, and to raise the awareness on the TF risks and possible vulnerabilities of individual sectors.

### **The Anti Money Laundering and Terrorist Financing Law**

The provisions of the Article 1 of this Law relating to the prevention of money laundering shall adequately apply to the prevention of terrorist financing for the purpose of preventing and detecting activities of individuals, legal persons, groups and organizations in relation with terrorist financing.

The terrorist financing under this Law is defined as the provision or collection of, as well as an attempt to provide or collect legal or illegal funds by any means, directly or indirectly, with the intention that they should be or in the knowledge that they are to be used, in full or in part, in order to carry out a terrorism offence by a terrorist or by a terrorist organization.

### **Anti-money laundering and counter terrorism financing system in the Republic of Croatia:**

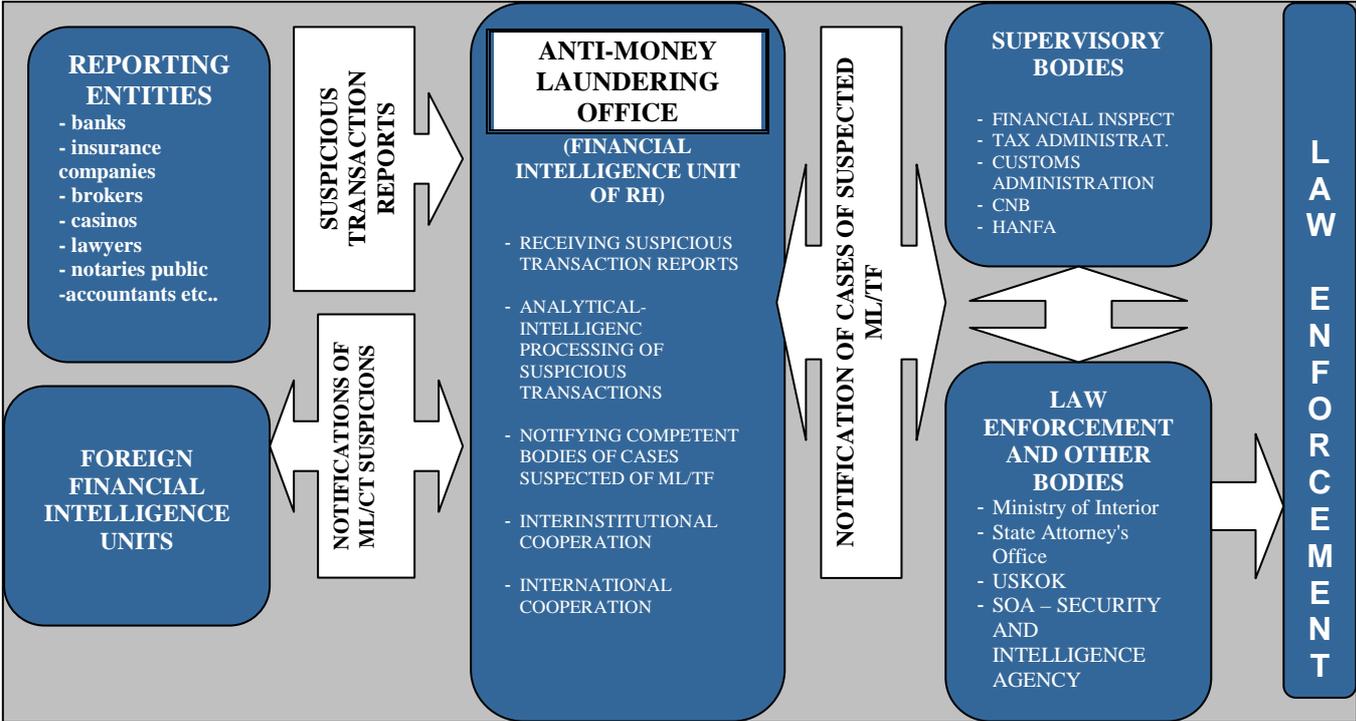
Under the Law and the international standards, counter terrorism financing system and the anti-money laundering do not fall under the competence of a single institution; quite the contrary, it is a system where the law clearly stipulates the roles of all participants and their mutual interaction and cooperation.

**As a financial intelligence unit, the AMLO is only a link in counter terrorism financing chain (as well as in the anti-money laundering), which can**

give its full contribution in terms of preventing the abuse of the financial system of the Republic of Croatia for terrorism financing purposes only in an interactive collaboration with other national competent authorities (State Attorney's Office, Office for Suppression of Corruption and Organized Crime, Ministry of Interior, Security and Intelligence Agency, Croatian National Bank, Croatian Agency for Supervision of Financial Services and the supervisory services of the Ministry of Finance) and foreign financial intelligence units.

The AMLO, as the central national unit which collects from banks and other reporting entities information on transactions linked with terrorism financing, conducts the analyses of transaction reports in order to confirm or reject the suspicion of terrorism financing, and notifies the competent bodies of any cases of suspected terrorism financing.

The AMLO is therefore an intermediary between on the one hand the financial and non-financial sectors (banks and other), which report the suspicious transactions to the AMLO, and on the other of the law enforcement authorities, as presented in the chart below:



**2. PREVENTION OF TERRORIST FINANCING:**

Terrorism is the one of the most complex, most challenging and most dangerous phenomenon of the political and security areas of the present time. In the last fifty years there have been done almost 100.000 terrorist acts in the World.

Terrorism is always a stroke on the state, political and social system of the one country and therefore its preventing and suppression requests joint and coordinated state and social action.

In that sense the basis for this action is country's legislative framework, both, national and international, since the terrorism as money laundering itself does not recognize the borders and there is no part of the World which is protected from its harmful impact.

Terrorist events of the 9/11 in the USA showed the destructive power of the terrorism and also intensified efforts to prevent terrorism by the entire international community.

As part of suppression of terrorism the special importance is on the prevention of terrorist financing. Namely, conducting terrorist acts requires financing, and the prevention of the funding has direct influence on suppression of terrorist acts.

## **2.1. INTERNATIONAL LEGAL FRAMEWORK**

International legal framework for the suppression of terrorist financing consist of 12 UN anti-terrorism Conventions and Protocols which were ratified b the end of April 2005. The overview of them are:

1. Convention on Offences and Certain Other Acts Committed on Board Aircraft,
2. Convention for the Suppression of Unlawful Seizure of Aircraft,
3. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
4. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents,
5. International Convention against the Taking of Hostages,
6. Convention on the Physical Protection of Nuclear Material,
7. Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation,
- 8.-9. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf,
10. Convention on the Marking of Plastic Explosives for the Purpose of Detection,
11. International Convention for the Suppression of Terrorist Bombings,
12. International Convention for the Suppression of the Financing of Terrorism.

The Republic of Croatia ratified as well the Protocol supplementary to the European Convention for the Suppression of Terrorism (2003). In May 2005 in Warsaw the Prime Minister of the Republic of Croatia signed the Council of Europe Convention on the suppression of terrorism.

**Concerning the suppression of terrorist financing there are three main sources of international obligation and norms (standards):**

1. **UN International Convention for the Suppression of the Financing of Terrorism (adopted by the General Assembly of the United Nations on 9 December 1999),**
2. **Nine Special Recommendation of FATF (Financial Action Task Force):**
  - 1.) Ratification and implementation of the UN instruments

- 2.) Criminalizing the financing of terrorism and associated money laundering
- 3.) Freezing and confiscating terrorist assets
- 4.) Reporting suspicious transactions related to terrorism
- 5.) International cooperation
- 6.) Alternative remittance systems
- 7.) Wire transfers
- 8.) Non-profit organizations
- 9.) Cash couriers

### **3. Resolutions of the Security Council of the UN dealing with the financing of terrorism:**

- a) 1267 (1999) on the freezing of the funds and other financial resources of the Taliban,
- b) 1333 (2000) on the freezing of the funds and other resources of Osama bin Laden and the Al-Qaida organization,
- c) 1363 (2001) on the establishment of a mechanism to monitor the implementation of measures imposed by Resolution 1267 and 1333,
- d) 1373 (2001) on threats to international peace and security caused by terrorist acts and mandating the formation of the Counter-Terrorism Committee,
- e) 1377 (2001) calling upon states to implement fully Resolution 1373,
- f) 1390 (2002) effectively merging the freezing measures of Resolution 1267 and 1333,
- g) 1455 (2003) on measures to improve the implementation of the freezing measures of Resolutions 1267, 1333 and 1390,
- h) 1566 (2004) on threats to international peace and security.
- i) 1988 (2011) and 1989 (2011) as successor resolutions to Resolution 1267 (1999). By adopting these resolutions, THE Security Council of the UN decided to split the AL-Qaida and Taliban sanctions regime, and consequently to split the UN Consolidated List.

## **2.2. BUILDING THE NATIONAL SYSTEM FOR SUPPRESSION OF TERRORIST FINANCING**

### **2.2.1. LEGAL FRAMEWORK WITH REVIEW OF THE ROLE OF ANTI-MONEY LAUNDERING OFFICE**

In the period of 22 November 2001 and 21 April 2005 and as a part of the process in fulfilling of international standards The Interagency Working group to suppress the terrorism was established by Decisions from the Government of the Republic of Croatia. The Anti-Money Laundering Office is the member of the group. The Interagency Working group is authorized for monitoring implementation of United Nations Security Resolution 1373 (2001.), Resolution 1267 (1999.) and Resolution 1566 (2004.) and all other relevant international documents and initiatives in the field of combating money laundering and terrorist financing within the European Union, NATO, the Council of Europe and OSCE.

Within the Ministry of Finance the Coordinative Working group has been established to implement the United Nations Security Council Resolution 1373

(2001.). The Coordinative Working group consists of supervisory bodies of the Ministry of Finance (Tax Administration, Customs Administration, Financial inspectorate and Anti-Money Laundering Office).The chairmanship belongs to the Anti-Money Laundering Department.

Moreover, in the course of 2008, the Government of the Republic of Croatia adopted National Strategy for the Prevention and Suppression of Terrorism. The Strategy defined the term of terrorism as designed, systematic, deliberate use of violence or threats of violence against people or material goods, as a means of inducing fear and exploitation, within certain ethnic or religious community, the public, country or all interventional community in order to achieve the changes that are political, religious, ideological or socially motivated. The strategy itself, *inter alia*, defines the measures of prevention and suppression of terrorism, and one of these measures is the measure of disabling funding of terrorist organizations or individuals who are associated with terrorism.

From 01 January 2009 a new Law on Prevention of Money Laundering and Terrorist Financing is in effect and it fully implements the provisions of so called the Third Directive of the European Parliament and of the Council on the prevention of the financial system for the purpose of money laundering and terrorist financing, as well as the 40 Recommendations and 9 Special Recommendations of the FATF.

By above mentioned Act of terrorism is defined as ensuring or fundraising and an attempt to provide or collect funds, legal or illegal, in any way, directly or indirectly, with the intention to be used or in the knowledge that they will be used, in whole or in part, for committing a terrorist offence, by a terrorist or terrorist organization. The risk of terrorism financing is defined as the risk that the party abused the financial system to finance terrorism, or that a business relationship, product or transaction will be directly or indirectly used to finance terrorism.

Besides, related to the above mentioned 9 Special Recommendations, particularly associated to Recommendations 4,6,7 and 8, the indicators for recognizing suspicion transactions and persons, with the obligation of creating and using a list of indicators , specific provisions of Article 41 of the Act on Prevention of Money Laundering and Terrorist Financing, include the reasons for suspicion of money laundering and the reasons for suspicion of terrorism financing.

Finally, the financing of terrorism has been characterized as a criminal offence of financing of terrorism prescribed by Article 187a of the Criminal Code applicable that is criminal offence of preparation of criminal offences against values protected by international law. The Amendments to Act of Criminal Code which is adopted by Parliament in Parliament session on 15 December 2008, which came into force on 1 January 2009 brought to a further harmonization of criminal offence with international standards. Furthermore, criminal offence of terrorism financing provided by Article 98 of the new Criminal Code will enter into force on 1 January 2012.

The current Criminal Code criminalizes the financing of terrorism as follows:

## Article 187a of the Criminal Code

(1) Whoever removes obstacles, makes plan or arrangements with others or undertakes any other action to create the conditions enabling direct perpetration of criminal offences referred to in Articles 156 through 160, Articles 169 through 172, Article 174 paragraph 3 and 4, and Articles 179 and 181 of the Code shall be punished by imprisonment for one o five years.

(2) The punishment referred to in paragraph 1 of this Article shall be imposed on whoever, in whatever directly or indirectly, gives or raises funds knowing that they will, fully or partially, be used for the purpose of committing the criminal offence referred to in paragraph 1 of this Article.

(3) The perpetrator of the criminal offence referred to in paragraph 2 of this Article shall be punished irrespective of whether the funds have been fully or partially used for the purpose of committing the criminal offence referred to in paragraph 1 of this Article irrespective of whether the act has been attempted.

(4) The funds referred to in paragraph 2 of this Article shall be forfeited.

Pursuant to new Penal Code («Official Gazette» No. 125/11), which will enter into force on 1 January 2013, financing of terrorism is criminalized with the provision of Article 98 of the Penal Code which prescribes that whoever directly or indirectly provides or collect funds with the intention that they will be used or knowing that they will be used, in whole or in part, in order to carry out one or more criminal offences and, *inter alia*, criminal offence of financing of terrorism in Article 97, the criminal offence of public instigation of terrorism in Article 99 , criminal office of recruitment for terrorism in Article 100, criminal offence of training for terrorism, or any other criminal offences relating to terrorism. Furthermore, whoever directly or indirectly provides or collects funds with the aim that it will be used or knowing that they will be used, in whole or in part, by terrorists or terrorist associations (regardless of the purpose of the use) shall be punished.

By provisions of the Article 102 of the new Penal Code the criminal offence of terrorist association is criminalized providing that whoever organizes or runs a criminal association aimed at committing, *inter alia*, criminal offences referred to in Article 97 through Article 101 shall be sentenced to imprisonment for a term of between three and fifteen years.

### **2.2.2. ROLE OF THE ANTI-MONEY LAUNDERING OFFICE**

In accordance with its authority as financial-intelligence unit and in order to prevent the financing of terrorism, the Anti-Money Laundering Office undertakes the following actions:

- activities of checking data on transactions regarding recorded in databases of the Office and the financial system of the Republic of Croatia;
- activities for the promotion of international co-operation.

Within the framework of these activities, the Office undertakes the analytical-intelligence processing of the transactions with suspicion on terrorist financing and informs relevant state bodies by submitting a report. Furthermore, the Office receives the Consolidated Lists of the UN pursuant to which checks the individuals and entities listed on them via own databases and via the banking system of the Republic of Croatia. On the results of these checks the Office shall inform the competent national authorities – Ministry of Foreign Affairs and European Integration, Inter-agency Working group for suppression of terrorism, The Public Prosecutor's Office and if necessary Security and Intelligence Agency ( in case when the banking system in Croatia has recorded from the list the individuals or entities whose identifying information partly coincides with the identification data of individuals and entities from the lists.

Regarding procedures of the banks and other reporting entities in relation to individuals and entities who are on the lists of individuals and entities associated with terrorism (so called terrorist list) in connection with timely and uniform application of the provisions of the Law and reporting to the Anti-Money Laundering Office on suspicious transactions related to terrorism (which does not exclude a possible suspicion of money laundering) in accordance with the Law and the Rulebooks. The Office issued on 11 November 2011 Guidelines on proceedings in the field of combating financing of terrorism and delivered them to the banks and other reporting entities. With said Guidelines the banks are required to constantly monitor of all changes on the Consolidated Lists, which includes the verification of bank's database of customers as well. Comparing the names of individuals and on the Consolidated Lists with those from database of customers of each bank, banks minimize the possibility that some of the individuals and entities from Consolidated Lists freely operate in the banking system. Banks must inform the Office (AMLO) about the said checks periodically.

### **2.3. THE TERRORIST / TERRORIST ORGANISATIONS REQUIREMENTS FOR FUNDS**

The first step in identifying and forestalling the flow of funds to terrorists is to understand the funding requirements of modern terrorist groups. The costs associated not only with conducting terrorist attacks but also with developing and maintaining a terrorist organization and its ideology are significant. Funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks. Often, a variety of higher-cost services, including propaganda and ostensibly legitimate social or charitable activities are needed to provide a veil of legitimacy for organizations that promote their objectives through terrorism.

The nature of funding for both operational and broader support activities will vary by the type of terrorist organization, with traditional, hierarchical quasi-state-like terrorist organizations on one side of the spectrum and small, decentralized independently supported organizations on the other. At its extreme, this second category has involved small, ostensibly self-directed networks seeking to meet their own funding requirements through means that differ little from their everyday activity. Purchases - even when used to procure the precursors for attacks - are not conspicuous.

Terrorist financing requirements fall into two general areas:

- funding specific terrorist operations, such as direct costs associated with specific operations and
- Broader organizational costs to develop and maintain an infrastructure of organizational support and to promote the ideology of a terrorist organization.

### 2.3.1. FINANCING OF TERRORIST OPERATIONS

Financing of terrorist operations includes direct costs for terrorist operations, living costs, salary costs, communication costs, training and travel costs and logistic.

As regards direct costs associated with terrorist operations or attacks, the precursor materials for conducting them are highly diverse and include, for example, vehicles, improvised bomb-making components, maps surveillance material etc. The direct costs of terrorist attacks are often very low relative to the damage they can yield as illustrated by the following estimates:

<b>Attack:</b>	<b>Date:</b>	<b>Estimated costs<sup>1</sup></b>
London transport system	7 July 2005	GBP 8 000 <sup>2</sup>
Madrid train bombings	11 March 2004	USD 10 000
Istanbul truck bomb attacks	15&20 November 2003	USD 40 000
Jakarta JW Marriot Hotel bombing	5 August 2003	USD 30 000
Bali bombings	12 October 2002	USD 50 000
USS Cole attack	12 October 2000	USD 10 000
East Africa embassy bombings	7 August 1998	USD 50 000

Individual operatives need to cover their day-to-day expenses and perhaps also those of their dependents. A cell will also need to communicate with its members and perhaps the parent network. This will be a more significant commitment if there is no other source of income for the operatives (such as employment or welfare payments).

Training of operatives continues to be an important investment for terrorists, both in terms of ideological indoctrination and practical skills. The financial facilitation of training and travel, which can include the procurement of false documentation, represents an important cost for many terrorist networks. Even in recent attacks where terrorist operatives were «home grown» and largely operationally independent of any overarching leadership structure, any operatives still traveled to receive training or other formats of indoctrination prior to the operational phase of a plot.

---

<sup>1</sup> Unless otherwise noted, all estimates adapted from the August 2004 report of the UN Monitoring Team Report on al-Qaeda and the Taliban

<sup>2</sup> The United Kingdom Home Office (2006)

### 2.3.2. FINACING OF BROAD ORGANISATIONAL REQUIREMENTS

Financially maintaining a terrorist network - or a specific cell - to provide for recruitment, planning and procurement between attacks represents the most significant drain on resources.

Terrorist organizations require funding to develop a supporting infrastructure, recruit members and promote their ideology. In addition, this infrastructure spending may go to support charitable organizations and media owned or controlled by the terrorist organizations.

Terror networks often use compromised or complicit charities and businesses to support their objectives. For example, some groups have links to charity branches in high-risk areas and/or under-developed parts of the world where the welfare provision available from the state is limited or non-existent. In this context, groups that use terrorism as a primary means to pursue their objectives can also, utilize affiliated charities as a source of financing that may be diverted to fund terrorist attacks and terrorist recruitment by providing a veil of legitimacy over an organization based terrorism.<sup>3</sup>

In addition to the civilian or social welfare function of organizations committed to paramilitary violence, there is often a sophisticated public relations and media operations component that sustains the ideology of terrorism. Terrorist groups such as Al-Qaida have been especially adept at manipulating television through the release of videos. In addition, virtually every terrorist organization has a website dedicated to recruitment and spreading the message of bloodshed. These major mass media tools emit powerful propaganda for violence, suicide bombings, and the killing of innocent civilians, posing a direct threat to international stability<sup>4</sup>.

---

<sup>3</sup> Kohlmann (2006)

<sup>4</sup> For al-Qaeda's use of the Internet, see Weimann (2004). For material relating to Al-Manar TV, see Jorisch (2004).

## 2.4. RAISING FINANCIAL FUNDS FOR TERRORISTS / TERRORIST ORGANISATIONS

Terrorists have shown adaptability and opportunism in meeting their funding requirements. Terrorist organizations raise funding from:

- legitimate sources
- criminal proceeds
- state sponsors; safe havens and failed states

Legitimate sources include abuse of charitable entities or non-profit organizations, abuse of legitimate business activities and self-funding.

### **Charities or non-profit organizations:**

- enjoy the public trust, have access to considerable sources of funds and their activities and their activities are often cash-intensive,
- some of them are of international character and provide a framework for national and international operations and financial transactions,
- finally, charities or non-profit organizations are subject to significantly lighter regulatory requirements than financial institutions or other publicly – held corporate entities,

and all these characteristics made charities and no-profit organizations very attractive sources for terrorist financing.

**Legitimate business activities** also can be abused as a source of funds to support terrorism financing. This is a particular risk in sectors which do not require substantial investments. The risk that a business will divert funds to support terrorist activity is greater where the relation between sales reported and actual sales is difficult to verify, as is the case with cash-intensive businesses.

**Self-funding includes** own sources of funds owned by terrorist himself or his family. Own financial assets include savings, credit or proceeds of terrorist's or terrorist's family legitimate business activities. Self-funding can include cases in which a financial facilitator is not directly involved in planning or carrying out an attack.

**Using of legitimate sources is the phenomenon known as «black-washing» where legal funds are diverted for purposes of terrorism.**

**Raising funds from criminal proceeds** is using of financial funds by illegal or criminal activities for the purpose of terrorism financing. The most often criminal activities used by terrorists are arms trafficking, drug trafficking, credit card fraud, cheque fraud, extortion.

**State sponsors, safe havens and failed** are crucial sources for providing support to terrorist organizations.

## 2.5. MOVING TERRORIST FUNDS

There are three main methods by which terrorists move funds or transfer value assigned to terrorism financing:

- use of financial system,
- physical movement of money ( for example, through the use of cash couriers)
- through the international trade system

Often, terrorists and terrorist organizations abuse alternative remittance system (ARS), charities, or other captive entities to disguise their use of these three methods to transfer funds.

**Formal financial system** with its speed and ease with which funds can be moved within the international financial system allows terrorists/terrorist organizations to move funds efficiently and effectively and often without detection between and within jurisdictions.

**The international trade sector** provides terrorists/ terrorist organizations the opportunity to transfer value and goods through seemingly legitimate trade flows.

Using of **physical movement of cash money** is one way terrorists/terrorist organizations can move funds without encountering the AML/CFT safeguards established in financial institutions. Likewise, some terrorist groups have converted cash into other goods such as gold or precious stones in order to transfer it outside of the financial system. It is established that cash couriers are often used to transfer funds in countries within the Middle East and South Asia and in countries where the electronic banking system is not developed, for example in large parts of Africa and Middle East. It is also shown that cash couriers are active even in Europe and between countries with a well functioning financial system. The aim of using cash couriers is to keep money outside the financial system to avoid detection.

In the use of **alternative remittance systems**, stands out hawala system. Hawala is an informal system that is an alternative way of transferring funds that works outside or parallel to traditional banking or other financial channels of transmission of monetary resources.

Abuse of charitable organizations is very common because it allows the use of legitimate financial transactions of such organizations in order to conceal the transfer of funds of terrorists / terrorist organizations. Because of the rather large amount of money and other property in the possession of charities, even the use of a small portion of such funds from charities for terrorist purposes provides substantial support to terrorists / terrorist organizations in their activity.

## 2.6. KEY FINDINGS

Terrorist financing is usually attributed to the prevention of money laundering, which is evident in the international regulatory framework. Namely, the FATF has determined that 9 Special recommendations in conjunction with the 40 Recommendations which are related to money laundering and make up the basic regulatory framework for the prevention and detection of both money laundering and terrorist financing. This stems from the fact that techniques used to launder money are essentially the same ones that are used to finance terrorism. Also, regardless of whether the funds used to finance terrorism derive from legitimate sources, illegal sources or from a combination of both sources, the acts of concealing the source of such funds are always present as only disguised sources allow smooth operation of current and future activities of terrorist financing

Preventing terrorism financing and setting up so called smart obstacles creates a hostile environment for terrorists and terrorist organizations, constrains their overall capabilities and helps to frustrate their ability to execute attacks which constitutes protection of the financial system.

Gathering and sharing financial intelligence on suspicious transactions by banks and other reporting entities have a key role in identifying terrorist financing and detecting funds for funding terrorists in cases of using formal financial system.

Namely, information on transactions, i.e. financial information has come to be one of the most powerful investigative and intelligence tools available. Trail the money leaves when moves through the financial system can raise suspicion on illicit activities, identifies persons involved in financial transactions and locate the criminal proceeds.

The development and application of international standards in prevention and detection of money laundering and terrorist financing within the financial but also within non financial sector, have increased significantly the value of financial information.

Efficiency and the effectiveness of competent authorities in prevention and detection of money laundering and terrorist financing are increased when financial information on transactions are used together with information on counterterrorism.

### 3. CASE STUDIES OF TERRORIST FINANCING TYPOLOGIES FROM INTERNATIONAL PRACTICE (source: FATF: Terrorist Financing)

#### 3.1. USING OF CHARITIES:

##### EXAMPLE 1:

#### **Case study: Exploitation of a legitimate charity**

A suspicious transaction report (STR) was made following an attempt by Individual A, to deposit substantial amounts of cash into the account of a charity – over which he had power-of-attorney – with the instruction that it be transferred onward to a notary as an advance for the purchase of real estate.

The investigation revealed that:

- Payments into the account consisted of multiple cash deposits (presumably donations) but also payments directly from the account of Individual A. In turn, A's personal account revealed multiple cash deposits that corresponded to donations from private individuals.
- The debit transactions consisted of transfers to the non-profit organization (NPO) and international transfers to Individual B. Police sources revealed that A had links with individuals that were known for terrorist activities, including B.
- Law enforcement assessed that the charity, which continues to fulfill an important social function, was being exploited both as a «front» to raise the funds and as a «means of transmission» to divert a portion of them to known terrorist associates of A.

*Commentary:* This case is indicative of the vulnerabilities to exploitation that arise with weak governance combined with high levels of cash deposits.

*Source:* Belgium

##### EXAMPLE 2:

#### **Case study: Charity embedded in terrorist finance laundering network**

An NPO with an office in Russia came to the attention of the authorities through the submission of STRs by credit institutions on an apparent discrepancy between the stated objectives of the NPO and its actual expenditure. The NPO was also known to have a poor history of reporting to the authorities on tax issues.

An investigation revealed that funds were being transferred from the NPO to apparently fictitious or shell entities and then being withdrawn in cash for onward transmission to illegal armed militants.

*Source:* Russia.

## 3.2. ABUSE OF LEGITIMATE BUSINESS

### EXAMPLE 1:

#### **Case study: Diversion of funds from legitimate business**

The personal bank account of Person A ( a restaurant manager) regularly received cheques drawn from wooden pallet Company B, as well as significant cash deposits. The account did not show any «normal» financial activity such as payment for food, travel etc. The bank account of Company B also showed significant cash withdrawals of between EUR 500.000,00 and EUR million.

The bank where A's account was held became suspicious because of the inconsistency between Person A's profession and the nature of Company B's business and submitted suspicious transaction report to the financial intelligence unit. FIU analysis revealed that the individuals concerned were linked to Salafist movements, and the case was referred to prosecutors for wider investigations.

*Source:* France

### EXAMPLE 2:

#### **Case study: Account monitoring reveals terrorist financing activity**

Routine monitoring of the bank account of a locksmith company revealed large-scale flow of funds that was disproportionate to the normal business activity of this kind of company. The company had also issued cheques to individuals involved in organizations defending prisoners detained for terrorist offences.

FIU analysis revealed link between the locksmith company and radical movements; with individuals sending money orders between themselves as well as to prisoners and to other individuals registered in police databases. This prompted wider investigation by judicial authorities.

*Source:* France

### 3.3. SELF-FUNDING

#### EXAMPLE 1 :

##### **Case study: A small, self-funded network launches major attack**

The official report into the 7 July 2005 attacks on the London transport system stated that:

«Current indications are that the group was self-financed. There is no evidence of external source of income. Our best estimate is that the overall cost is less than GBP 8.000. »

«The bombs were homemade, and that the ingredient used were readily commercially available and not particularly expensive.»

«The group appears to have raised the necessary cash (for overseas trips, bomb making equipment, rent, car hire) by methods that would be extremely difficult to identify as related to terrorism or other serious criminality. «

Terrorist A «appears to have provided most of the funding. He had reasonable credit rating, multiple bank accounts (each with just a small sum deposited for a protracted period), credit cards and a GBP 10.000 personal loan. He had 2 periods of intensive activity – firstly in October 2004 and then from March 2005 onwards. He defaulted on his personal loan repayments and was overdrawn on his accounts.»

Terrorist B: « made a number of purchases with cheques (which subsequently bounced) in the weeks before 7 July. Bank investigators visited his house on the day after the bombings.»

*Commentary:* Though Terrorist B was not specifically identified as a terrorist until after an attack took place, this case demonstrates that financial intelligence on its own was sufficiently accurate to prompt investigation by financial institutions.

*Source:* United Kingdom

### 3.4. USING CRIMINAL PROCEEDS

#### 3.4.1. RAISING FUNDS THROUGH DRG TRAFFIKING

EXAMPLE 1:

##### **Case study: Terrorist organization raises money through drug trafficking**

Since 1990, Person A led an international heroin-trafficking organization (the «Organization») responsible for manufacturing and distributing millions of dollars worth of heroin in Afghanistan and Pakistan. The Organization then arranged for the heroin to be transported from Afghanistan and Pakistan into United States, including New York City, hidden inside suitcases, clothing and containers. Once the heroin arrived in the United States, other members of the Organization received the heroin and distributed drugs. These co-conspirators then arranged for millions of dollars in heroin proceeds to be laundered back to Person A and other members of the Organization in Afghanistan and Pakistan. To launder the funds, Person A used several import/export commercial enterprises to wire his funds. Funds were placed in the financial system as proceeds and/or expenses related to those diverse concerns and remitted under that cover.

The Organization was closely aligned with the Taliban in Afghanistan. During the course of their cooperation, the Organization provided financial support to the Taliban. More specifically, between 1994 and 2000, the Organization collected heroin proceeds in the United States for the Taliban in Afghanistan. In exchange for financial support, the Taliban provided the Organization protection for its opium corps, heroin laboratories, drug transportation routes, and members and associates.

*Source:* United States

EXAMPLE 2:

##### **Case study: Terrorist organization financed using proceeds of drug trafficking**

During a drug investigation in relation to cocaine importation from South America to Europe, the FIU found out that the organization involved in the drugs trafficking used money transfers to send funds from the Netherlands to Paraguay and Brazil to invest in drugs and profits to Lebanon. Police investigations indicated that the profits were used to fund a terrorist organization.

*Source:* The Netherlands

### EXAMPLE 3:

#### **Case study: Terrorist organization extorts money from drug traffickers**

An investigation and prosecution carried out by Turkish authorities revealed that drug trafficking is the principal source of funds for a terrorist organization. Drugs are grown in Pakistan, Afghanistan and Iran; and sent from there to Europe, both through known members of the organization, and through their associates and other non-designated militants.

In 2007, more than 10 members of the organization terrorist group were arrested and large amounts of money seized. Investigation and testimony by these members revealed that the organization extorts money from smugglers at points of entry in the North of Iraq in the form of «taxes» worth around 7% of the value of smuggled items. The groups also collect money for each person or each car crossing their «customs points». One such «customs point» earns USD 20.000 – 30.000 per week. One member of the group stated that the most important income for the group is the money collected from drug traffickers as «taxation».

*Source:* Turkey

### **3.4.2. RAISING FUNDS BY CREDIT CARD FRAUD**

#### EXAMPLE1:

#### **Case study: Stolen card details purchased online**

Person A frequented criminal Internet sites that specifically bought and sold credit card information (including shadowcrew.com, investigated by the United States Secret Service in 2003). Stolen credit card numbers were passed to Associate B, and then on to C, a computer expert specializing in facilitating the creation and management of websites that provided forums for extremists and downloads of highly violent material intended to incite attacks.

The associates were later found to be linked, via telephone and e-mail records to a terrorist cell in Bosnia and Herzegovina, and were arrested on the brink of launching an attack.

*Commentary:* The case illustrates how terrorists' need for funds can go far beyond those required to launch specific attacks. In this case, terrorist facilitators fully exploited the opportunities of new technology to acquire funds illicitly and anonymously- extending the distance between their identity and their actions. The case also highlighted how sophisticated forensic skills can be needed to recover financial data.

*Source:* United Kingdom

## EXAMPLE 2:

### **Case study: Credit card fraud**

A North African terrorist funding group accumulated details of nearly 200 stolen cards and raised more than GBP 200.000 to fund al-Qaida terrorist network through international credit card fraud. Twenty to thirty «runners» collected the names and credit card details of almost 200 different bank accounts from contacts working in service industries such as restaurants.

These details were not used in their country of origin (the UK) but sent on to associates in Spain and the Netherlands. These associates used the cards to fraudulently collect more than GBP 200000 for al-Qaida cells around Europe.

Commentary: The case illustrates that the high returns achievable from credit card fraud are not lost on terrorists and that sophisticated arrangements can be put in place to operate a fraud ring linked to terrorism

*Source:* United Kingdom

### **3.4.3. RAISING FUND BY CHEQUE FRAUD**

Several cases have been identified in which a basic model of bank fraud has been applied to generate funds for terrorism. These cases involved bank accounts being opened using false identity documents and fraudulent deposits. Cheque books are then stockpiled; and when a large number have been accumulated, they are used to purchase goods from department stores costing under the amount that would trigger verification to ensure sufficient funds were available in the account. The goods are returned for a cash refund. This activity can be carried out by organized individuals, who draw on cheques from the same account simultaneously in several locations.

Chequebook fraud, which has figure in a number of terrorist finance cases, allows terrorist to raise and move significant amounts of cash quickly. There are often limited preventative measures in place to obviate

## EXAMPLE 1:

### **Case study: Cheque fraud**

A network of North African terrorist used organized, low-level bank fraud against a number of UK banks to raise funds in support of terrorist activity. Using in excess of 50 individuals the group raised at least GBP 550.000 within 120 months. Once raised this money was used to support terrorist training, procurement, travel and subsistence costs incurred by terrorists and extremists across Europe.

*Source :* United Kingdom

### 3.5. USING OF SAVE HAVENS, FAILED STATES AND STATE SPONSORS

#### EXAMPLE 1:

#### **Case study: State sponsorship of the terrorism by the Taliban regime in Afghanistan**

When the Taliban regime swept to power in Afghanistan in late 1996, it became a critical safe haven and source of support for Osama bin Laden and al-Qaida until it was removed from power by international coalition forces following the terrorist attacks against the United States on 11 September 2001.

On 15 October 1999, the United Nations Security Council unanimously adopted Security Council Resolution (UNSCR) 1267 against the Taliban regime in Afghanistan in response to the Taliban's continuing support for terrorist organizations and activity, including providing sanctuary to Osama bin Laden and al-Qaida. In particular, UNSCR 1267 cited the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and planning of terrorist acts, and the safe haven provided by the Taliban to Osama bin Laden and al-Qaida to allow the continued operation of terrorist training camps from Taliban-controlled territory and the use of Afghanistan as a base from which to sponsor international terrorist operations.

UNSCR 1267 also noted the indictment of Osama bin Laden and his associates by the United States for, *inter alia*, the 7 August 1998 bombings of the United States embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania and for conspiring to kill American nationals outside the United States, and the continued refusal of the Taliban to surrender them for trial.

Finally, as noted in UNSCR 1267, the Taliban facilitated the largest production of opium in the world as a means of financing their activities and providing further support for international terrorism and a war effort that devastated the humanitarian conditions of the people of Afghanistan.

*Source:* United States

### 3.6. USE OF FORMAL FINANCIAL SECTOR

#### EXAMPLE 1:

#### **Case study: Terrorist organization uses wire transfers to move money across borders**

A terrorist organization in Country X was observed using bank wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organization used «bridge» or «conduit» accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organization but who were linked to another by kinship or similar ties. There were thus the apparent family connections that could provide justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organization were deposited into bank accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organization's future needs. Alternatively, the money was transferred to other bank accounts managed by the organization's financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organization in its clandestine activities.

*Source: FATF Typologies Report 2003-4*

### 3.7. USE OF TRADE SECTOR

#### EXAMPLE 1:

#### **Case study: Terrorist use of the trade sector to move funds**

An FIU received disclosures from several banks concerning account holders: Person A and B and Company C, all active in the diamond trade. In the space of a few months, A, B and C's accounts saw a large number of fund transfers to and from foreign countries. Moreover, soon after the opening of his account, person B received several bank cheques large amounts in US dollars.

Financial information collected by the FIU showed that Company C was received large US dollar transfers originating from companies active in the diamond industry and debited by several transfers to the Middle East in favour of Person A, a European citizen born in Africa and residing in the Middle East. One of the directors of Company C, a Belgian citizen residing in Africa, held an account at a bank in Belgium through which transfers took place to and from other countries in Europe,

Africa, North America, and the Middle East. Inward transfers from foreign countries mainly took place in US dollars. There were then converted to EUR and used to make transfers to foreign countries and to accounts in Belgium belonging to Person B and his wife.

Police information collected by the FIU showed that the prosecutor had opened a file related to trafficking in diamonds origination in Africa. The largest transfers of funds by the company trading in diamonds were mainly destined to the same person, A, residing in the Middle East. Police sources revealed that both Person A and Person B were suspected of having bought diamonds from the rebel army of an African country and of smuggling them into Belgium for the benefit of a terrorist organization.

Moreover, it appeared that certain persons and companies linked with Persons A and B had already been referred to prosecutors by the FIU in other cases for money laundering derived from organized crime

*Source:* Belgium

### **3.8. USE OF CASH COURIERS**

#### **EXAMPLE 1:**

#### **Case study: Terrorist financing using cash couriers**

The activities of Terrorist Organization A in Southeast Asia clearly show the critical role of cash couriers in support of their terrorist operations. Organization A avoided using the conventional banking system in order to evade safeguards and to avoid leaving an audit trail for law enforcement. The funding for the Bali bombings that took place in October 2002 were provided by Al-Qaida chief of operations to Person H, Organization A's head of operations, who was hiding in Thailand in 2002. Person H passed USD 30.000,00 to the perpetrators of the Bali bombings in two batches using several cash couriers. The couriers took several weeks to complete the runs. The funding for the JW Marriott Hotel bombing in Jakarta was also provided by Person H from Thailand. Again, a total of USD 30.000,00 of Al-Qaida's funds was sent to Indonesia in April 2003 through a string of couriers.

*Source:* Asia Pacific Group (APG) Annual Typologies Report 2003-2004

## BIBLIOGRAPHY:

- FATF-GAFI, Terrorist Financing, 29 February 2008