Márton Tibor Serbakov: The latest techniques and sources of terrorist financing[1]

1. Introduction

In this study I intend to examine the latest techniques and sources of terrorist financing with special attention to the techniques and sources related to modern technology. The COVID-19 pandemic[2] has generated various government responses, which range from social assistance and tax relief initiatives, to enforced confinement measures and travel restrictions. While unintended, unfortunately these measures may provide new opportunities for criminals and terrorists to generate and launder illicit proceeds.[3] With the spread of the pandemic, almost all regions have implemented lockdowns, shutting down activities that require human gathering and interactions – including colleges, schools, malls, temples, offices, airports, and railway stations. The lockdown has resulted in most people taking to the internet and internet-based services to communicate, interact, and continue with their job responsibilities from home. Internet services have seen rises in usage from 40 % to 100 %, compared to pre-lockdown levels.[4] The pandemic has accelerated the shift towards a more digital world.[5] As Zoltán András Nagy warns us of the fact, members of organized crime and also terrorists abuse the opportunities provided by the fast technical development, and they exploit the freedom and the borderless nature of the internet[6], as they use it for their own ignoble purposes.[7] Terrorist financers and other criminals are constantly adjusting their techniques, to always stay one step ahead of law enforcement; they gladly use unique or experimental products and services to further their goals.[8] Viorel Pasca and Daniela Simona Orza shed light on the alarming fact, that "the way in which terrorist groups collect and transfer funds needed to fund their operations reveal that modern technologies that are in line with new trends (cryptovalute and darknet) but traditional means (zakat and hawala) are also used."[9]

1. The fundamentals of terrorist financing

How can we define terrorist financing? According to the definition of István László Gál: „Terrorist financing means the activity during which directly or indirectly financial means are submitted for the execution of terrorist attacks.”[10]
Although the costs of specific terrorist operations can be relatively low, terrorist organizations need much larger budgets to function. Recruiting, building training camps, food and housing, the necessary equipments for conducting acts of violence (guns, explosives etc.) and communication devices cost money. Terrorists may need funds to bribe officials and many groups pay stipends to their „retired” members and the families of dead terrorists or suicide bombers. Budgets of larger and more active terrorist goups can range up to hundreds of millions of dollars per year.[11] The necessary costs of executing terrorist attacks can be divided into three groups: operational costs, administrative costs and the donation given to the family members of the perpetrator.[12]
As Acharya strikingly states about the nature of terrorist financing:

„If radical ideology and extremism are at the heart of terrorism today, finance is its lifeblood. The threat of the so-called „new terrorism” lies not only in the weapons that the terrorists can yield, but also in their ability to procure and use those weapons through innovative, discreet and complex fund-raising and fund-transfer techniques. Like any commercial venture, access to finance and the means of transfer is crucial for sustenance of terrorist organizations and vital in the formulation and implementation of their activities.”[13]

There are links between terrorist financing, money laundering, cybercrime and traditional criminal activity. The lines between fraud and money laundering and terrorist financing are blurred, and they should not be approached as separate events. Although organised crime, cybercrime and financial fraud can and are being committed by terrorist organisations, not all terrorist financing comes from illegal sources. Money laundering and terrorist financing do not necessarily go hand-in-hand, as a large amount of money laundering activity is for private profiteering only and not for political purposes.[14] The Financial Action Task Force on Money Laundering (FATF) is the most important international standard setter for anti-money laundering and Combatting Terrorism Financing (CTF).[15] It was established by the G-7 summit held in Paris in 1989.[16] It currently comprises 37 member jurisdictions and 2 regional organisations representing most major financial centres in all parts of the globe.[17] According to the FATF, terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding terrorist financing risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of counter terrorist financing measures.

Developing and maintaining an understanding of evolving terrorist financing risks can often present unique challenges for jurisdictions. The low value of funds or other assets used in many instances, and the wide variety of sectors misused for terrorist financing purposes, makes identification of terrorist financing vulnerabilities and threats challenging. Countries can also face challenges due to the limited availability of terrorist financing or terrorism information domestically, or the limited amount of criminal/intelligence cases under investigation. The lack of terrorism and terrorist financing expertise or personnel, and limited information on unregulated or unsupervised activities can pose further challenges for lower capacity countries. Due to such challenges, terrorist financing risk is often given limited attention in National Risk Assessments and is sometimes not differentiated from the risk of terrorism. Similarly, in developing a methodology for assessing risks, jurisdictions sometimes fail to take into account the uniqe threats posed by terrorist financiers and sympathisers as opposed to criminals.[18]

III. The sources and techniques of terrorist financing

Researchers express different views on how terrorists raise funds.
According to István László Gál, the sources and techniques of terrorist financing are the following: committing criminal offences, donations, and legal businesses.[19]

Ulrich Sieber's and Benjamin Vogel add another source to the ones mentioned above. According to them, the financing sources of terrorist organizations are donations, criminal offences, prima facie legal businesses with the help of corporations, and the income from controlling a territory.[20]

Freeman divides the different sources of financing into four general categories: state sponsorship, illegal activities, legal activities and popular support. State sponsorship was much more common during the Cold War, it has decreased significantly in recent years. Seeking funding through illegal activities include extortion or „revolutionary taxes", kidnapping and ransom, theft, smuggling, petty crime, pirating and counterfeiting goods. For profit, terrorists often operate legal businesses. As a source of funding lot of terrorist groups rely on the support of a symphatetic population or constituency. This includes charitable donations, tapping into symphatetic diaspora communities living overseas and relying on membership dues.[21]
According to Bell, there are four sorces of terrorist funding: contributions from sympathisers, finance derived from crime, finance from legal businesses, and funding from the assistance of

a foreign government. These four sources might suggest four different models of terrorist funding, in theory: the Popular Support model (where funding comes from donations), the Criminal Proceeds model (where funding is derived from crime), the Entrepreneurial model (where businesses generate funding) and the State Sponsor model (where funding comes from a foreign state). Bell also adds that this categorisation would be simplistic and misleading. Suggesting a more sophisticated model, where finance comes from multiple sources and where oppurtunity is the main factor which influences the combination of funding sources for a particular group is a more realistic approach.[22]
According to the Emerging Terrorist Financing Risks FATF REPORT of October 2015, the traditional terrorist financing methods and techniques are private donations, abuse and misuse of non-profit organisations, proceeds of criminal activity, extorting local and diaspora populations and businesses, kidnapping and ransom, self-funding, legitimate commercial enterprise, state sponsorship of terrorism.[23] The traditional methods and techniques described above continue to be prevalent today and are still significant risks.[24] According to the FATF REPORT emerging terrorist financing threats and vulnerabilities are are foreign terrorist fighters (FTFs), fundraising through social media, new payment products and services, exploitation of natural resources.[25] In this article, I introduce the latest techniques and sources of terrorist financing while following the categorisation of the emerging terrorist financing threats and vulnerabilities of the Emerging Terrorist Financing Risks FATF REPORT of October 2015, and I add other varied sources.

1. Emerging terrorist financing threats and vulnerabilities

IV.1 Foreign Terrorist Fighters (FTFs)

A foreign fighter is “an individual who leaves his or her country of origin or habitual residence to join a non-State armed group in an armed conflict abroad and who is primarily motivated by ideology, religion, and/or kinship”.[26] The issue of FTFs is not new, but the recent scale related to Syria and Iraq is worrying. They are not considered a significant source of funding for ISIS or Al-Nusrah Front at the moment, but they contribute to the larger terrorist financing threat posed by these groups. They are one of the main forms of material support to terrorist groups. The two most common methods used to raise funds for FTFs are self-funding by individuals and funding by recruitment/facilitation networks.
FTFs generally have modest funding needs. These include transportation, accommodation while in route, outdoor clothing, etc. To finance their travel to conflict zones, individuals often use funds from legitimate sources (e.g., employment income, social assistance, family

support, bank loans). In some cases, small businesses were established and used to generate revenue that supported FTF travel. Some jurisdictions have also noted the sudden sale of assets including personal belongings and assets purchased on credit just before the FTFs planned travel. Family and associates have also intentionally or unintentionally transferred their legitimately obtained funds to individuals engaged in conflict. To travel to conflict zones and join terrorist groups, recruitment networks and individuals facilitate FTFs. Family, friends or facilitation networks also provide financial support to FTFs once they start their journey. Most groups are informal or ad hoc, depending on what kind of support is needed by the FTF and there are often links between facilitators in the home country and areas bordering the conflict zone. FTFs have used some of the traditional methods and techniques to move and get access to funds. These mainly include the physical movement of cash, use of ATMs to access funds from bank accounts and use of MVTS. [27]
In March 2019 The Islamic State in Iraq and the Levant was militarily defeated in the Syrian Arab Republic.[28]According to the UN Security Council report of 15 July 2019: „The issues of foreign terrorist fighters, dependants, returnees, relocators and "frustrated travellers"… remain acute. Up to 30,000 of those who travelled to the so-called "caliphate" may still be alive, and their future prospects will be of international concern for the foreseeable future. Some may join Al-Qaida or other terrorist brands that may emerge. Some will become leaders or radicalizers, including in prisons if they are successfully prosecuted in Member States that are unable to manage this challenge within their penal systems."[29] According to Clarke , the threat posed by returning foreign fighters to their countries of origin has been lower than anticipated, but there is still a significant number of militants unaccounted for, some of whom may travel to other conflict zones and serve as force multipliers for jihadist groups fighting civil wars or insurgencies in weak and failed states. There is also the question of what will happen to Islamic State members being held in detention camps throughout northeast Syria and elsewhere. 2020 may also signal an uptick in terrorism perpetrated by Shia militants. Iran remains the primary state sponsor of terrorism in the world today.[30]

IV.2 Fundraising through social media

Terrorists exploit the widespread access and the anonymity of the internet, especially the rapid growth of social media, to raise funds from sympathetic individuals on a global scale. The phenomenon is a growing terrorist financing threat. Terrorist organizations spread their propaganda by social network, and reach out to sympathisers. They also use social networks for fundraising campaigns. Terrorists are able to reach a wide audience trough peer-to-peer

horizontal communication (such as Facebook, Twitter, Instagram etc.) and sometimes that continues through mobile messenger applications (such as WhatsApp or Viber) and even more secure communication networks (such as Surespot). Terrorists' use of organized crowdfunding is also a growing terrorist financing risk.[31] Terrorist financing on social media can take several forms, donors may sometimes not even realize, that they are financing terrorists, because terrorists also conduct fundraising under fake charities, where donors believe they donate for humanitarian purpose. Platforms of social media are mouthpieces for broadcasting explicit calls for financial support. Terrorist supporters direct potential funders to communication platforms. Terrorists encourage donors to use encrypted mobile applications[32], to hide from external surveillance. This means serious difficulty for efforts against terrorist financing.[33]

27 jurisdictions responded to the questionnaire of the APG/MENAFATF SOCIAL MEDIA & TERRORISM FINANCING REPORT of January 2019 and provided case examples of terrorist financing through the abuse of social media services. These 27 cases show social networking services (e.g. Facebook), content hosting services (e.g. YouTube), crowdfunding services (e.g. GoFundme.com) and Internet Communication Services (e.g. WhatsApp) are being abused in a variety of ways for terrorist financing, as follows: „Social networking and content hosting services are primarily used to solicit donations, promote terrorism through propaganda and radicalization. Consistent with the current limited integration of payment methods in these services, most cases provided as part of the report show donated funds are moved using traditional payment methods i.e. banks. Internet communication services were used in many cases to privately communicate with campaigners or terrorist groups. They mainly discussed means of support and payment methods. The vulnerabilities of these services, for example, encrypted communication and the number of active users, are factors driving their abuse for terrorist financing. Crowdfunding services were used in a number of cases, with campaigners often disguising the use of funds for humanitarian causes. These services often integrated traditional and new payment services, which due to their vulnerabilities may hinder terrorist financing detection and investigation by competent authorities."[34]
Fundraising advertisements are usually planted in social networks and thematic sites, as well as in specialised media, closed forums and sent in private messages. To obscure the true purposes of fundraising, these advertisements usually do not contain direct references to fundraising for terrorist financing, but use ambiguous language or the pretext of collecting funds for charitable and humanitarian purposes. These fundraising advertisements and the financial details may be in other formats rather than in a text (e.g. as an image or video), which makes it impossible to detect them through standard search engines and makes it challenging to identify sites that contain these advertisements, as well as to explore

advertisements using known financial details.[35]
Charities play such a big role in terrorist financing, because charitable giving, „zakat" is one of the five pillars of Islam.[36] It is the compulsory giving of a set proportion of the believer's wealth to charity. While most of these charities in the Muslim world exist to help the poor and spread the message of the religion of Islam, unfortunately they have also been used, especially in wealthy Middle Eastern nations, to finance jihad. Weeding out ill-intentioned charities from the benevolent is a difficult job.[37]

IV.3 New payment products and services

According to the Emerging Terrorist Financing Risks FATF REPORT of October 2015 new payment products and services are virtual currencies, prepaid cards and internet-based payment services.[38]
New Payment Methods include the use of Internet-Based Payment Services such as E-money, PayPal, and Bitcoin.[39]
According to the Emerging Terrorist Financing Risks FATF REPORT of October 2015 electronic, online and new payment methods pose a vulnerability which may increase over the short term with the growth of the overall use of these systems. Many of these systems can be accessed globally and used to transfer funds quickly. A number of online payment systems and digital currencies are also anonymous by design, making them attractive for terrorist financing, particularly when the payment system is based in a jurisdiction with a comparatively weaker anti money laundering /counter terrorist financing regime. Virtual currencies represent a great opportunity for financial innovation, but they have also attracted the attention of various criminal groups, and may pose a risk for terrorist financing. This technology allows for anonymous transfer of funds internationally. While the original purchase of the currency may be visible (e.g., through the banking system), all following transfers of the virtual currency are hard to detect. [40] There are „similar regulatory challenges in the fight against money laundering, terrorist financing and tax evasion via cryptocurrencies."[41] These are the following: Anonymity: „…the anonymity prevents cryptocurrency transactions from being adequately monitored, allowing shady transactions to occur outside of the regulatory perimeter, allowing criminal organisations to use cryptocurrencies to obtain easy access to "clean cash" (both cash in/out)."[42] The cross-border nature of cryptocurrencies, crypto markets and crpyto players. „There is often no central intermediary, such as an issuer, that would normally be the focal point of regulation."[43] Cryptocurrencies are falling between the cracks: „There are simply no rules

unveiling the anonymity associated with crypto-currencies, making the question whether they are taken at the right level or to whom they apply a superfluous one. Because of the absence of rules unveiling anonymity, more substantive rules that currently could already have cryptocurrencies in scope completely miss effect."[44] Also, there is a difficult dividing line with cybersecurity, data protection and privacy.[45] Further: „… legislative action should always be proportionate so that it addresses the illicit behaviour while at the same time not strangling technological innovation at birth." [46]

IV.4 Virtual Currencies

Financial transactions on the internet are on the rise. As Dávid Tóth warns: „Newer type of payment instruments, virtual currencies appear (e.g. bitcoin, Litecoin etc) appear and their legal status is not fully clear. On one hand the development of information technology made it easier to undertake financial services, on the other hand offenders have more and more option to misuse[47] these."[48]

Virtual currencies -which include cryptocurrencies such as Bitcoin, as well as a range of other digital value-transfer methods –are innovative new technologies that enable digital transactions and the delivery of financial products and services in new online networks, environments and marketplaces."[49] They have features that present risks for facilitating criminality, including money laundering and terrorist financing. The borderless, peer-to-peer (P2P) nature of certain virtual currencies offers the prospect for terrorists to transfer funds outside the regulated sector and beyond the purview of anti-money laundering and counter terrorist financing authorities.[50] Terrorists can use the Dark Web for fundraising, money transfers, and illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies. For example, the "Fund the Islamic Struggle without Leaving a Trace" is a Deep Web page which invites donations for Jihad through transactions to a particular Bitcoin address. A PDF document posted online under the pseudonym of Amreeki Witness titled "Bitcoin wa Sadaqat alJihad," which translates to "Bitcoin and the Charity of Violent Physical Struggle," is a guide for using the Dark Web for secretive financial transactions.[51]

There are documented instances of virtual currencies' illicit use in cybercrime and in encrypted Dark Web marketplaces. However, there are still only a few documented and confirmed cases of terrorist financing involving virtual currencies. In their current form and at current levels of adoption, they may not present terrorists with substantial advantages over other methods of funding and financing they already use. Nevertheless, the public record

shows that religiously and politically-inspired extremists have utilised virtual currencies, if in relatively low-volume and unsystematic fashion, and may be seeking to expand their use. In the near future, terrorists' use of virtual currencies is most likely to involve occasional use for specific and limited purposes, including: raising funds or procuring illicit items on the Dark Web; soliciting donations in crowdfunding campaigns conducted on social media and encrypted messaging platforms; and transmitting funds internationally among members of terrorist networks using P2P value transfers.[52]

While there have been isolated instances of terrorist groups and their supporters soliciting funds in virtual currencies and using them to move funds or purchase goods or services, according to the 2018 NATIONAL TERRORIST FINANCING RISK ASSESSMENT (2018 NTFRA): „virtual currencies do not currently present a significant terrorist financing risk, but bears close monitoring as it is only likely to grow. However, lack of regulation and supervision in most jurisdictions worldwide exacerbates the illicit finance and sanctions evasion risks that virtual currency payments present."[53] Tom Keatinge and Florence Keen have also judged the terrorist financing risks of cryptocurrency low, but they recognise the potential for abuse: „In light of Facebook's recent announcement of plans to launch its own cryptocurrency 'Libra', the convergence of social media and cryptocurrency is inevitably attracting considerable scrutiny and remains an area to watch regarding the potential for terrorist-financing abuse."[54]

Cryptocurrencies are introducing new forms of crowdfunding, making, in most cases, a clear distinction between crowdfunding online campaigns to finance terrorism behind a false intent and those made for explicit militaristic purposes. Crowdfunding campaigns requiring donations in digital currencies are more explicit about their terrorist financing purposes. These campaigns do not encourage interaction among users, but rather provide instructions on how to keep themselves as anonymous as possible.[55]

At the end of January 2019 the military wing of Hamas, the al-Qassam Brigades, called on its supporters to send Bitcoin to the group. Soon after announcing its intention to crowdfund through Bitcoin, the al-Qassam Brigades posted infographics about Bitcoin on social media and provided a Bitcoin address to which the donors could send funds. Within a day, the Hamas digital wallet received roughly $900, although it can not be verified if all funds came from external parties. Most donations were less than $100, although a few were larger. Then, days later, the group posted an additional Bitcoin address. In less than a week, its wallets received over $2,500 worth of Bitcoin.[56] Later Hamas changed the donation mechanism, with its website generating a new digital wallet with every transaction. Originally, al-Qassam Brigades asked donors to send bitcoin to a single digital address, or wallet. This makes it harder for companies around the world to keep tabs on the group's cryptocurrency financing. A single digital wallet can be red-flagged to cryptocurrency exchanges, in theory allowing

them to prevent funds moving through their systems to that destination. But a different wallet for each donation makes this so-called tagging far more complicated. Between March 26 and April 16, 0.6 bitcoin – worth around $3,300 – was sent to the website-created wallets. The fundraising campaign has raised around $7,400 in four months.[57]
In the first five months of 2020, crypto thefts, hacks, and frauds totaled $1.36 billion, indicating 2020 could see the greatest total amount stolen in crypto crimes outside 2019's $4.5 billion. Coronavirus-inspired fraud is generally executed by luring victims off legitimate platforms into chat rooms where payment in bitcoin can be requested. COVID-19-related phishing sites were found to be the most popular COVID-19 related products sold on the dark web; dark web PPE sales have been mostly unsuccessful.[58]

IV.5 The risk of Stablecoins

Stablecoins are cryptocurrencies that are increasingly gaining traction. The are much more fixed than normal cryptocurrencies. This is because their values are pegged to other assets such as the US dollar or gold. In general, a stablecoin is a cryptocurrency that is collateralized to the value of an underlying asset. As a result of this, stablecoins enjoy the many benefits of being a cryptocurrency (such as transparency, security, privacy, etc.) without the extreme volatility that comes with most other types of digital coins. Stablecoins aim to mimic traditional, stable currencies, in the form of digital money. What that underlying asset may be varies from coin to coin.[59] The FATF recognised that these stablecoins have the potential to spur financial innovation and efficiency and improve financial inclusion. However, like other large-scale value transfer system, stablecoins have potential to be abused for money laundering or terrorist financing. The FATF found that its Standards apply to stablecoins and a range of businesses in a stablecoin arrangement will have Anti-Money Laundering/Combating the Financing of Terrorism obligations. The FATF highlights that it is important that money laundering/terrorist financing risks are analysed in an ongoing and forwardlooking manner and are mitigated before stablecoins are launched.[60] The FATF has found that stablecoins share many of the same potential money laundering/terrorist financing risks as some virtual assets, in virtue of their potential for anonymity, global reach and layering of illicit funds. Depending on how they are designed, they may allow anonymous peer-to-peer transactions via unhosted wallets. These features present money laundering/terrorist financing vulnerabilities, which are increased if there is mass adoption.[61]

IV.6 Prepaid Cards

The increasing use of prepaid cards and other magnetic-stripe products to hide illicit proceeds, launder money and to fund acts of terrorism, is an increasing threat.[62] What are prepaid cards? "Prepaid cards are cards with data encoded directly in the card, or stored remotely, that are preloaded with a fixed amount of electronic currency or value. While there are a wide variety of prepaid cards, the category of card of most concern is open-loop cards where funds can be withdrawn at ATMs worldwide."[63] With a prepaid card, one can load a balance ahead of time and use it anywhere one's card network—Mastercard, Visa, Discover, or American Express—is accepted. In that respect, it's very much like a debit card, but without the bank account attached.[64] Prepaid cards are replacing travellers' cheques as a method of moving money offshore. These cards can be loaded domestically via cash or non-reportable electronic methods and carried offshore inconspicuously with no requirement to declare their movement across the border. When one arrives in a high-risk country or transit country for terrorist financing, then the funds can be converted back to cash through multiple offshore ATM withdrawals, restricted only by ATM withdrawal limits. Once a loaded card has been carried offshore, funds are accessible with minimal chance of detection.[65]

IV.7 Internet based payment services

What are internet based payment services? "Internet-based payment services provide mechanisms for customers to access, via the Internet, prefunded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider."[66] Pre-funded accounts that consumers use for online auction payments are among the most dominant Internet based payment services. Recipients may or may not be required to register with the payment service provider to receive a funds transfer. Some terrorist financing cases involving low-value transactions via online payment systems such as PayPal have also been linked to a number of terrorist suspects. The extent to which these transactions have been used to finance terrorism is unclear. Terrorist suspects have been observed using multiple online payment accounts, combining both verified and guest accounts. Payments appear to be linked to online purchases of equipment and clothing prior to the departure of persons travelling to conflict zones rather than direct payments to associates to fund terrorist activities.[67] According to the FATF REPORT Emerging Terrorist Financing Risks October 2015 the use of an online payment system to assist in terrorist financing is more of a reflection of the prevalence of this payment system in the wider financial system rather than

any indication that online payment systems are more vulnerable to terrorist financing.[68] Islamic militants based in the Middle East used bitcoin and online-payment services such as PayPal to fund terrorist activities in Indonesia, in 2017: „…militants sent the money to their terror cells across Indonesia, largely in Java, through PayPal and bitcoin exchanges. Since internet access is limited in rural areas, they would have to change virtual money back to cash to pay for the real-life transactions…"[69]

IV.8 Exploitation of natural resources

As FATF states, criminal activity related to this sector includes extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes.[70] Taliban and ISIS made dollar millions from mining Afghan minerals.[71] Groups that are involved in illegal logging and mining include the Taliban and the Haqqani network in Afghanistan, FARC and other leftist guerrillas and rightist paramilitaries in Colombia, the RUF (Revolutionary United Front) in Sierra Leone, and Khmer Rouge in Cambodia, and many other groups.[72]
Some terrorist organizations fund themselves by poaching and by the associated illegal wildlife trafficking. Wildlife poaching is a very lucrative and the least-riskycriminal venture, so it is a very comfortable income for terrorist financing. [73]

IV.9 Other varied revenue streams

In Sweden, loans have been used as as a way to finance terrorism, which primarily are raised by individuals who are travelling to other countries to join terrorist organisations. For example, student loans, quick (unsecured) loans and business loans are the types of loans that have been abused for terrorist financing purposes.
Value addad tax (VAT) fraud is also a lucrative method to finance terrorism. This type of fraud can generate very large sums, particularly in consumer goods that are easily resold. These schemes often involve designated 'fall-guys' who take the legal and financial consequences when the fraud is detected.
Social insurance fraud and frauds related to car leasing and counterfaited goods are also used to finance terrorism. [74]

1. Virtual environments/MMOs

The ease in which MMOs[75] such as Second Life, World of Warcraft and Entropia Universe can be used for crimes such as money laundering, fraud and terrorist financing and the opportunity they offer for allowing large sums of money to be moved across national borders without restriction and with little risk of being detected are raising concerns."[76]At the moment, these virtual environments are not subject to the strict financial controls and reporting requirements of the real world, so they offer an excellent opportunity for criminals and terrorist financers to carry out their illegal activities unchecked and with impunity.[77]

1. Some Examples for sources of funding

VI.1 ISIS' sources of funding

The Islamic State has been described as the wealthiest terrorist group in history.[78] ISIS earned revenue primarily from five sources, listed in order of magnitude: 1. illicit proceeds from occupation of territory, such as bank looting, extortion, control of oil fields and refineries, and robbery of economic assets and illicit taxation of goods and cash that transit territory where ISIS operates; 2. kidnapping for ransom; 3. donations including by or through non-profit organisations; 4. material support such as support associated with FTFs and 5. fundraising through modern communication networks. These revenue streams are/were inconsistent and shift based on the availability of economic resources and the progress of coalition military efforts against ISIS. [79] Two sources of revenue generated the lion's share of its war chest: oil and taxation (that incudes extrortion). ISIS' overall 2015 revenues have been estimated to range from $1 billion to $2.4 billion.[80]
With the fall of Baghuz, Syrian Arab Republic, in March 2019, the geographical "caliphate" of Islamic State in Iraq and the Levant (ISIL) has ceased to exist and the group has continued its evolution into a mainly covert network.[81]
ISIS is reported to lack liquid funds to run operations and therefore to be exploring ways to raise money. It has been undertaking new criminal activity and benefiting from funds that it had generated through legitimate businesses. With the end of the "caliphate", some ISIS leaders in the Syrian Arab Republic have been dispersed to other areas around the country, and the group was seeking to transfer money to them while concealing their locations. This is the priority for available ISIS financial resources. The Islamic State is estimated to have

between $50 million and $300 million remaining from the revenues of the “caliphate”.[82]

VI.2 Boko Haram’s sources of funding

Boko Haram, like other terrorist organizations, depends on resources to carry out its activities. Several methods, instruments, and strategies have been used by Boko Haram to finance its activities across the region. These sources, as detailed above, include membership contributions, granting loans to members, support from local and international sympathizers, as well as other black-market operations such as the trafficking of persons, narcotics, arms sale, armed robbery, kidnapping, and other unverified sources such as the collection of taxes in areas perceived to be under their control, and the control of the agricultural activities in the Lake Chad region. These methods and channels have assisted the terrorist organization with recruiting more members and consolidating its position.[83]

VII. The effect of the coronavirus pandemic on terrorist financing and its online aspects

The kex findings of the FATF regarding the problem are the following: The increase in COVID-19-related crimes, such as fraud, cybercrime, misdirection or exploitation of government funds or international financial assistance, is creating new sources of proceeds for illicit actors. Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour so that profit-driven criminals may move to other forms of illegal conduct. The COVID-19 pandemic is also impacting government and private sectors’ abilities to implement anti-money laundering and counter terrorist financing obligations from supervision, regulation and policy reform to suspicious transaction reporting and international cooperation. These threats and vulnerabilities represent emerging money laundering and terrorist financing risks. Such risks could result in: Criminals finding ways to bypass customer due diligence measures; Increased misuse of online financial services and virtual assets to move and conceal illicit funds; Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds; o Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds; Misuse and misappropriation of domestic and international financial aid and emergency funding; Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries. Anti-money laundering and counter terrorist financing

policy responses can help support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities. These responses include: Domestic coordination to assess the impact of COVID-19 on anti-money laundering and counter terrorist financing risks and systems; Strengthened communication with the private sector; Encouraging the full use of a risk-based approach to customer due diligence; Supporting electronic and digital payment options.[84]

According to the survey of Moneyval[85], it appears that during the COVID-19 restrictions, the overall level of criminality remained stable or slightly decreased. This was a result of restrictions in physical movement and cross-border travelling. However, in case of a limited number of crimes, a rise was reported. While some trends have been noted, as described below, it is still pre-mature to devise any typologies, as the COVID-19 crisis is novel, and authorities do not yet have sufficient information on their hands. There was no reported increase in crimes related to drug trafficking, terrorist financing, abuse of NPOs and insider trading. On the other hand, several jurisdictions highlighted instances where medicrime, cybercrime and corruption grew. All jurisdictions noted a significant and rapid growth in the number of frauds related to COVID-19 and the adaptation of well-known fraud to the new (confined and more remote) lifestyle of individuals and businesses. Despite the economic downturn, illicit financial flows continue to run, criminals seeking to exploit temporary weakness in anti-money laundering and counter terrorist financing controls of financial institutions, designated non-financial businesses and professions and virtual asset service providers (VASPs). Due to the financial standstill caused by preventing further spread of COVID-19 pandemic there is a risk that anti-money laundering and counter terrorist financing measures will be relaxed or considered less of priority in order to boost the economy and expedite process of payments.[86]

VIII. Conclusion

A country’s regime to counter money laundering and terrorist financing has three primary objectives. The first is to deter money launderers and terrorist financiers from using a country’s financial system for illicit purposes. The second is to detect money laundering and terrorist financing when and where they occur, and the third is to prosecute and punish those involved in such schemes.[87] Because money laundering and terrorist financing are complex crimes, multiple national agencies must be involved in the various aspects of preventing, detecting, and prosecuting them. The specific agencies involved may vary from country to country, but the collaboration of the following areas is needed for an effective, overall

AML/CFT regime: legislature; executive branch or ministries; judiciary; law enforcement, including police, customs, and so forth; FIU; supervisors of banks, including the central bank, of other financial institutions, and of DNFBPs. It is important to establish a unified set of objectives and priorities for the overall regime, and to have collaboration and coordination among the various public sector constituencies.[88] Legislation may not be enough to combat terrorist financing, even with improvements in compliance, anti-money laundering/counter-terrorist financing legislation may remain less than effective in many countries for three main reasons: First, many developing countries' economies are cash-based. Direct cash payments often leave no paper trail and this makes enforcement of any regulations around monetary flows impossible. Second, the ways in which terrorist organisations fund themselves are evolving. Similarly to organised crime, terrorists adapt quickly, they recognise financing opportunities and utilise small-scale sources of funds. Third, the cost of perpetrating acts of terrorism are decreasing, as terrorist tactics are changing, groups increasingly rely on self-funded individuals.[89] Terrorist financing needs to be countered in an efficient way, as this is a key phenomenon that lets terrorist groups to thrive. Terrorists are continuously increasing and evolving their ability to diversify and renew not only the source of their funds, but also the channels and instruments they use to transfer those funds. Efficient coordination and cooperation among financial intelligence units, law enforcement entities and intelligence services, and to ensure strong political commitment on all levels is essential. Given its transnational nature, terrorist financing needs to be analysed and assessed not only from a national perspective but also from a sectoral, regional, supranational and even global perspective. Financial assets continue to adapt to the globalized nature of the economy and of financial systems, and regional, supranational and global risk assessments are needed. An international approach to countering terrorism and terrorist financing has become increasingly important.[90] Keeping up to date with the latest and constantly evolving techniques and sources of terrorist financing is crucial in the fight against terrorism and terrorist financing.

[1] The „sources and techniques of terrorist financing" or „a terrorizmus finanszírozásának forrásai és technikái" in Hungarian is Gál's phrasing. István László Gál: A terrorizmus finanszírozásának fogalma és technikái a XXI. században, Szakmai Szemle, No. 2, (2016), 91.

[2] „Coronaviruses (CoV) are a large family of viruses that cause illness ranging from the common cold to more severe diseases. A novel coronavirus (nCoV) was identified on 7

January 2020 and was temporarily named “2019-nCoV”. It was subsequently named the “COVID-19 virus”.
WHO announced COVID-19 outbreak as a pandemic on 11 March 2020.” https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19 (accessed 05 December 2020)

[3] COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, Paris FATF, 2020, 4. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (accessed 05 December 2020)

[4] Rahul De’ – Neena Pandey – Abhipsa Pal: Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice, International Journal of Information Management Vol. 55, (2020), 1.

[5] Covid 19 and E-commerce: Findings from a survey of online consumers in 9 Countries. United Nations Conference on Trade and Development, 2020, 4. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf (accessed 05 December 2020)

[6] On crimes committed by computer in detail: Zoltán Nagy: Bűncselekmények számítógépes környezetben, Budapest, Ad Librum, 2009.

[7] Zoltán András Nagy: A kiber-háború új dimenzió – a veszélyeztetett állambiztonság, in Gyula Gaál – Zoltán Hautzinger (eds.): Pécsi Határőr Tudományos Közlemények, Vol. 13: Tanulmányok. „A biztonság rendészettudományi dimenziói – változások és hatások” című tudományos konferenciáról, Pécs, Magyar Hadtudományi Társaság Határır Szakosztály Pécsi Szakcsoportja, 2012, 221-235.

[8]Sean McCrossan: Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles, CAMS-FCI, 2015, 15.

https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (accessed 05 December 2020)

[9] Viorel Pasca – Daniela Simona Orza: Terrorism: between the need for funding and obtaining funding sources, Journal Of Eastern-European Criminal Law No.1 (2019), 227.

[10] István László Gál: A tőkepiac büntetőjogi védelme Magyarországon, Pécs, Kódex Nyomda

Kft., 2019, 153.

[11] Michael Freeman: The Sources of Terrorist Financing: Theory and Typology, Studies in Conflict and Terrorism Vol. 34, No. 6, (2011), 462.

[12] István László Gál: A tőkepiac büntetőjogi védelme Magyarországon, Pécs, Kódex Nyomda Kft., 2019, 153.

[13] Arabinda Acharya: Targeting Terrorist Financing: International Cooperation and New Regimes, London and New York, Routledge, 2009, 7.

[14] Angela Irwin – Jill Slay: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraf, in Craig Valli (ed.): Proceedings of the 2010 International Cyber Resilience Conference ICR2010, Perth, Edith Cowan University, 2010, 41-42.

[15] Maria Bergström: The Global AML Regime and the EU AML Directives: Prevention and Control, in Colin King – Clive Walker – Jimmy Gurulé (eds.): The Palgrave Handbook of Criminal and Terrorism Financing Law, London, Palgrave Macmillan, 2018, 35.

[16] https://www.fatf-gafi.org/about/historyofthefatf/ (accessed 05 December 2020)

[17] https://www.fatf-gafi.org/about/membersandobservers/ (accessed 05 December 2020)

[18] FATF REPORT: Terrorist Financing Risk Assessment Guidance, Paris, FATF, 5. www.fatf-gafi.org/publications//methodsandtrends/documents/Terrorist-Financing-Risk-AssessmentGuidance.html (accessed 05 December 2020)

[19] István László Gál: Bejelentés vagy feljelentés? A pénzmosás és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek, Budapest, Penta Unió, 2009, 169-171

[20] Ulrich Sieber – Benjamin Vogel: Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht, Max-Planck-Institut für ausländisches und internationales Strafrecht, Berlin, Duncker & Humblot, 2015, 10.

[21] Freeman: The Sources of Terrorist Financing: Theory and Typology, 465-470.

[22] R. E. Bell: The Confiscation, Forfeiture and Disruption of Terrorist Finances, Journal of

Money Laundering Control, Vol. 7, No. 2, (2003), 106-107.

[23] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 13-20. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[24] Ibid., 23.

[25] Ibid., 30-31.

[26] Geneva Academy of International Humanitarian Law and Human Rights, Academy Briefing No. 7—Foreign Fighters under International Law, Geneva, 2014, 3. cited by Foreign Terrorist Fighters Manual for Judicial Training Institutes South-Eastern Europe. Vienna, United Nations Office on Drugs and Crime, Vienna, 2017, 3.

https://www.unodc.org/documents/frontpage/2017/Foreign_Terrorist_Fighters.pdf (accessed 05 December 2020)

[27] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 24-30. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[28] S/2019/570 Twenty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, United Nations Security Council, 2019, 5.

[29] Ibid., 6.

[30] https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/ (accessed 05 December 2020)

[31] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 30-31. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[32] More on the topic: István László Gál – Márton Tibor Serbakov: How Acts of Terrorism are

Financed and Orchestrated in Secrecy Today: Criminal Offenses, Donations, Legal Businesses and Smartphone Applications, Journal Of Eastern-European Criminal Law No.1 (2019), 66-76.

[33] https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html (accessed 05 December 2020)

[34] Social Media & Terrorism Financing Report, Sydney South, APG/MENAFATF, 2019, 1. http://menafatf.org/sites/default/files/FINAL-TM-SF-en.pdf (accessed 05 December 2020)

[35] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 32. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[36] John Roth – Douglas Greenburg – Serena Wille: National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing. Staff Report to the Commission, National, Washington D.C., Commission on Terrorist Attacks upon the United States, 2004, 21. https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf (accessed 05 December 2020)

[37] https://www.cfr.org/backgrounder/tracking-down-terrorist-financing (accessed 05 December 2020)

[38] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 35-38. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[39] Sylvia Windya Laksmi: Terrorism Financing And The Risk Of Internet-Based Payment Services In Indonesia, Counter Terrorist Trends and Analyses Vol. 9, No. 2, (2017), 21.

[40] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 35. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[41] Robby Houben – Alexander Snyers: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion, Brussels, Policy

Department for Economic, Scientific and Quality of Life Policies (European Parliament), 2018, 53.

http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (accessed 05 December 2020)

[42] Ibid., 53.

[43] Ibid., 54.

[44] Ibid., 54

[45] Ibid., 55.

[46] Ibid., 56.

[47] More on the options of misuse of virtual currencies: Dávid Tóth: A virtuális pénzekkel kapcsolatos visszaélések, in Noémi Emőke Baráth – József Mezei (eds.)? Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével, Budapest, Doktoranduszok Országos Szövetsége Rendészettudományi Osztálya, 2019. 242-250.

[48] Dávid Tóth: Credit card fraud with a comparative law approach, International Scientific Conference "Towards a Better Future: Democracy, EU Integration and Criminal Justice", Conference Proceedings, Volume I, Bitola, Faculty of Law – Kicevo, University "St. Kliment Ohridski" – Bitola, 2019. 232.

[49] Tom Keatinge – David Carlisle – Florence Keen: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Brussels, Policy Department for Citizens' Rights and Constitutional Affairs, 2018, 9.

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (accessed 05 December 2020)

[50] Ibid., 9.

[51] Gabriel, Weimann: Terrorist Migration to the Dark Web, Perspectives on Terrorism Vol. 10, No. 3, (2016), 42. o.

[52] Tom Keatinge – David Carlisle – Florence Keen: Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Brussels, Policy Department for Citizens' Rights and Constitutional Affairs, 2018, 9.

http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (accessed 05 December 2020)

[53] National Terrorist Financing Risk Assessment, 2018, 3.

https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf (accessed 05 December 2020)

[54] Tom Keatinge – Florence Keen: Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, London, Royal United Services Institute for Defence and Security Studies, 2019, 8.

https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf (accessed 05 December 2020)

[55] https://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone/ (accessed 05 December 2020)

[56] https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f (accessed 05 December 2020)

[57] https://www.jpost.com/middle-east/crypto-terror-financing-hamas-shifts-tactics-in-bitcoin-fundraising-587930 (accessed 05 December 2020)

[58] https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/ (accessed 05 December 2020)

[59] https://www.cbinsights.com/research/report/what-are-stablecoins/ (accessed 05 December 2020)

[60] FATF Report 2019-2020, Paris, FATF, 2020, 14. www.fatf-gafi.org/publications/fatfgeneral/documents/annual-report-2019-2020.html (accessed 05 December 2020)

[61] FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, Paris, FATF, 2020, 2. www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html (accessed 05 December 2020)

[62] Growing Threat Of Electronic Money Laundering And Terrorism Financing: POIDN Alert No. 1/2017, Jakarta, United Nations Office on Drugs and Crime, (2017), 1.

http://www.unodc.org/documents/indonesia/publication/alert/POIDN_Alert_No._1_-_2017_-_English.pdf (accessed 05 December 2020)

[63] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 36. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[64] https://www.investopedia.com/are-prepaid-cards-right-for-you-4590082 (accessed 05 December 2020)

[65] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 36-37. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (accessed 05 December 2020)

[66] Ibid., 37.

[67] Ibid., 37-38.

[68] Ibid., 38.

[69] https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198 (accessed 05 December 2020)

[70] FATF REPORT: Emerging Terrorist Financing Risks, Paris, FATF, 2015, 39. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pd

f (accessed 05 December 2020)

[71] https://www.bloomberg.com/news/articles/2018-05-22/taliban-islamic-state-make-millions-from-mining-afghan-minerals (accessed 05 December 2020)

[72] https://www.brookings.edu/articles/wildlife-and-drug-trafficking-terrorism-and-human-security/(accessed 05 December 2020)

[73] Balázs Elek: From poaching to financing terrorism: Thoughts on poaching endangering society, Journal of Eastern European Criminal Law No.1, (2016), 192-193.

[74] Terrorism financing – a summary, Finansinspektionen, 2016, 4.

https://www.fi.se/contentassets/1944bde9037c4fba89d1f48f9bba6dd7/terrorism-financing-summary-160315_eng.pdf (accessed 05 December 2020)

[75] „MMO is an online multiplayer game which a large number of people can play simultaneously.” https://plarium.com/en/blog/difference-between-mmo-and-mmorpgs/ (accessed 05 December 2020)

[76] Irwin – Slay: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraf, 43.

[77] Ibid., 41.

[78] Colin P. Clarke – Kimberly Jackson – Patrick B. Johnston – Eric Robinson – Howard J. Shatz: Financial Futures of the Islamic State of Iraq and the Levant Findings from a RAND Corporation Workshop, Santa Monica, RAND Corporation, 2017, 3.

https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF361/RAND_CF361.pdf (accessed 05 December 2020)

[79] FATF REPORT: Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL), Paris, FATF, 2015, 12. http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf (accessed 05 December 2020)

[80] Ibid., 8.

[81]S/2019/570 Twenty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities, United Nations Security Council, 2019, 3.

[82] Ibid., 7.

[83] Kangdim Dingji Maza – Umut Koldaş – Sait Aksit: Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram. *SAGE Open* (2020), 6. https://doi.org/10.1177/2158244020934494

[84] COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses, Paris, FATF, 2020. 4. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (accessed 05 December 2020)

[85] „The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems." https://www.coe.int/en/web/moneyval (accessed 05 December 2020)

[86] Committee Of Experts On The Evaluation Of Anti-Money Laundering Measures And The Financing Of Terrorism Moneyval: Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis, Strasbourg, Council of Europe, 2020, 5. https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3 (accessed 05 December 2020)

[87]Pierre-Laurent Chatain – John McDowell – Cédric Mousset – Paul Allan Schott – Emile van der Does de Willebois: Preventing Money Laundering and Terrorist Financing: A Practical Guide for Bank Supervisors, Washington, D.C., World Bank Publications, 2009, 3.

[88] Ibid., 9.

[89] http://visionofhumanity.org/news/combating-the-financing-terrorism/ (accessed 05 December 2020)

[90] Guidance manual for Member States on terrorist financing risk assessments, Vienna, United Nations, 2018, 1.https://www.unodc.org/documents/terrorism/Publications/CFT%20Manual/Guidance_Manual_TF_Risk_Assessments.pdf (accessed 05 December 2020)