**ADMINISTRATION FOR THE PREVENTION OF MONEY LAUNDERING**

**August 2024**

**GUIDELINES FOR AML/CFT OBLIGED ENTITIES FOR IDENTIFYING, DETECTING AND PREVENTING TERRORISM FINANCING**



Contents

[INTRODUCTION 3](#_Toc188604980)

[OBJECTIVE AND METHODOLOGY 4](#_Toc188604981)

[LEGAL FRAMEWORK 5](#_Toc188604982)

[INTERNATIONAL FRAMEWORK 7](#_Toc188604983)

[FINANCING OF TERRORISM 8](#_Toc188604984)

[NATIONAL STRATEGY FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING 10](#_Toc188604985)

[NATIONAL TERRORIST FINANCING RISK ASSESSMENT 11](#_Toc188604986)

[ANALYSIS OF THE TERRORISM FINANCING RISK 13](#_Toc188604987)

[INDICATORS FOR IDENTIFYING TERRORIST FINANCING 16](#_Toc188604988)

[DIGITAL (VIRTUAL) ASSETS 18](#_Toc188604989)

[Legal framework 18](#_Toc188604990)

[National risk assessment, legal framework, international standards 18](#_Toc188604991)

[Prohibition of the use of digital assets in regulated sectors 19](#_Toc188604992)

[Terrorist Financing Risk Assessment in the Digital Asset Sector (NRA) 20](#_Toc188604993)

[International practice, FATF indicators 21](#_Toc188604994)

[APML experiences 22](#_Toc188604995)

[Results achieved – international experience with FATF Recommendation 15 22](#_Toc188604996)

[NON-PROFIT ORGANIZATIONS (NPOs) 23](#_Toc188604997)

[Legal framework for NGOs in Serbia 23](#_Toc188604998)

[Analysis of the NPO sector from the TF perspective 23](#_Toc188604999)

[Analysis of risk assessment for NPOs as a form of organization, and categorization client risk (low, medium, high) 24](#_Toc188605000)

[Analysis of the NPO sector in the Serbian context (NRA findings) 24](#_Toc188605001)

[Some recommendations (guidelines) for obliged entities under the AML/CFT Law – how to know your NPO client better (establishing business relationship, monitoring) in order to reduce suspicion of terrorist financing 24](#_Toc188605002)

[DESIGNATED PERSON –DESIGANTION PROCEDURE 26](#_Toc188605003)

[Designation process 26](#_Toc188605004)

[Updating the list and searching for designated persons 27](#_Toc188605005)

[The process of reporting a designated person 27](#_Toc188605006)

[METHODS AND TRENDS OF TERRORISM FINANCING IN THE REPUBLIC OF SERBIA 29](#_Toc188605007)

[THREE TRENDS IN TERRORISM, CHALLENGES, OBSERVED SHORTCOMINGS AND CAPACITY BUILDING NEEDS 30](#_Toc188605008)

[Trend 1 30](#_Toc188605009)

[Trend 2 30](#_Toc188605010)

[Trend 3 30](#_Toc188605011)

[Identified gaps and capacity needs 30](#_Toc188605012)

[REFERENCES 32](#_Toc188605013)

# INTRODUCTION

It has long been known that terrorism is a global threat to peace and stability throughout the world. Terrorism as such knows no borders, specific regions, nor is it tied exclusively to individual states. It threatens, sows fear, kills, impoverishes, and economically and psychologically destabilizes entire social communities and people as individuals.

"Terrorism is identified in the Republic of Serbia as a threat to the fundamental values on which the rule of law, human rights and freedoms are based, including peace and security of citizens, sovereignty and territorial integrity, stability and security of the state and legitimately elected authorities, as well as international peace and other goods protected by international law. At the same time, the Republic of Serbia opposes linking terrorism to any religious, ethnic or other group and continuously advocates for sustainable development and the advancement of a peaceful and inclusive society in which equal access to justice is ensured for all.”

The Republic of Serbia unequivocally condemns terrorism in all its forms, as well as all forms of extremism and radicalism, and in this field it is making strong efforts to oppose and combat such phenomena. The international complexity of terrorism, the phenomena and forms of terrorist acts require coordinated action in a global sense and addressing all aspects of terrorism in order to provide a comprehensive response to threats, acts and consequences. In this sense, the Republic of Serbia understands, undertakes and provides assistance and comprehensive cooperation to the global community at the international level. More precisely, the state is ready to contribute, in coordination with regional and global actors through various forms of bilateral and multilateral cooperation and networking, to the identification of security challenges, risks and threats at the national and regional levels, as well as to the timely fight against them and the elimination of possible consequences.

In this context, the Republic of Serbia is actively involved in combating terrorist phenomena and challenges through the United Nations (UN) and other relevant international and intergovernmental organizations, as well as in providing support to counter-terrorism policies.

# OBJECTIVE AND METHODOLOGY

The aim of this document is to indicate and assist the obliged entities under the Law on the Prevention of Money Laundering and Financing of Terrorism (hereinafter: AML/CFT Law), in taking appropriate preventive action and measures in relation to identifying, detecting and preventing terrorist financing (TF). From the obliged entity’s perspective, one of the questions is how to objectively identify possible TF activities. These guidelines intends to highlight that in addition to complying with the law, the obliged entity will best do so by developing a proper and objective, mandatory client risk analysis, which is an approach favoured by the international standards (FATF). There is often a practice of applying a list of indicators as the way to identify suspicious activities of both ML/TF. The approach to risk analysis, applied knowledge and invested effort are the best prevention and fight against terrorist financing. Since a good risk analysis is not solely based on it being drafted in accordance with the law, but it should also address a broader context of the applicable domestic and international experiences and knowledge (typologies, trends, guidelines, etc.), this document provides obliged entities with insight into the complexity of the situation, phenomena and forms of terrorist financing.

This document is divided in two parts, the first of which comprises introduction, chapters on the legal and international framework and provides the definition to highlight importance of the TF phenomenon. The second part provides practical tips regarding the development of a risk analysis. Data from the National Risk Assessment, domestic trends (typologies), the application and importance of indicators, the emergence of digital assets - virtual currencies, international trends and challenges can contribute to a broader and higher-quality approach to the development of risk analysis, i.e. a more comprehensive approach to understanding the issues of terrorism and its financing.

# LEGAL FRAMEWORK

The most significant legal acts in the field of preventing and combating the financing of terrorism for the Republic of Serbia are the instruments of the United Nations (UN), starting from the General Assembly Resolution of December 1972 to the Security Council Resolution of March 28, 2019.[[1]](#footnote-2)

Relevant domestic TF-related legislation are the Criminal Code[[2]](#footnote-3), Criminal Procedure Code[[3]](#footnote-4), Law on the Organization and Competences of State Authorities in Suppressing Organized Crime, Terrorism and Corruption[[4]](#footnote-5), Law on Freezing of Assets with the Aim of Preventing Terrorism and the Proliferation of Weapons of Mass Destruction (LAF)[[5]](#footnote-6), Law on the Prevention of Money Laundering and Financing of Terrorism (AML/CFT Law)[[6]](#footnote-7), and Law on International Restrictive Measures.[[7]](#footnote-8)

The TF criminal offense in Serbia:

* First criminalised in 2005 by the Criminal Code (CC), the act of commission was generally defined as the provision or collection of funds intended for financing the commission of criminal acts of association for the purpose of unconstitutional activity, terrorism and international terrorism;
* In 2009, the Criminal Code was amended to expand the definition in order to criminalize any method of collecting or securing funds, indirectly or directly, intended to finance the same criminal offenses;
* According to the 2013 amendment, terrorist financing also includes the provision of financial support to individuals, groups or organised criminal groups with the aim of committing the following criminal offences: terrorism, public incitement to commit terrorist offences, use of a deadly device, destruction and damage to a nuclear facility and endangering a person under international protection. Providing financial support in the context of these legal amendments does not necessarily require a plan to commit a specific terrorist act as a condition for incrimination;
* In 2019 , amendments to the Criminal Code further specified that financing of terrorism, within the meaning of the provisions of this law, is considered to be the provision of financial support to individuals, groups and organizations that aim to finance the commission of criminal offenses, listed in previous legal amendments, that may be considered criminal offenses of terrorism and other related criminal offenses. These amendments criminalized the provision of the same financial support for the commission of criminal offenses: kidnapping, unauthorized acquisition of nuclear materials and endangering safety with their use, endangering traffic by a dangerous act and a dangerous means, endangering the safety of air and maritime traffic or a fixed platform, and hijacking of aircraft, vessels and other means of transport. The expansion to the aforementioned criminal offenses intends to substantially align the criminalisations with relevant international conventions that also include the raising of funds to finance the commission of these criminal offenses that may indirectly be linked to terrorist offenses.

The above amendments describe in detail what is considered funds, the provision and collection of which may be considered terrorist financing within the meaning of these legal amendments.

This resulted in TF criminalisation that is in accordance with a number of conventions aimed at preventing terrorism, as well as with the recommendations of the Moneyval Committee.[[8]](#footnote-9)

Article 393 of the Serbian Criminal Code, which relates to the financing of terrorism, provides:

Whoever directly or indirectly secures or raises funds with the aim of using them or with the knowledge that they will be used in whole or in part to finance the commission of criminal offences under Articles 134, 287, 291, 292, 293 of this Code or to finance organisations whose aim is to commit such offences or members of such organisations or persons whose aim is to commit such offences, shall be punished by imprisonment for a term of one to ten years.

The assets referred to in paragraph 1 of this Article shall be considered to be all assets, tangible or intangible, movable or immovable, regardless of the method of acquisition and the form of the document or official document, including electronic or digital, evidencing title to or interest in those assets, including bank loans, traveller’s checks, money orders, securities, letters of credit and other instruments.

The funds referred to in paragraph 1 of this Article shall be confiscated.

The 2017 AML/CFT Law defined terrorist financing in Article 2, which further aligned it with EU standards and FATF recommendations. The law regulates the operations, activities and powers of the APML and the competent supervisory authorities. This law largely adopted relevant EU directives and provisions in line with the strategic goals of the Republic of Serbia.

Supervisory authorities under the AML/CFT Law monitor the implementation of regulations and the compliance of obliged entities ' internal systems with the tasks assigned to them by regulations, including whether obliged entities ' internal systems are established in a way that allows them to promptly identify phenomena, persons and activities that indicate suspicion of terrorist financing.

# INTERNATIONAL FRAMEWORK

The FATF[[9]](#footnote-10) standards highlight the obligation for countries, under international instruments in this area , to criminalise terrorist financing as a separate criminal offense by law, covering all elements of the Terrorism Financing Convention, as well as to implement mechanisms for transposing the obligations of the UN Security Council Resolutions adopted in this regard.

The FATF Recommendations provide a comprehensive and consistent framework of measures that countries should implement to effectively combat ML/TF, while implementing measures at the national level tailored to their specific circumstances. The Recommendations provide a comprehensive legal and institutional framework that gives countries the necessary tools to combat terrorist financing, including the following obligations:

* to identify, assess and understand the risks of terrorist financing (Recommendation 1);
* to comprehensively criminalize terrorist financing as a separate criminal offense (recommendation 5);
* to have targeted financial sanctions and asset freezing measures (Recommendation 6);
* to provide law enforcement agencies (LEAs) and financial intelligence units (FIUs) with all necessary powers and resources (Recommendations 29-31);
* to identify and prevent the illicit cross-border transportation of cash (Recommendation 32);
* to ensure urgent and constructive international and domestic cooperation (Recommendation 2, Recommendations 37-40);
* to take preventive measures to protect sectors that may be abused – FIs, DNFBPs, NPOs (Recommendations 8-23).

The UN Resolution of March 28, 2019, reiterated the extremely important role of the FATF in setting global standards in combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction (WMD), and encouraged member states to actively cooperate with that body.

# FINANCING OF TERRORISM

Terrorist financing is defined in Article 2 of the AML/CFT Law.[[10]](#footnote-11)

Terrorist financing is considered to be: the provision or raising of assets or the attempt to provide or raise it with the intention of using it or with the knowledge that it may be used in whole or in part:

* for committing a terrorist act;
* by terrorists;
* by terrorist organizations;

Terrorist financing also includes incitement and assistance in securing and collecting assets, regardless of whether a terrorist act has been committed and whether the assets have been used to commit a terrorist act.

What are the funds used or intended for from the TF perspective:

* for the execution of the terrorist act (attack) itself, as well as the preparatory phases;
* raising funds for terrorist training;
* promoting war and extremist ideology;
* for the purpose of establishing and operating terrorist organizations and groups;
* organizing training camps and terrorist training;
* recruiting supporters and members for terrorist organizations and groups;
* procurement of various military equipment;
* financing various trips whose purpose is "terrorism";
* social aspect: financial compensation to members of a terrorist organization for their engagement before and after a terrorist act, as well as support for their families;
* corrupt practices to secure: quasi-legitimate activities and businesses, legitimate personal documents ("quasi-citizenship");
* financing various forged documents.

The volume and sources of funds generated depend on many things, including:

* the degree of acceptance of the ideology of the terrorist organization, the level of organization of the terrorist organization (group, cell), its goals and effects;
* sponsors and donors that support terrorism in order to achieve certain goals that can be implemented by terrorist organizations;
* from financing channels: legitimate channels - financial and non-financial sectors of the economy, the more difficult way or through cash flow;
* from the degree of possible abuse of legitimate financial channels and their weak "resilience and vulnerability" to such financing (weak risk analysis from many aspects);
* Skill in using numerous and complex financial sector products, whereby the provider of services and products ignores the possible misuse of them;
* from the creativity and organization of money flows by terrorist organizations or individuals engaged in financing terrorist activities.

When it comes to the origin - the source of funds of terrorist organizations, they can come from:

* legal sources;
* state sponsorships;
* through seemingly legal social and charitable activities;
* abuse of non-profit organizations (NPOs);
* self-financing (from business income, social assistance, etc.).

Obliged entities under the AML/CFT Law should be clear that the role of the authorities, the private sector and NPOs in preventing TF is multiple and is reflected in:

1. detecting terrorism
2. deterrence from terrorism
3. preventing terrorism

Terrorism detection and terrorism deterrence are essentially interconnected and achieved through preventive interaction of the above CFT stakeholders.

NATIONAL STRATEGY FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING**[[11]](#footnote-12)**

In February 2020, the Government of the Republic of Serbia adopted the Strategy for the Prevention of Money Laundering and Terrorism Financing for the period 2020 - 2024 (AML/CFT Strategy) and the Action Plan for its implementation. The AML/CFT Strategy builds on the previous two strategies, from 2008 and 2015, and aims to develop the AML/CFT system of Serbia in order to successfully address the risks identified in the 2018 ML/TF National Risk Assessments, take measures in accordance with FATF standards, thus contributing to the achievement of the strategic AML/CFT goals.

Starting from the high-level and intermediate objectives and immediate outcomes of the global AML/CFT system, the following overall objective of the AML/CFT Strategy has been formulated: *Fully protect the economy and financial system of the Republic of Serbia from the threat caused by money laundering and terrorism financing and proliferation of weapons of mass destruction, whereby the integrity of the financial and non-financial sector institutions is strengthened through public-private partnerships and risk based approach, and safety, security and rule of law are contributed to*.

The overall objective of the national AML/CFT Strategy is further elaborated through four specific objectives, namely:

1. Mitigate money laundering, terrorism financing and proliferation of WMD risk through continuous improvement of the strategic, legislative and institutional framework, coordination and cooperation of all AML/CFT stakeholders and international cooperation;
2. Prevent suspected proceeds from crime or funds intended for terrorism or proliferation of weapons of mass destruction, from entering the financial and non-financial sectors or improve their detection if already in the system;
3. Sanction money launderers in an efficient and effective manner and confiscate proceeds from crime;
4. Detect and eliminate terrorism financing threats and sanction terrorist financiers.

# NATIONAL TERRORIST FINANCING RISK ASSESSMENT

The Government of the Republic of Serbia adopted the National TF Risk Assessment in April 2021 (TF NRA).[[12]](#footnote-13)

The TF NRA covered the period 2018-2020, assessing the threat from terrorism, the threat from TF at the national level, the sectoral TF risk and the country's vulnerability to TF.

The overall TF risk in Serbia was assessed as medium-low, taking into account that:

* The threat of terrorist financing posed by terrorists and terrorist organizations rated as low
* The threat from terrorist financing at the national level is assessed as medium to low
* Sectoral risk of terrorist financing assessed as medium.

**The country's vulnerability to terrorist financing is assessed as low.**

Considering that no criminal prosecutions were undertaken in the covered period for the commission of the criminal offense of terrorism or other related criminal offenses it, including the financing of terrorism, the threat of terrorist financing is assessed as low.

**Suspicious money flows and channels**

In the period under review, by analysing the funds that were believed that may be used for financing the above threats, a high risk has been identified in relation to:

* the inability to fully identify counterparties in monetary transactions;
* most of the rapid money transfer transactions in smaller amounts;
* the link of individual financial transactions with countries where intensive terrorist activities take place (Global Terrorism Index list), the regions where these countries are located, as well as with countries that pose a risk to the Republic of Serbia from the aspect of terrorist financing (hereinafter: risk areas).

The analysis of suspicious financial transactions of the examined entities identified the most common directions of movement of funds from risk areas to Serbia, as well as from Serbia to certain countries from risk areas. These funds, the amount of which in 90% of cases was less than 1,000 EUR, were transferred mainly as assistance from family members, and originate from personal income, as well as religious groups to help compatriots in their home countries. Also, the channels most commonly used funds transfers in this period were those of international payment institutions, i.e. money transfer agents.

From the aspect of TF abuse, the sectoral risk assessment showed that the financial sector was more susceptible to abuse than the DNFBP sector. Sector analysis indicates that not all sectors face the same level of risk; nevertheless, the products of the following sectors are the most vulnerable from the point of view of TF abuse:

* electronic money issuers;
* payment institutions;
* public postal operator;
* authorized currency exchange operators;
* providers of services related to digital assets;
* real estate sale and lease brokers;
* banks



Chart 1 Sectoral risks

# ANALYSIS OF THE TERRORISM FINANCING RISK

The risk-based approach (RBA) is essential for an effective implementation of the FATF recommendations. An RBA means that AML/CFT obliged entities understand, assess and identify the TF risks they are exposed to and implement adequate measures and policies to mitigate those risks. This approach enables obliged entities to protect their business integrity, economy and the stability of their country from TF. It also provides them with insight into the resources and the extent to which they should be (re-)allocated to the highest risk areas. Supervisory authorities should also have the same or similar approach in order to avoid any dissagreements with the supervised entity in the course of their supervisory activity, when it comes to risk analysis and in order to objectively assess its compliance in this regard.

Risk analysis is defined in Article 6 of the AML/CFT Law:

The obliged entity is required to prepare and regularly update an ML/TF risk analysis in accordance with this Law, the guidelines issued by the authority supervising the compliance with this Law and the National ML/TF Risk Assessment.

The risk analysis must be proportionate to the nature and scope of the business, as well as the size of the obliged entity, and must take into account the basic types of risks:

1. client risk;
2. geographic risk;
3. transaction risk;
4. service risk.

And other types of risks that the obliged entity has identified due to the specifics of the business.

**Geographic risk**

When it comes to risks, it is desirable to pay special attention to the geographical risk of the client, because the National Risk Assessment has also highlighted the geographical factor as an important factor in assessing the risk, given the events of recent years in terms of terrorist activities and their financing. Support for radical ideologies has been observed, as well as the departure and return of Serbian citizens to the battlefields of the Middle East, the migrant crisis and, in connection with this, the transit nature of the movement of people from numerous countries in the Middle East and Asia through the Republic of Serbia. There is a statement of suspicious financial transactions (flows) recognized for "support" of terrorism through "transit" countries or directly to the territories of war activities. Also, foreign cash inflows to support radical ideologies from certain countries to Serbia indicate the international character of the phenomenon of terrorism and its financing. In this regard, the geographical starting point of the risk analysis is closely related to the client risk, especially if they gravitate from areas or environments affected by war and where there is an indication of terrorism. Therefore, appropriate and due attention to geographical risk is certainly a desirable starting point for an objective assessment of the risk analysis.

Supervisory authorities have, by law, developed separate guidelines as specific and binding in the application of risk assessment and risk analysis so that each obliged entity applies and adapts the instructions in the preparation of risk analysis according to the nature of their business.

The risk analysis includes:

1. risk analysis in relation to the obliged entity's entire business;
2. risk analysis for each group or type of client, i.e. business relationship, i.e. services that the obliged entity provides within the scope of its activity, i.e. transaction.

The obliged entity is obliged to submit the risk analysis to the APML and the authorities responsible for supervising the implementation of the law, at their request, within three days of the issuance of such a request, unless the authority responsible for supervision sets a longer deadline.

Based on the risk analysis, the obliged entity classifies the client into one of the following risk categories:

1. low risk of ML/TF;
2. medium risk of ML/TF ;
3. high risk of ML/TF.

In addition to the above, the obliged entity may, through internal acts, provide for additional risk categories and determine adequate actions and measures from this law for those risk categories.

The Rulebook on the Methodology for Performing Transactions in Accordance with the ML/TF Act ("Official Gazette of the Republic of Serbia", No. 80/2020) regulates the manner and reasons on the basis of which the obliged entity classifies a client, business relationship, service provided within its scope of activity or transaction into the category of low risk of ML/TF.

Furthermore, when it comes to adequate risk analysis, attention should be paid to Articles 34 and 35 of the law, which significantly affect risk analysis.

**Special forms of CDD**

Article 34 states that in addition to general CDD carried out in accordance with the provisions of Article 7, paragraph 1 of this law, in cases prescribed by this law, special forms of CDD must be undertaken, as follows:

1. enhanced CDD;
2. simplified CDD.

In the case of enhanced CDD (Article 35 of the Law), in addition to the actions and measures referred to in Article 7, paragraph 1 of the Law, the last paragraph of the Article states that the obliged entity is obliged to carry out enhanced CDD in cases where, in accordance with the provisions of Article 6 of this Law (risk analysis), it assesses that due to the nature of the business relationship, the form and manner of performing the transaction, the business profile of the customer, or other circumstances related to the customer, there is or could be a high level of ML/TF risk. The obliged entity is required to specify in its internal act (policies and procedures) the enhanced CDD it will apply in each specific case and to what extent.

When it comes to simplified CDD in relation to Article 6 (risk analysis) and the general provisions in Article 42 of the Law, the obliged entity may apply them to a person who, based on Article 6, paragraph 5 of this Law, has been found to have a low level of ML/TF risk, and in accordance with Article 6 of the Law, if the obliged entity assesses that due to the nature of the business relationship, the form and manner of conducting the transaction, the business profile of the client, or other circumstances related to the client, there is an insignificant or low level of ML/TF risk.

**Adequate level of client monitoring – frequency of client monitoring**

In accordance with the risk analysis and knowledge of the client, the frequency of updating customer monitoring in accordance with the guidelines for obliged entities is at least:

1. low level of terrorist financing risk - once every two years;
2. medium level of risk of terrorist financing - once a year;
3. high level of risk of terrorist financing - twice a year;

It is up to the obliged entity to realistically assess the adequacy of up-to-date monitoring of the customer given the newly emerging circumstances of business cooperation with the customer, so for a high level of risk, more frequent updating of the customer monitoring is possible (quarterly, monthly) depending on the emerging circumstances and threats to possible TF.

It is useful to know that the NRA indicated that obliged entities ’ knowledge must be improved and that the private sector must keep up with the developments and constantly improve its knowledge when it comes to TF.

# INDICATORS FOR IDENTIFYING TERRORIST FINANCING

The obliged entity must prepare a list of indicators for identifying persons and transactions for which there are grounds for suspicion that they are TF. When preparing the list of indicators, the obliged entity is also required to include indicators prepared by the competent authority, which are published on the APML website.

The obliged entity is required to apply the list of indicators and take other circumstances into account when determining the grounds for TF suspicion. It is particularly important that all employees be familiar with the indicators and apply them when facilitating transactions, i.e. before their execution, in accordance with the Law and guidelines.

The APML publishes a list of indicators for identifying suspicious activities related to the financing of terrorism (see the APML website). The list of indicators may be subject to periodic changes and amendments, so it is necessary to regularly monitor the information published on the APML's website and to change and/or supplement the internal documents of the obliged entity accordingly.

When preparing the list, the obliged entity takes into account the complexity and scope of transactions, the unusual manner of their execution, the value or links of transactions that do not have an economically or legally justified purpose, i.e. they are inconsistent with or are disproportionate to the usual or expected business of the client, as well as other circumstances related to the client’s status or other characteristics.

When determining grounds for suspicion of terrorist financing, the obliged entity must apply a list of indicators and to take into account other circumstances indicating the existence of grounds for suspicion of terrorist financing.

When developing a list of indicators in the process of determining the existence of elements for qualifying a certain transaction or person as suspicious, a broader framework should be considered in accordance with the principle that the obliged entity knows his client best and assess whether a certain transaction falls outside the scope of the client’s usual, or expected, business operations.

When it comes to identifying suspicious activities related to terrorist financing, experience shows that there is a dilemma among obliged entities as to what is a real "trigger", i.e. a "red flag" for reporting suspicious activities and transactions to the APML, more precisely, whether to rely primarily on an identified indicator from the list of indicators or to approach a broader aspect of the suspicion assessment, giving priority to the assessment of the client's risk analysis for making a final decision.

There have been many cases where obliged entities reported suspicious activities (transactions) of their clients, whereas their risk management departments did not consider such clients to be risky and allow them to use all services and products as a low-risk customers, which certainly indicates that there may be a lack of the much needed communication between the responsible departments in one and the same obliged entity for the purpose of assessing the client risk properly (business security assessment).

The previous section of this document highlighted that RBA is essential for an effective implementation of FATF recommendations. Inndicators assist in risk analysis and assessment of the client, and they are a good starting point towards a more comprehensive assessment of the level of risk and suspicion of terrorist financing. Indicators often represent a "broad description of suspicion", and experience has shown that such lists do exist (domestic, foreign, international institutions); however, if obliged entities apply only these lists to assess suspicion, it lead to a significant percentage of their clients being suspected of terrorist financing, which would not be objectively true.

The application and combination of good indicators and objective risk analysis (risk matrices) provide a more realistic picture and basis for assessing suspicions of terrorist financing.

"It is necessary to define indicators that would serve the public and private sectors, including the NPO sector, to more easily identify activities related to terrorist financing during the raising, movement, storage and eventual use of funds (meaning financial). A distinction should be made between requests for direct financial support to terrorist organizations and the need to finance broader organizational requirements."[[13]](#footnote-14)

In terms of good development and application of indicators, and in the context of the above, attention should be drawn to the NRA section on TF "Sectoral risk from terrorist financing", which sends a message to obliged entities on what they should pay attention to based on observed cases of suspicious behaviour by their clients (transactions, use of products and services).

Therefore, a good analysis of previous practices and the probability of events can contribute to a more functional and applicable development of a list of indicators, both by obliged entities and by supervisory authorities.

# DIGITAL (VIRTUAL) ASSETS

Technological development of IT and human creativity have lead to a "virtual world of finance" in which hundreds of billions of dollars and euros are traded. Without going into the economic aspects of digital (virtual) assets, due to their technological - informational - economic specificities, they have become a constant and growing threat, from the point of view of the threat of terrorism and TF. They are suitable ground because their attributes and operating characteristics enable the anonymity of financial transactions and participants, the rapid movement of assets beyond usual financial channels, a specific method of data storage, and importantly, until recently this area was almost legally unregulated. Experience shows that complex technologies and software are increasingly being used in the commission of criminal acts of all kinds, mainly in the dark area of the Internet (Darknet) .

Aware of the risks and threats to the entire system, the Republic of Serbia has regulated this area:

## Legal framework

Digital assets are regulated by the Law on Digital Assets.[[14]](#footnote-15)

Certain terms within the meaning of this law have the following meanings:

Digital assets, or virtual assets, means a digital record of value that can be digitally bought, sold, exchanged or transferred and that can be used as a medium of exchange or for investment purposes, whereby digital assets do not include digital records of currencies that are legal tender and other financial assets regulated by other laws, except as otherwise provided for in this law;

Virtual currency is a type of digital asset that is not issued and whose value is not guaranteed by a central bank or other public authority, which is not necessarily tied to a legal tender and does not have the legal status of money or currency, but is accepted by natural and legal persons as a medium of exchange and can be bought, sold, exchanged, transferred and stored electronically.

A digital token is a type of digital asset and refers to any intangible property right that represents in digital form one or more other property rights, which may include the right of the user of the digital token to be provided with a certain service.

## National risk assessment, legal framework, international standards

Virtual currencies, as a type of digital asset that is subject to abuse, were regulated for the first time in Serbia through the AML/CFT Law in December 2017, six months before the adoption of the Fifth EU AML Directive (Fifth Directive) in May 2018. Persons engaged in the provision of purchasing, selling and or the transfer of virtual currencies or the exchange of such currencies for money or other assets via internet platforms, devices in physical form or otherwise, or which mediate in the provision of these services, have been introduced into the system of combating ML/TF, thus which are explicitly recognized as obliged entities and must undertake all actions and measures to prevent and detect ML/TF, including the identification of clients by inspecting their personal documents in the physical presence of the person being identified. Supervision of these persons was then assigned to the National Bank of Serbia. However, the AML/CFT Law at that time regulated only one aspect of the VASP business, namely the one related to AML/CFT safeguards, and therefore the supervision of the National Bank of Serbia was limited exclusively to that aspect of their business. Keeping pace with the Fifth Directive, the amendments to the AML/CFT Law, which entered into force on 1 January 2020, defined the term and meaning of virtual currency, while custodian wallet providers were added to the list of obliged entities, whose definition is also aligned with the Fifth Directive.

By continuously assessing the ML/TF risks in the virtual currency sector and by exercising supervision in this area since 2018, the competent authorities of Serbia identified the need to regulate the VA area in Serbia in a comprehensive manner, i.e. to regulate all aspects of the VASP business. In this regard, December 2020 saw the adoption of the Law on Digital Assets (LDA), amendments to the AML/CFT Law, as well as the laws amending the tax laws, which took effect in June 2021, goveringin all aspects of VASP operations and the VA market in Serbia, including the issuance of digital assets (virtual currencies and digital, or investment tokens) and secondary trading in digital assets , provision of VA-related services, as well as supervision of the issuance of digital assets and providing services related to digital assets.

The competence for decision-making in administrative proceedings and supervision in the field of digital assets is divided between the National Bank of Serbia and the Securities Commission. Thus the National Bank of Serbia supervises virtual currencies, whereas the Securities Commission performs supervision in relation to digital tokens. The same division of competence is made in the AML/CFT Law, which is fully aligned with the LDA. In the event that a certain digital asset has characteristics of both virtual currency and digital token, i.e. in the case where VASP provides related services. Both the National Bank of Serbia and the Securities Commission are responsible for both virtual currencies and digital tokens.

Digital asset issuers also have obligations under the AML/CFT Law which is explicit that issuing digital assets that directly or indirectly enable the concealment of client identity (anonymous digital assets) is prohibited, as well as that digital asset issuers and VASPs iare prohibited from using information system resources (software components, hardware components and information goods) that enable and/or facilitate client’s identity concealment and/or which make it impossible and/or difficult to track transactions with digital assets.

The provision of services related to anonymous digital assets is also expressly prohibited. AML/CFT Law. VASPs are obligations and regulations that regulate the restriction of the disposal of property in for the purpose of preventing terrorism and the proliferation of weapons of mass destruction, based on an explicit provision of the LDA.

The LDA and AML/CFT Law are aligned with international standards, i.e. with the revised FATF Recommendation 15, as well as with the Fifth directive. In addition, the Decision on the Guidelines for Complying with the AML/CFT Law by obliged entities supervised by the National Bank of Serbia (in hereinafter referred to as the NBS Guidelines), the FATF Red Flags have also been implemented into the preventive AML/CFT system, i.e. VA-related ML/TFindicators.

## Prohibition of the use of digital assets in regulated sectors

The LDA introduced a set of prohibitions for FIs supervised by the National Bank of Serbia (banks, companies/obliged entities in the life insurance sector, financial leasing providers, companies for management of voluntary pension funds, payment institutions and electronic money institutions money) to own digital assets (as well as instruments related to digital assets) and to provide and use services related to digital assets .

## Terrorist Financing Risk Assessment in the Digital Asset Sector (NRA)

Although a large number of crimes related to digital assets essentially concern predicate crimes or the crime of money laundering, some perpetrators use digital assets and to avoid financial obligations to the state and possibly collect funds for financing terrorism. The most common type of abuse in Serbia are criminal offences related to ransomware, various forms of cryptocurrency theft (theft of private keys) and transfers to addresses cryptocurrency under the control of the perpetrator of the crime, as well as various forms of fraud related to with cryptocurrencies. Common problems related to this type of crime are reflected, among other things, in the fact that virtual currencies provide their users with greater freedom, but also require them to greater responsibility, which is usually absent. Namely, in more and more cases of digital asset theft, harming Serbian citizens, a circumstance that often contributes to theft is that the "keys" are not adequately secured, primarily due to technical ignorance of how the system of generation and the storage of public and private keys works with digital assets.

According to VASPs, the most common crimes related to the misuse of digital assets or VASPs are initial coin offering fraud, Ponzi schemes (which are in special focus of supervisory authorities after OneCoinaffair that affected the region), blackmail software, namely ransomwaresoftware resulting from hacker attacks, theft of virtual currencies such as consequences of hacker attacks, as well as drug trafficking and arms trafficking (available on the black market) market – dark net ). However, VASPs believe that after the commission of these crimes, there is rarely use VASPs, because the perpetrators want to remain anonymous, so they more often use OTC trading (direct trading between persons without intermediaries).

In the coming period, it is necessary to invest in technological equipment, software tools and necessary knowledge. in terms of human resources for the successful conduct of investigations, seizure of digital assets and management seized digital assets, when it comes to the aforementioned criminal offenses.

According to the experience of the APML, in the period from 2018 to 2020, there are increased number of suspicious transaction reports by foreign financial intelligence agencies services related to the gambling sector, in which, as perpetrators of criminal acts of fraud, identity theft, unauthorized access to computers and registered accounts at casinos and betting shops are reported by citizens of Serbia or persons temporarily residing in Serbia.

Abuse *of FinTech* and anonymity of participants in transactions, with fast transaction execution high limit, as well as the ability to exchange, buy and sell cryptocurrencies for official currencies that This sector provides a fertile ground for the rapid transfer of funds derived from criminal activities from one country to another and for the exploitation of looser laws to get to KYC procedure carried out by certain *FinTech* business entities, as well as casinos and betting shops, money withdraw cash from electronic money institutions or from an ATM in a third country.

The analysis conducted nevertheless concluded that the threat of money laundering is currently low and terrorist financing using cryptocurrencies,considering that it is about middle and lower amounts in which these criminal acts are committed, with a tendency for medium threat, due to the constant increase the value of cryptocurrencies through market capitalization, as well as the very nature of ransomware, theft and fraud related to cryptocurrencies that motivate perpetrators to further transactions through transactions to private cryptocurrencies, mixer or *coin join* services they hide the origin cryptocurrency, and then they exchange them for official currency.

**By client profile**

Risks exist, but are mitigated owing to strict regulatory requirements under the AML/CFT Law with enhanced CDD in cases of increased risk.

**By type of digital asset**

The risk of using anonymous digital assets

**By type of service**

* In terms of the type of service – there is a medium risk in terms of receiving, transmitting and executing orders relating to the purchase and sale of digital assets for the account of third parties;
* Trading for cash.

## International practice, FATF indicators

International practice shows that terrorist organizations have often financed themselves through digital currencies, which makes this sector vulnerable. However, no case of misuse has been recorded so far of VASPs in Serbia.

According to FATF indicators, VASPs should, among other things, pay attention in cases where:

* there is a suspicion that cryptocurrencies are being used to pay for goods and services on the "darknet";
* there is a suspicion that ransomware is being used;
* there is a suspicion that cryptocurrencies are being used for extortion – Blackmail and Sextortion;
* there is a suspicion of unauthorized access to client wallets, hacking of registered accounts and similar computer fraud;
* there is suspicion of business abuse and the creation of a Ponzi scheme;
* when executing transactions, software is used to increase the anonymity of participants in transactions – Tumblers and Mixers or when exchanging crypto or fiat currencies for cryptocurrencies with enhanced anonymity – Monero and similar;
* register transactions related to risk areas;
* provide services to foreign citizens originating from risk areas, who possess a document of the Republic of Serbia issued on the basis of temporary residence;
* incomplete details regarding the order to execute transactions in favour of an NPO (endowment, association, foundation, etc.) or in favour of individuals associated with the said organization ;
* funds arrive or are sent to digital asset trading platforms – Peer2Peer platforms;
* funds are received or directed to unregistered and unlicensed providers services related to digital assets in the country or abroad.

## APML experiences

The APML has also noticed that obliged entities such as exchange offices and payment institutions sign bilateral and tripartite agreements on business cooperation with VASPs, cryptocurrency trading exchanges and financial platforms whose work permits were issued by a third country, i.e. which are registered abroad. In this way obliged entities registered for currency exchange operations also operate as a cryptocurrency exchange, adopt blockchain technology from foreign business entities and provide payment institution services, that is, financial platforms, which exposes them to additional risk. The vulnerability of the system is reflected in that the supervision of the different services performed by the exchange is carried out by inspectors from different units, so that related activities that may separately seem benign can pass "under the radar" radar" during control.

## Results achieved – international experience with FATF Recommendation 15

How important it is to regulate the field of digital (virtual) assets is also demonstrated by the Moneyval typologies document on money laundering and financing of terrorism risks in the world of virtual assets, which states that Moneyval members continue to struggle with the implementation of FATF Recommendation 15, with around 80% of assessed members only partially or not compliant with FATF requirements.[[15]](#footnote-16)

# NON-PROFIT ORGANIZATIONS (NPOs)

International experience highlights the vulnerability and risk of terrorist financing of the non-profit sector - NPOs (associations, endowments, foundations, various other organizations), given their wide range of activities, as well as the high level of population participation in supporting the implementation of various programs such as: health - humanitarian, poverty eradication, environmental protection, education, environmental protection and many other activities and programs related to raising social communities to a higher level. In addition to its functions and intentions, the NPO sector is not immune to abuse by criminal and terrorist organizations, and for this reason, international standards (FATF) require that countries should address the issue of governing the NPO sector in order to predict and measure risks and vulnerability, and thus reduce potential abuses and the channelling of the spread of terrorist financing.

Legal framework for NGOs in Serbia**[[16]](#footnote-17)**

In the Republic of Serbia, the term "non-profit sector, i.e. non-profit organizations", as defined by law, organizations based on freedom of association are included more natural or legal persons that are not established for the purpose of gaining profit, and have the status of a legal entity persons (associations, endowments, foundations, funds), as well as any other form of voluntary association for the purpose of achieving a common and/or general goal and interest that does not involve funds and property used for profit, i.e. for the earnings of founders, members, employees or other persons associated with that association and whose work is not regulated by a separate law. The basis of the definition is in Article 55 of the Constitution of the Republic of Serbia and the following laws: Law on Associations, Law on Endowments and Foundations and the Law on Endowments, Foundations and Funds.

The above definition is aligned with the FATF definition.

In accordance with the definition, registrations of NPOs were also carried out, recording the dominant presence of associations in relation to foundations and endowments.

The Law on the Central Records of Beneficial Owners established the Central Records of Beneficial Owners as a public, unified, central, electronic database on natural persons that are the beneficial owners of a registered entity, which is managed by the Business Registers Agency.

## Analysis of the NPO sector from the TF perspective

Based on the developed typologies of terrorist financing, Serbian authorities have identified specific indicators regarding the possibility of abuse of the NPO sector by terrorist financing:

* Responsible persons in an NPO carry out activities that are not in accordance with the statutory objectives (e.g. creating and distributing materials and organizing lectures that justify terrorism or the activities of a terrorist organization);
* Responsible persons in an NPO spend funds in a manner that is not in accordance with statutory goals (purchase of various assets: vehicles, military equipment, martial arts training equipment, providing financial assistance to the families of convicted and deceased terrorists);
* An NPO facility that is not registered for the provision of accommodation and food services is equipped with and used for short stays of several people (beds, kitchen, etc.);
* Individuals believed to support terrorist activities often visit NPO premises .
* An association from Serbia cooperates with NGOs suspected of supporting terrorist activities.

### Analysis of risk assessment for NPOs as a form of organization, and categorization client risk (low, medium, high)

It should be highlighted, for the financial sector, that banks are mainly **medium risk** (based on established business relationships).

Others (insurance, leasing) – **particularly low risk.**

The analysis was also performed for the DNFBP sector, where the results also indicated that a smaller number clients are entities organized in the form of associations that are rated as high-risk.

In the DNFBP sector, endowments and foundations have been assessed by accountants and auditors as higher risk, more so than associations.

In the reporting period, associations were not subject to TF-related suspicious activity reports by obliged entities.

### Analysis of the NPO sector in the Serbian context (NRA findings)

General and specific criteria for supervision by NPO Supervision Working Group

Based on the analysis, it was determined that the majority of NPOs are not at risk from the aspect of misuse of terrorist financing. In accordance with the above application of the criteria, the following data were obtained: which relate to the expressed percentage of the number of registered and the degree of risk of the NPO.

1. High risk level **-** 0.53% (of the number of registered NPOs)
2. medium to high risk - 3.54%
3. medium risk - 9.25%
4. low risk and low to medium risk (together) - 86.68%.

### Some recommendations (guidelines) for obliged entities under the AML/CFT Law – how to know your NPO client better (establishing business relationship, monitoring) in order to reduce suspicion of terrorist financing

Most or almost all have a website from which you can learn a lot.

* check the purpose, goals and mission of the NPO (by browsing the internet - getting basic information)
* check the Business Registers Agency website (registration, statutes - reasons for establishment and existence)
* social networks provide a lot of useful information (forums and opinions)
* a comprehensive and exhaustive interview with the client can contribute greatly to a better understanding of the purpose of the NPO's work;
* check via the portal (free of charge); "Open Data Portal of the Government of Serbia" which contains reports in open format from various NPOs (associations, foundations and endowments) operating in Serbia. The reports are compiled to increase transparency of NPOs [[17]](#footnote-18);
* check the UN Consolidated list of designated persons via the APML website – designated person search engine ( http://www.unsearch.apml.gov.rs/)
* search through the online platform " Neprofitne.rs " , launched by the Catalyst Balkans Foundation. The platform is designed to facilitate the verification of the integrity and transparency of the work of non-profit organizations;[[18]](#footnote-19)
* check whether NGOs operate in or distribute aid to countries or territories where terrorist groups are active. The Australian Institute for Economics and Peace provides useful information for this purpose.[[19]](#footnote-20)

# DESIGNATED PERSON –DESIGANTION PROCEDURE

The UN Security Council has adopted a series of resolutions mandating the implementation of measures against terrorists, terrorist organizations and their financiers. One of the measures relates to preventing the use of the property and funds of the listed persons and organizations. Countries are obliged to adopt legislation that regulate the freezing of assets and funds located in their territory. UNSC Resolution 1373 (2001) calls on all member states to act on preventing and combating the financing of terrorist acts. The UN, in accordance with resolutions 1267 (1999), 1989 (2011), 2253 (2015) and 1988 (2011), have also published the names of individuals and organizations subject to UN financial sanctions for affiliation with Al Qaeda, ISIS or the Taliban. Based on Chapter VII of the UN Charter, UN member states are obliged to take measures to implement resolutions that it adopts within its powers.

In accordance with the above, the Republic of Serbia has adopted the Law on Freezing of Assets with the Aim of Preventing Terrorism and WMD Proliferation which governs the designation of persons and the procedure for freezing their assets.

A designated person is a natural or legal person, as well as a group or association, which is designated and placed on the list of terrorists, terrorist organizations or financiers terrorist based on:

1. relevant United Nations Security Council resolutions or acts international organizations of which the Republic of Serbia is a member;

2. proposals from competent state authorities or

3. a reasoned request from a foreign state.

## Designation process

UNSCR lists are applied automatically and do not require a Governmental regulation to be implemented.

A person can be designated on two different grounds:

1. designation of persons by the Government of the Republic of Serbia at the proposal of the competent state authorities, based on a reasonable belief that the person is a terrorist, to finance terrorism, being involved in the activities of or aiding a terrorist group or committing a terrorist act. Reasonable belief is a legal standard, which is completely separate from criminal standards, and which is introduced as a criterion which the Government must rely on when making decisions on designations.

A reasonable belief is formed on the basis of information htat the competent state authorities (Ministry of Interior, the competent prosecutor's office, the authority responsible for security and intelligence or financial intelligence) have about a specific person.

2. Designation of a person at the reasoned request of another state, under UN Security Council Resolution 1373, which requires countries to give serious consideration to any requests for designation from another country, and if there is reasonable belief, adopt a decision listing the persons.

## Updating the list and searching for designated persons

In accordance with the LAF, the APML shall update without delay any change to the list of UNSCR designated persons, on its website, informing those who are obliged to implement the actions and measures for preventing TF.

The APML’s website also has a search engine for the list of designated persons. UN Security Council (http://www.unsearch.apml.gov.rs/). The search engine allows all interested individuals and legal entities to quickly and easily check whether they have any contacts, i.e. business cooperation with listed persons, in order to implement the measures and actions under the Law without any delay.

The development of this information tool has enabled direct search of lists designated persons by the UN Security Council pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL, Al-Qaeda and associated individuals, groups of individuals, businesses and other entities, Resolution 1718 (2006) and its successor resolutions regarding the DPRK, as well as Resolution 1988 (2011) related to the Taliban and associated individuals, groups of individuals, businesses and other entities.

The search engine is designed in such a way that all interested individuals or legal entities can check if they have contacts with the designated person by entering at least one piece of information they have on the person. The person performing the search must choose the group of obliged persons/entities they belongs to (banks, insurance companies, lawyers, notaries, NPOs, endowments...). If a broad search range is specified, the search engine will return all persons that fall within the given search (e.g. all persons with the specific name, etc.), while simultaneously displaying all available data for specific persons (name, surname and nickname, date of birth, country of origin, date of listing designated persons, which resolution covers them).

Data on designated persons is automatically downloaded from the relevant UNSC sanctions list database every day, which allows for accurate and timely results when using a browser.

## The process of reporting a designated person

The LAF requires from any legal or natural person, when performing a job or activity, to establish whether there have business or any other similar relationships with a designated person. In the event that they identify that they have such relationship with a designated person, they are obliged to freeze the assets of the designated person within the shortest possible time and to immediately, and no later than within 24 hours, notify the APML thereof.

Notifications and information are delivered:

* by phone;
* electronically;
* by direct delivery or
* by registered mail.

Notification of a designated person and their property, as well as information relevant to the identification of the designated person and their property, must be submitted on the Form for reporting a designated person that can be found on the APML’s website (apml.gov.rs/REPOSITORY/1384\_obrazac-za-prijavu-oznacenih-lica-sajt-230615.doc).

Notifications and information delivered by telephone are confirmed in writting.

# METHODS AND TRENDS OF TERRORISM FINANCING IN THE REPUBLIC OF SERBIA**[[20]](#footnote-21)**

The 2019 TF Typologies document, based on the above-mentioned cases handled in Serbia, elaborates in detail on the modalities (methods) of terrorist financing, i.e. identifies red flags, as follows:

* criminal activities;
* providing various services;
* monetary donations;
* sale of movable and immovable property;
* providing various services;
* non-financial assets;
* abuse of social benefits;
* misuse of NPO.

These methods have not lost their importance, and if they are still identified to be a trend, it is necessary to conduct analyses and checks, collect documentation and undertake other activities in order to determine whether such activities are logically directed towards the financing of terrorism or have a broader dimension (economic-social).

CFT practice (case law) in Serbia

* financing and recruitment of Serbian citizens through religious associations, international transit support for "warriors" to go to the battlefield in Syria;
* terrorist association and financing of terrorism by a group of citizens for the purpose of going to the battlefield in Syria.

Possible trends based on domestic and international experiences (scenario):

* abuse of the NPO sector;
* links to organized crime;
* distribution of money originating from legitimate business;
* misuse of bank accounts;
* abuse of procedures related to weapons of mass destruction (armaments and military equipment and dual-use goods);
* abuse of digital platforms (commerce and finance);
* abuse of short-term accommodation and food providers (hotels, hostels, motels, etc.), as well as low-budget and uncategorized short-term accommodation service providers (daily apartments, etc.);
* abuse of a payment institution (money transfer agents - money transfer service provider);
* abuse of passenger transport service providers.

## THREE TRENDS IN TERRORISM, CHALLENGES, OBSERVED SHORTCOMINGS AND CAPACITY BUILDING NEEDS

TF is a dynamic process that is not finite or shaped by specific rules and procedures. Countries and their competent authorities, as well as various institutions, are fighting terrorism and its financing, and despite investing in this fight, shortcomings and the need for capacity building for a more efficient fight are still there. For this reason, it may be useful to refer to the text from 2023 UNOCT Third Quarterly Briefing to Member States (19.12.2022.), Remarks by Mr. Weixiang Chen, Acting Executive Director of the Counter-Terrorism Committee Executive Directorate (CTED).[[21]](#footnote-22)

### Trend 1

First, the exploitation of information and communication technologies, including the Internet, social media platforms, and emerging online spaces, is certain to evolve and grow. Innovative ways to disseminate and weaponize terrorist propaganda, together with sophisticated techniques aimed at circumventing content moderation, will continue to present challenges to crafting a tailored and effective counter-terrorist response.

### Trend 2

Terrorists are opportunistic and adaptive, and will continue to take advantage of the rapid evolution of financial services made possible by the emerging technologies. They continue to find innovative methods to raise funds for terrorist purposes, including the misuse of social media services as well as crowdfunding platforms[[22]](#footnote-23), with an uptick in the misuse of mobile payment systems, virtual assets, and privacy coins, as well as online exchanges and wallets.

### Trend 3

Unmanned aerial systems (UAS), including drones, which terrorists have used for reconnaissance, criminal purposes, and other illicit activities, are now being “weaponized”. The increase in their range and precision poses a further serious threat to critical infrastructure,

civil aviation, and society in general..

## Identified gaps and capacity needs

Identification of the following areas where there are “ gaps” and capacity needs in responding to new threats and challenges:

1. Developing technological capabilities to identify and track terrorist activity across multiple platforms and to increase the level of accuracy in removing terrorist content in accordance with human rights;
2. Expanding the use of digital and social media literacy campaigns, as well as developing tailored counterterrorism narratives across multiple platforms;
3. Understanding the exact nature of the threat posed by terrorists using new payment and fundraising methods, with the aim of developing risk-based, outcome - based responses in accordance with human rights;
4. Improving technical and analytical capacities for more efficient money trail tracking, as well as developing appropriate safeguards for new solutions to combat terrorist financing;
5. Conducting dedicated risk assessments and gap analyses to develop effective countermeasures to the use of drones for terrorist purposes, as well as implementing tailored public education programs, with improved regulations in zones where drone flights are permitted.

# REFERENCES

* Law on the Prevention of Money Laundering and Financing of Terrorism, "Official Gazette of the Republic of Serbia", No. 113/17, 91/19, 153/20 and 92/23.
* "National Money Laundering Risk Assessment and National Terrorist Financing Risk Assessment" (website of the APML)
* "Modalities and trends of terrorist financing in the Republic of Serbia" (2023)
* "Third Quarterly Briefing UN Office of Counter Terrorism to Member States (19.12.2022) Remarks of Mr. Weixiang Chen, Acting Executive Director COUNTER TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED) "
* Decisions on Guidelines for the implementation of the provisions of the AML/CFT Law for obliged entities from the financial and non-financial sectors (APML website)
* "Instructions for the implementation of LAF provisions on the prevention of terrorist financing" (APML website)
* Brochure: KPMG “ Preventing the Financing of Terrorism, a Guide for Donors”
* Brochure: KPMG "Guidance for complying with the AML/CFT Law – Accountants"
* FATF Report "Crowdfunding for terrorism financing" , October 2023
* Moneyval document Money Laundering and Terrorist Financing in the World of Virtual Assets
1. Resolution 2462 (2019) reminds States of their obligation to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in support of the commission of terrorist acts is brought to justice and, in addition to taking other measures against such persons, to ensure that such terrorist acts are recognized as serious crimes under domestic laws and regulations and that the punishment is proportionate to the gravity of such terrorist acts. [↑](#footnote-ref-2)
2. Official Gazette of the Republic of Srpska No. 85/2005, 88/2005-ispr, 107/2005-corr., 72/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019. [↑](#footnote-ref-3)
3. Official Gazette of the Republic of Serbia No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021-decision of the Constitutional Court and 62/2021-decision of the Constitutional Court. [↑](#footnote-ref-4)
4. Official Gazette of the Republic of Serbia No. 94/2016, 87/2018-other laws and 10/2023. [↑](#footnote-ref-5)
5. Official Gazette of the Republic of Serbia No. 2972015, 113/2017 and 41/2018. [↑](#footnote-ref-6)
6. Official Gazette of the Republic of Srpska No. 113/2017, 91/2019, 153/2020 and 92/2023. [↑](#footnote-ref-7)
7. Official Gazette of the Republic of Serbia No. 10/2016. [↑](#footnote-ref-8)
8. Moneyval is the Committee of Experts for the Evaluation of Measures to Prevent Money Laundering and the Financing of Terrorism. It is a supervisory body of the Council of Europe that aims to improve the capacity of national authorities to effectively combat money laundering and the financing of terrorism. The Moneyval Committee's assessment system is based on the FATF model, but also includes compliance with international conventions and European Union legislation. [↑](#footnote-ref-9)
9. The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 with the mission to set standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction. [↑](#footnote-ref-10)
10. Official Gazette of the Republic of Serbia 113/2017, 91/2019, 153/2020 and 92/2023. [↑](#footnote-ref-11)
11. National Strategy for Combating Money Laundering and Terrorist Financing (website: Anti-Money Laundering Authority, Library Section) [↑](#footnote-ref-12)
12. The full text of "Money Laundering and Terrorist Financing Risk Assessment" can be found at the link https://www.apml.gov.rs/uploads/useruploads/Documents/NRA2021.pdf [↑](#footnote-ref-13)
13. "Modalities and trends of terrorist financing in the Republic of Serbia" [↑](#footnote-ref-14)
14. "Official Gazette of the Republic of Serbia", issue 153/20 [↑](#footnote-ref-15)
15. Moneyval, Typologies work "Money Laundering and Terrorist Financing in the world of virtual assets" This report was prepared by a team led by the Project Leader Mr. David Baker (Isle of Man) with the support of experts from Gibraltar, Malta, Principality of Monaco, Slovak Republic, and Slovenia, and was adopted by MONEYVAL in May 2023.

“ The report aims to present an integrated overview of the risks of money laundering and terrorist financing in the world of virtual assets and their service providers in the Moneyval member countries. It provides an overview of the measures taken to regulate and supervise virtual asset service providers, as well as some characteristics of the identified risks that criminals use virtual asset service providers and virtual assets to launder the proceeds of crime. M anival members continue to struggle with the implementation of FATF Recommendation 15, with around 80% of assessed members only partially or not compliant with FATF requirements . The report also examines whether law enforcement agencies have adequate powers and tools to investigate, locate and impose provisional measures in relation to virtual assets, and includes examples of the types of virtual asset platforms used to financially support criminal activities and cases investigated by relevant authorities. It also highlights good practices and challenges in implementing risk-based supervision of the sector . [↑](#footnote-ref-16)
16. National Risk Assessment 2018-2020 [↑](#footnote-ref-17)
17. KPMG " Preventing the Financing of Terrorism - A Guide for Donors " [↑](#footnote-ref-18)
18. KPMG " Preventing the Financing of Terrorism - A Guide for Donors " [↑](#footnote-ref-19)
19. KPMG " Preventing the Financing of Terrorism - A Guide for Donors " [↑](#footnote-ref-20)
20. Brochure "Modalities and Trends of Terrorism Financing in the Republic of Serbia", 2023 [↑](#footnote-ref-21)
21. " Third Quarterly Briefing UN office of Counter T errorism to Member States (19.12.2022) Remarks of Mr. Weixiang Chen, Acting Executive Director, Counter Terrorism Committee Executive Directorate (CTED) " [↑](#footnote-ref-22)
22. For more: FATF Report "Crowfunding for terrorism financing" October 2023. Definition: As is noted by FATF in 2021 “crowdfunding” is a completely legitimate way of seeking and obtaining funds and the vast majority of crowdfunding is legitimate. Crowdfunding helps raise money to finance personal, commercial, non-profit, non-governmental or other initiatives. It can be used for a variety of purposes, including disaster relief, community and organization support, political campaigns , business financing , creative venture support and investment generation. While the key to traditional fundraising is to raise money from a limited set of sources, in crowdfunding, a large number of people fund an idea or project through an online platform, i.e. the internet, social media and other means of communication, which are used to connect people who can contribute relatively small amounts to a business idea, project , charity ... Online “crowdfunding” involves three key elements: a contributor who gives money digitally, a recipient who receives the money digitally, and a payment method to transfer the money from the donor to the recipient. The appeal of “crowdfunding” compared to traditional funding mechanisms is that it allows the applicant to reach large numbers of potential donors. Even small individual contributions can add up and have a significant impact. [↑](#footnote-ref-23)