ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

DEPARTMENT OF INTERNATIONAL, EUROPEAN AND AREA STUDIES

POSTGRADUATE STUDY PROGRAMME

"INTERNATIONAL AND EUROPEAN LAW AND GOVERNANCE"

SPECIALISATION: INTERNATIONAL LAW AND DIPLOMATIC STUDIES

"The funding of terrorist groups through cryptocurrencies under International and European Law"

Master's Thesis

Evangelia Panousi

Athens 2023

Τριμελής Επιτροπή

Χατζόπουλος Βασίλης, Καθηγητής Παντείου Πανεπιστημίου (Επιβλέπων)

Μαρία- Ντανιέλλα Μαρούδα, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου

Σοφία Γαλάνη, Επίκουρη Καθηγήτρια Παντείου Πανεπιστημίου

Περίληψη

Η χρηματοδότηση της τρομοκρατίας δεν είναι μια νέα πρόκληση και θα μπορούσε να χαρακτηριστεί ως μια ατέρμονη επιδίωξη. Αν μη τι άλλο, οι μέθοδοι που χρησιμοποιούνται περιοδικά καταδεικνύουν την εφευρετικότητα όσων εμπλέκονται στη χρηματοδότηση της τρομοκρατίας.

Τα κράτη και οι διεθνείς οργανισμοί προσπαθούν να αντιμετωπίσουν το πρόβλημα και να εντοπίσουν τις μεθόδους που θα προσφέρουν λύσεις στην καταπολέμηση του φαινομένου. Κανείς δεν μπορεί να αμφισβητήσει ότι στον τομέα αυτό επιτελείται εξαιρετική δουλειά σε διεθνές επίπεδο. Ωστόσο, παρά τις προσπάθειες αντιμετώπισης των νέων μορφών χρηματοδότησης, αυτές δεν φαίνεται να είναι επαρκείς, με αποτέλεσμα το φαινόμενο να επιμένει και να εξελίσσεται.

Οι νέες τεχνολογίες που περιστρέφονται γύρω από τα κρυπτονομίσματα παρέχουν νέες διεξόδους χρηματοδότησης στις τρομοκρατικές ομάδες. Τα τελευταία χρόνια, γίνονται προσπάθειες να νομοθετηθούν τα κρυπτονομίσματα σε διεθνές και ευρωπαϊκό επίπεδο, αλλά το προβάδισμα φαίνεται να έχει εξασφαλιστεί από την αντιμαχόμενη πλευρά.

Η παρούσα εργασία επικεντρώνεται σε δύο κεντρικά ζητήματα. Πρώτον, κατά πόσο οι τρομοκρατικές ομάδες χρησιμοποιούν τα κρυπτονομίσματα για τη χρηματοδότηση των δράσεών τους και δεύτερον, ποια είναι η αντίδραση της διεθνούς κοινότητας και της Ευρωπαϊκής Ένωσης στην αντιμετώπιση αυτής της απειλής.

Για να απαντηθούν αυτά τα ερωτήματα, αξιοποιήθηκαν επιστημονικά έργα, ειδησεογραφικά δημοσιεύματα σχετικά με την χρηματοδότηση τρομοκρατικών ομάδων, καθώς και εκθέσεις διεθνών και ευρωπαϊκών οργανισμών σχετικά με την χρήση των κρυπτονομισμάτων στην χρηματοδότηση τρομοκρατικών ομάδων. Η παρούσα εργασία χρησιμοποιεί μια ερευνητική προσέγγιση βασισμένη σε έγγραφα και οι πληροφορίες και τα δεδομένα που λαμβάνονται είναι δευτερογενή μέσω της ανάγνωσης και της ανάλυσης.

Abstract

Terrorist financing is not a new challenge and could be described as a never-ending pursuit. If anything, the methods used periodically highlight the inventiveness of those involved in terrorist funding to secure and transfer funds.

Legal jurisdictions and international organisations have been circling the problem to identify the methods and offer solutions to counteract the phenomenon through legislation. Nobody can deny that a significant amount of excellent work is being done in this field. However, despite the efforts to tackle new technologies, they do not appear to be sufficient, and as a result, the phenomenon persists and evolves.

New technologies revolving around Blockchain and cryptocurrencies give new outlets to those interested in terrorist funding. Because these new technologies are still evolving in terms of legislation, one could argue that they are operating uncontrolled. Attempts have been made recently to legislate cryptocurrencies at the international and European levels, but the lead seems to have been secured.

This dissertation focuses on two major issues. First, whether terrorist groups are currently using cryptocurrencies to fund their operations and second, what is the response of the international community and the European Union in countering this threat.

To answer these questions, scholarly works, electronic media, news reports on terrorist organisations, terrorism finance and economics, and cryptocurrencies and international organisations reports were utilised.This paper employs a document-based research approach and the information and data obtained is secondary through reading and analysing.

Table of Contents

Introduction

On October 31, 2008, Satoshi Nakamoto published a white paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System', introducing a remarkable technological breakthrough with far-reaching implications. In 2022, institutions, governments, and businesses worldwide are debating distributed ledger technology (DLT), cryptocurrencies and FinTech. Fast technological developments and the rising popularity of cryptocurrencies elevated crypto assets from a marginal territory into the international regulatory agenda.[1] The rapid innovation rate challenges regulators to formulate an effective response, protect the financial system, and mitigate risks of terrorist funding while fostering technological innovation. The financial sector's modernisation as a result of these technological advances necessitates the creation of new regulatory tools and the development of new regulatory solutions. It also provides a one-of-a-kind opportunity to reconsider current policies and organisational structures in the fight against terrorist funding.

In some ways, terrorist adoption of cryptocurrencies reflects the general public's behaviour. This also implies that as public cryptocurrency adoption grows, terrorist organisations will likely begin to transfer money more in virtual currencies. Furthermore given the critical role of funding in terrorist operations, counter-terrorism finance (CTF) actions frequently concentrate on locating money and blocking financial transactions that could be used to support terrorist activities.[2] However, the effectiveness of these schemes from the international community, in reducing terrorist access to fiat currencies has raised the prospect that terrorist organisations may expand their use of cryptocurrencies to counter for the loss.

Terrorist organisations cannot operate unless they have the financial capacity to plan and carry out violent acts. As terrorist financing techniques develop, so must the responses from the international community. The current international framework establishes national obligations to combat terrorist financing and calls for cooperation to counter the threat. Nevertheless, there is a regulatory gap in cryptocurrencies, which adds to the legal uncertainty and facilitates criminal behaviour like terrorist funding. Many jurisdictions are looking for appropriate regulation while the European Union stepped forward with advanced regulatory strategies for countering terrorist financing.

Although international and European bodies still need to extract more data about their use to be alarming, they have increasingly confronted these new financing methods in recent years. Evidence from international bodies tasked with combating terrorist financing indicates an increasing trend in using cryptocurrencies for terrorist financing purposes, suggesting that it is indeed a developing phenomenon. For this reason, this paper attempts to shed light on the understanding of this technology, on the laws that govern the financing of terrorism and to

1 Agata Ferreira, Philipp Sandner,Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure, Computer Law & Security Review, Volume 43, 2021, https://doi.org/10.1016/j.clsr.2021.105632. (https://www.sciencedirect.com/science/article/pii/S0267364921001059)

2 Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html. Also available in print form.

explore its future uses by terrorist groups that will eventually contribute to preventing this phenomenon.

The essay is divided into three chapters. The first chapter addresses the main features of cryptocurrencies, like the encryption and decryption processes that take place, their relation to fiat currencies and the possible dangers that arise from the limitations of regulation in the existing legal framework. This brief reference to the technologies supporting cryptocurrencies is to familiarise the reader with the basic characteristics of new technologies. Furthermore, this chapter outlines the attempts at the International and European levels to address the definition of terrorism and proceed with the findings concerning the use of cryptocurrencies for terrorist financing. The second chapter outlines the current legal status of counter-terrorism financing at both international and European levels. Finally, the third chapter tackles the current and future needs of terrorist organizations for the use of cryptocurrencies. Through an analysis of the different characteristics of cryptocurrencies, it becomes apparent which factors will encourage terrorist groups to use them and which will act as deterrents.

Chapter 1. Cryptocurrencies and terrorism financing

Before analysing the key aspects of cryptocurrencies and terrorist financing, first it must be outlined that the purpose of this chapter is to analyse some key aspects of the use of cryptocurrencies and the financing of terrorist groups. This chapter will not focus on the technical aspects of crypto-assets, and only a few key concepts will be highlighted to help the reader grasp the challenges, prospects and regulatory difficulties that may arise from the use of cryptocurrencies. In addition to that for the purposes of this paper the terms cryptocurrencies and virtual currencies are both used. The study focuses on cryptocurrencies as a form of virtual currency mainly due to its abilities for enhanced anonymity that poses greater risks in terrorist financing. Nevertheless, due to a lack of common terminology in International and European Law, the terms are interrelated and are used alternately.

The chapter is split into two main sections. The first section briefly explains key notions and underling technologies of cryptocurrencies, while the second sections analysises the notion of terrorism and terrorist financing with an aim to improve the understanding of the potential risks that cryptocurrencies serve to the international community's fight against terrorist financing.

1.1. Everything you need to know about cryptocurrencies

1.1.1. Physical and digital money

In today's world, digital assets are becoming increasingly significant. They are used for a growing number of things, such as purchasing products and services or representing other objects or rights, and they are utilised in increasing quantities[3]. The nature of money has thus

3 Sarah Green, 'Digital assets Call for evidence. (Law Commission, 30 April 2021) available at: <https://www.lawcom.gov.uk/project/digital-assets/>

evolved. Money was originally a commodity, that is, an item made of a material with a market value, such as a gold coin and precious metals or standardised quantities of goods that made them both scarce and of an intrinsic value[4], and prior to that, transactions were conducted by trading goods.

Money grew more representational over time. Today, currency also exists in non-physical forms, such as in a bank account or as an electronic entry. A monetary value held on a prepaid debit card or a smartphone is, for example, digital or electronic money. Direct debits, online payments and transfer of funds via cards are also forms of payment in which there is no cash. Although modern economies rely primarily on physical money, currency also exists in non-physical forms, such as in a bank account or an electronic entry.

1.1.2.Cryptocurrencies

Cryptoasset is any decentralised digital currency which is exclusively transmitted (earned or exchanged) through blockchain technology, including but not limited to digital coins and tokens or any other type of digital medium of exchange.[5] Thus, cryptocurrencies are digital assets, but not all digital assets are crypto assets. Any text or media formatted into binary code that includes permission to use it is referred to as a digital asset.[6] Digital assets include photos, videos, company branding, word documents, PDFs etc. Cryptocurrencies do fall under the umbrella of digital assets, but they form a distinguished category.[7] In that sense, cryptocurrencies form a new asset class that divides into different categorisations (Digital currency, magic internet money, digital cash, virtual currency).[8] Crypto assets have numerous names, just like conventional money, but at their core, they are a virtual form of money.

Cryptocurrencies are digital assets that act as a medium of exchange between two parties.[9] There are "virtual currencies," "digital currencies," and "central bank digital currencies" (which may or may not use blockchain technology at some point), in addition to "cryptocurrencies," "tokens," "protocol tokens," "app coins," "alt-coins," and "meta-coins."[10] According to the Law Library of Congress, although all forms are known as cryptocurrency and use the same type of technology, the terms countries use to refer to cryptocurrency are different, digital currency (Australia), virtual commodity (Canada and China), crypto-token

4 European central bank, 'What is money?' (European Central Bank, 24 November 2015 (updated on 20 June 2017) available at: <https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.en.html>

5 Antony Lewis, The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT) (Mango Media Publications 2018)

6 Ibis.4

7 Ibis.5

8 Durr, Wayne Allen, "A Separate Asset Class for Cryptocurrency" (2021). Doctoral Dissertations and Projects. 2881. available at: <https://digitalcommons.liberty.edu/doctoral/2881>

9 Lee, David. Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press, 2015

10 Walch, Angela, The Path of the Blockchain Lexicon (and the Law) (March 24, 2017). 36 Review of Banking & Financial Law 713 (2017), Available at < SSRN: https://ssrn.com/abstract=2940335>

(Germany), a payment token (Switzerland), cyber currency (Italy), electronic currency (Colombia), and virtual asset (Mexico).[11]

Unlike digital money, virtual currency resides within a blockchain network and is an uncontrolled digital currency safeguarded and managed by cryptographic algorithms, making it a unique type of digital currency. Furthermore, cryptocurrencies can be mined or purchased from cryptocurrency exchanges and are usually stored in crypto wallets.

1.1.3.Brief introduction to the Encryption and decryption process

The word "crypto" literally means "hidden" or "secret," and cryptography refers to the practice of writing in secret. It refers to the capacity to send communications only visible to the intended recipient. Cryptography is used daily to protect data that travels across the Internet and is deployed precisely to guarantee that the communications, searches, and interactions we conduct online are secure and private.

Total anonymity, or pseudo, can be achieved depending on the level of cryptographic technology deployed. Cryptography also serves as a means of security in cryptocurrencies, ensuring transactions, and independence of operations from a central authority, preventing double-spending, controlling the generation of new currency units, and verifying the transfer of digital assets and tokens[12]. Cryptography is utilised for a variety of objectives when it comes to crypto-assets.

Although cryptography is used for many more purposes, encryption keys are the most critical aspect. Multiple methods exist for encryption in cryptography. However, encryption in the blockchain, encrypted data, cryptography used extensively in the blockchain, and digital signatures should not be confused as not all are relevant to blockchains.

On the other hand, decryption is the averted process of transforming encrypted texts into their original format. In addition to the above, digital signatures allow both parties to prove their identities. Digital signatures can vary in form and comprise a unique form of electronic signatures, as not all digital signatures are electronic.

1.1.4.Cryptocurrencies and fiat currencies

In recent years, new decentralised digital currencies or virtual payment systems, such as Bitcoin, have surfaced that are not controlled by a central authority, such as a central bank[13]. Cryptocurrencies and fiat money both have the same functions. As a means of exchange, they can be used for payments and as a store of value. So one can send, receive, spend, store or

11 Law Library Of Congress, U.S.. Global Legal Research Directorate. Regulation of Cryptocurrency in Selected Jurisdictions. [Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018] Pdf. Retrieved from the Library of Congress, <www.loc.gov/item/2018298388/>.

12 Bellés-Muñoz, Marta, Barry Whitehat, Jordi Baylina, Vanesa Daza, and Jose Luis Muñoz-Tapia. 2021. "Twisted Edwards Elliptic Curves for Zero-Knowledge Circuits" Mathematics 9, no. 23: 3022. https://doi.org/10.3390/math9233022

13 OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. available at: www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emergingtax-policy issues.htm

give away cryptocurrencies like with fiat money. However, while fiat currencies have legal tender, cryptocurrencies do not, and this is the first significant difference between them. Fiat money is backed by a central government and can circulate in physical and electronic forms (bank credit). At the same time, cryptocurrencies are decentralised (not backed by any central government or bank) and are represented digitally (bank credit sans the bank).

Fiat money and cryptocurrencies operate due to the consumers' trust. Nevertheless, while fiat money acquires a major part of its value from debt, cryptocurrencies have intrinsic value beyond the trust of their community.[14] Furthermore, unlike fiat money, cryptocurrencies can be transferred by anyone, anywhere in the world, without the need for an intermediate bank or government and with instant settlements, unlike other transactions that can take days to process.

Finally, privacy is the most crucial aspect that makes cryptocurrencies so attractive. Of course, when talking about fiat money, data protection is guaranteed at least more than credit or debit cards. Nonetheless, anonymity is only partially promised to both forms of transaction but whwn it comes to cryptocurrencies, the owner's identity can remain fully private mainly because they operate in a decentralised and encrypted environment.

So as it happens with all kinds of money, there are advantages and disadvantages to using virtual assets. In reality, only some e-commerce sites accept cryptocurrency purchases, and even popular ones like Bitcoin have not been extensively utilised for retail transactions in previous decades. However, there appears to have been a rapid shift in practice in recent years, which suggests that cryptocurrencies are being used widely and for different purposes.

1.1.5.Limitations in the existing legal frameworks

The emergence of cryptocurrencies brought to the fore legal issues that previously did not exist with virtual currency. The dispute over cryptocurrencies was sparked by the states' differing legislative approaches and the nature of cryptocurrencies. As there is not a single definition of cryptocurrencies globally, the term virtual currencies appear more often to describe all the existing technologies. However, terminology needs to be more accurate in regulating, as the above differing depictions may be misleading.

The legal characterisation of crypto assets is a precondition for their legal treatment and systematic inclusion in the rule of law. Although the term relates to currencies, the solution may be more complex as only some of the cryptocurrencies are used as such. Intangible things question all ideas of possession, regardless of the legal system, because the primary concept of all presupposes physical possession[15].

14 For example, Bitcoin doesn’t lean on a system of debts, its value boils down to how effective it is as a medium of exchange.

15 Antony Lewis, The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT) (Mango Media Publications 2018) p. 231-232.“Take, for example, Bitcoins, one may think that Bitcoins are stored in wallets, but that does not really happen. Ownership of Bitcoin is recorded in the blockchain, but in your wallet, what you really have is a private key and not a bitcoin, and that is because Bitcoin's blockchain does not store balances of accounts but transactions, and their software makes it easy for the user of the wallet to see how many coins they control and to make payments. If you cloned your wallet, you would be cloning your private keys, not doubling your bitcoins.”

Furthermore, anonymity, hybrid characteristics, including financial instruments and intangible assets, and the rapid evolution of technology[16] are also contributing to the challenge. It is worth noting that although the use of cryptocurrencies by individuals and businesses is now widespread, there are still questions about their legal status worldwide. Given the lack of a standard definition, regulators and international standard-setting bodies use different terminology,[17] which can be risky as ambiguous definitions certainly differentiate the uniformity of the rules and make their application in international law more complex.

Decentralised finance has evolved into a new architectural notion, resulting in a financial system that is considerably more efficient, speedier, anonymous, and globalised with its trading methods and quasi-banking services. However, the legislative and supervisory framework is the most challenging task in a continually evolving environment like the crypto-economy. Because many jurisdictions lack a regulatory framework, the system is vulnerable. Fraud, financial loss, criminal activity, money laundering and terrorist funding are to name a few, which is why many academics and regulators are harshly critical of crypto assets and push for stricter regulations.

Undisputedly, cryptocurrencies and other digital finance technologies are not inherently illicit or illegal. Millions of people use them every day, and there is nothing inherently suspect about using technologies that aim to protect users' privacy. Nevertheless, it is also vital to understand how these instruments can enable malicious activity that threatens global peace and security.

The lack of uniformity worldwide reveals flaws in the system that anyone can exploit. Many jurisdictions still need to clarify their regulatory position on cryptocurrencies, resulting in an incoherent international framework.[18] The abuse of digital finance platforms and technologies has jumped into the public eye in recent years due to a rise in ransomware attacks and the use of digital financial tools by terrorist actors to funnel support for their activities. The international community has a long history of detecting and preventing terrorist funding. However, terrorists are constantly looking for legal loopholes, illegal pathways, and new technology to stay one step ahead of law enforcement and governments, especially when funding their operations.

1.2.The study of terrorism and the funding of terrorist groups

1.2.1.Attempts of the definition of terrorism by the United Nations

16 OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emergingtax-policy issues.htm

17 Ibis, 16

18 KEATINGE,CARLISLE ,KEEN, (2018) Virtual currencies and terrorist financing: assessing the risks and evaluating responses,European Union available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

There is no clear definition of terrorism in international law. Despite the United Nations' efforts to gather a consensus and form a horizontal definition of terrorism, it proved to be challenging, as the term carries political and ideological connotations. Although the definition varies throughout legal systems, international or governmental agencies and scholars, there is a precise meaning, at least from a linguistic point of view, that terrorism is simply extreme fear. The problem of legally defining terrorism arises from the fact that the mere context of language can not exist disentangled from the world around it. That was reasonably evident from the earlier efforts and conceptual debates about the definition of terrorism, where the term seemed to have entered into a geopolitical discourse[19].

However, the challenge to define terrorism is not only political but also reflects fundamental normative differences, whether ideological, philosophical, religious, or moral. Differences that sometimes even boil down to whether the use of violence itself should be considered justified or legitimate[20]. Furthermore, the struggle magnifies when the word centres on various causes, such as liberation movements and self-determination. Considering that fact is still challenging to define terrorism in an all-inclusive and unambiguous way, as the primary challenges stem from the core values at play in accepting or dismissing terror-inspiring violence as a method of achieving a specific goal.

The first breakthrough came with RES/49/60 (1994) of the General Assembly on Measures to eliminate international terrorism, where is stated that *"Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them"*. Nevertheless, a clear definition was not given.

Because of disagreements in the international community regarding the definition of terrorism, from 1960 onwards, a series of treaties were enacted[21], addressing the most

19 After World War II, the International Law Commission (ILC), attempting to codify international crimes, saw out to draft a definition of terrorism in 1954. The exact definition was amended in 1995, but the final ILC draft code of international crimes that was approved in 1996 did not include an autonomous definition of terrorism. The same year, the UN General Assembly drew to the attention of the Preparatory Committee on establishing an International Criminal Court the ILC's draft code so that terrorism would be included as an autonomous crime. After revisions and deliberations of the definition at the Rome Conference, 34 states favoured including terrorism as an autonomous crime, but eventually, it was not included in the Rome Statute. One of the Conference resolutions stated that no generally acceptable definition could be agreed upon (UN Diplomatic Conference 1998, Resolution E), pragmatically because some states feared that terrorism would politicise the ICC. Hence, it was a better fit for national jurisdiction. Similarly, after the attacks at the Munich Olympics in 1972, the debate at the UN General Assembly was vivid. However, the states could not agree on a standard definition, the causes of terrorism or the measures to address it.

20 Dumitriu, E. (2004). The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism. German Law Journal, 5(5), 585-602. "For some, the protection of the State and of the democratic values of the society laid at the heart of the debate, whereas others were more concerned with the risk of an unjustified repression of "freedom fighters.". On the 25 September 1972, during the twenty-seventh session of the United Nations' General Assembly, the United States of America brought in a draft convention on terrorism (U.N. Doc.A/CN.6/L.850). The failure of this project is due in particular to the fact that some delegations from Third World countries insisted on the need of studying the causes of terrorism before drafting a convention on this issue"

21 The 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft
The 1970 Convention for the Suppression of Unlawful Seizure of Aircraft
The 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation
The 1979 International Convention against the Taking of Hostages
The 1979 Convention on the Physical Protection of Nuclear Material

common methods of terrorist violence while avoiding the use of the term terrorism per se, instead requiring states to criminalise specific behaviours and follow the aut dedere aut judicare principle. The International Convention for the Suppression of the Financing of Terrorism, signed on Dec. 9 1999, is the one that comes closest to providing a general definition. Art. 2.1.b defines terrorism as *"Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act."*

In Resolution 1566 (2004) concerning threats to international peace and security caused by terrorism, the Security Council elaborates the context of terrorism as

> *"criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature".*

The above resolutions were subsequently followed by similar phrasing on different occasions (UNGA RES60/43 "*criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes.*"), reaffirming this attitude by the United Nations. However, the international community continues to differentiate their definitions in domestic legislation as the fundamental conception of terrorism that the U.N. advocated for is not based on a legal norm, nor is establishing customary law.[22]

Finally, the war crime of terror differs from terrorism as one is addressed in jus in bello and the other in jus ad bellum circumstances. Contrary to the non-existent definition under international law for terrorism in times of peace, in International Humanitarian Law, various treaties prohibit terrorism and provide a more precise definition.[23] To that end, it might not be a distinctive crime under the Rome Statute. However, as a war crime, it has been adjudicated by international criminal courts[24], providing a better conceptualisation of the definition.

The 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation
The 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
The 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
The 1991 Convention on the Marking of Plastic Explosives for the Purpose of Identification
The 1997 International Convention for the Suppression of Terrorist Bombings
The 1999 International Convention for the Suppression of the Financing of Terrorism
The 2005 International Convention for the Suppression of Acts of Nuclear Terrorism

22 Antonio Cassese, The Multifaceted Criminal Notion of Terrorism in International Law, Journal of International Criminal Justice, Volume 4, Issue 5, November 2006, Pages 933–958, Cassese argues that although states have so far been unable to lay down a general definition of the whole phenomenon of terrorism in a general treaty, a generally accepted definition of terrorism as an international crime in time of peace does exist in the international community at the level of customary law.

23 Geneva Convention IV,1949, art. 33(1), Protocol I Additional to Geneva Conventions,1977, art. 51(2) and Protocol II Additional to Geneva Conventions,1977, arts. 4(2) and 13(2).

1.2.2.Attempts of definition of terrorism at the European level

At the European level, the first attempt came as early as 1977, with the European Convention on the Suppression of Terrorism, signed at Strasbourg on Jan. 27 1977. Although the E.U. had a slight advantage in drafting and enacting laws due to the homogeneous interests of its member states, the Council of Europe acted sooner. The Convention did not provide a clear definition but rather a list of already existing terrorist acts referred to other international conventions. Nevertheless, it was the first Convention to address a broad range of terrorist acts and impose on states the responsibility not to regard them as related offences or offences motivated by political factors. Moving forward, the Council has implemented several anti-terrorism measures. Its primary counter-terrorism framework treaty, superseded by the Convention on the Prevention of Terrorism adopted on May 16, 2005, and entered into force June 1 2007. The Convention's main objective is to improve the effectiveness of existing international anti-terrorism treaties. Furthermore, it aims to improve Member States' efforts to prevent terrorism by criminalising acts which may lead to the commission of terrorist offences and strengthening cooperation both internally and internationally.

An Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism was adopted on October 22, 2015, in response to Security Councils Resolution 2178 (2014). It criminalises many acts, including affiliation with a terrorist organisation, receiving terrorist training, travelling abroad for terrorist purposes, and financing or organising such travel. For the first time in international law, this instrument criminalises the preparatory work of terrorist acts at the initial stage, such as recruitment, training, and preparing and financing travel for terrorist purposes. Furthermore, the Committee of Ministers and the Parliamentary Assembly actively adopted several declarations, resolutions, and recommendations on terrorism-related issues. Amongst these are a number of innovations, such as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime and the Financing of Terrorism adopted on May 16 2005, which is the first international treaty to cover both the prevention and control of money-laundering and terrorism financing.

Since then, the European Union has established a clear and exhaustive legal definition of terrorism. In the Council Framework Decision of Jun. 13 2002, on combating terrorism. According to art.1. terrorist offences are

> *"offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:*
> *— seriously intimidating a population, or*
> *— unduly compelling a Government or international organisation to perform or abstain from performing any act, or*
> *— seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation shall be deemed to be terrorist offences: a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; (c) kidnapping or hostage-taking; (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private*

24 ICTY Prosecutor v Galic, 2003, par. 137-138, 592,596-597, Special Courts for Sierra Leone Prosecutor v Brima et al.,2007, par. 662,666 and Prosecutor v Taylor,2012, par. 112,408-410

property likely to endanger human life or result in major economic loss; (e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and developmentof, biological and chemical weapons; (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life; (i) threatening to commit any of the acts listed in (a) to (h).".

The same decision in art.2(1). proceeds further to define the offences relating to a terrorist group stating that

" 'terrorist group' shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure".

Although the above definition of terrorism is closer to that of war crime, the Framework Decision states in the introductory paragraphs that "*the actions by the armed forces of a State in the exercise of their official duties are not governed by this Framework Decision*", effectively exempting from the scope situations of armed conflicts.

In March 2017, the EU adopted a directive on combating terrorism. The new regulations strengthen the EU's legal framework for preventing terrorist attacks and dealing with the phenomenon of foreign terrorist fighters[25]. The Directive replaced Framework Decision 2002/475/JHA as the cornerstone of the EU member states criminal justice response to terrorism and amended parts of Decision 2005/671/JHA on information exchange and collaboration in relation to terrorist offences. The Directive was passed to align EU law with global changes, such as the adoption of UN Security Council Resolution 2178(2014) and the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism.

The Directive contains an exhaustive list of serious offences that EU countries must characterise as terrorist offences in their national laws when committed. To that end, in article 3 par.1. it states that: *"Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2"* actively introducing a definition of terrorism when the terrorist offences are acts committed with the aim of:

"(a) seriously intimidating a population; (b) unduly compelling a government or an international organisation to perform or abstain from performing any act; (c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation."

25 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA

The definition of terrorism-related offences by the European Union takes a horizontal approach to terrorism, and although it is considered a first step, it establishes an intricate and detailed definition.

1.2.3. Terrorism Financing-Evidence of utilisation of cryptocurrency for funding terrorist activities

Terrorist financing is the foundation of terrorist activities. In recent years, terrorist organisations have transcended traditional methods of raising funds to more elaborate and innovative ones. Of course, traditional methods and techniques continue to be prevalent today and are considered significant. Every institution that facilitates funds transfer is potentially vulnerable to terrorist funding. The banking sector has been exploited for years to transfer illicit funds. However, while the physical transportation of money continues to be a prevalent aspect of terrorist operations, funds may be raised in several ways.

While Anti-Money Laundering/Combating the Financing of Terrorism regulations helped protect some aspects of the international financial sector, terrorist groups are constantly evolving. Foreign terrorist fighters (FTFs), social media, new payment products and services, and natural resource exploitation[26] are some of the new trends that the international community is facing.

The use of cryptocurrencies remains limited, compared with the more traditional ways of funding, as international reports and literature suggest.[27] Nevertheless, cryptocurrencies can appeal to terrorist organisations, primarily because of their unique features but also because task forces and international organisations crack down on the standard methods terrorist groups operate. At the same time, international organisations and literature suggest that the use of cryptocurrencies in funding terrorist groups has increased in recent years, necessitating more comprehensive and immediate responses from the international community and states at a legislative and operational level[28].

---

26 FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

27 According to Europol, *"the number of cases involving cryptocurrencies for the financing of terrorism remains limited."* (Europol 2021, Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.)
At the same time according to the report of the attorney generals; cyber digital task force of United States "*There is also evidence that certain terrorist groups are raising funds using cryptocurrency. While public data on terrorist use of cryptocurrency is limited, it is clear that terrorist networks have conducted fundraising operations through Internet based crowdsource platforms in an attempt to evade stopgaps built into the international banking system.In August 2015, for example, an individual was sentenced to over 11 years in federal prison for conspiring to provide material support and resources to the Islamic State of Iraq and al-Sham ("ISIS"), including by using social media to instruct donors on how bitcoin could provide untraceable financial support to terrorist groups. More recently, in August 2020, the Department of Justice announced the government's largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns involving the al-Qassam Brigades (Hamas's military wing), that used cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns."* (US Department of Justice (2020), Cryptocurrency Enforcement Framework, accessible at https://www.justice.gov/archives/ag/page/file/1326061/download).

28 In June 2015, the FATF published guidance to apply a risk-based approach to virtual currencies, using the findings of the June 2014 typologies report Virtual Currencies: Key Definitions and Potential AML/CFT

Terrorist groups benefit from numerous of the same tools that so many of us rely on in our everyday lives, just as they did in the past when they exploited widely used financial systems. Online platforms and the advancement of financial technology make it simple for thousands of users to donate money or transfer funds via online campaigns. For example, crowdfunding platforms such as PayPal, GoFundMe, and Amazon have become popular ways for terrorist groups to raise funds.

Understanding the funding needs of modern terrorist groups is crucial in determining and preventing the transfer of funds to terrorists. The costs of not only carrying out terrorist attacks but also of establishing and sustaining a terrorist organisation and its ideology are considerable. In order to provide a veneer of legitimacy for terrorist groups, a wide range of higher-cost services is frequently required. Funds are directed to promote ideology, pay operatives and their families, organise travels, train new members, falsify documents, pay bribes, acquire weapons, and stage attacks.[29]

As with the conceptualisation of terrorism, terrorism financing is equally vague. The Security Council, in Resolution 2462 (2019), outlines terrorist financing as the *"raising, moving, transferring and accessing of funds for and by terrorists"*. And although the resolution refers directly to FATF's recommendations, it does not assert its definition of terrorist financing.[30] Considering the above, in literature, there are also three main categories of terrorism financing, which combine the activities and the goals that terrorist groups engage in. The generation of funds (raising funds), the transfer of funds (moving and storing funds) and the use of funds (managing and obscuring funds). [31]

The nature of funding differs depending on the terrorist group, whereas terrorist financing requirements usually fall under two broader categories. On the one hand, the funding of terrorist operations (costs that produce violence-financing of potential attacks and their preparatory methods) and, on the other hand, the costs of maintaining and developing the group's infrastructure (operating/organisational costs, financing of the terrorist groups' day-to-day activities, like training). The distinction of the purpose of funding is sometimes vital as it underprints the nature and the tools of financial activities involved.

Reports of terrorist groups employing cryptocurrencies for funding surfaced as early as 2015. That year, an American teenager admitted teaching Islamic State members how to employ Bitcoin. He advised sponsors on creating bitcoin wallets and using the 'dark wallet' service. [32] The 'Fund the Islamic Struggle without Leaving a Trace,' is another example, of a dark

---

Risks. (Guidance for a risk-based approach to virtual currencies, June 2015, available at: www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html). In the report is stated that virtual currencies have been increasingly adopted as a new payment mechanisms and pose challenges for national authorities as they consider regulatory action to prevent the abuse of this payment mechanism to transfer funds in support of terrorism.

29 (FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html)

30 UNSCR 2462 (2019); FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated March 2022

31 Martin S Navias, Finance & Security: Global Vulnerabilities, Threats and Responses (London: C Hurst & Co., 2019), p. 49.; Jessica Davis, Illicit Money: Financing Terrorism in the 21st Century (London: Lynne Rienner, 2021),p. 5.

32 Irwin, A.S.M. and Milad, G. (2016), "The use of crypto-currencies in funding violent jihad", Journal of Money Laundering Control, Vol. 19 No. 4, pp. 407-425. <https://doi.org/10.1108/JMLC-01-2016-0003>

Internet website that transfers bitcoins to jihadis[33], while there is even an article titled "Bitcoin wa Sadaqat al Jihad" (Bitcoin and the Charity of Jihad) which describes how to transfer valuable bitcoins from North America and Western Europe to jihadists.[34]

Nevertheless, the threat posed by digital currencies is not limited to Bitcoin. Many different cryptocurrencies have developed in recent decades, such as MasterCoin, BlackCoin, and Monero, which are regarded as more secure and private than Bitcoin. Moreover, FATF's reports have previously stated that terrorist groups will engage in various illegal activities to raise funds.[35] To that end terrorist groups use cryptocurrencies to trade drugs, weapons, and other products[36].

Many of the crimes mentioned above are accomplished through online black markets. Much of the illicit cryptocurrency activity takes place through dark net websites and trading platforms, which allow individuals from all over the world to interact in unregulated virtual trade with complete anonymity. And while the objectives of terrorists and criminals diverge, the goal is the same as both groups benefit financially from trading.

The utilisation of crowdfunding techniques also poses a new terrorist funding risk. Crowdfunding is an Internet-enabled method for organisations or individuals to raise funds from numerous individuals through contributions or investments. Websites make it simple to create a fundraising page and collect donations.[37] Crowdfunding, however, is susceptible to being exploited for illicit purposes, including cases in which the original purpose of the fundraising effort is concealed. Charitable and non-profitable organisations have for years been in the cross arrow of terrorists. Several cases show that donors were unaware of the final destination of funds raised through crowdfunding and social media

Most recently, in August 2020, the Department of Justice of U.S. announced the government's largest-ever seizure of cryptocurrency in the terrorism context, stemming from the dismantling of terrorist financing campaigns involving the al-Qassam Brigades (Hamas's military wing), al-Qaeda, and ISIS.[38] Each of those groups used cryptocurrency technology and social media platforms to spread their influence and raise funds for terror campaigns. The government seized four websites, four Facebook pages, over 300 cryptocurrency accounts, and millions of dollars. The government's investigation also revealed that al-Qaeda and affiliated terrorist groups operated a bitcoin money laundering network using social media platforms and posing as charities. In the case of ISIS, the investigation uncovered a scheme whereby individuals associated with ISIS marketed fake personal protective equipment

33 Weimann, G. (2016). 'Going Dark: Terrorism on the Dark Web.' Studies in Conflict & Terrorism 39(3): 195–206

34 Azani, E., & Liv, N. (2018). Jihadists' Use of Virtual Currency. International Institute for Counter-Terrorism (ICT). <http://www.jstor.org/stable/resrep17688>

35 FATF's 2008 Terrorist Financing report available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>

36 Shacheng Wang, Xixi Zhu, Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing, Policing: A Journal of Policy and Practice, Volume 15, Issue 4, December 2021, Pages 2329–2340, < https://doi.org/10.1093/police/paab059>

37 FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html

38 Press Release, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," U.S. Dept. of Justice (Aug. 13, 2020), available at: < https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns >

("PPE")—such as N95 respirator masks—to customers across the globe in an effort to take advantage of the COVID-19 pandemic. The funds from such sales would have been used to support ISIS's operations, as terrorists and extremists claimed to raise funds for legitimate charitable or humanitarian activities.

In 2017 Zoobia Shahnaz, a woman from Long Island, was sentenced to 13 years in prison for providing material support to ISIS[39]. The investigation revealed that she fraudulently obtaining six different credit cards and later purchase bitcoin and other cryptocurrencies which she transferred via banks through various countries to ISIS sympathisers in Pakistan, China, and Turkey.

Terrorist groups also use cryptocurrency to buy and sell "tools of the trade," items that might not be illegal prima facie but are used for subsequent illegal activity. Examples of such tools include raw materials for producing explosives and equipment and technology (including servers and domains) for engaging in cyberspace or conducting malicious influence campaigns on social media. Terrorists acquire these products and services with cryptocurrency, expecting their activity and planning to go unnoticed.

Chapter 2. Counter-Terrorism Financing

The legislative and supervisory framework is possibly the most challenging task in a continually evolving environment like the crypto-economy. Because many jurisdictions lack a regulatory framework, the system is vulnerable to dangers and misuse. Decentralised finance has evolved into a new architectural notion, resulting in a financial system that is considerably more efficient, speedier, anonymous, and globalised with its trading methods and quasi-banking services. It is still difficult to envision a legal environment where the freedom that cryptocurrencies represent and the protection that law provides can coexist constructively. Reports from international organisations are becoming more common these days, indicating the pressure and stagnation the international community has been subjected to. We are currently dealing with regulatory challenges and will most likely continue to do so in the future.

This chapter analyses the legal framework that encloses the counter-terrorism funding efforts of the international community. The chapter is split into two main sections. The first section elaborates on the international legal framework, while the second section refers to the European Union’s efforts to combat terrorist funding. In addition to setting out the legal basis of counter-terrorist funding, a critical approach to the FATF’s recommendations is provided as they comprise an essential part of the international standard for battling terrorist funding, in the author’s opinion.

39 Press Release, “Long Island Woman Sentenced to 13 Years’ Imprisonment for Providing Material Support to ISIS” U.S. Dept. of Justice (March 13,2020), available at <https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>

2.1. Introduction to the international legal framework

2.1.1. The International Convention for the Suppression of the Financing of Terrorism

For years, the international community attempted to combat terrorism, adopting various international treaties, including the United Nations International Convention for the Suppression of Terrorist Financing, also known as the Terrorist Financing Convention. To that end, the UN Security Council has adopted several binding resolutions under Chapter VII of the UN Charter dealing with terrorist financing[40].

In recent years, conventional approaches to terrorist financing have been supplemented by non-traditional mechanisms, such as the Financial Action Task Force (FATF) and its recommendations. These recommendations are not traditional sources of international law, as identified, for example, by article 38 of the Statute of the International Court of Justice (ICJ), and are regarded as nonbinding in the technical normative sense. Nonetheless, they have accomplished normative status and exceptional levels of implementation by states, establishing them as the international standard for countering terrorist financing.

In international law, the CTF regime consists primarily of the Terrorist Financing Convention, UN Security Council Resolutions under Chapter VII, and FTFA recommendations. The recommendations encompass, refer to, and supplement the first two binding norms.

The persistence of terrorism throughout the years and its growth during the 1960s prompted the international community to take action attempting to codify international law on this matter.[41] Although the League of Nations took the first step in adopting an international counter-terrorism convention, the plan was abandoned. Subsequently, giving its place to The United Nations, which, under their auspices, prepared and adopted a set of conventions that are considered the basis of international counter-terrorism law. In parallel with preparing these conventions, the General Assembly and the Security Council adopted several resolutions focusing on preventing terrorism and adopting counter-terrorism measures.

In Res 2625(XXV) of Oct. 24, 1970, it is stated that *"Every State has the duty to refrain from organising, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organised activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force".*

This Resolution was later supplemented by the Declaration on Measures to eliminate international terrorism (General Assembly Res.49/60), which laid the basis for the United Nations counter-terrorism policy. The Resolution stated that:

> *"States must also fulfil their obligations under the Charter of the United Nations and other provisions of international law with respect to combating international terrorism and urged to take effective and resolute measures in accordance with the relevant provisions of international law and*

40 SC Resolutions 1267 (1999) and 1373 (2001)

41 Muller,Kälin, Goldsworth 2007, Anti-Money Laundering: International Law and Practice,Wiley; 1st edition

international standards of human rights for the speedy and final elimination of international terrorism, in particular:

(a) To refrain from organising, instigating, facilitating, financing,encouraging or tolerating terrorist activities and to take appropriate practical measures to ensure that their respective territories are not used for terrorist installations or training camps, or for the preparation or organisation of terrorist acts intended to be committed against other Statesor their citizens;

(b) To ensure the apprehension and prosecution or extradition of perpetrators of terrorist acts, in accordance with the relevant provisions of their national law;

(c) To endeavour to conclude special agreements to that effect on a bilateral, regional and multilateral basis, and to prepare, to that effect, model agreements on cooperation;

(d) To cooperate with one another in exchanging relevant information concerning the prevention and combating of terrorism;

(e) To take promptly all steps necessary to implement the existing international conventions on this subject to which they are parties, including the harmonisation of their domestic legislation with those conventions;..."

Following a series of resolutions in the 1990s condemning the financing of terrorism, in 1996, UN General Assembly adopted resolution 51/210 on measures to eliminate international terrorism, which complemented the above Resolution (A/RES/49/60), particularly noting that all member states are urged

"*To take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organisations, whether such financing is direct or indirect through organisations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities, and in particular to consider, where appropriate, adopting regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes without impeding in any way the freedom of legitimate capital movements and to intensify the exchange of information concerning international movements of such funds; ".*

Shortly afterwards, to implement the above Resolution, the General Assembly drafted the International Convention for the Suppression of the Financing of Terrorism (1999), which came into force in 2002 and supplemented the existing conventions. The Convention criminalised terrorist financing in art.2(1), stating that:

"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or
(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act".

Moreover, it required states to pose restrictions on financial institutions (art.18) and argued that international cooperation was the key factor in combating terrorism financing.

The Convention's key provisions were later included in Resolutions adopted by the Security Council under Chapter VII of the Charter, attaining normative status for the obligations, even for the States who had not become parties to the Convention.[42]

The Convention laid the foundation for the legal Regulation of this issue at the international level. The signatory states undertook the commitment to establish the criminal nature of terrorism financing in their respective domestic legislations to engage in extensive cooperation with other participating states and to enforce specific rules concerning the role of financial institutions in identifying and reporting indicators of terrorist financing[43]. The authors of the Convention did not necessitate evidence of any relation between the act of financing and a specific terrorist act to establish the independent offence of terrorist financing. The drafters framed the offence in such a way that it largely depends on the financer's mental element, that is, the financer's intention or knowledge that the funds collected or provided will be used for a terrorist act[44].

2.1.2.The Security Council's counter-terrorism policy

The Security Council implemented its counter-terrorism policy through a number of supplementary interconnected initiatives, the first of which was of symbolic importance. In Resolution 1368 (2001), Adopted by the Security Council, on Sept. 12, 2001, in par.1 is stated that the council *"Unequivocally condemns in the strongest terms the horrifying terrorist attacks which took place on Sept. 11, 2001, in New York, Washington, DC and Pennsylvania and regards such acts, like any act of international terrorism, as a threat to international peace and security."*

This declaration provided the Security Council with a legal basis for taking all necessary measures and coercive ones under Chapter VII of the Charter to respond to terrorist acts. However, the extension of the principle was not universally accepted, with some member states claiming that the council expanded its authority, considering that there was no consensus on a legal definition of terrorism.

Nevertheless, this initial Resolution was followed by Resolution 1373 (2001), which outlined the initiatives the council sought to promote as part of a focused global counter-terrorism effort. This Resolution addresses all counter-terrorism aspects but focuses mainly on the financial aspect by enforcing specific obligations on states. The two central notions of the Resolution focus on criminalising the financing of terrorism and cooperation with financial bodies.

42 see Res. 1267 Adopted by the Security Council on Oct. 15, 1999, Res.1373 Adopted by the Security Council on Sept. 28, 2001

43 Hamed Tofangsaz; Criminalization of Terrorist Financing: From Theory to Practice. New Criminal Law Review 1 February 2018; 21 (1): 57–140. doi: https://doi.org/10.1525/nclr.2018.21.1.57

44 Ibis 42

For the former the resolutions do not diverge from the language of the Convention for the Suppression of the Financing of Terrorism of 1999 stating that the Security Council acting under Chapter VII of the Charter of the United Nations

> *"1. Decides that all States shall: (a) Prevent and suppress the financing of terrorist acts; (b) Criminalise the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts;…..*
>
> *2. Decides also that all States shall: (e) Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts;"*

Concerning the later, the Security Council stressed that states should

> "*work together urgently to prevent and suppress terrorist acts, including through increased cooperation and full implementation of the relevant international conventions relating to terrorism.*" and "*3(d) Become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of Dec. 9 1999; and (e) Increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);".*

From a legal and political standpoint, the Resolution is crucial because it represents a fusion of many normative provisions and expressions of a body of rules established in previous declarations and conventions. The Resolution also gave these provisions special status because it was acting under Chapter VII, rendering it binding for all United Nations members, according to articles 25 and 48 of the Charter.

The security council's counter-terrorism policy also entails collaboration with many international organisations and entities that can support its actions. The FATF's mandate expanded to encompass terrorist financing, as initially it was limited to money laundering, at the proposal of its most prominent members, also permanent members of the Security Council[45].

In the years that followed, the FATF developed a series of recommendations on terrorist financing, accompanied by technical procedures on implementation and guidance for states. In the absence of other such norms, the Security Council endorsed these standards through its specialised body, the Counter-Terrorism Committee, and they rapidly evolved into the only international standards for the prevention of terrorist financing.[46] The security council communicated the importance of these non-binding recommendations in Resolution 1617(2005), supporting the FATF's work and establishing collaboration between the two bodies.

45 Ibis 40
46 Ibis 44

Resolution 1617 (2005), adopted by the Security Council on Jul. 29, 2005, reads that acting under Chapter VII of the Charter of the United Nations, the Council "*Strongly urges all Member States to implement the comprehensive, international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing."*

To that end, also important is the fact that the security council did not dissociate the recommendations on terrorist funding from the FATF's recommendations on money laundering, thus widening the scope of protection,[47] endorsing the entirety of the system developed by the FATF and reaffirming the interaction between money laundering and financing of terrorism.

2.1.3. The Financial Action Task Force (FATF)

The Financial Action Task Force is an intergovernmental organisation founded in 1989 as an initiative of the G7 ministers. Its mandate is to establish standards and foster the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, the proliferation of weapons of mass destruction, and other threats to the international financial system's integrity.[48] As a standard-setting and policymaking body, the FATF is committed to creating technical competence and reforming the national regulatory frameworks to harmonise them as much as possible.

The FATF examines money laundering and terrorist financing methods and prevention measures, providing a forum for discussing best practices. In addition, it attempts to emphasise areas of common concern and promote and monitor its members' progress in enacting and implementing worldwide regulatory measures. The FATF also engages with other international partners to address regional vulnerabilities, protect the international financial system from misuse, and develop standards for domestic best practices. The Egmont Group of Financial Intelligence Units is one of the most prominent and recognised in the field that acts as an observer organisation to the FATF. The European Bank for Reconstruction and Development (EBRD), The European Central Bank, Europol, Eurojust, Interpol, International Monetary Fund (IMF) and the Basel Committee are also amongst them.

As mentioned in previous paragraphs, the FATF has created a set of Recommendations that are widely accepted as international standards for combating money laundering and terrorist financing. FATF members are charged with enforcing the standards at a national level in order for the private sector to comply. These recommendations lay the groundwork for a coordinated global response to these challenges.

The original FATF Forty Recommendations were developed in 1990 to respond to the misuse of monetary institutions by those laundering drug money. The Recommendations were initially revised in 1996 to reflect advancing money laundering techniques and widen their scope beyond drug-money laundering. In October 2001, the FATF expanded its mandate to include the funding of terrorist acts and terrorist organisations and established the eight, now

47 Ibis 45

48 https://www.fatf-gafi.org/about/

nine, Special Recommendations on Terrorist Financing.The FATF Recommendations were amended ever since and are now universally acknowledged as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

Combating terrorist financing is a major challenge. An effective AML/CFT system is critical for countering terrorist financing, and most measures initially centred on terrorist financing are now incorporated across the Recommendations. The FATF also recognised the importance of including virtual-asset-related activities in its provisions in 2014 and, in 2015, issued its global guidance.[49] The same guidance was amended in 2021 to encompass the new technologies behind virtual assets and prepare for future developments.[50]

2.1.4.Special Recommendations on Terrorist Financing

The nine special recommendations[51] include ratifying and implementing UN instruments, criminalising the financing of terrorism and associated money laundering, freezing and confiscating terrorist assets,[52] and reporting suspicious transactions related to terrorism, international cooperation and measures to prevent the misuse of non-profit organisations.

The first recommendation reaffirms the close relation and cooperation of the FATF and the UN, as it addresses the ratification and implementation of UN instruments.

> "*Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005."*

The second recommendation addresses criminalising the financing of terrorism and associated money laundering as it states that

> *"Countries should criminalise terrorist financing on the basis of the Terrorist Financing Convention, and should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences".*

On the interpretive note is explained that the recommendation aims to ensure that states would have the capacity to prosecute and penalise those offences and, at the same time, underprint

49 FATF Guidance for a risk-based approach -Virtual currencies, June 2015, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

50 FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html

51 FATF 2012-2022, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, available at:www.fatf-gafi.org/recommendations.html

52 Jayasuriya, D. (2003). Money laundering and terrorist financing: the role of capital market regulators. Journal of Financial Crime, 10, 30-36.

the close relationship between financing terrorism and money laundering. On the same note, it also provides a detailed review of the characteristics of the terrorist financing offence. In that, the offence of terrorist financing is disassociated from any act of terrorism being carried out, in correlation with the International Convention for the Suppression of the Financing of Terrorism, the element of financing is distinguished from the elements of an "actual" terrorist attack.

The third recommendation is tackling targeted financial sanctions related to terrorism and terrorist financing.

> "*Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001). "*

This recommendation focuses on preventive measures that are both essential and exceptional in preventing the transfer of money or other assets to terrorist organisations and utilising these funds. In the explanatory comment, it is also stressed that members must safeguard human rights, the rule of law, and the rights of innocent third parties when defining the limits of, or encouraging broad support for, an effective counter-terrorism financing regime. This fact is addressed explicitly due to the later resolutions stated in the recommendation and evolves around the identification and designation of persons and entities (listing).

The fourth recommendation appeals to financial institutions and their obligation to report suspicious transactions related to terrorism. *"If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)".* The recommendation applies to all illegal behaviour that constitutes a predicate money laundering offence. The term terrorist financing relates to financing terrorist acts, groups or autonomous terrorists, even if there is no link to a direct terrorist act.

The fifth recommendation refers to international cooperation. It suggests that *"Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings…."* To that end, the FATF suggests that countries should adapt their legal requirements in order to be able to adequately respond when needed. This involves the establishment of official authorities that will ensure that requests are effectively transmitted and executed. Also national authorities should not refuse to carry out a request solely because the crime involves fiscal matters or on the basis that domestic regulations require from financial institutions to maintain the privacy of their users. At the same time the authorities must protect the confidentiality and the integrity of the inquiry. The recommendation also tackles the principle of dual criminality, providing that *"Where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied*

regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.".

The sixth recommendation encompasses targeted financial sanctions related to the proliferation of weapons and their funding. The emphasis is on prevention methods that are essential and exceptional concerning the flow of funds or other assets to proliferators or proliferation, as required by the United Nations Security Council.

> "*Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations."*

Tackling the proliferation of weapons and illicit arms trafficking is linked with terrorist financing. Terrorist attacks frequently employ illicit weapons, and the illicit arms trade is a predicate offence to money laundering. Furthermore, arms trafficking is a financially rewarding source for terrorist organisations, enabling them to expand their activities while increasing their threat.

The seventh recommendation engages wire transfers and addresses the information qualification that states should enact in order to accurate collect and preserve in the chain the information of the user. This recommendation mostly targets the financial institutions since they are charged with the monitoring of the transactions and the detection of any misuse or lack of information concerning the originator or the beneficiary. Their obligations also extend to the reporting of such anomalies in the transfers and the freeze of actions if prohibited transactions are in motion. That suggestion refers to designated persons or entities according to the United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing (resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001)).

The eighth recommendation appeals to non-profit organisations. *"Countries should review the adequacy of laws and regulations that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse…"* Terrorist organisations often impersonate legitimate entities; using them as channels for terrorist financing, ofthen to avoid the freezing of their assets. Through the activities of non-profit organizations they tend to gather, conceal and diverge funds, to terrorist organisations.

The FATF defines NPOs as *"a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".*

Finally, the ninth recommendation involves cash couriers *"Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system..."* The national authorities are tasked with the effective and proportionate termination of this phenomenon by restraining currency or bearer negotiable instruments that are suspected to be related to terrorist financing.

Apart from the above, the recommendations encompass virtual currencies and new technologies. According to Recommendation 5, states and financial institutions must be vigilant in identifying and evaluating terrorist financing risks associated with the introduction of new services and business practices. This includes new delivery mechanisms and the adoption of emerging technologies for both recent and pre-existing products. Specifically, this assessment should occur before the introduction of new products, business practices, or the use of emerging technologies, as the necessary measures to manage and mitigate the risks should already be in place.

The risk-based approach (RBA) is vital to implementing the recommendations. A risk-based approach requires states, supervisory authorities, and financial institutions to identify, assess, and understand the terrorist financing threat to which they are exposed and then assume appropriate mitigation actions in accordance with the level of threat.

For the purposes of the recommendations, a terrorist is defined as

> "*any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act".*

It also provides a definition for terrorist acts -not terrorism- which follows the similar language of the UNSC and the Conventions. Finally, defines terrorist organisations as

> *"any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act".*

In the context of the recommendations, the FATF also provides for the legal characterisation of virtual assets.

> "*A virtual asset is a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets". In another instance, it refers to virtual assets as "property," "proceeds," "funds," "funds or other assets," or other "corresponding value."*

The definition given is vague, therefore, potentially misleading. Nevertheless, it covers a regulatory gap in international law concerning virtual currencies and provides the authorities with a broad field of action when it comes to countering the financing of terrorism.

All the above are not only theoretical recommendations but, at the same time, "real-life" counter-terrorist practices and measures, that if implemented worldwide, can produce results. The FATF Recommendations provide a comprehensive set of policies that a state can implement to prevent terrorism financing effectively. While these requirements attempt to be as detailed and straightforward as possible, some countries may require additional assistance to understand the various technical prerequisites properly. Correctly analysing FATF Recommendations is essential for creating an effective AML/CFT system. To supplement the Recommendations, the FATF has created an extensive body of guidance and best practises papers over the years.

Furthermore, as stated in previous paragraphs, the FATF, in 2015, published guidance relating to terrorist funding and the use of virtual currencies.[53]The guidance provides specific recommendations in correlation with the use of virtual currencies.

According to the first recommendation, states should use a risk-based approach to ensure that the actions are proportionate to the threats identified. That implies firm cooperation between national authorities and the private sector. It is also recommended that public authorities should consider whether to regulate exchange platforms (virtual currency exchangers). That last recommendation, even though it is subject to domestic needs and is based on each country's risk assessment and regulatory policy, comes with a warning in case of prohibition from national authorities concerning the impact of such a prohibition. So, countries should assess the risk of using virtual currencies and the implications of regulating or prohibiting them.[54]

The second recommendation advises national authorities to create and enforce effective legislation and consider inter-agency task forces, including legislators, the national FIU, and law enforcement agencies. In case virtual currencies become a significant element of the financial sector, countries could investigate whether this is a result of their already existing AML/CFT or non-AML/CFT regulation and supervision.

The third recommendation concerns registering or licencing individuals or legal entities that provide services related to money exchange and virtual currency transfer services. This refers primarily to convertible virtual currencies. Because digitally exchanged and transferred value does not succumb to any national boundaries, the FATF believes that it is critical for countries to establish sufficient cooperation and information exchange in jurisdictions where those services are provided.

The fourth recommendation reinforces the risk-based approach obligation relating to developing technologies. Countries must identify and evaluate ML/TF risks associated with

53 FATF Guidance for a risk-based approach -Virtual currencies, June 2015, available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

54 The FATF highlights that such an action can redirect virtual currency-related activities to the black market, where they will remain operational without AML/CFT controls or oversight.

developing new services and practices for new and pre-existing products. Furthermore, national authorities must ensure that licenced financial institutions or entities operating within the country conduct the appropriate risk management and place risk mitigation measures prior to launching or employing new or developing technologies.

The fifth recommendation lays out the requirements in terms of wire transfers for both national and cross-border transfers. A wire transfer is any transaction conducted electronically through a financial institution. The main focus is the originator's and beneficiary's personal information in case the transaction takes place through virtual currencies. In that regard, the recommendation suggests that countries consider setting a de minimis threshold for cross-border wire transfers.

The sixth recommendation suggests that convertible virtual currency exchanges must be sufficiently regulated and supervised and that countries should amend, if necessary, their domestic legislation to encompass the exchange of decentralised virtual currencies under AML/CFT regulation.

The seventh recommendation addresses the above challenge by providing specific guidance for the required changes in domestic law, for example, licencing virtual currency exchanges and implementing customer identification and recordkeeping. The FATF believes that anonymity is a key issue because it allows the participants in the transactions to operate without proper identification and verification methods. That is also facilitated by the underlying technology and protocols in which virtual currencies operate. In that way, anonymity limits the blockchain's utility for monitoring transactions and detecting suspicious activity, challenging the national authorities' ability to trace illegal transfers. To that end, the recommendation suggests that countries should assess the difficulties that arise to identify gaps in domestic legislation and take the necessary steps.

Finally, the eighth recommendation requires countries to assist other jurisdictions in the fight against money laundering and terrorist funding. This involves operational assistance to identify, freeze and seize the assets and extradition and legal assistance. The national or regional FIUs are usually tasked with this work, as part of their assignment is the assistance of cross-border counterparts with sharing intelligence and assisting in operations.

Summarising all of the above at first glance, it is evident that the FATF has a detailed and elaborate plan of action to combat the financing of terrorist groups and money laundering. FATF's recommendations cover all fronts where illegal activity can emerge and propose operational and legislative actions. Moreover it addresses the threats of new technologies and appeals to the core of of the problem which evolves around financial institutions and private actors as far as cryptocurrency exchanges concerned. Simultaneously, the recommendations address these activities by combating the effects they generate and establishing a framework to identify potential threats and prevent crime from an early stage. The preventive role of the recommendations is vital as it reveals the willingness and importance to identify new challenges, direct the effort in research and training and put in place strategies that prevent the

misuse of new financial technologies by monitoring and regulating them before they can become widely disseminated.

A more critical review, although reveals inefficiencies. Reviewing FATFs methodology, it is evident that it delivers a limited view of effectiveness.[55] Although the methodology's goal is to evaluate the effectiveness of the recommendations, the findings are often ambiguous or lack measurability.[56]. The FATF work at the assumption that the measures it asserts, whether preventing or tackling the problems, ultimately contribute to "outcome effectiveness", but at the same time, it provides no details or measures as to how much and why. The ambiguity of the effectiveness of the measures taken to disrupt terrorist funding also manifests in the target of the evaluation. FATF primarily does not focus the evaluation on the performance of the state authorities or their financial intelligence units that are tasked to enforce and oversee the implementation, but instead on the private sector and financial institutions and their technical compliance with the domestic regulations. This can exacerbate the problem as financial institutions and the private sector tend to automate tasks to generate better data and ultimately trade effectiveness with efficiency. This is evident considering the number of money banks spend annually to reduce their "false positive rates" to meet their view of the requirements, even if doing so will result in no meaningful prevention of terrorist funding.

Moreover, modern terrorist funding can be more sophisticated and employ different vehicles to achieve the objective as new technologies are becoming increasingly important. Currently, many countries lack the ability or are unwilling to provide constructive international cooperation. Many jurisdictions cannot fully comply with the recommendation due to the inadequacy of their investigative powers, the lack of expertise, training and resources, or even the lack of regulation in the domestic framework. As a result, the FATF frequently refers to reforms in national laws and the need for modernisation.

Also, to add to the problem, there is a discectomy between the private and public sectors which increases the complexity of compliance and the possibility of errors. Nevertheless, as the only international body considered an expert in countering terrorism financing, FATF has assumed the lead in this field, requiring cooperation from its members, handling pressing issues and pushing for changes and uniformity in the international arena that otherwise would not exist. The FATF AML/CFT strategy has grown into a powerful international regulatory framework that strongly affects countries' compliance with its standards. The resilience of its structure, and endorsement from other international and regional organisations have all attributed to its legitimacy, generating significant compliance. Those characteristics have over the years defined the compliance performance of countries, leading to the adoption of the AML/CFT reccommendations of a number of countries.

In light of the above the FATF could tackle some of the issues by emphasising the assessment on the financial units and incorporating law enforcement into the strategy. It could also consider incentivising the private sector by rewarding innovation to fight terrorist funding. Finally, the FATF should consider redefining its methodology to encompass the quality of the

55 FATF (2013-2021), Methodology for Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems, updated October 2021, FATF, Paris, France, http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html

56 Ronald F Pol, 'Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?', Journal of Money Laundering Control (Vol. 21, No. 2, 2018), p. 221

implementations of its recommendations, reform the domestic legislation and include a subfield of effectiveness based on operational costs of the supervisory and implementation prosses and outcomes.

2.2. The European legal framework and the 5th anti-money laundering Directive

---

Virtual currencies were first addressed at the EU level in 2012 when the European Central Bank (ECB) released a report on cryptocurrencies. In response to the increasing popularity of Bitcoin, the ECB stated that the levels of anonymity provided by virtual currencies could pose terrorist funding risks. The European Banking Authority (EBA) issued a consumer warning in 2013, emphasising that the possibility of cryptocurrencies being used in criminal activity could place consumer funds at risk.[57] The EBA published an official opinion on the matter in 2014, stating that virtual currencies pose high risks to the EU's financial system because of the prospect of being used for money laundering and terrorist financing. To mitigate these risks, the EBA suggested that virtual currency transactions be included in the context of the EU's Anti money Laundering Directives (AMLDs).

In 2015 the European Commission issued the 4th AML (Directive 2015/849 on preventing the use of the financial system for money laundering or terrorist financing) and repealed the previous ones. After the Paris attacks in 2015, the FATF issued its guidance, which followed the response of the Commission announcing its intention to amend the 4th AML to encompass a variety of terrorist financing risks. The Commission also noted that, in accordance with the FATF's recommendations and the EBA's previous guidance, the amendments would include measures to address the risks posed by virtual currencies.

In 2018 the 5th anti-money laundering Directive (Directive 843/2018) was published, which amended the 4th AML and gave the EU's member states until Jan. 10, 2020, to transpose it to their national legislations.Although the Commission underlined that the inclusion of virtual currencies in the 5thAMLD did not correspond to actual evidence of their use in Europe but instead, a concern about the possibilities emerging, Europol in 2016 reported changes in the modus operandi of terrorist attacks.[58]

The EU's approach to counter terrorist financing integrates into the AML framework, the FATF recommendations. The EU, much like FATF, seeks to encourage responsible technological innovation while mitigating the risks. The preamble to 5AMLD's highlights this, stating, *"For the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT), competent authorities should be able, through obliged entities, to monitor the use of*

57 Keating,Carlise,Keen, Virtual currencies and terrorist financing: assessing the risks and evaluating responses,2018 European Union, Directorate General for Internal Policies.

58 Europol, Changes in the modus operandi of Islamic State terrorist attacks, Europol, The Hague, January 2016, available at: https://www.europol.europa.eu/sites/default/files/documents/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

virtual currencies. Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship."[59]

Even though the AMLD requirements have expanded in scope and detail, the key aspects remain unchanged. Terrorist financing is criminalised, and the financial institutions are required to act as the financial's system gatekeepers. The private sector must therefore conduct various levels of customer due diligence (CDD) to identify potential financiers and monitor customers' behaviour to identify unusual activities that may be connected to terrorism funding.[60] In addition to the regulatory framework, the EU has several agencies with AML/CTF expertise, the most important of which is the European Banking Authority (EBA), Europol, which serves primarily as an intelligence hub on CTF, housing the European Counter-Terrorism Centre (ECTC), the European end of the EU-US Terrorist Finance Tracking Program (TFTP), and the European Financial Intelligence Public/Private Partnership (EFIPPP).

In addition to the above, in 2020, the EU issued the Crowdfunding Regulation for return-based platforms, requiring customer due diligence (CDD) for those raising funds.[61] Although the Regulation does not fall under the AML/CTF regime, the Commission considers including those platforms under the new AML plan.

The 5th AMLD introduced considerable improvements in preventing terrorist financing. Initially, it increased the transparency of the owners by creating publicly accessible registers for corporations, trusts, and other legal arrangements. This expanded access to a portion of the beneficial owner's information, thus increasing public scrutiny and preventing the misuse of entities for terrorist financing. Information is accessible without restrictions to authorities, Financial Intelligence Units, and individuals who demonstrate a legitimate interest.

Furthermore, it enhanced the work of Financial Intelligence Units by directly linking information via centralised bank account registers to enable cooperation and intelligence exchange among Member States. Also, the 5th AMLD tackled terrorist financing risks related to anonymity and the use of virtual currencies and pre-paid mechanisms, like pre-paid cards, mainly when used online. The regulations are also implemented for institutions that hold, store and transfer virtual currencies and individuals who provide similar services to those provided by auditors and accountants, currently subjected to the 4th Anti-Money Laundering Directive. To that end, the requirement of identifying and reporting suspicious activities to Financial Intelligence Units also applies to the new actors.

---

59 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Preamble, recital 8.

60 Reimer,Redhead, Bit by Bit Impacts of New Technologies on Terrorism Financing Risks,2022, RUSI Occasional Paper

61 Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European Crowdfunding Service Providers for Business, and Amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937', 20 October 2020 available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1503&rid=4

Additionally, centralised bank account registers or retrieval systems are established to identify bank and payment account owners. Through these centralised registers, the Financial Intelligence Units from different EU member states will gain increased access to information, thus enhancing the powers of the FIUs and, at the same time, facilitating further cooperation. The Directive improved communication and cooperation among the financial supervisory authorities, including the European Central Bank, considering the fact that terrorist funding and money laundering can jeopardise a bank's financial stability.

The last change that the 5th AMLD introduced broadend the criteria for assessing high-risk third countries and improved verifications on transactions involving such countries. The Directive introduced new criteria, including that of transparency of beneficial ownership. Sectors that deal with countries identified by the European Commission as having deficiencies in their anti-money laundering and counter-terrorism financing regimes will face stricter regulations on financial transactions from and to these countries. The list of evaluations has also been harmonised to ensure that EU legislation does not have any gaps.

While the EU's desire to address the potential terrorist funding risks from new technologies is commendable, its policy response has yet to be thorough. The EU's strategy to merge elements of the FinTech sector into the pre-existing AML/CTF regulatory framework has obvious advantages, as it provides comprehensive coverage of emerging FinTech threats[62]. However, at the same time, it might be seen as counterproductive. Instead of seeking the application of standard counter terrorism funding compliance procedures, it would have been more suitable to formulate a more adjusted response to the risks within each sub-sector of FinTech, as lower-risk areas, like investments, may have pointed towards a softer approach, whereas higher risk areas, as new payment service providers, may have necessitated more stringent and focused compliance measures. The above suggestion has been implemented in one sector, Crowdfunding, where low-risk platforms are outside the scope of counter terrorism funding, whereas higher-risk donations are included.

The Directive also considers the autonomy of the FIUs very serious and appears to be going even a step further by introducing that *"FIU shall be free from any undue political, government or industry influence or interference".* In this way, the EU directs the focus on the need to assure that the operations of the FIU's would not be affected. Furthermore, the implementation of AML/CTF is based on the private sector. Financial institutions and other legal entities have an obligation to identify and provide the authorities with financial intelligence about terrorist funding. However, because this is only sometimes the case,[63] and the EU is aware of that, it sought to redress this issue with the introduction of Europol's Financial Intelligence Public Private Partnership (EFIPPP).[64] Although this is a welcoming step, given the fragmented state of available intelligence on terrorist funding risk in the private sector and the concerns between EU policymakers about technologies such as virtual assets, more effort is needed in the field.[65]

62 Ibis.59

63 Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime', SWIFT Institute Working Paper No. 2020-001, January 2020, pp. 5–8; In the report, the research indicates that the intelligence provided is limited in value, bureaucratic and untimely in delivery

64 Ibis 61

65 Ibis 63

2.2.1 Disentangling Terrorist Financing and Money Laundering

Money laundering is defined broadly as the processing of criminal money to conceal its illegal origin, as the goal is to "clean" and "legalise" the proceeds of criminal activity. As a result, the process begins with dirty-illegal money and concludes with clean-legal money. Terrorist financing, on the other hand, is defined as the provision or collection of funds, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out any of the offences that have been defined as terrorism.

As the definition highlights, the emphasis is on the intention for using the funds rather than the cleaning procedure of the money, as funding for terrorism may come from both legitimate and illegal sources. As a result, some academics argue that terrorist financing is reverse money laundering because the process may begin with "clean" money, but the purpose for which the money is used is illegal[66]. Indeed, the dirty/clean money dichotomy is not strict, but it overlaps, provided that terrorist organisations receive the majority of their funds from illegal activities such as drug trafficking, kidnapping, smuggling, and human exploitation.

Although those two crimes reveal similarities, there are some fundamental differences, namely the source of the funding, the motivation, the purpose, and the money cycle. The primary distinction between money laundering and terrorist financing is the source of the funds. While money laundering is used by criminals to make illegal funds seem legitimate, terrorist financing involves raising funds to sustain and support terrorist activities. Terrorist financing raises funds for illegal purposes. however, the source of such funds is sometimes legal. Terrorists can raise funds through corporate contributions, government sponsorship, donations, and even legitimate business transactions, but in money laundering, an illegal source of funds is always included.

Another issue with terrorist financing is the very definition of terrorism. Depending on the standards used to define terrorism, a group may be designated as a terrorist organisation by one state but not by another. Such discrepancies may shape evaluations of the different channels of financing that do not encompass crime. Due to the critical distinctions between money laundering and terrorist financing, it is debatable whether anti-money laundering measures are appropriate for countering terrorist financing. Effective counter-terrorism initiatives cannot rely solely on the same anti-money laundering policy response as it will fail to detect and appropriately address the problem if the resources for financing terrorism come from legitimate actions.

Money laundering is difficult to quantify, but it is regarded to be significant. According to the United Nations Office on Drugs and Crime (UNODC), 2 and 5% of global GDP is laundered yearly. This amounts to between EUR 715 billion and 1.87 trillion[67], with the legalisation of

66 Roberge, I. (2007), “Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing from MoneyLaundering.” Politics 27 (3) p.196-203

67 Rhoda Weeks-Brown, Cleaning Up: Countries are advancing efforts to stop criminals from laundering their trillions Finance & Development Magazine, December 2018, p. 44-45 available at: <https://www.imf.org/en/Publications/fandd/issues/2018/12/imf-anti-money-laundering-and-economic-stability-straight> also see: <https://www.unodc.org/unodc/en/money-laundering/overview.html,> <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/money-laundering.>

the proceeds being the primary goal. Mainly all lucrative offences result in money laundering Terrorists, on the other hand, seek to achieve specific goals and require funding to carry out their activities, so the motivation for the two crimes is entirely different, as the goal of terrorism financing is not to collect, profit, or accumulate wealth but to finance terrorist activities. To that end, terrorist income requirements are frequently insignificant compared to the devastating disruption their activities cause, which also sometimes renders them undetectable to the vast amounts usually laundered from and solely for criminal activities other than terrorism. For instance, the Financial Action Task Force (FATF)[68] estimates that the direct cost for the London bombing in July 2005 was 8,000 GBP and the Madrid bombing in March 2004 at 10,000 euros, with as a sum of money could be easily gathered without the process of money laundering taking place.

Finally, when it comes to the actual procedure taking place, money laundering works cyclically, which is also used to identify the source of funds. For instance, money obtained through illicit activities like drug trafficking is first concealed through financial transactions before being incorporated into the economy and then re-included in the monetary system through laundering. Consequently, when the money appears legitimate, it is repurposed to fund other criminal operations that produce more illicit funds. This cycle is never-ending. However, when it comes to terrorism financing, neither the process nor the identification method moves most of the time cyclically. In terrorist funding, the money is raised, stored in the economic system, subsequently hidden, and finally incorporated into the monetary system and ultimately used to fund terrorist activities. The exact process, in this case, may never take place in the same way as the source of the funding; the procedure and the purpose of the funding may differ each time.

Nevertheless, whatever the differences, money laundering and terrorism financing cannot be fought in isolation. A common approach is essential since financial crime recognises no borders, and a weakness in one area of the economy exposes the entire single market to abuse[69]. Even though the objectives are diverse, money laundering and terrorist financing use similar methods of integrating money into the financial system. Because of the similarity of these routes, regulatory authorities are trying to prevent both crimes by accumulating similar approaches and differentiating them when necessary.

The laws against money laundering and terrorist financing are parallel and complementary. These two should perhaps be regulated differently due to their disparities. However, it is still being determined whether a completely different approach to the two crimes would produce the desired outcome, mainly because they are frequently interconnected regarding how the money is produced or its concealment. The active legislative framework at the international and European levels confirms the treatment of these two crimes on a common front and the need for additional legislation and actions in specific areas, such as terrorism financing.

68 FATF, terrorist financing 29 February 2008, available at: <file:///C:/Users/Eva/Downloads/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>

69 Allam, Miriam and Gadzinowski, Damian. (2009) Combating the financing of terrorism: EU policies, polity and politics. EIPAScope, 2009 (2). pp. 37-43.

Chapter 3 Evaluation of cryptocurrency abilities in terrorist financing

The rise of cryptocurrency-based digital services and transactions may provide terrorists with new ways to transfer funds and hide their financial footprints. Nonetheless, users have a variety of options for open exchange from buyer to seller, all of which are secure methods of concealing financial transactions. Having familiarised from previous chapters with the technical characteristics of cryptocurrencies and the international community's measures to address the problem of terrorist funding, this chapter will proceed to a comparative analysis of all the above to evaluate the competency of cryptocurrencies' use in terrorist financing.

This chapter is split into three sections. The first evaluates the characteristics of cryptocurrencies that prompt their use by terrorist organisations. On the contrary, the second section addresses those elements that tend to discourage the use, while the third section analyses the current and future needs of terrorist organisations for using cryptocurrencies.

3.1 Factors that encourage the use of cryptocurrency by terrorist organisations

Anonymity is the most important characteristic that differentiates cryptocurrencies from traditional fiat money. This enables cryptocurrency users to conceal their identities, preventing legal authorities from identifying and monitoring them. The anonymity of cryptocurrencies is enhanced over the years with the advancement of technology. Furthermore, cryptocurrency developers utilise various methods to increase anonymity, such as combining different virtual currencies and exchanging IP addresses to conceal the owner's identity or use the dark web. The adoption of these methods significantly improves cryptocurrency anonymity. Monero, for example, is the coin of choice of terrorists because it uses that kind of enhanced technology to create full anonymity and not pseudo as Bitcoin. Transaction anonymity is essential in terrorist organisations' financing activities as it guarantees that the funds are difficult to be traced by authorities. Moreover, individuals attempting to support donations are more likely to use this tool as it reduces the risk of tracking and, eventually, prosecution. As a result, increased anonymity is a key factor in encouraging terrorist organisations to use cryptocurrencies.

Another threat is the rise of dark online markets, which maximise the anonymity of actors and prompts illicit exchanges. Even for an inexperienced user, using the Tor anonymising browser is a simple process.As stated in previous paragraphs the dark market is being used by terrorist organizations not only to buy goods but in an attempt to sell them too in order to gain money or in order to launder their money. If we double that with the use of cryptocurrencies, it can become an increasingly harmful feature. Because of their ideal characteristics, cryptocurrencies are progressively being employed by the dark web market. There is no

conclusive evidence of terrorist organisations using cryptocurrency in darknet markets. Nevertheless, the growth in exchanges on the dark web market will eventually encourage terrorist groups to use cryptocurrency more.

The expansion of the cryptocurrency industry is also one of the prerequisites for the more extensive use of cryptocurrency by terrorist groups. Because the financial market is constantly expanding, users' trust and acceptance of cryptocurrencies are growing. Even though the continued development of virtual currency innovation is uncertain, terrorist groups are likely to expand their use if the number of individuals using cryptocurrency grows globally.

The most useful feature and the most significant disadvantage of any cryptocurrency is that it is nearly impossible to monitor the transfer of funds. Most cryptocurrencies are anonymous and do not require identification, unlike bank accounts. As a result, it is an excellent method of financing, transferring and concealing illicit purposes. Another appealing feature is international availability. The system eliminates the need to transfer money from anywhere at any time for any amount. Users can conduct transactions in other countries and remove traces by using different exchange services from multiple countries. Furthermore, because such operations are much faster than conventional transactions, the chances of them being intercepted and blocked are much lower.

Nevertheless, the absence of a comprehensive and consistent legal framework for cryptocurrencies worldwide is probably the most appealing feature of them. Both national and international bodies, face a significant challenge in countering illegal transactions in the digital economy. From the standpoint of state supervision , the problem with cryptocurrencies is their anonymity and limited capacity to determine the direction of profits, which complicates the monitoring of terrorism financing.

Although FATF and other international bodies have developed several AML/CTF programmes, the supervision in different jurisdictions has been inconsistent. This may be due to differences in the growth of their monetary institutions or because states are unwilling or incapable of efficiently supervising the financial system. Ambiguity and inconsistency in cryptocurrency regulation impede the efforts to counter terrorism financing, allowing terrorists to exploit new technologies. A number of jurisdictions around the world have created special agencies to oversee cryptocurrency regulation. Most countries, however, have yet to take any measures concerning virtual currencies. These flaws in the global legal mechanism allow terrorists to exploit cryptocurrencies. Moreover, several countries do not recognise the terrorist financing threat of cryptocurrency, and some lack the ability to detect the use of cryptocurrency for terrorist financing. So terrorist organisations may be able to use cryptocurrencies more often to fund their purposes as a consequence of this.

3.2. Factors that discourage the use of cryptocurrency by terrorist organizations

The spread of different types of cryptocurrency triggered confusion and uncertainty, significantly reducing cryptocurrency reliability. The volatility of cryptocurrencies has made it difficult for terrorist groups to finance their operations and that is because terrorists simply do not trust their money in this unstable investement. The cryptocurrency's volatility is primarily reflected in its price. The cryptocurrency market is not stable due to fluctuations in the global market. In 2021 from 800$ billion at the start of the year, the total capitalisation of cryptocurrencies reached 2.5 trillion dollars mid July before dropping back to nearly 1.5 trillion dollars moths later. This remarkable market volatility is a feature of the crypto-economy world. Such extreme price fluctuations are easily influenced by human factors, posing a risk to cryptocurrency use for direct investment. This creates a considerable impact on users. Cryptocurrencies are now a high-risk investment option. The rising number of different kinds of cryptocurrencies demonstrates the internal challenge of the FinTech market.

Given that they hold decentralised features, there is no regulatory oversight body to control their fluctuation, and once there is an adequate variety between users, miners and investors, the system will saturate due to technological and management limitations. The cryptocurrency's system for now is insufficient to support such a complicated structure. As a result, the immaturity, as well as the system's uncertainty and complexity, favoured a low rate of currency credit, which is extremely unfavourable to cryptocurrencies' long-term use, especially if they are used for investing purposes. All the above have a significantly preventive character for anyone considering investing in cryptocurrencies. This is one of the reasons that terrorist groups would most likely not favour the widespread use of cryptocurrencies in the near future.

In addition, the international community's efforts to crack down on the use of cryptocurrencies and combat terrorist financing are another preventing reason. As discussed in previous paragraphs, the FATF increasingly considers the growth of virtual currencies in recent years. Furthermore, regulators and enforcement agencies around the world are becoming more interested in cryptocurrencies and developing expertise in monitoring their use. With implementing the FATF's recommendations, terrorist organisations will have to conduct an elaborate scheme if they want to use cryptocurrencies, which is not likely to appeal to them. Terrorist organisations using virtual currencies, like any other user, must engage in a constant risk assessment process to assess if cryptocurrencies are suitable for their use and whether the risks they encounter are reasonable to them.

Also, terrorists who use cryptocurrencies face the challenge of converting cryptocurrency into fiat money, as the monitoring in this sector is more rigorous. Furthermore, terrorist organisations will have to find transmitters and exchangers they can trust or hope will not notice or care for their malicious transactions. And to that end is important to note that, terrorist groups do not always “operate” in countries with a fully advanced technological sector, thus complicating their cryptocurrency operations.

Terrorist financing methods are becoming more diverse and sophisticated as the global economy and technology advance. Terrorist organisations frequently use a combination of techniques to move money. When the stability of cryptocurrencies is in question, terrorist organisations will most likely avoid them in order to avoid the risk. As countries continue to regulate cryptocurrencies, their use is most likely to decrease. This is evident in countries that have already enacted regulations and monitoring of cryptocurrencies, even for taxation purposes. In those countries, the cryptocurrency community took a hit in cryptocurrency trading, resulting in the loss of users. In this instance, the stable development of traditional financing means is maybe more attractive to terrorist organisations. Additionally, government agencies are monitoring popular blockchain transactions, forcing terrorist groups to operate under their own payment system, which is not an easy task.

The rise in the price of cryptocurrencies resulted in the rise of cyber attacks on exchangers and users' crypto wallets. Fraudulent transactions, theft, technical attacks, and other activities exposed the security flaws that cryptocurrencies can carry. Even though these defects may be a result of technical procedure issues, they can result in significant losses. The security of cryptocurrencies has always been an essential factor in their development but also for their popularity. Nevertheless, crypto ATMs and digital wallets have been attacked multiple times in the last few years. And although many of the attacks have been initiated by cyber-terrorists, terrorist organisations are unlikely to use them in the near future for transferring or storing value. All the above renders the widespread use of cryptocurrency to fund terrorism unsuitable. As a result, terrorists will most likely continue to use the traditional hawala payment system and other financial channels.

3.3. Terrorist organisation's current and future needs for cryptocurrencies

Bitcoin was the first decentralised virtual currency to emerge in 2009. Whereas previous virtual currencies used centralised agencies as financial intermediaries, cryptocurrencies gained popularity due to the lack of third parties in transactions. Its use of online tools in conjunction with cryptography reflected an entirely new transfer system in which a secure payment is transferred directly without using an intermediary, such as a central bank or government agency. Since then, cryptocurrencies have grown in popularity as a means of payment, investment, and fund transfer. The development of an innovative payment system that enables dependable, end-to-end real-time transactions worldwide has raised regulatory concerns. Because of the innovative character of this type of currency, there was no quick regulatory or enforcement response.

Anti-Money Laundering (AML) and Know-Your-Customer (KYC) procedures that were in place were not intended to accommodate cryptocurrencies but at the same time cryptocurrency exchanges allow users to buy and convert cryptocurrencies into other currencies or fiat money. These online financial service providers can accept various payment

methods via wire transfers and credit cards, including other tokens and fiat currencies. Under European Union law, these services operate legally, provided they meet the required due diligence, as they are subject to the same regulatory framework as banks and other financial institutions. Nevertheless, these services frequently impose weak regulatory requirements that enable illegal cryptocurrency transactions by transferring assets across multiple markets, even facilitating, in some cases, illegal transactions through the use of forged or stolen identities.

Cybercriminals and terrorist groups took advantage of the favourable environment and began using cryptocurrencies for dark web trading as well as fraud and extortion schemes.[70] Aside from that, cryptocurrencies allow actors (and states) to profit directly from mining cryptocurrencies via legal mining activities or illegal "cryptojacking" mechanisms, in which case trading is not even required. Al Qaeda and its affiliates, the Islamic State of Iraq and Syria (ISIS), Hezbollah, and lone-wolf attackers are among the terrorist organisations utilising cryptocurrencies and deploying virtual fundraising methods. Even though their objectives vary, their need for anonymous and secure funding sources has led them to use cryptocurrencies as potentially valuable to them.

Anonymity, usability, security, acceptance, reliability, and volume are some of the properties that cryptocurrencies exhibit and are desirable. Anonymity is the ability to conceal and protect a person's identity, whereas usability refers to the fact that everyone can conduct a transaction from everywhere with easy access. Security ensures that the infrastructure in which one operates is confidential and accurate; and acceptance to the degree to which cryptocurrencies are accepted, adopted and used by the community. Finally, reliability is perceived by the frequency, speed and availability that the currency offers, whereas volume, to the size of the transactions of cryptocurrencies over time.

Although as of this moment, there is not a single cryptocurrency that offers all the above functions, if a single cryptocurrency emerges that offers broad acceptance, enhanced anonymity, and improved security while being subject to poorly enforced or ambiguous regulation, the utility of this cryptocurrency, as well as the potential for its use by terrorist organisations, would dramatically be increased.

In terms of terrorist funding methods, cryptocurrencies can be used in raising funds (through donors or criminal behaviour), moving funds (by moving money through financial institutions or simply physically moving cash after exchanging them) and storing funds (by maintaining reserves that can subsequently be diverted on operations or other actions).[71] In terms of terrorist actors, there is a wide range, namely, lone actors, small -cells (inspired or connected to terrorist groups like facilitation networks), command and control organisations (such as Al-Qaeda) and territory-controlling groups (like Al-Shabaab and ISIS) .[72]

Given these nuances, it is critical to consider how different terrorist actors could exploit cryptocurrencies for various applications instead of treating them as homogeneous blocks. Lone actors and small cells often do not need high financial resources to fund their attacks, so

70 U.S. Department of Justice (2020), Cryptocurrency Enforcement Framework, accessible at <https://www.justice.gov/archives/ag/page/file/1326061/download>

71 Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html. Also available in print form.

72 Ibis 71

it is not likely that those terrorist actors will require cryptocurrencies to fund their attacks. Even so, cryptocurrencies may prove attractive to specific small cells operating online, or to inform bigger terrorist groups of how to utilize cryptocurrencies for their purposes. For example, the American teenager, referred to in the first chapter, who, in 2015, used Twitter to inform peers on how Bitcoin could be utilised to disguise the acquisition of large amounds of funds in support of ISIS. While his effort did not appear to have been successful, this case represents a younger generation of terrorists who have grown up with the Internet and feel comfortable with new technologies. This also showcases that popular belief about the lack of understanding and competence among supporters of terrorist organisations does not correspond to reality. Even if we assume this possibility, it is important to note that most cryptocurrencies are rather simple to use.

Moreover, concerning the funding of larger terrorist groups, like al-Qaeda and ISIS, the use of cryptocurrencies appears to be more appealing to their ongoing operations. Terrorist groups may find utility in transferring money among members, mainly due to the pear-to-pear technology (P2P) or for targeted crowdfunding campaigns online. Cryptocurrencies can become easily convertible and can be used for various purposes, including the purchase of weapons, the facilitation of travel, the funding of propaganda campaigns, and the purchase of everyday supplies and services.

The observations above concern mostly terrorist groups motivated by religion. However, extremist political activity should also be considered, as it appears to be an increasing number of violent attacks by right-wing extremists in recent years. Of course, some of their activity, such as propaganda, may not fall within the European Union's definition of terrorism, which includes activity such as seriously intimidating a population and destabilising or destroying political, economic and social structures.[73] Nevertheless, looking at broader patterns can help comprehend how terrorist groups might use cryptocurrencies. In either case, the far embrace of cryptocurrencies by terrorist groups and extremists can also be fueled by an ideology of deep distrust of institutions.

The prospective utility of cryptocurrencies is unknown as terrorist techniques and cryptocurrencies evolve. Nevertheless, several recent advancements in cryptocurrency will make it easier for people to use them. The use of cryptocurrencies will be particularly beneficial to actors already involved in global fundraising and the most sophisticated terrorist groups. Continued cooperation among international law enforcement and advances in monitoring and control are all factors that tend to discourage use.[74]

73 Keating,Carlise,Keen, Virtual currencies and terrorist financing: assessing the risks and evaluating responses,2018 European Union, Directorate General for Internal Policies

74 Ibis 73

Conclusion

This paper examined how cryptocurrencies have created new terrorist funding risks or amplified those that existed in the international scene prior to the rise of financial technology. Nevertheless, it barely scratched the surface of the most technical and legal issues of cryptocurrencies that can disturb even more the international legal order and pose a significant threat to international security. In addressing the issue of terrorist use of cryptocurrencies for funding purposes, the first problem to encounter is the lack of definitions of cryptocurrencies and their different forms and properties of various virtual assets.

It is difficult to envision the international community agreeing on a single definition when it has not yet addressed the most important one, that of terrorism. Understandably, the issue is sensitive, unique, and possibly quite politicised. However, in this sense, it is not that dissimilar to the issue of cryptocurrency's definition if the implications of a legal definition are considered (taxation, anti-terrorism, money laundering, economics, etc.)

Formulating a regulatory framework is a complex process. First and foremost, categorising the nature and functionalities of the many crypto-assets that now exist in the ecosystem is challenging. So, how do we set up something so unique and with so many features when most countries refer to tokens and cryptocurrencies in the same way but usually categorise and distinguish bitcoin and other crypto-assets popular in their jurisdiction separately? "Bitcoin is a regulatory platypus, one that does not fit neatly," said American banker Marco Santori, former head of blockchain practice at law firm Cooley.

And it is the author's view that this may be the point for law systems and the international community to find new ways to adapt to the challenging reality they have been facing for years. Legal science and regulations in general advance because they meet the needs of society, technology, politics and economy in a sober and relevant manner. While the law is necessary for a functioning society, it "survives" because it adapts. So, if cryptocurrencies do not fit into the existing system, the next best thing to do is make the legal system fit into them. As the use of cryptocurrencies in terrorism financing is an evolving phenomenon that seems to be developing rapidly in recent years, perhaps it is the right time for legislators and policymakers to implement the above approach.

Reviewing the previous chapters is understandable that the International community has come a long way in combating terrorism. Given the inherent complexity of the structure and various phenomena of terrorist activity, it is not surprising that financial monitoring has yielded inconsistent results in combating terrorist financing. Much of the difficulty stems from the fact that terrorist funding can be generated from legitimate sources. Terrorists are also quick to adapt to the new environment of financial surveillance and implement counter-measures. The actual difficulty for the international community is to place terrorism in context and assess the risks of threats that they pose. The regulations for monitoring and supervising that are put in place are effective, but they need to cover the range of emerging threats. However, it is only reasonable to end with an optimistic position. Terrorists continue to prefer traditional

currency for various reasons, the most important being that the international community is cooperating in handling the problem of terrorist funding and the implementation of laws and recommendations governing the funding of terrorism makes it even harder for terrorists to gain access to cryptocurrencies.

The international community should evaluate the potential risks of cryptocurrencies in funding terrorism. Advanced legislative initiatives, such as those of the European Union, are welcome, as they set the standard for extensive harmonisation beyond its member states. However, the important thing now is for the rest of the international community to follow that paradigm to establish a solid framework to combat international terrorism, particularly the financing of terrorist groups, through virtual currencies.

Bibliography

Agata Ferreira, Philipp Sandner,Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure, Computer Law & Security Review, Volume 43, 2021, https://doi.org/10.1016/j.clsr.2021.105632.

Allam, Miriam and Gadzinowski, Damian. (2009) Combating the financing of terrorism: EU policies, polity and politics. EIPAScope, 2009 (2). pp. 37-43.

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) - Review of the Effectiveness of the Program INTERNATIONAL MONETARY FUND, 2011.

Antony Lewis, The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Derivatives Investments, Futures Trading, Digital Assets, NFT) (Mango Media Publications 2018)

Azani, E., & Liv, N. (2018). Jihadists' Use of Virtual Currency. International Institute for Counter-Terrorism (ICT). <http://www.jstor.org/stable/resrep17688>

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies(2010)

Bellés-Muñoz, Marta, Barry Whitehat, Jordi Baylina, Vanesa Daza, and Jose Luis Muñoz-Tapia. 2021. "Twisted Edwards Elliptic Curves for Zero-Knowledge Circuits" Mathematics 9, no. 23: 3022. https://doi.org/10.3390/math9233022

Bossong, r. (2008), the us mature counterterrorism policy: a critical historical and functional assessment. lse challenge working paper june 2008 available at: <https://www.lse.ac.uk/international-relations/assets/documents/efpu/lse-challenge-working-papers/EFPU-Challenge-Working-9.pdf>

Bradford, Anu.The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020.

Brill, Alan and Keene, Lonnie, Cryptocurrencies: The Next Generation of Terrorist Financing? (January 15, 2014). Defence Against Terrorism Review, Vol. 6, No. 1, Spring&Fall 2014, pp. 7- 30, Available at SSRN: https://ssrn.com/abstract=2814914

Chatain, Pierre-Laurent; Van der Does de Willebois, Emile; Bökkerink, Maud. 2022. Preventing Money Laundering and Terrorist Financing : A Practical Guide for Bank Supervisors. © Washington, DC : World Bank. http://localhost:14773//entities/publication/2054e13f-915d-5f0d-876e-fd69226b1491 License: CC BY 3.0 IGO."

Christian Kalin, John G. Goldsmith, Wouter H. Muller, Anti-Money Laundering: International Law and Practice, John Wiley & Sons, Incorporated,2015.

Clive Walker, Colin King, Katie Benson, Assets, Crimes and the State: Innovation in 21st Century Legal Responses.Taylor & Francis, 2020.

Dill, Alexander. Anti-Money Laundering Regulation and Compliance: Key Problems and Practice Areas Edward Elgar Publishing Limited, 2021.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. available at: <https://www.rand.org/pubs/research_reports/RR3026.html.>

Dumitriu, E. (2004). The E.U.'s Definition of Terrorism: The Council Framework Decision on Combating Terrorism. German Law Journal, 5(5), 585-602. doi:10.1017/S2071832200012700

Durr, Wayne Allen, "A Separate Asset Class for Cryptocurrency" (2021). Doctoral Dissertations and Projects. 2881. available at: <https://digitalcommons.liberty.edu/doctoral/2881>

Elagab, Omer., Elagab, Jeehaan. International Law Documents Relating To Terrorism. Taylor & Francis,2007.

European central bank, 'What is money?' (European Central Bank, 24 November 2015 (updated on 20 June 2017) available at: <https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.en.html>

Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

Europol (2022), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.

Europol, Changes in the modus operandi of Islamic State terrorist attacks, Europol, The Hague, January 2016, available at: <https://www.europol.europa.eu/sites/default/files/documents/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf>

FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France

FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris, available at: <www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html>

FATF Annual Report 2020-2021 available at: <https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf>

FATF, terrorist financing 29 February 2008, available at: <file:///C:/Users/Eva/Downloads/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf>

Fiona de Londras, Josephine Doody, The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism. Taylor & Francis, 2015.

Fox, D. and Green, S. (2019) Cryptocurrencies in public and private law: Edited by David Fox, Sarah Green. Oxford: Oxford University press.

Goldbarsht, D. (2020). Global counter-terrorist financing and soft law: multi-layered approaches. Edward Elgar Publishing. https://doi.org/10.4337/9781789909999

Goldbarsht, D., & de Koker, L. (Eds.) (2022). Financial technology and the law: combating financial crime. (Law, Governance and Technology Series ; No. 47). Springer, Springer Nature. https://doi.org/10.1007/978-3-030-88036-1

Hamed Tofangsaz; Criminalization of Terrorist Financing: From Theory to Practice. New Criminal Law Review 1 February 2018; 21 (1): 57–140. doi: https://doi.org/10.1525/nclr.2018.21.1.57

Houben, Robby., Snyers, Alexander. Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion : Study Requested by the TAX3 Committee European Parliament, 2018.

Irwin, A.S.M. and Milad, G. (2016), "The use of crypto-currencies in funding violent jihad", Journal of Money Laundering Control, Vol. 19 No. 4, pp. 407-425. <https://doi.org/10.1108/JMLC-01-2016-0003>

Jayasuriya, D. (2003). Money laundering and terrorist financing: the role of capital market regulators. Journal of Financial Crime, 10, 30-36.

Jessica Davis, Illicit Money: Financing Terrorism in the 21st Century (London: Lynne Rienner, 2021),p. 5.

Keating,Carlise,Keen, Virtual currencies and terrorist financing: assessing the risks and evaluating responses,2018 European Union, Directorate General for Internal Policies.

Law Library Of Congress, U.S.. Global Legal Research Directorate. Regulation of Cryptocurrency in Selected Jurisdictions. [Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018] Pdf. Retrieved from the Library of Congress, <www.loc.gov/item/2018298388/>.

Lee, David. Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press, 2015

Liaw, K.T. (Ed.). (2021). The Routledge Handbook of FinTech (1st ed.). Routledge. https://doi.org/10.4324/9780429292903

Ligeti, Simonato, Chasing Criminal Money Challenges and Perspectives On Asset Recovery in the EU,2019, Bloomsbury Publishing

Martin S Navias, Finance & Security: Global Vulnerabilities, Threats and Responses (London: C Hurst & Co., 2019), p. 49.;

Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime', SWIFT Institute Working Paper No. 2020-001, January 2020, pp. 5–8

Monar, J. (2007). Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and its Problems. Government and Opposition, 42(3), 292-313. doi:10.1111/j.1477-7053.2007.00225.x

Motsi-Omoijiade, Cryptocurrency Regulation A Reflexive Law Approach, 1st edition 2022, Routledge

Muller,Kälin, Goldsworth 2007, Anti-Money Laundering: International Law and Practice,Wiley; 1st edition

Narayanan, Arvind. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton, NJ: Princeton University Press, 2016.

Nouri, Lella, Maura Conway, Lee Jarvis, Stuart Macdonald, and Orla Lehane. "Terrorists' Use of the Internet: Assessment and Response." Terrorists' Use of the Internet 136 (2017)

OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. available at: < www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emergingtax-policy issues.htm>

Parkman,Mastering Anti-Money Laundering and Counter-Terrorist Financing: A Compliance Guide for Practitioners, 2019, FT Press

Policing: A Journal of Policy and Practice, Volume 15, Issue 4, December 2021, Pages 2329–2340, https://doi.org/10.1093/police/paab059

Raihan Zahirah Mauludy Ridwan,The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes,2019

Rébé, Nathalie. Counter-Terrorism Financing, (Leiden, The Netherlands: Brill | Nijhoff, 21 Nov. 2019) doi: https://doi.org/10.1163/9789004409675

Reimer,Redhead, Bit by Bit Impacts of New Technologies on Terrorism Financing Risks,2022, RUSI Occasional Paper

Rhoda Weeks-Brown, Cleaning Up: Countries are advancing efforts to stop criminals from laundering their trillions Finance & Development Magazine, December 2018, p. 44-45

Roberge, I. (2007), "Misguided Policies in the War on Terror? The Case for Disentangling Terrorist Financing from MoneyLaundering." Politics 27 (3) p.196-203

Ronald F Pol, 'Anti-Money Laundering Effectiveness: Assessing Outcomes or Ticking Boxes?', Journal of Money Laundering Control (Vol. 21, No. 2, 2018), p. 221

Sarah Green, 'Digital assets Call for evidence. (Law Commission, 30 April 2021) available at: <https://www.lawcom.gov.uk/project/digital-assets/>

SCHEININ, Martin, VERMEULEN, Mathias, Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines that Seek to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism, EUI LAW, 2010/08, - http://hdl.handle.net/1814/14178 Retrieved from Cadmus, EUI Research Repository

Schwarz,Nadine,Kao,Kathleen.,Jackson,Grace.,Chen,Ke.,Poh,Kristel.,Fernando,Francisca., Markevych,Maksym.Virtual Assets and Anti-Money Laundering and Combating the

Financing of Terrorism (1): Some Legal and Practical Considerations.International Monetary Fund, 2021.

Shacheng Wang, Xixi Zhu, Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing, Policing: A Journal of Policy and Practice, Volume 15, Issue 4, December 2021, Pages 2329–2340, < https://doi.org/10.1093/police/paab059>

Terrorism Financing and State Responses: A Comparative Perspective.Stanford University Press, 2007.

The Palgrave Handbook of Criminal and Terrorism Financing Law Springer International Publishing, 2018.

Thomas, Sam., Hyde, Dan., Armstrong KC, Dean. Blockchain and Cryptocurrency: International Legal and Regulatory Challenges. Bloomsbury Academic, 2023.

Walch, Angela, The Path of the Blockchain Lexicon (and the Law) (March 24, 2017). 36 Review of Banking & Financial Law 713 (2017), Available at < SSRN: https://ssrn.com/abstract=2940335>

Weimann, G. (2016). 'Going Dark: Terrorism on the Dark Web.' Studies in Conflict & Terrorism 39(3): 195–206