Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 19-05-2016 / Revisado: 25-05-2016
Aceptado: 25-05-2016 / Publicado: 31-05-2016

CISDE Journal, 1(1), 2016

Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago

Terrorist financing risk: Vulnerabilities in the payment systems

María Julia Martínez Martínez[1]

[1] Analista de riesgos, España

mjulia.martinezmartinez@gmail.com

RESUMEN. Este artículo evalúa el riesgo de financiación del terrorismo en los canales de pago tradicionales. Combatir la financiación del terrorismo es uno de los principales frentes en la lucha contra la actual amenaza yihadista y una prioridad global. Las recomendaciones del ente intergubernamental independiente Grupo de Acción Financiera Internacional (GAFI) son reconocidas universalmente como el estándar en la lucha contra la financiación del terrorismo. La recomendación número 1 establece que los países deben identificar, evaluar y entender sus riesgos en materia de financiación de terrorismo, aplicando un Enfoque Basado en el Riesgo (EBR) que depende de tres factores: amenaza, vulnerabilidad y consecuencia. En este contexto, se estudia el funcionamiento de los canales de pago tradicionales, así como sus vulnerabilidades. Finalmente, se destaca la importancia de disponer de un sistema de pagos eficiente, para evitar la proliferación de las actividades informales y prevenir usos indebidos, como la financiación del terrorismo.

ABSTRACT. The aim of this article is to assess the terrorist financing risk through the traditional payment systems channels. Combating terrorist financing is on the front line against the current threat posed by the jihadi terrorism and a global priority. The inter-governmental body Financial Action Task Force (FATF) recommendations are recognized as the global counter-terrorist financing standard. Recommendation number 1 calls countries to identify, assess, and understand their terrorist financing risks, applying a Risk Based Approach (RBA) which depends on three factors: threat, vulnerability and consequence. Within this context, the way traditional payment systems channels operate is studied, so as their vulnerabilities. Finally, the importance of an efficient payment system is highlighted in order to avoid the proliferation of informal activities and to prevent misuses such as terrorist financing.

PALABRAS CLAVE: Financiación del terrorismo, GAFI, Riesgo, Vulnerabilidad, Sector bancario, Entidades de pago, Sistemas de transferencia informal de fondos, Hawala.

KEYWORDS: Terrorist financing, FATF, Risk, Vulnerability, Banking sector, Money value transfer systems, Alternative remittance systems, Hawala.

1. Introduction

The growing threat posed by some jihadi terrorist groups is one of the most worrisome phenomena for the international community. The great-sized terrorist organizations require a substantial amount of funds for their own subsistence and the security of their own members, they need financing for the acquisition of weapons as well as for fighter training, member recruitment and propaganda diffusion. However, small terrorist groups require less funds, and those who act in solitude need even less. Combating terrorist financing is at the front line when fighting against the current jihadi threat, and therefore it has become a global priority to prevent the access to funds.

The Financial Action Task Force (FATF[1]) is the worldwide reference organization in the fight against terrorist financing. Their recommendations are universally recognized as the standard in the combat against terrorist financing. According to Recommendation number 5, countries should criminalize terrorist financing, and as Recommendation number 1establishes, countries should identify, assess and understand their terrorist financing risks, applying a risk-based approach (RBA), in accordance to the International Monetary Fund (IMF) national risk assessment methodology. In the RBA model, risk is assessed as a function of three factors: threat, vulnerability and consequence. The aim is that countries take measures to mitigate those national risks in a proportional basis.

In this context, all institutions in the financial system, mainly entities, supervisors and markets, should be able to measure their specific terrorist financing risks, according to their particular circumstances, in order to allocate resources efficiently to those fields which pose a higher risk level.

In next section terrorist related terms are defined, according to the FAFT recommendations. Hereafter, recommendation number 1 is analyzed to identify, assess and understand terrorist financing risks, applying the RBA model. Afterwards, the way through which the traditional payment systems channels operate is studied, and the terrorist financing risk in those channels is evaluated.

2. Terrorism and terrorist financing

Terrorism is a phenomenon of a peculiar nature, and consequently conceptualizing the term has been a cause of great controversy (Tofangsaz, 2015). Some people only focus on the mere terrorist attack while others extend the phenomenon to insurgency issues or to territorial claim fights. In order to establish a homogeneous definition, the main difficulties arise when trying to establish the factors which characterize the terrorism itself, such as types of behavior, circumstances and motivations. Furthermore, there is also no consensus on the delimitation of the victims of terrorism, specifically, whether it should be limited to people which have been directly affected by the violent actions, or it should be extended also to people which have been indirectly affected, institutions, nations, or, even, the whole humanity.

In the glossary of specific terms used in the FAFT recommendations (Financial Action Task Force, 2012), the following terrorism and its financing terms are defined:

- Terrorist act: An act which constitutes an offence according to international treaties[2] or which is an attempt to cause death or severe injuries to civilians or people not taking an active part in armed conflicts, when the aim of this act is to annoy the population or to interfere with the decisions of a government or an international organization.
- Terrorist: Natural person who commits terrorist acts, as well as those who attempt, participate as accomplices, organize, run or contribute to commit terrorist acts.
- Terrorist organization: Group of people that commits terrorist acts, as well as those who attempt, participate as accomplices, organize, run or contribute to commit terrorist acts.
- Terrorist financing: Financing of terrorists, terrorist organizations or terrorist acts.

[1] Financial Action Task Force (FATF). www.fatf-gafi.org

FAFT is an inter-governmental body that was born in 1989 with the mandate to establish standards and promote the implementation of policies to fight against money laundering, terrorist financing, and the financing of weapons of mass destruction, among other threats.This implies identifying vulnerabilities in order to protect the international financial system from improper use. In 1990, the Forty Recommendations were developed, as a measured framework to be implemented when combating the misuse of the financial system by drug money launderers. Afterwards, in 1996, given the scale and complexity of the new money laundering financial engineering techniques, those recommendations were revised and their scope was expanded to incorporate the laundering that resulted from other criminal activities. In the aftermath of the events of September the 11th, in October 2001, FAFT developed Eight (at a later stage expanded to Nine) Special Recommendations on Terrorist Financing. The Forty Recommendations and the Nine Special ones merged into the new Forty Recommendations in 2012. The review and update of those recommendations results from the cooperation of FAFT with several Regional Institutions, as well as other observer organizations, such as the United Nations, the World Bank and the International Monetary Fund. At present, FAFT recommendations are universally recognized as the standards to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction. The recommendations have been endorsed by more than 180 countries, which have committed to implement in their national jurisdictions, although they have to be adapted to their own specificities.

Recommendation 5 FAFT states that countries[3] should criminalize terrorist financing, according to article two on the International Convention for the Suppression of the Financing of Terrorism. The terrorist financing offence shall:

- include either the financing of terrorist acts or the monetary contribution to terrorist organizations, groups and individuals, even when there is no a direct link to specific terrorist acts;
- extend to any person who deliberately provides or raises funds, both directly and indirectly, with the purpose of financing specific terrorist acts, as well as for other uses by individuals, organizations or groups which are related to terrorism;
- consider that the sources of funding may be either legitimate or illegitimate;
- qualify similarly the attempt of terrorist financing, the organization, the participation as an accomplice and any action which contributes to commit such a crime.

Combating terrorism is ineffective when it is outlined in isolation and within the individual national legal frameworks. It is incomplete when Law-Enforcement Agencies, together with Intelligence Services, focus only in the identification of those individuals who are prepared to take action imminently. Terrorist threat is a challenge which affects society as a whole: public institutions, the private sector and civil society.Within the security and defense terms, the situation has led to the development of an integral security concept, a goal shared by all of us, which is the basis[4] for society to develop, to preserve its freedom and prosperity, ensuring its stability and the proper functioning of institutions. Combating terrorism is a joint effort for all of us, that is, a process incardinated in the national strategies, which considers security as a public good of the highest priority.

2 The international treaties are: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for 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 (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005), International Convention for the Suppression of Terrorist Bombings (1997) and International Convention for the Suppression of the Financing of Terrorism (1999).

3 Terrorist financing constitutes an offence in Spain according to article 576 of the current Penal Code.

4 Law 36/2015, of 28 September, national security.

Combating terrorism requires international cooperation. It is more effective when it reaches an international dimension. In addition, it requires the involvement of the financial system as a whole; including supervisors, financial institutions and Designated non-financial Businesses and Professions[5] (DNFBPs), who establish the mechanisms to detect monetary flows linked to terrorism. Therefore, the fight against terrorism is more effective when one of the strategic objectives is to combat its financing. The financial system has to participate as a whole at the tactical level, implementing prevention measures, as well as at the operational level, preventing that isolated monetary flows could either finance terrorist acts and be used by terrorist organizations, groups or individuals.

3. RBA Model for the assessment of the terrorist financing risk

The RBA approach (Financial Action Task Force, 2007) proposes an assessment risk system (Financial Action Task Force, 2013b) for countries, financial institutions and DNFBPs on the basis of some key elements or identified risk factors. According to this approach, terrorist financing risk is determined upon three factors: threat, vulnerability and consequence.

The threat is an object, activity, individual or group with the potential of causing damage. As reported in the Annual Report of National Security 2014, the terrorist threat is an international and multiform phenomenon, which is able to innovate, to create new forms and ways and to be adapted to the new national preventive measures.Thus, martyrdom actions have been widely spread amongst the new terrorist organizations. This implies a reduction in the number of fighters who have to be replaced. They spend a lot of resources on propaganda and dissemination of information, apart from the fact that some of them have their own mass media. Furthermore, they use narratives addressed to groups of dozens of thousands supporters. At first, they spread explicit calling messages appealing to religion, which mainly reached the most marginalized segments of society. But they are muting and very quickly moving to a new reality, based on a strict Darwinian sense. The religious ideal is not called upon any more, but it has been replaced with the idea of a hero. The new targeted segment is the adolescent population, thus taking advantage of the typical psychological instability of that age. Threat is a concept which has been redefined in geopolitical terms during the last decades. In order to determine the threat, a broad diversity of actors who interact jointly must be taken into consideration: both countries and non-state actors, such as terrorist groups, organized crime frameworks, private companies and the civilian population. The current threat scope is transnational while in the past it was restricted to specific geographical locations. Although it is difficult to determine the future threats, what is certain is that terrorism is a phenomenon which requires continuous monitoring. The more the threat is understood, the better the contribution to the terrorist financing risk can be determined.

Vulnerability comprises the group of objects, activities, individual or groups, whose weaknesses could be exploited by the threat to support or ease its activities.

Consequence is the impact or damage which could be caused by a terrorist activity on the civilian population, business networks, national and international interests, as well as on the financial system, its reputation and that of its institutions. The terrorist acts' consequences are assessed in compensatory terms. The severity of the destructive impact on damaged infrastructures is estimated according to their cost of reconstruction. Regarding personal damage, claims criteria are applied, cross referencing them with the actuarial tables of expected mortality. In order to determine the impact over the financial system and the economic structures, eventual economic losses are estimated. It may be possible to calculate an amount in monetary terms, as the sum of losses from diverse nature, including the cost of human death. However, the consequence of a terrorist actcould never be measured, as the value of a human life is immeasurable.

The current terrorist threat is a worldwide challenge. Consequently, combining threat, vulnerability and

[5] The Designated non-financial Businesses and Professions are casinos, real estate agents, dealers in precious metals and precious stones, lawyers, notaries, other independent legal professionals and trust and company services providers.

consequence in a terrorist financing risk assessment model such as RBA provides benefits for the three main involved actors. First, for public institutions as state actors, since they take their political decisions on security and defense terms. Second, for private companies as non-state actors, which take their commercial decisions within an economic intelligence context. And finally, for the civilian population, concerned for its own safety, who has experienced a growing awareness of the terrorist threat, especially the jihadi one.

4. Traditional payment system channels

In the financial system, a great number of commercial transactions are channeled. Among these, there are different types of transactions that contribute towards terrorist financing; hidden flows for illicit activities but also legitimate and illegitimate transactions with concealed links to terrorism financing.

Financial institutions and other intermediate agents are necessary subjects in the payments resulting from economic activities, especially when transactions of significant value are involved or when a direct or face to face transaction is unfeasible due to the physical distance between the sender and receiver. The intermediates, who are named obliged entities under the Spanish legal framework, must establish preventive and control procedures in order to avoid being used in money laundering activities and, mainly, in flows linked to terrorist financing. The level of exposure to the terrorist financing risk is quite different among the obliged entities. It depends on qualitative and quantitative factors, which are directly linked to the nature of thespecific activities in every type of entity.

Currently, funds are transferred and a large variety of financial assets are managed through different channels or payment systems, in which several institutions are involved. On the one hand, institutions which order transfers of financial assets on their own account or on behalf of their clients (payment originators) and, on the other hand, the institutions which receive those financial assets on their own accounts or on behalf of their clients (payment beneficiaries). Transactions flow through channels; direct transactions from institution to institution, as well as other transactions which require a third intermediate institution to settle the transaction in a correspondent account. The prevention and control procedures in the payment systems are complex, considering the significant amount of transactions which are processed. Specialized software tools are needed to detect flows linked to either money laundering or terrorist financing.

Moreover, apart from some isolated areas, most of the world population carries out economic activities which require the participation of the financial system to a greater or lesser extent. Implementing preventing measures which jointly involve financial institutions, payment systems and supervisors is the most effective way to detect suspicious transactions in which persons linked to terrorism are taking part. The profile of those persons may be highly diverse: terrorists integrated in a solid group, terrorists who are parts of small cell structures, recruiters attempting to attract new supporters, fighters in their return, fund raisers, funds suppliers, sympathizer…Nevertheless, preventive measures should be able to distinguish between persons who intentionally misuse from those who inadvertently participate, as their aim is merely to provide funding for charity purposes, for instance zakat mandatory begging or voluntary charity acts, such as waqf or sadaqah.

Terrorists groups are organized according to their own needs, which are very diverse. From a functional point of view, terrorist organizations or groups have differing requirements depending on their own organizational frameworks: structures composed by a significant number of geographically grouped members (as in the case of Boko Haram), dispersed structure formed by semi-independent franchises (Al Qaeda), organizations who run a territory where a pseudo-state (Daula Al Islamí or better known as Daesh) intends to be established, small cells composed by a small number of people, lonely wolf, recruiter,… Their financial needs depend on their organizational structures.

The great terrorist organizations require a considerable amount of funds, for their own subsistence and the security of their own members. They need to finance weapons acquisition, fighters training, recruitment and propaganda diffusion. In most parts of the developed world, control procedures have been established by

financial institutions and traditional payment systems in order to detect flows linked to terrorist financing, within what is called the AML/CFT preventive measures: AML Anti Money Laundering and CFT Countering the Financing of Terrorism. The great terrorist organizations have had to evolve, adapting and taking advantage of the vulnerabilities of the new payment systems, which have emerged thanks to the new technological innovations are significantly widespread. They have enough resources to hire specialized professional services, which offer them the opportunity to keep transferring funds while not being detected by the financial system control procedures. Software tools do not always have the flexibility to be able to respond to the latest developments in order to prevent those terrorist organizations from being financed.

However, small terrorist groups and those individuals acting in isolation often lack the necessary resources, knowledge and opportunity to access these new services. Consequently, they tend to continue using the traditional payment systems.

According to a FAFT report (Financial Action Task Force, 2015), in the past transactions have been detected in which beneficiaries were local extremist groups who received funds from international terrorist organizations. However, Daesh seems to be an exception, due to its ability to raise considerable amount of funds within it its territory without requiring any external financing. Nevertheless, it has received a relatively small quantity of funds from external sources. These transactions, according to the same report, in addition to cash, the foreign terrorist fighters[6] (FTFs), have been predominantly been carried out using the traditional payment systems, that is, their banking current accounts (mainly withdrawing cash from automatic teller machines) as well as wire transfers through Money Value Transfer Services (MVTS).

In the following sections, the financial terrorism risk in the traditional payment system channels is analyzed, which consist of transactions through formal systems (banking transfers and MVTS remittances) and informal systems (the most commonly known are the Hawala).

4.1. Banking sector transfers

Transactions in the banking sector flow through financial structures interconnections by multilateral systems interconnections, ensuring that the processing, clearing and settlement systems take place. The payment systems and the securities clearing and settlement systems are the main infrastructures of the financial markets in which the banking sector intervenes.

TARGET2 is the European gross settlement system owned by the Eurosystem, whose legal structure is a set of national systems operating in a centralized way. 1.007 institutions are directly involved and other 837 indirectly involved (Bank of Spain, 2015). TARGET2 has extended its scope to be connected to Securities transaction system in June 2015. TARGET2-Securities T2S connection implies the European integration of both payment systems and securities clearing and settlement systems. The European payment systems operate under the Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO[7]) principles, which mainly concerns Systemically Important Payment Systems (SIPS). A payment system is considered a SIPS when at least two of the following four criteria are met: financial impact (the total daily average value of processed payments exceeds 10.000 million euros), market share (at least one of the following criteria: 15% of the total volume of euro-denominated payments, 5% of the total volume of euro-denominated cross-border payments or 75% of the total volume of euro-denominated payments at the level of a member state whose currency is the euro), cross-border relevance (it involves five or more countries other than the SIPS operator and it generates a minimum of 33% of the total volume of euro-denominated payments) and direct interdependence (it provides services to other infrastructures).

[6] According to Resolution 2178 (2014) adopted by United Nations Security Council, foreign terrorist fighters (FTFs) are "individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training".

[7] The International Organization of Securities Commissions establishes standards in securities markets. It has a permanent secretariat based in Madrid. It regulates more than 90% of the world's securities markets.

TARGE2-BE is the Spanish part of the European system for processing high-value payments. It is number five in the ranking by number of transactions and the fourth in terms of volume behind Germany, France and The Netherlands. It has sufficient relevance and weight to be considered a SIPS. It processed 7,2 million transactions totaling 62 billion euros value in 2014. The National Electronic Clearing System (SNCE) is the Spanish retail payment system, which processed 1.688 million transactions totaling 1,5 billion euros in 2014.

The banking sector transfers funds in the most reliable and efficient way, but it is at the same time vulnerable to misuse. Henceforth, each financial entity should establish their own control procedures, within the AML/CFT preventive measures, in order to detect suspicious flows within the millions of transactions which are processed in their systems.

Financial institutions which operate in the Spanish banking sector must establish an Internal Control Body[8] (ICB), which is the unit responsible for the application of the policies and procedures regarding due diligence[9] for the purpose of preventing and deterring transactions linked to money laundering or terrorist financing. The due diligence measures include customers identification procedures (formal and real beneficiaries), as well as an understanding oftheir activities, including the source of the funds that customers are channeling through the institution. Internal control measures must be established in accordance with the level of risk exposure inherent to the nature of the institution's activities. Risk assessment depends on objective elements, such as "the sector in which it operates, the size of the business, the number of employees, the geographical areas in which it works, the payment methods and where they come from, the countries involved in the transactions, the use of agents in transactions, etc." (Sepblac, 2013). The aim of this internal assessment is to define the adequacy of their policies, procedures and manuals.

In addition, the ICB must actively participate in the decision-making process at the development phase of the computer systems involved in the detection, management and resolution of unusual transactions, as well as the appropriate alerts by typology, customer and transactional amount, adapting them to the specific risk-based activity of the institution. Those computer developments should mitigate the risk of channeling transactions linked to illicit activities in general and terrorist financing in particular. Furthermore, the systems must comply with the obligation to verify that customers and their counterparts are not included in the sanctions lists. The systems must be able to automatically block transactions that involve a listed person unequivocally. In the case of transactions that have already been processed, the systems should be able to cancel or reverse them. There must be a technical unit which include appropriately trained full-time experts, in accordance with article 35 Royal Decree 304/2014 of 5 May, implementing Law 10/2010, of 28 April, prevention of money laundering and terrorism financing.

Banking system customers can channel financial flows through international financial systems quickly and easily. This provides criminal groups with an opportunity to execute their financial activities, which are unnoticed in the normal and usual transactions. It is difficult to detect small magnitude terrorist financing transactions in the banking sector amongst the immensely large number of legitimate transactions that are processed on a daily basis. However, the AML/CFT preventive measures, which have been implemented in the banking sector, makes the improper use of the financial system more difficult for canalizing illicit activity transactions in general and terrorist financing flows in particular. Nevertheless, certain risks still remain. Traditional financial instruments may still be misused. For instance, bank accounts which have been opened by sympathizers of a terrorist group and the associated card has been delivered to members of this terrorist group to allow them to withdraw cash money from automatic teller machines in either national or international banks (Financial Action Task Force, 2015). Another example, which is also a matter of concern for FAFT is that Daesh might be using Iraqi or Syrian bank branches, as well as any other financial institution to transfer funds abroad as a payment to buy weapons or any other goods to keep on operating (Financial Action Task Force, 2015).

8 Chapter IV – Internal control, Law 10/2010, of 28 April, prevention of money laundering and terrorism financing.

9 Chapter II – Due diligence, Law 10/2010, of 28 April, prevention of money laundering and terrorism financing.

4.2. Money or Value Transfer Services

The Migrant Remittances are the payments carried out to the immigrant'scountry of origin as savings generated when undertaking economic activities in the country of residence. Migrant population coming from countries with a tradition of a high banking usage (Europeans, Americans, Canadians,…) order their remittances through the banking system, while migrants from countries with a limited banking usage (South Americans, Asians and Africans) tend to use other type of financial intermediaries.

The main non-banking financial intermediates are the Money Value Transfer Services (MVTS). According to the Spanish legal framework, MVTS are obliged entities, and therefore they must establish control procedures in the AML/CFT prevention measures, in order to avoid processing transactions linked to money laundering or terrorist financing. They must establish an Internal Control Body (ICB) who should be responsible for applying prevention policies and procedures adapted to the specific circumstances of this type of entity.

According to the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offence Typology Report (Sepblac, 2008b), the MVTS are characterized by: (1) a wide agent framework in whose commercial establishments (known as locutorios) there could be other non-financial economic activities carried out simultaneously; (2) the nationality of the agent or the proprietor frequently coincides with that of their clients; (3) funds are channeled in aggregated amounts through accounts settled in correspondent banks, without providing details regarding individual payments information; (4) their own dynamics facilitate that agents could be recruited to joina criminal organization, in order to get control of sender and beneficiary clients in occasional transactions. As the agents have an extended degree of autonomy in managing their activities, they have the capacity to alter some information in specific transactions, which makes them more difficult to be detected by the ICB. Consequently, this is a channel specially exposed to money laundering. The foreign exchange and wire transfer establishments have been used by criminals to launder money in different ways (Sepblac, 2008a). However, some measures have been taken in Spain during the last few years, mainly an increase in the supervisory inspections. These have resulted in a purging process in this sector (Financial Action Task Force, 2016), whose main consequences are: (1) the disappearance of several MTVS, (2) an overall improvement in the control procedures in those MVTS which remain in operation, (3) the creation of a database of agents whose activity has been considered suspicious, and (4) a significant reduction in the monetary flows from illegal origin through this sector.

On the whole, MVTS are highly vulnerable to terrorist financing, especially when they may be misused by agent counterparts who are located in areas of proximity to conflicts, where the access to banking services is quite limited. Some of those counterpart agents are neither legally regulated nor subject to appropriate AML/CFT supervision, operate without license (so then there is a lack of AML/CFT preventive measures) or are associated with Alternative Remittance Systems (ARS) agents; all without the knowledge of the ICB.

Nevertheless, the MVTS highest risk becomes when one of its agents (or an employee in the establishment) transfers funds on behalf of a terrorist group by counterfeiting the transactional documents. Taliban are believed to have used the banking sector to launder drug trafficking proceeds, but they returned to the use of MVTS when stricter banking rules were implemented in Afghanistan (Financial Action Task Force, 2013a). There are also reports about the usage of MVTS to provide funds to FTFs recruitment and help them cover travel costs to the areas of conflict (Financial Action Task Force, 2013b).

4.3. Alternative Remittance Systems

The Informal Fund TransferSystems (IFTS), better known as Alternative Remittance Systems (ARS) were born as a result of the need for financial instruments in the ancient trade routes, due to the danger of bearing gold or any other form of payment instrument. In order to avoid losing the proceeds while travelling, traders used the rudimentary services provided by those early financial intermediates. They were widely used in East Asia and they are still in use under various names (El Qorchi, 2002): Fei-Ch'ien in China, Padala in Filipinas,

Hundi in India, Hui Kuan in Hong Kong and Phei Kwan in Thailand. IFTS became less relevant after the birth of modern banking. However, the recent migratory flows from East Asia and Africa to Europe, United States, Canada and Gulf regionhave given those systems a renewed impetus. The Hundi (better known as Hawala) is the IFTS most worldwide used, in which funds are transferred by hawaladars (service providers or agents), regardless of the nature, country of origin or destination of the transaction.

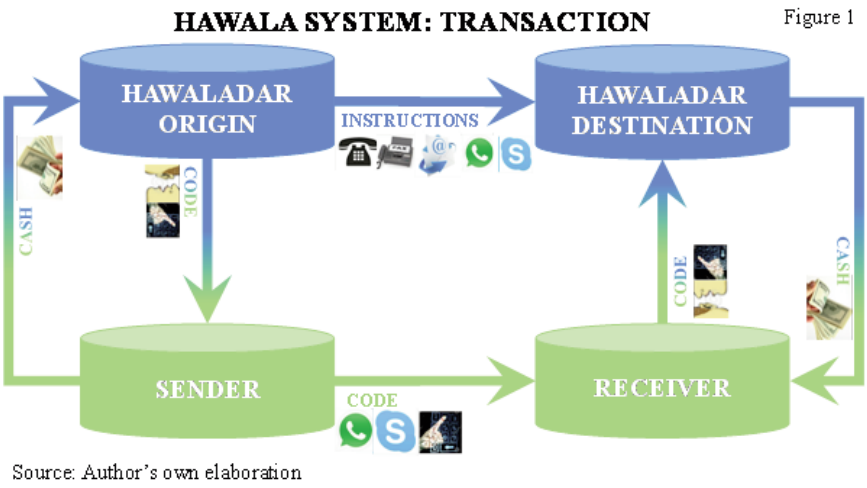

Figure 1. Hawala System: Transaction. Source: Author's own elaboration.

In the Hawala system, the sender gives the amount in cash to the sending hawaladar, receiving a transactional code in return. This sending hawaladar sends the payment instructions (such as the amount and transactional code) to the destination hawaladar by telephone, fax, mail or any other mean of communication. Meanwhile, the sender provides the beneficiary with the transactional code by their usual means of communication. The destination hawaladar will give the money to the recipient upon the presentation of that transactional code.

The hawaladars operate outside of the financial channel regulations. They record their transactions by making a note in a book registry. The transactions do not imply physical movement of flows, as they are simply settled by clearing balances. As a consequence, financial flows among hawaladars are only small portions of their turnover.

Hawala users prefer these providers to banks or any other formal systems because hawaladars provide the following benefits:

¬ They are cheaper: Commissions are lower, as they are not obliged to fulfill the bureaucratic requirements which are demanded by the regulated financial systems to process transactions. Besides, unlicensed agents pay no taxes, as fiscal authorities only demand tax burden on legal financial intermediates.

¬ They are faster: Due to the simplicity of the mechanism, money is transferred in less than 24 hours, even if the origin or destination is located in a remote area, hundreds of miles away from the nearest conventional financial operator. The Hawala user's availability usually does not coincide with the banking business hours or other formal systems commercial opening hours. Similarly, the hawaladars do not have the abovementioned limitations, as their working times are flexible and adapted to the particular circumstances of their clients.

¬ They have social advantages: Users normally do not trust bank employees or formal system agents as much as their hawaladar, given that they usually have an ethnic link, a family connection or a personal relationship. When there is mutual trust, it is possible to advance payments, which means that the destination hawaladar provides the beneficiary with the funds even before the sender gives the money to the originator hawaladar.

¬ They have cultural advantages: Hawaladars share with their users the same cultural links and respect the social codes. An example occurs when the recipient is a woman whose tradition or religion prohibit any contact apart from family members. To provide her with those funds, the hawaladar would use a socially acceptable intermediary, which would avoid her to contact the outside world, especially bank employees who could force her to identify herself by showing her face.

¬ They have less restrictions: The AML/CFT prevention systems have increased controls, decreased the transactional threshold (limited amounts in specific risk transactions) and increased the requirements for sending funds to certain countries. Therefore, the use of conventional channels is quite complex, even for migrants trying to send part of their legally obtained salaries to their families, which still reside in countries with high levels of risk especially those located near the conflict areas. Moreover, conventional institutions are inaccessible to those irregular migrants who want to hide their situation as illegal residents. Furthermore, some entities may establish restrictive policies, explicitly avoiding fund transfers to certain areas or even not authorizing transactions involving senders or beneficiaries from a specific nationality. The hawaladar removes all those obstacles that users experience when usingthe conventional systems.

The costs, the restrictions and the slow and inefficient functioning of the conventional institutions have contributed to the development and spreading of the IFTS, which connect financially a wide area of the world where there is neither regulation nor control.

It is quite complex to regulate the IFTS functioning, as it would imply a uniform legal framework, which is not feasible due to the quantity and diversity of existing jurisdictions. IFTS are prohibited in some countries, since regulation would imply legitimization. However, a restrictive regulation in those countries where they are legally accepted would eventually cause higher opacity in the transactions. Hawala and other IFTS have been used by terrorists for channeling their financial transactions (Financial Action Task Force, 2013c). Therefore, monetary authorities and financial supervisors should focus efforts in preventing the IFTS to be used in money laundering or terrorist financing.

Currently, the IFTS remain vulnerable to be misused for terrorist financing as:

¬ They lack supervision: Insufficient supervision resources and the absence of supervisory determination coexist in some jurisdictions.

¬ They operate under a settlement system: Transactions are cleared and settled by unregulated financial channels established between different jurisdictions. Consequently it is difficult for the financial authorities to bear the full liability.

¬ They operate through agents: Agents often coordinate their hawaladar work with the management of any other type of business, so it is difficult to define their dedication to each activity.

¬ The nature of the transaction: Payments of different nature are cleared: (1) licit flows, (2) illicit flows from criminal activities, and (3) flows with either licit or illicit origin whose final recipients or beneficiaries are persons related with terrorism.

Some of the known cases in United States which have used the Hawala system for terrorist financing are (Financial Action Task Force, 2013c): Hamza Case, Time Square Bomber Case and Carnival Ice Cream Case.

There are also known cases in Spain that have used the Hawala system for terrorist financing (Financial Action Task Force, 2013cand Lombardero Expósito, 2015):

¬ Judgment National Court, Criminal Division, number 6284/2006: "It is accredited that the accused exercised Hawala functions. The accused claims to be responsible for Hawala system in Spain, so as to be part of a higher order structure which is monitored by others".

¬ Judgment Supreme Court, Division II, number 4947/2007: "The accused managed a locutorio, where relevant monetary flows were carried out, such as deposits and transfers, he was responsible for a Hawala network in Spain and there were at least to accredited payments for financing terrorist activities".

¬ Judgment Supreme Court, Division II, number 2754/2008: "It is analyzed an alleged transfer of funds through the Hawala system by two Pakistani from locutorios located in El Raval neighborhood".

¬ Judgment National Court, number 2591/2010: "The accused moved funds through a hawaladar to Algeria on behalf of terrorist groups through money transfer systems".

¬ Judgment National Court, number 1943/2011: "The accused financed the escape of some terrorists who had participated in the 2004 Madrid attacks, providing them accommodation and financing their travelling expenses".

5. Conclusion

Jihadi terrorism is one of the phenomena of serious concern to the international community. Facing the threat posed by terrorism tackles a challenge both in security and defense terms. In the last few years, the situation has led to the development of the integral security concept, as a goal and an effort shared by all of us, public institutions, private sector and the civilian population. What is more, international cooperation related with this item has been improved.

One of the key reasons of the expansion of terrorist groups is their capacity to obtain a substantial amount of economic resources. Being aware of that situation, strategies addressed to combat the terrorist threat take into account fighting against their financing resources.F or this purpose, the involvement of the financial system is required, whose institutionsare able to establish the mechanisms to detect monetary flows linked to terrorism. The aim is to prevent monetary flows from financing eventual terrorist acts or from being misused by terrorists, terrorist organizations or terrorist groups.

A large number of countries have accepted to implement the FAFT international standards, although they have had to adapt them to their own specificities. This implies assessing their own national risks, as a function of the terrorist threat, their systems vulnerabilities and the terrorist consequences. Research and analysis of the terrorist threat, as well as of its consequences has been sufficiently studied in both the security and defense professional fields and the scientific and academic fields. Therefore a closer study of the vulnerabilities is most needed. For this reason, all the institutions in the financial system (entities, supervisors and markets) have to undertake an internal detailed review for the purpose of detecting their own vulnerabilities. This is an essential prerequisite to quantify their terrorist financing risk, whose purpose is adequately allocate resources in order to mitigate such risk.

Financial flows are channeled through payment systems. The way through which traditional payment systems channels operate has been studied, as well as banking transactions, MVTS and the ARS, such as the Hawala system. Both the banking sector and the MVTS have implemented internal control bodies, who are responsible for internal regulation and policy application related toterrorist financing. Since the implementation of such bodies, there has been a considerable risk reduction in those channels used for terrorist financing,

although additional measures may still be taken to mitigate the risk even further.

However, some traditional payment systems remain vulnerable, in particular, the ARS, such as the Hawala system, which could be misused by terrorists for their financial transactions. ARS regulatory policies would be quite complex, and they would result in a higher level of opacity.

Henceforth, it is fundamental that efforts focus on encouraging the utilization of formal payment systems, at the expense of the informal ones. An appropriate and efficient payment system, less vulnerable and with lower costs, will prevent informal activities from developing. It will also contribute to prevent misuses, such as terrorist financing. Simultaneously, it is essential to avoid any eventual traditional payment system funding reduction, both formal and informal, implying the transfer of funds to the new payment products and channels, such as virtual currencies, prepaid cards and Internet-based payment services. The widespread use of these methods involves a newset of risks, whose assessment exceeds the scope of this article and deserves greater study.

Cómo citar este artículo / How to cite this paper

Martínez, M. J. (2016). Riesgo de financiación del terrorismo: Vulnerabilidades de los canales de pago. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 66-78. (www.cisdejournal.com)

References

Banco de España (2015). Memoria anual sobre la vigilancia de los sistemas de pago 2014. Madrid.

El-Qorchi, M. (2002). Hawala ¿Cómo funciona este sistema de transferencia informal de fondos? ¿Debe ser regulado? Finanzas & Desarrollo.

Financial Action Task Force (2007). Guidance on the risk-based approach to combating money laundering and terrorist financing: High level Principles and Procedures. FATF, Paris.

Financial Action Task Force (2012). International standards on combating money laundering and the financing of Terrorism & proliferation. FATF, Paris.

Financial Action Task Force (2013a), Financial flows linked to the production and trafficking of Afghan opiates. FATF. Paris.

Financial Action Task Force (2013b). National Money Laundering and Terrorist Financing Risk Assessment. FATF. Paris.

Financial Action Task Force (2013c). The role of Hawala and other similar service providers in money laundering and terrorist financing. FATF. Paris.

Financial Action Task Force (2015). Emerging Terrorist Financing Risks. FATF. Paris.

Financial Action Task Force (2016). Money or Value Transfer Services. FATF. Paris.

Law 10/2010 (2010). Of 28 April, prevention of money laundering and terrorism financing.

Lombardero Expósito, L. M. (2015). El nuevo marco regulatorio del blanqueo de capitales. Bosch, Barcelona.

Presidencia del Gobierno. Departamento de Seguridad Nacional (2014). Informe anual de Seguridad Nacional 2014.

Royal Decree 304/2014 (2014). Of 5 May, implementing Law 10/2010, of 28 April, prevention of money laundering and terrorism financing.

Sepblac (2008a). Factores clave para la prevención del blanqueo de capitales en la gestión de transferencias. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/La_gestion_de_transferencias.pdf)

Sepblac (2008b). Tipologías de blanqueo de capitales. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/informe_sobre_tipologias.pdf)

Sepblac (2013). Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo. Madrid. (http://www.sepblac.es/espanol/informes_y_publicaciones/documento%20_recomendaciones_sobre_medidas%20_control_interno_PBCFT.pdf)

Tofangsaz, H. (2015). Terrorism or not terrorism? Whose money are we looking for? Journal of Financial Crime, 22(3), 378-390.