# General Assembly 1

## Implementing measures to trace and prevent terrorism financing

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Daan de Klein

| | |
|---|---|
| **Forum** | General Assembly 1 |
| **Issue:** | Implementing measures to trace and prevent terrorism financing |
| **Student Officer:** | Daan de Klein |
| **Position:** | Deputy President |

## Introduction

Not many of us ever think: “How did the terrorists pay for their attack?” However, it is a valid question to ask as terrorists do need the means to pay for their attacks as they aren't free. The first thought is that everyone in a cell contributes to the attack and that they are self-funded. This is far from true, as terrorists are paid a salary, and the attacks are funded by central command. All of this means that we can cut terrorist funding to be able to proactively prevent attacks.

This is especially true as one al Qaeda operative once said, “There are two things a brother must always have for jihad, the self, and money.” If a terrorist organization is not able to sustain itself financially, it cannot operate. However, how does one cut funding from terrorist organizations? This can be done in either of two ways, Stopping the source of money and seizing it while it is moving. Sadly terrorist attacks are inexpensive, so deep cuts have to be made, requiring extensive international cooperation.

## Definition of Key Terms

### Terrorism

Terrorism is “The unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims.” (Oxford Languages) Examples of prominent terrorist groups are Al Qaeda which was behind the September 11 attacks, the Taliban, which is currently in control of Afghanistan, and Islamic State (IS), which has played a part in the wars in Syria and Libya.

### Money Laundering

Money Laundering is the act of making proceeds from a profit-making crime seem as if they are coming from a legitimate origin. A Basic example of money laundering would be claiming that the proceeds from a bank heist came from a long-lost relative.

### Terrorist Financing

Terrorist Financing is “the provision, collection, or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism or any act intended to cause death or serious bodily injury.” (Central Bank of Ireland)Terrorist financing is very similar to money laundering. However, the funds could be coming from anywhere, including legitimate sources like donations. So to some extent, terrorist financing is the opposite of money laundering, as clean money is used for illegal activities.

### Money Service Business (MSB)

According to the United States Department of Treasury Financial Crimes Enforcement Network (USDT FinCEN), A MSB is “any person doing business, whether or not regularly or as an organized business concern, in one or more of the following capacities: Currency dealer or exchanger, Check casher, Issuer of traveler's checks, money orders or stored value, Seller or redeemer of traveler's checks, money orders or stored value, Money transmitter, U.S. Postal Service.” (USDT FinCen)

### Jihad

“A struggle or fight against the enemies of Islam” (Oxford Languages)

### Tax Haven

“A tax haven refers to a country or jurisdiction that enables multinational corporations and individuals to escape the rule of law in the countries where they operate and live and to pay less tax than they should in those countries.  tax haven can also refer to jurisdictions that specialize in enabling individuals to hide their wealth and financial affairs from the rule of law, more than in enabling multinational corporations to shift tax out of the countries where they operate to pay less tax.” (Tax Justice Network)

### Zakat

Zakat is one of the five pillars of Islam. It is a compulsory tax that is mandatory for all Muslims. Zakat is required to be paid by people who meet a certain threshold and is redistributed to those in need.

# General Overview

## How do Terrorists Earn Money

Terrorists need to raise funds to be able to carry out attacks and sustain day-to-day operations like logistics and recurring costs, as terrorist organizations surprisingly work similarly to normal companies in the way that they need to pay their bills and workers. However, terrorists also tend to earn part of their money in more unethical ways. Terrorists earn money via a variety of non-legal methods, including human trafficking.

As someone with a Western perspective, it seems unimaginable that any Westerner would voluntarily join ISIS or any other terrorist organization, as we are often on the receiving end of terrorist attacks and live to see the consequences of these awful attacks. However, terrorist groups like ISIS have started using deplorable tactics similar to the grooming of minors in the recruitment of young Western women.[1]

ISIS recruiters target women in vulnerable positions, making them more susceptible to trafficking. Vulnerable positions may include people that do not have a stable living situation, are a victim of domestic violence, have family members who (have) abused (ed) substances or abuse substances themselves, are in the foster care system, or have run away from parents, illegal immigrants, people with economic difficulty and people who have been in contact with previous sexual abuse.[2] After ISIS finds an individual that meets one or more of these circumstances, they contact them using one of the many ISIS-affiliated social media accounts on the internet and promise these women a glorious life in an Islamic State where they are presented with a romanticized view of living with a Jihadi man. Recruiters also use grooming tactics on these women, like befriending them and telling them they are loved while showering them with compliments leading to a false trust. Victims of grooming don't recognize themselves as such. They genuinely think that they are going to be with a man that loves them even though often the opposite is true.

[1] See the 6 stages of grooming: https://www.albertacacs.ca/blog/stages-of-grooming

[2] More Characteristics of people vulnerable to human trafficking: https://polarisproject.org/vulnerabilities-and-recruitment/

Women are often placed in the role of domestic servitude and are often passed from one man to the next without having any freedom to do what she wants as well. However, in the worst case women as young as 14 are placed in prisons and face mass rape by multiple men every day and are sold off as sex slaves for as little as twenty-five dollars. Women may also be forced to participate in the terrorist organizations' schemes as expendable assets, and if they refuse their instructions, they will be executed with one report saying, “One girl refused, and the instructors reported that she had been eviscerated and chopped up into several pieces.” (Binetti)

In the grand scheme of things, human trafficking is not a major source of income for terrorist groups as it is not very profitable. However, the main value of human trafficking is the cheap labor and expendable forces it provides for the groups.

Now the main question probably is: “Since Human trafficking provides so little money, how do terrorists earn all of their money?” Before the September eleven attacks, al Qaeda funding was thought to come from the illegal production of replica trademarked goods, the forgery of consumer coupons, the trafficking of drugs, insider trading, Bin Laden's wealth, and support with sympathizing governments (Roth et al.**)** However, after 9/11, the 9/11 Commission took a closer look inside al Qaeda’s financing using top-secret sources and the interrogation of al Qaeda operatives that al Qaeda was mostly funded by donations.

Al Qaeda relies mainly on donations from sympathizers towards its jihadi cause and unwitting donors in order to stay afloat and finance its terrorist activities. To collect money, they used a network of facilitators that would go around and collect donations from different sources. One of the main sources of donations was the Imam of a mosque turning all the Zakat donations over to al Qaeda for use in their operations. Zakat donations are supposed to go to charitable causes, and terrorism isn't one for most people. The theft of Zakat is an example of people unwittingly donating to terrorism, but there are also many people knowingly donating large sums of money with the intent of it going to terrorism, even requiring proof of its intended use.

Even in the West, you can't be one hundred percent sure that your charitable donation will not go to terrorists. Before 9/11, al Qaeda was influencing large internationally recognized charities to divert donations from unknowing people to terrorism. This was possible for al Qaeda to do because charities may have had little supervision of foreign branches that allowed al Qaeda to gain

control and move money away from its real destination. Or the charity as a whole could be corrupted, which allowed al Qaeda to control all of the charity's finances, allowing them to divert more money. An example of a charity that was fully corrupted[3] was the Wafa Humanitarian and the US-based Benevolence International Foundation[4]. These charities helped supply al Qaeda with weapons, including assault rifles and rocket launchers. They also provided the money needed to run the organization's vast training programs. These two charities and more were sanctioned by the UN under QDe.015 and QDe.093, respectively.

Terrorists often control large swaths of land and can exploit it to their advantage to earn money. For example, in ISIS-controlled territory in Iraq, Syria, and Libya, oil production and refinement infrastructure has been captured. The control of oil infrastructure allows ISIS to trade oil on the black market for heavily discounted prices. Oil sales in 2015 earned ISIS around 480 million USD, according to an analysis by the RAND Corporation [5]. Crane also mentions in his report that Operation Inherent Resolve, led by the USA in Iraq, brought down ISIS oil production by 33% in 2016, pushing ISIS closer to financial collapse as it will be less able to pay the salaries of its fighters and fund attacks worldwide. This proves that military action against commercial activities hosted by terrorist groups, including oil production, is effective in suppressing the financing of terrorists. Another way oil production could be impacted is through the sanctioning of oil coming from countries that are run by the IS.

Apart from oil, ISIS also trades in historical artifacts. In their controlled territories, ISIS excavates and loots archeological sites or taxes third-party excavators. The artifacts are then sold to collectors to earn ISIS around 36 million USD per month. The looting of artifacts became so profitable that ISIS had 4500 archeological sites under its control by 2017. This was recognized in the UN Security Council under resolution UNSCR 2199[6], where it is said that the money generated from the sales of the artifacts is used to support the training and recruitment of fighters and finance attacks.

[3] For a more comprehensive list see: https://home.treasury.gov/news/press-releases/js1703

[4] The Benevolence International Foundation did not exist solely in the US but also operated in Canada under the Alias Benevolence International Fund and In the Netherlands under “Stichting Benevolence International Nederland.”

[5]Report by Keith Crane on The Role of Oil in ISIL Finance: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT448/RAND_CT448.pdf

[6] Cultural Heritage, Clause 16

All in all, Terrorists use a large variety of means to earn money, with some being more violent than others. Cutting the revenue streams will affect the operation of terrorist organizations as they will not be able to pay salaries and thus recruit more soldiers. However, striking terrorism at its core by cutting its revenue streams often requires military action in a foreign nation which is expensive and frowned upon, making it extremely unlikely to happen. Thus the easiest way for foreign powers to counter terrorist financing is to intercept and seize the money while it is being moved from place to place.

## How do Terrorists Move Money

Once terrorists have earned money, they need to move it to where it can be spent, but this is difficult as illegally earned money is almost impossible to move unless it is made to look legitimate or investigators can't follow it to find where it comes from. Money launderers and terrorists alike use common money laundering techniques to move money and transport it to its final destination and use it for an attack.

Terrorists need to decide how they will move their money. They choose based on a few general criteria: How much money can be moved, how fast it can be moved, how much time it takes to move it, what is the risk of the money being stolen, lost, or seized, and most importantly, is it simple? Because of these criteria, terrorists tend to shy away from overly sophisticated schemes involving many high-maintenance small businesses. They prefer to use existing financial institutions such as banks and MSBs, exploit illegal or unregulated financial systems like hawala or cryptocurrencies, or they might take the old-fashioned way and transport cash or high-value commodities like gold.

### *Unregulated Banking and Tax Havens*

One way dirty money is moved is by using regular banks. Using ordinary banks provides many benefits to terrorists as they can theoretically move an infinite amount of money through them reasonably quickly and simply. However, when transactions get large, they might take days to clear and go through. Another downside of using banks is the cost.

The cost of the transaction will be around 3-4%[7] of the transaction, which, when multiple transactions of large volumes are processed, can add up, especially if the transaction is bounced between multiple banks. Lastly, the main downside for banks in the eyes of terrorists is the risk of being detected by law enforcement and having their money seized.

This risk can be negated by using banks in countries with weaker financial legislation. For example, countries can pass legislation that provides the utmost secrecy to bank customers using anonymous, numbered bank accounts. They also require banks not to comply with foreign subpoenas and prevent investigators from determining the origins of the money. In the 1990s, with the rise of telebanking and the internet, previously disconnected countries saw a way to earn extra money on taxes in the banking center. Seeing this opportunity, these countries immediately passed this legislation, becoming a magnet for dirty money and an annoying roadblock for Western investigators investigating money laundering as money trails ended in non-compliant states. Two examples of states infamous for their non-compliance are Switzerland and The Caymen Islands. These countries were especially attracted to shady money because of their stable political situation and location, being close to tightly regulated financial sectors.

Western countries wanted to crack down on these nations, allowing laundered money through their borders as money laundering was a growing issue in the 1990s. At the time, money laundering made up around 2-5% of the global economy and was costing MEDCs[8] and LEDCs[9] on average 50 billion dollars per year in lost taxes. (Wechsler) Because of this, at the 2000 G7 summit, countries identified by the OECD[10], FATF[11], and the FSF[12] were named and shamed for their mis compliance in the form of the extent of cooperation with law enforcement and global efforts to counter money laundering. The OECD identified

[7] Number will vary from bank to bank, usually being higher. Fixed rates exist for lower value transactions. In the USA these are about USD$50.

[8] More Economically Developed Country

[9] Less Economically Developed Country

[10] Organization for Economic Cooperation and Development

[11] Financial Action Task Force

[12] Financial Stability Forum - Part of the G7 Group

nations that supported tax evasion and money laundering with their anonymous and secret banking systems[13]. This threat from the G7 had an effect as the ratings of banks in the newly identified weak nations as they were immediately downgraded by organizations like Standard & Poor.

However, even though there are no nations left on the OECD's list of tax havens, there is still much to be wished for in the name of improvement. For example, Euractiv reported[14] that Monaco still has room for improvement in its very globalized financial sector. For example, they mention that non-financial institutions like private banking and real estate are under supervision, creating a risk that money could be laundered through property. Monaco was also recently accused of protecting the assets of Russian oligarchs in the wake of the Russia-Ukraine war showing malpractice regarding compliance with international sanctions. Also, Monaco has shown a lack of following up on cases of fraud and money laundering, with there only being 5 convictions of such crimes seeing its rather steep risk profile for such crimes. However, to Monaco's credit, it has been very active in improving its international cooperation, and it has improved in asking for external international assistance. Even Though there is significant room to grow in Monaco, there are signs of improvement.

### *Hawala*

Money laundering is a game of cat and mouse between the government and the money launderers. When there is more oversight and regulation in one sector, the money launderers move on to the next. This could be, for example, the use of Hawalas. Hawalas are usually a family-based informal banking and money transfer system found primarily in South-East Asia and the Middle East. Hawala's common work is as such: Person A in the UAE gives Hawalader A 1000 USD to transfer back to his family in Pakistan. Person A receives a transaction code from Hawalader A and will share that with their family back in Pakistan. In Pakistan, the family will find Hawalader B, who will most likely be a family member of

[13] Every nation from the list published by the OECD has either passed more transparent regulation to combat money laundering or has committed to the OECD to do so. However change is slow and meaningful results aren't seen in all of the 31 nations yet.

[14] Article By Euractive: https://www.euractiv.com/section/economy-jobs/news/monacos-anti-money-laundering-system-inadequate-risks-name-and-shame/

Hawalader A, and share the transaction code. The transaction codes will be verified, and if they match, Hawalader B will give the family their money.

The main advantages of the use of hawala to move money for terrorists are mainly their speed, lack of costs, and risks. Hawalas can complete transactions in a matter of hours, facilitating swiffer action. Hawalas also do not employ any KYC[15] regulation that formal banks are strictly forced to follow, allowing terrorists to move money often anonymously and without any questions asked. It is also cheaper for terrorists to use hawala to transfer money as they charge less of a transaction fee than formal banks of only around 0.1-0.2% of the transaction (compared to 3-4% in a formal wire transfer) Hawalas do, however, have one large downside, that being the volume of money that can be transferred. Hawalas often do not have many funds available to them as they do not make much profit, and therefore the receiving hawala will run out of money quickly, requiring the books to be balanced via moving money another way, often through the smuggling of cash and high-value commodities, which brings along its risks. These limitations can be overcome by using a large network of hawalas, but this does increase the complexity and decrease the transaction, making it a less attractive method to move large sums of money.

An example of the use of Hawalas is in the financing of the East African US embassy bombings performed by Al Qaeda in 1998. The use of Hawalas was more of a requirement for al Qaeda to move money at the time as the financial system in Afghanistan was old and error-prone, creating an unnecessary risk that al Qaeda did not want to take. To overcome this, Bin Laden turned to Hawala, located throughout the middle east, to move the necessary funds. Bin Laden used a network of 12 trusted hawaladars who were aware of or involved in his operations. Bin Laden also used many unknowing hawaladars to move funds. (Roth Et. Al.) The 1998 bombings caused the world to become increasingly scrutinous about the world financial system and forced modern protection to be put in place to stop attacks like these from happening again.

[15] Know Your Customer. Requires the bank to collect significant amounts of personal information on customers and to check their backgrounds to make sure their work is legitimate.

### *Money service businesses*

When larger sums of money need to be moved quickly and reliably, MSBs[16] can be used. A money service business is a person that runs an organized business in the capacity of currency exchanger, check casher, issuer or redeemer of traveler's checks, money transmitter, etc. (USDT FINCEN) MSBs are regulated and, like formal banks, are subject to regulation and audits. MSBs are attractive to terrorists as MSBs don't require one to have an account there, allowing them to bypass the need to follow KYC regulations that banks must comply with. To use an MSB, often only a valid form of ID has to be provided. MSBs are also attractive to terrorists due to the speed and reliability of their transactions. Established MSBs like Western Union can finish transfers expeditiously, and the money usually can arrive within a few minutes to almost anywhere in the world.

An example of MSBs Being used is in the Bojinka plot that unfolded in January 1995. The Bojnika plot was run by Khalid Sheikh Mohammed and Ramzi Youssef (Two future al Qaeda members). The plan was to murder Pope John Paul II and bomb eleven airliners flying from Asia to the USA with the plan to kill around 4000 people. Also, a plane would be flown into the CIA headquarters in Virginia. The plan was never fully executed as a chemical fire broke out in the apartment of Khalid Sheikh Mohammed and Ramzi Youssef, which caused the Philippine National Police to become interested and shut down the grunt of the attack. Only one test bomb went off on Philippine Airlines Flight 434, which only killed 1 person and injured 10, with the plane landing safely. The plot was financed using a UAE-based MSB called Al Ansari Exchange Establishment (AAEE).

The infamous September 11 attacks also relied heavily on MSBs to be financed. Al Qaeda financier Abdul Aziz Ali sent USD$120,000 from two Dubai-based MSBs to the hijackers in the US. Even Though MSBs in Dubai do require ID to be able to transfer money, a simple alias was used to mask the transfer's true purpose and avert any suspicion that might occur. The transaction was also commingled with so many other money transfers leaving Dubai that it seemed regular and did not raise any suspicions. This commingling is also leveraged in charities corrupted by terrorist organizations Such as the Benevolence International organization. The integration of dirty money with clean money is a common

[16] Money Service Business

money laundering practice that can prove effective as it gives the reason for the funds to be moved and it provides a legitimate-looking origin for the money.

### *False Invoice Trading*

False invoice trading is the over- or underpricing of goods to secretly transfer funds from one part of the world to another. False invoice trading works by trading products and then fixing their price to be either lower or higher than they should be, allowing excess money to be transferred. For example, if two Hawaladars needed to balance their books Hawaladar A from the USA could buy USD$50000 worth of honey from an American honey producer and then sell that honey to Hawaladar B for USD150000. By doing this, Hawaladar B, in essence, transfers an extra USD$100000 to Hawaladar using over-invoicing. This extra money allows Hawaladar A to pay off the honey and receive money that can be used in future transactions.

Next to the simple over and under-invoicing of products.[17] Money launderers can also send out multiple invoices for the same shipment of goods. One of these will be provided as a mistake and is said to be refunded. The refund on the second invoice will never be processed, and the money launderer will make double the money. Money launderers can also misrepresent the goods sent. Perpetrators can do this in three ways: short shipping, over shipping, and phantom shipping. Short shipping is when fewer goods are shipped than invoiced, which gives the seller more profit and therefore transfers money from B to A (A being the seller and B being the recipient). Over shipping is when more products are shipped than are invoiced, giving the recipient more value than what they paid for, transferring money from A to B. Lastly, phantom shipping is when no goods are shipped and forged documents are created to prove the transfer of goods.

False invoice trading has many benefits to move money internationally. First, it satisfies the criteria of volume, as an unlimited volume of money can be transferred in any given transaction. It is also a very low risk as it is difficult for authorities to trace every single

[17] Document describing more TBML Techniques: https://files.simmons-simmons.com/api/get-asset/Trade_based_money_laundering.pdf?id=bltf46079bfc4e90532

invoice made, as invoicing doesn't always take place in government-regulated channels. Governments are also not able to screen every single business package against its invoice to determine if the products are valued correctly, and the stated number of products are shipped. When an invoice passes through a bank, a banker is only able to see the invoice, not also the products, so the banker is unable to even check whether the invoice is true. The process is also fairly simple, only requiring small changes in an invoice. All of this makes false invoice trading a deadly weapon for terrorists to transfer money internationally without fear of detection.

Some red flags that help identify false invoice trading are a discrepancy between the product, quantity, price, and quality of the product and what is listed in the invoice. (Arslan) For example, if an inspector had both access to the shipped product (in either its physical form or a range of digital imaging, i.e., Volumetric CT/X-Ray/Still images) and the invoice, the inspector could find these discrepancies and flag the package for further investigation. Another factor that can be analyzed to find whether a package is at risk of being fraudulent is the frequency of transactions between the seller and the recipient. Different degrees of sporadicity and lack thereof might be able to indicate whether the transaction could be part of a terrorist financing or money laundering scheme.

### *High Value Commodities*

Another way terrorists will move money is by moving high-value commodities like gold, diamonds, and other precious metals and stones (PMS). PMS are a very convenient method of moving a large volume of money across borders due to their small size and high weight-to-value ratios. PMS are useful as PMS have a very stable value which can be useful during times of war and disruption that may cause devaluation or instability in a local currency. PMS can provide an alternate form of payment for goods like weapons and drugs. Also, it doesn't raise much suspicion if one wants to convert PMS into currency, as many establishments like liquidators and jewelry stores will gladly convert these into cash. PMS also has its downsides. If terrorists want to acquire less expensive diamonds from conflict regions like Libya, they will have to be transported by a courier, which leads to more risk of theft and seizure.

The main advantage of PMS is that they are easy to transport. For example, gold can be molded into any shape allowing it to be disguised into everyday items like screws in a suitcase. Diamonds are also easily smuggled by couriers because of their small size and their lack of magnetic proporties, so they are susceptible to being transported through airports without detection by a courier. PMS are also targets for the previously mentioned false invoice trading as they are high value and provide little cost to ship due to their high value-to-weight ratio.

A few examples of the use of PMS in terrorist financing is the transport of PMS in jewelry meant for bridal dowries, which are still required in marriage as part of some Asian cultures and, because of that, don't raise many red flags when they are seen transported. For a time, al Qaeda also offered gold rewards and incentives for future jihadists. Diamonds were also used by al Qaeda after the 1998 East Africa US embassy bombings when President Clinton froze around USD$220 million of al Qaeda's assets. To be able to recover, al Qaeda converted most of its liquid assets into diamonds as they are transportable and cannot be frozen or seized indirectly by governments.

### *Crypto Currencies*

Cryptocurrencies are a relatively new addition to the money laundering playbook. Cryptocurrencies are decentralized currencies meaning they don't use a central reserve of sorts and operate purely on a peer-to-peer basis. All Crypto Currencies also use a form of the blockchain. The blockchain is a series of "blocks" containing the previous owners and the transaction histories of each coin. Coins can be owned by wallets which are a long string of hexadecimal characters. Transactions between wallets are verified by a network of computers all around the world to check if they are legitimately using complicated algorithms. This process is called mining, as a small percentage of the transaction is rewarded to the miners for verifying the transactions.

Crypto poses a new risk for money laundering as the crypto industry is completely void of regulation, meaning that any person or group can get their hands on it. Crypto is also anonymous as wallets are only a series of letters and numbers that contain no personal information of the holder. Crypto can also really easily cross borders as it can simply be spent all over the world or transferred to a different wallet with minimal cost and no checks and balances or customer due diligence. All of this poses a new challenge for governments as

crypto assets are very easy to follow due to the nature of the blockchain, but it is impossible to know who owns what wallet. Money launderers also use a specific tool called a mixer to obscure where their money comes from and mix it with other money. A mixer works by a large group of people, creating a large pool of cryptocurrency. This crypto is then "mixed" and then randomly redistributed proportionally to the stakeholders in the pool, obscuring where the crypto came from.

An example of the use of crypto in Money laundering is North Korea's recent hack of the Estonian company Atomic Wallet leading to a loss of around USD$35 million that will most likely be used to fund nuclear programs. In 2022 North Korea was also very active in the crypto space, stealing around USD$1.7 billion in hacking attacks by Lazarus group[18] and stealing NFTs[19] North Korea probably didn't earn all of the $1.7bn as it was probably sold at a discounted price to Chinese buyers who were willing to take the risk with the stolen crypto.

### How can we combat money laundering

Imagine trying to get 195 different people to agree with each other about one thing and comply in a quality and timely manner. Impossible right? The same situation is true when trying to stop terrorist financing and money laundering. Every single country has to cooperate for sanctions and countermeasures to be effective. International cooperation is paramount as every nation has to be willing to accept foreign help when it comes to investigations and give help to its neighbors.

International cooperation started strong with the creation of the Financial Action Task Force (FATF) in 1989. The FATF is a multi-government organization that regulates and audits nations on their risk of being prone to money laundering and compliance with international laws and standards. In the year 1990, the FATF published 40 general recommendations to all states. The FATF doesn't have a way to enforce its policies and regulation. The main way it acts is by naming and shaming any nation that is not complying with the global effort to combat money laundering and terrorist financing. This naming and shaming would often work as countries on the non-compliance list are avoided in international business because they pose a risk to everyone, and banks do not want to be involved in any illegal funds as this may lead to repercussions.

[18] Top secret elite group of North Korean hackers

[19] Read More: https://www.bbc.com/news/world-asia-64494094

Sadly in the 90s and 2000, money laundering and counter-terrorist financing were not seen as much of a priority as it was expensive and seemed less important than local issues. Then this was all turned around by the soul-crushing reminder provided by the September 11 attacks on the USA in 2001. These attacks reminded all nations how important countering money laundering and terrorist financing is and how important international cooperation is.

In the wake of the attacks, the USA passed the PATRIOT (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act which gave the government free reign to combat terrorism. It also finally required American banks to implement real KYC policies. It also allowed the US government to freeze or seize any assets if enough evidence was provided they were linked to terrorism.

The US also took action in the UN, exploiting the anti-terrorist sentiment at the time to pass resolution 1373 (S/RES/1373). 1373 was, in essence, a treaty between all member states because it required changes to domestic policy, like the criminalization of terrorism and the denial of a haven to terrorists under all circumstances. 1373 also started the counter-terrorism committee (CTC), which expands on the committee that began in resolution 1267 (S/RES/1267).

One main issue with the current way of anti-money laundering is that it is very focused on nations with already established modern financial systems. Neither the Egmont Group nor the FATF contains many LEDCs that are in the most need of assistance when it comes to anti-money laundering and anti-terrorist financing, as they are the most susceptible to becoming new hubs.

## Major Parties Involved

### Financial Action Task Force (FATF)

The FATF is a trans-governmental organization with 37 member states that leads the global push to combat money laundering and terrorist financing. The FATF meets three times a year for its plenary session to evaluate the current status quo and pass new and improved recommendations that counter evolving threats.

### Egmont Group

The Egmont group is a group of 166 nations that allows FIU (financial intelligence units) to share information. The Egmont group allows members to collaborate on issues of related to AML and CTF schemes. They also help educate nations with weaker legislation on how risks emerge and possible legislation to avert them.

### USA

The USA is very active in the field of anti-terrorism and aggressively pushes the rest of the world to follow its examples. The PATRIOT act passed after the September 11 attacks, in essence, gives the US government full authority to do whatever they want to prevent terrorism. An example of this was the war on terror against al Qaeda in Afghanistan.

### EU

The EU is a group of 27 nations that make broad decisions on policy together using the EU parliament. The European Union has made strong commitments against money laundering and terrorist financing and makes sure all of its member states follow the gold standard.

### UNSC

The United Nations Security Council (UNSC) is the only UN body that has the potential to pass legally binding resolutions. The UNSC has played a pivotal role in the post-9/11 terrorism scare allowing the US to pass many far-reaching resolutions to counter the issue.

## Timeline of Key Events

| Description of Event | Date |
|---|---|
| OECD Formed | September 30, 1961, |
| FATF Formed | July 1989 |
| FATF's 40 Recommendations Submitted | 1990 |
| Egmont Group Formed | June 9, 1995 |
| 2000 G7 Summit | July 21, 2000 |
| September 11 Attacks | September 11, 2001 |
| Resolution 1373 Passed | 28 September 2001 |
| American Invasion of Afghanistan | October 7, 2001 |
| PATRIOT act passed | October 26, 2001 |
| Death of Osama Bin Laden | May 2, 2011 |

## Possible Solutions

### Crypto Regulation

Since Cryptocurrency is still a very technology, there has only been very little regulation on it. To prevent terrorists and money launderers from using cryptocurrencies from using it for wrong. Crypto exchanges should be regulated in the same way as banks implementing customer due diligence practices. Crypto exchanges should also be held liable for doing business with illegal money the same way banks are, and there should be repercussions for a failure to comply.

### Package Screening against Invoiced Contents

The current disconnect that compliance officers face when checking for false invoice trading is the lack of access to inspect the shipped products. Using photography or CT technology, compliance offers would have the ability to inspect the contents of the package and compare them with the products listed on the invoice. Because this test is non-intrusive, this would happen without disrupting the package's transport and causing possibly costly delays.

### Further Disclosure and Transparency in Banking

Bank secrecy exists to protect a bank's clients and keep customer banking information confidential. Money Launderers and terrorists are often drawn to move money through countries with tight bank secrecy as it allows them to prevent authorities from investigating. Banks should verify all transactions in and out are not going or coming from any suspicious accounts. Banks should also be held partially liable if it is found a crime is committed using their financial services.

### Crackdown on Hawalas

Hawalas are a very unregulated part of the financial sector and allow illegal funds to move over borders without the usual checks and balances that are required to be put in place by formal financial institutions. Hawalas pose a serious risk to governments as it reduces their capability to monitor terrorists and asses the possibility of an attack. This could lead to a failure to prevent an attack and prove to be deadly to many. Hawalas should either be forced to be registered and disclose transactions or be illegalized completely.

### Wider Know Your Customer (KYC) and Customer Due Diligence (CDD) Regulation

KYC and CDD regulations are essential for banks to be able to know who they are doing business with. This prevents suspicious or risky individuals from gaining access to financial institutions. KYC and CDD regulations should be required for all financial entities that can transfer money internationally, including MSBs and (regulated) Hawalas.

### Regular Audits for Charities operating in At-Risk Countries

Charities that operate in countries that are involved with or have internationally listed terrorist organizations operating should be regularly audited to screen for malpractice and corruption. These audits would take place at least once a year and must be conducted by an unbiased third party. The audits would be top-down: screening every part of the operation, including those at the highest level. Charities also must remain transparent about the destination of the donated funds and provide evidence of delivery of these.

### FATF 40 Recommendations

In 1990 the FATF published 40 recommendations to end money laundering and terrorist financing. Find the most recent edition here: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

## Bibliography

The 9/11 Commission. “https://www.jstor.org/stable/26915562.” *9/11 Commission*. *The 9/11 Commission*, 9/11 Comission, https://9-11commission.gov/report/911Report.pdf. Accessed 7 July 2023.

Arslan, Serkan. “How to detect commonly used Trade-Based Money Laundering 'TBML' techniques.” *Finextra Research*, 1 February 2021, https://www.finextra.com/blogposting/19829/how-to-detect-commonly-used-trade-based-money-laundering-tbml-techniques. Accessed 7 July 2023.

Binetti, Ashley. “A New Frontier: Human Trafficking and ISIS’s Recruitment of Women from the West.” *Georgetown Univeristy Giwps*, 2023. *Georgetown University*, Georgetown Institute for Women, Peace & Security, https://giwps.georgetown.edu/wp-content/uploads/2017/10/Human-Trafficking-and-ISISs-Recruitment-of-Women-from-the-West.pdf. Accessed 7 July 2023.

Blannin, Patrick. “Islamic State’s Financing: Sources, Methods, and Utilisation.” *Counter Terrorist Trends and Analyses*, vol. 9, no. 5, 2017, pp. 13-22. *JSTOR*, https://www.jstor.org/stable/26351519. Accessed 7 July 2023.

Bourgery, Théo. “Monaco's anti-money laundering system inadequate, risks name-and-shame.” *EURACTIV.com*, 22 January 2023, https://www.euractiv.com/section/economy-jobs/news/monacos-anti-money-laundering-system-inadequate-risks-name-and-shame/. Accessed 7 July 2023.

Central Bank of Ireland. “Anti-Money Laundering and Countering the Financing of Terrorism.” *Central Bank of Ireland*, https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism. Accessed 7 July 2023.

Clunan, Anne L. “The Fight against Terrorist Financing.” *Political Science Quarterly*, vol. 121, no. 4, 2007, pp. 569-596. *JSTOR*, https://www.jstor.org/stable/20202763?searchText=terrorist+financing&searchUri=/action/doBasicSearch?Query%3Dterrorist+financing&ab_segments=0/basic_search_gsv2/control. Accessed 7 July 2023.

Crane, Keith. “The Role of Oil in ISIL Finances.” Testimony. *The Rand Corporation*, 10 December 2015. *Rand*, The Rand Corporation, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT448/RAND_CT448.pdf. Accessed 7 July 2023.

Egmont Group. “About.” *About the Egmont Group*, https://egmontgroup.org/about/. Accessed 9 July 2023.

Egmont Group. “Egmont Group.” *Egmont Group: Home*, 2023, https://egmontgroup.org/. Accessed 9 July 2023.

European Council. “Fight against money laundering and terrorist financing.” *Consilium.europa.eu*, 2019, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/. Accessed 7 July 2023.

FATF. “About the Non-Cooperative Countries and Territories NCCT Initiative.” *FATF*, 2007, https://www.fatf-gafi.org/en/publications/Fatfgeneral/Aboutthenon-cooperativecountriesandterritoriesncctinitiative.html. Accessed 7 July 2023.

FATF. “INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION.” *FATF*, February 2023. *FATF*, FATF, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf. Accessed 7 July 2023.

FATF. “Outcomes of meetings.” *FATF Plenary meetings - Chairman's Summaries*, https://www.fatf-gafi.org/en/the-fatf/outcomes-of-meetings.html. Accessed 9 July 2023.

FATF. “What we do.” *What we Do*, 2023, https://www.fatf-gafi.org/en/the-fatf/what-we-do.html. Accessed 9 July 2023.

Freeman, Micheal, and Moyara Ruehsen. “Terrorism Financing Methods: An Overview.” *Perspectives on Terrorism*, vol. 7, no. 4, 2013, pp. 5-26. *JSTOR*, https://www.jstor.org/stable/26296981?searchText=terrorist+financing&searchUri=/action/doBasicS

earch?Query%3Dterrorist+financing&ab_segments=0/basic_search_gsv2/control. Accessed 7 July 2023.

Human Trafficking Search. "ISIS Continues to Engage in Sex Trafficking." *Human Trafficking Search*, 10 November 2014, https://humantraffickingsearch.org/isis-continues-to-engage-in-sex-trafficking/. Accessed 7 July 2023.

International Monetary Fund. "Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) - Topics." *International Monetary Fund*, https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm. Accessed 7 July 2023.

Jojarth, Christine. "1. Money Laundering: Motives, Methods, Impact, and Countermeasures." *Transnational Organized Crime: Analyses of a Global Challenge to Democracy*, vol. 1, no. 1, 2013, pp. 17-34. *JSTOR*, https://www.jstor.org/stable/j.ctv1fxh0d.5. Accessed 7 July 2023.

Liberto, Danial. "Zakat: The Basic Rules for One of the Five Pillars of Islam." *Investopedia*, 26 July 2022, https://www.investopedia.com/terms/z/zakat.asp. Accessed 7 July 2023.

Lyngaas, Sean. "North Korea hackers suspected in new $35 million crypto heist." *CNN*, 7 June 2023, https://edition.cnn.com/2023/06/06/tech/north-korea-crypto-heist/index.html. Accessed 7 July 2023.

Myers, Joseph M. "The Silent Struggle Against Terrorist Financing." *Georgetown Journal of International Affairs*, vol. 6, no. 1, 2005, pp. 33-41. *JSTOR*, https://www.jstor.org/stable/43134071. Accessed 7 July 2023.

Neumann, Peter R. "Don't Follow the Money: The Problem With the War on Terrorist Financing." *Foreign Affairs*, vol. 96, no. 4, 2017, pp. 93-102. *JSTOR*, https://www.jstor.org/stable/44823895. Accessed 7 July 2023.

Ng, Kelly. "Crypto theft: North Korea-linked hackers stole $1.7b in 2022." *BBC*, 2 February 2023, https://www.bbc.com/news/world-asia-64494094. Accessed 7 July 2023.

OECD. “List of Unco-operative Tax Havens.” *OECD*, OECD, 2009, https://www.oecd.org/ctp/harmful/list-of-unco-operative-tax-havens.htm. Accessed 7 July 2023.

Polaris. “Vulnerabilities & Recruitment - Polaris.” *Polaris Project*, https://polarisproject.org/vulnerabilities-and-recruitment/. Accessed 7 July 2023.

Roth, John, et al. “Monograph on Terrorist Financing. Staff Report to the Commission.” The *University of Toronto*. The *University of Northern Texas*, National Commission on Terrorist Attacks Upon the United States, https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf. Accessed 7 July 2023.

Sanction Scanner. “Blog / The "Follow the Money" Method.” *Sanction Scanner*, https://sanctionscanner.com/blog/the-follow-the-money-method-513. Accessed 7 July 2023.

Simmons & Simmons. “Trade-Based Money Laundering.” *Simmons & Simmons*. *Simmons & Simmons*, Simmons & Simmons, https://files.simmons-simmons.com/api/get-asset/Trade_based_money_laundering.pdf?id=bltf46079bfc4e90532. Accessed 7 July 2023.

Sypher, Ford. “Rape and Sexual Slavery Inside an ISIS Prison.” *The Daily Beast*, 28 August 2014, https://www.thedailybeast.com/rape-and-sexual-slavery-inside-an-isis-prison. Accessed 7 July 2023.

Tax Justice Network. “What is a tax haven?” *Tax Justice Network*, 2023, https://docs.google.com/document/d/1vyWcYOirXmqga5TnW1R0WufLpiBazoztCNP_s4zQ8A4/edit. Accessed 9 July 2023.

“Trade-Based Money Laundering Risk Indicators.” *Flu Nederland*, March 2021. *FLU Nederland*, FATF, https://www.fiu-nederland.nl/wp-content/uploads/2022/03/202103_fatf_trade-based-money-laundering-risk-indicators-1.pdf. Accessed 7 July 2023.

United Nations. “Combating Terrorist Financing.” *unodc*, https://www.unodc.org/unodc/en/terrorism/expertise/combating-terrorist-financing.html. Accessed 7 July 2023.

UNSC. "BENEVOLENCE INTERNATIONAL FOUNDATION | United Nations Security Council." *the United Nations*, 27 June 2008, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/benevolence-international-foundation. Accessed 7 July 2023.

UNSC. "Resolution 2199." *UNODS*, 12 February 2015. *United Nations Official Documents System*, United Nations, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/040/28/PDF/N1504028.pdf?OpenElement. Accessed 7 July 2023.

UNSC. "WAFA HUMANITARIAN ORGANIZATION | United Nations Security Council." *the United Nations*, 27 June 2008, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/wafa-humanitarian-organization. Accessed 7 July 2023.

USDT. "Additional Al-Haramain Branches, Former Leader Designated by Treasury as Al Qaida Supporters Treasury Marks Latest Action in Joint Designation with Saudi Arabia." *Treasury Department*, United States Treasury OFFICE OF PUBLIC AFFAIRS, 2 June 2004, https://home.treasury.gov/news/press-releases/js1703. Accessed 7 July 2023.

USDT FinCEN. "Money Services Business Definition." *FinCEN*, USDT FinCEN, https://www.fincen.gov/money-services-business-definition. Accessed 7 July 2023.

Warren, Jonathan M. "A Too Convenient Transaction: Bitcoin and Its Further Regulation." *Journal of Law & Cyber Warfare*, vol. 8, no. 1, 2020, pp. 5-29. *JSTOR*, https://www.jstor.org/stable/26915562. Accessed 7 July 2023.

Wechsler, William F. "Follow the Money." *Follow the Money*, vol. 80, no. 4, 2001, pp. 40-57. *JSTOR*, https://www.jstor.org/stable/20050225?searchText=follow+the+money&searchUri=/action/doBasicSearch?Query%3Dfollow+the+money&ab_segments=0/basic_search_gsv2/control. Accessed 7 July 2023.

Wikipedia contributors. “Bojinka plot.” *Wikipedia*, Wikipedia, The Free Encyclopedia., 1 May 2023, https://en.wikipedia.org/w/index.php?title=Bojinka_plot&oldid=1152571005. Accessed 7 July 2023.

Zhou, Sheng. “Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet.” *Journal of Law & Cyber Warfare*, vol. 3, no. 1, 2014, pp. 103-142. *JSTOR*, https://www.jstor.org/stable/26432561. Accessed 7 July 2023.