SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 03 (2025), pp. 297-311
Research Article
doi: https://doi.org/10.70710/sitj.v2i3.66

Funding Modes of Terrorist Groups in the Digital Age: Challenges and Solutions Based on Information Technology

Muhammad Sofyan[1,a,*], Tubagus Ami Prindadi[1,b]

[1]Terrorism Studies, SKSG, University of Indonesia
[a]yahyaayyash2001@gmail.com; [b]tubagusami1974@gmail.com
*Corresponding author

Article Info
Received: 4-July-2025
Revised: 30-Aug-2025
Published: 8-Sept-2025

Keywords
Artificial Intelligence; Big Data Analytics; Blockchain; Cybercrime; Information Technology; Terrorism Financing

Abstract
The digital era has changed the landscape of terrorism financing, where information technology such as blockchain, crypto assets, and digital platforms are strategically used to disguise cash flows and evade authority surveillance. This study aims to identify and analyse the modus operandi of terrorist group funding in the digital age and formulate information technology-based solutions to address it. The approach used is qualitative, employing a literature review method, integrating Crime Script Analysis (CSA) theory to map the stages of crime and Rational Choice Theory (RCT) to understand the rational motives of perpetrators in choosing digital means. The research findings indicate that funding methods include using cryptocurrency through illegal exchanges, exploiting nominee accounts, misusing digital charitable institutions, and cross-border peer-to-peer money transfer systems. Blockchain provides high anonymity and cross-border flexibility, which are exploited to obscure transaction traces. The main challenges identified include regulatory limitations, a lack of interoperability in financial surveillance systems, and law enforcement agencies' low capacity to address high-tech crimes. As a response, this study proposes five technology-based solutions: Cyber Crime Big Data Analytics, the use of Artificial Intelligence (AI) in Open Source Intelligence (OSINT), the establishment of an integrated Command Centre, the enhancement of Data Surveillance systems, and the strengthening of national Data Centres. These solutions are believed to enhance the effectiveness of real-time prevention and detection of digital terrorism financing. This study recommends cross-sector collaboration and strategic investment in information technology development as the key to mitigating the threat of digital terrorism financing in the future.

1. Introduction

Terrorist financing is one of the main pillars supporting the activities of terrorist groups such as those affiliated with Al-Qaeda and ISIS. According to Interpol's Global Crime Trends report published in 2022, technology-based crimes, including money laundering and phishing, dominate global crime trends through foundations. Non-profit foundations have long been misused as a cover for terrorist groups to channel funds covertly (Kohlmann, 2006). Some international charitable organisations, such as the Global Relief Foundation in the US, are suspected of channelling a significant portion of donations to support armed groups like Al-Qaeda and jihadist groups in Asia and Africa (Global Relief Foundation, 2002). The Global Relief Foundation case involved USD 5 million annually, with 90% of funds sent abroad; most of which was used to support terrorist activities (Global Relief Foundation, 2002). Another example is the Al-Haramain Foundation, which is alleged to have channelled funds to Jemaah Islamiyah and Al-Qaeda, including the perpetrators of the 2002 Bali bombings (UN Security Council, 2004). Similarly, the International Islamic

Relief Organisation in Indonesia and the Philippines is suspected of being used by Mohammed Jamal Khalifa to channel funds to Abu Sayyaf and Al-Qaeda (Abuza & AS, 2003).

Research at the University of North Sumatra shows that foundations in Indonesia are vulnerable to misuse due to anonymous donations, overvaluation of assets, and suspicious transactions; they call for implementing due diligence procedures (Sirait & Rangkuti, 2023). Ika Veni Anisa & Muhamad Syauqillah (2022) highlight that Jamaah Islamiyah uses foundations as funding channels and recommend defensive and offensive counterintelligence strategies, including regulatory reform and public education (Anisa & Syauqillah, 2022). A case study of the legal ruling against JI (Ruling No. 308/PID.SUS/2020) notes various modus operandi, such as palm oil plantations, member donations, and foreign funds from Al-Qaeda. It emphasises the importance of collaboration between PPATK and law enforcement agencies (Yulianti & Nachrawi, 2024). Technological advancements such as blockchain and cryptocurrency complicate the tracing of funds. At the same time, the increase in internet users from 6.7% in 2000 to 64.2% in 2021, according to the World Bank (2021), in the International Telecommunication Union (ITU), expands opportunities for cybercrime.

Data from the Financial Transaction Reports and Analysis Centre (PPATK), Indonesia's financial intelligence agency, shows that suspicious financial transactions related to terrorism financing have increased significantly. In its 2023 Annual Report, PPATK received 171 suspicious financial transaction reports (LTKM) with strong indications of terrorism financing (PPATK, 2024). The report also reveals new patterns of financing that use money remittance services, digital wallets (e-wallets), third-party accounts, and smurfing methods, which are used to break up funds so that they do not exceed the reporting threshold. At the global level, the Financial Action Task Force (FATF), as the international body that sets standards for anti-money laundering and counter-terrorist financing (AML/CFT), has placed Indonesia in the group of countries that need to improve the effectiveness of their oversight systems for the non-profit sector and cross-border transactions (FATF, 2023). The FATF notes that terrorist financing often infiltrates through charitable organisations, educational institutions, and digital channels that are difficult to monitor comprehensively. Although Indonesia has a legal framework such as Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing Crimes, the main challenges still revolve around compliance, cross-sector coordination, and adaptation to new financial technologies.

Terrorist groups have utilised digital technology to raise funds through various methods, including the use of cryptocurrency and online crowdfunding. Prasetya, Subroto, and Nurish (2021) explain that terrorist organisations utilise digital financial transaction technology, such as cryptocurrency, as part of their funding activities. They use cryptocurrency in every stage of fund utilisation, both as a medium and a source of funding, as demonstrated through models or schemes related to the use of cryptocurrency for terrorism financing. Some examples of modus operandi in the digital age carried out by resistance groups include Hamas, which has developed funding methods that utilise crypto technology. Through its military wing, the Izz ad-Din al-Qassam Brigades, Hamas openly publishes Bitcoin wallet addresses on its official website to receive donations from supporters worldwide. Hamas even provides technical guidelines for sending funds anonymously, leveraging the anonymity and decentralisation of the blockchain system to evade detection by conventional financial systems (Elliptic, 2019). This campaign marks a significant shift from traditional methods to a digital model to evade financial oversight by international authorities (Whyte, 2019). 'Your donations will be used for jihad in the path of Allah' is one of the narratives Hamas uses to frame fundraising as part of their religious struggle (Elliptic, 2019).

ISIS then exploited the COVID-19 pandemic as an opportunity to run a fake e-commerce-based funding scheme. The U.S. Department of Justice (DOJ) uncovered a website named FaceMaskCenter.com, which claimed to sell personal protective equipment (PPE) such as masks in large quantities. The site was managed by an ISIS network and designed to deceive consumers and accept payments in Bitcoin and Ethereum, so that funds could be transferred to digital wallets controlled by ISIS (U.S. Department of Justice, 2020). This strategy shows how terrorist groups exploit public needs and digital financial technology to cover up their illegal activities.

At the domestic level, Jamaah Ansharut Daulah (JAD), which is affiliated with ISIS, has utilised digital technology in its funding methods. According to a report by PPATK (2022), JAD uses QR codes and digital wallet applications (e-wallets) to collect funds from its supporters through social media and messaging applications such as Telegram and WhatsApp. Transactions are conducted in large-scale micro-donations (smurfing) to various accounts under the names of individuals not directly affiliated with the group, making

tracking difficult. These funds are then used for the purchase of weapons, electronic equipment, or the financing of jihadist training in regions such as Poso and Lamongan. Additionally, the Jamaah Islamiyah (JI) group, which disbanded on 30 June 2024, also employed various funding methods while active, including establishing business entities, member contributions, funds from the public, operations in the palm oil plantation sector, and funds from foreign terrorist organisations such as Al Qaeda. An analysis of Judgment No. 308/PID.SUS/2020/PN JKT.TIM shows that JI utilised businesses in the palm oil plantation sector in Sumatra as its primary source of income, highlighting the strategy of diversifying income sources employed by JI.

In recent years, various cases have shown that former terrorism convicts (napiter) in Indonesia have re-engaged in funding terrorist groups. One notable case involves Ari Kardian and Rudi Heriadi, two Indonesian citizens sanctioned by the U.S. Department of the Treasury for allegedly facilitating ISIS's financial operations. Both are former terrorist convicts who, after being released from prison, resumed their activities in fundraising and facilitating ISIS's international networks (Kompas.com, 2022).

Another notable case is that of Dwi Djoko Wiwoho, a former civil servant who sold his house and donated more than Rp300 million to an ISIS sympathiser to fund a trip to Syria with his family. He was subsequently deported and sentenced to three years in prison for terrorism financing (The Conversation, 2020). Additionally, Hendro Fernando, a former member of the East Indonesia Mujahidin (MIT), was known to act as an intermediary for fund transfers between ISIS in Syria and the MIT network in Indonesia. He even requested Rp1.3 billion from the ISIS Amir in Syria. He transferred it through Turkey using money transfer services such as Western Union with the 'smurfing' method (breaking down funds into small amounts so they are not detected) (SuaraIndo.id, 2021). In another case, Aris Budianto was sentenced to five years in prison by the East Jakarta District Court for being a fundraiser for the Jemaah Islamiyah (JI) group. He actively collected funds from 2014 to 2020 through infaq (charitable donations) and distributed them to the JI network, including to a wanted person named Sirojudin in the amount of Rp80 million (Detik.com, 2024).

Equally important, two Indonesian citizens deported from Syria in 2017 were also designated as terrorism financing suspects after being proven to have collected and channelled funds to send other Indonesian citizens to ISIS-controlled conflict zones (Kompas.com, 2017). This indicates that former terrorists and ISIS sympathisers remain a threat, particularly in terms of increasingly complex funding mechanisms in the digital age. In this regard, a study by Putri and Lisanawati (2022) specifically shows that fintech is not merely a tool prone to misuse but also has significant potential in efforts to mitigate terrorism financing. They emphasise that fintech providers must implement know your customer (KYC) and customer due diligence (CDD) systems, as well as become part of official associations such as the Indonesian Fintech Funding Association (AFPI). These steps strengthen transaction monitoring systems and reduce the risk of misusing digital platforms for illegal purposes. Thus, technology can be a preventive tool, not just a security loophole (Putri & Lisanawati, 2022).

The growth of financial technology (fintech) in Indonesia has created new challenges in combating terrorism financing. Ramadianto and Wicaksono (2023) highlight that during the COVID-19 pandemic, digital banking in Indonesia grew rapidly, making transactions easier for customers. However, if the government does not take significant steps to combat terrorist financing with the existing regulations, this will become a problem. Therefore, to stop terrorist financing in Indonesia, digital banks must have an AML-CFT system that includes customer due diligence and regular client evaluations. Furthermore, the use of cryptocurrency in terrorism financing has become an international concern. Anggriawan and Susila (2024) emphasise that cryptocurrency has become a tool used in money laundering and terrorism financing, posing challenges for financial institutions and regulators to detect and prevent these illegal transactions.

Moreover, the development of digital asset regulations in Indonesia has entered a new phase with the enactment of Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (UU PPSK), which stipulates that supervision of digital financial assets, including cryptocurrency, will be gradually transferred from the Commodity Futures Trading Supervisory Agency (Bappeti) to the Financial Services Authority (OJK) by 2025 at the latest (Law No. 4 of 2023). This transfer reflects a paradigm shift in which cryptocurrencies are no longer viewed solely as digital commodities but as financial instruments that could potentially be used for illegal activities, including money laundering (TPPU) and terrorism financing (TPPT).

Based on the commodity trading framework, Bappebti has been performing its supervisory function over cryptocurrency exchanges in Indonesia. However, this approach is deemed insufficiently comprehensive in addressing the complexity of digital financial crimes, particularly regarding Know Your Customer (KYC) and Anti-Money Laundering – Counter Financing of Terrorism (AML-CFT) aspects, which are the primary domains of financial institution supervision by the OJK (Bappebti, 2023; OJK, 2024). Therefore, the transfer of authority to the OJK is expected to strengthen risk-based supervision mechanisms and expand the scope of legal protection for investors and the public. This step is also in line with the recommendations of the Financial Action Task Force (FATF), which, in its Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, states that countries must ensure that supervision of digital assets involves financial authorities with full authority in the implementation of AML-CFT principles (FATF, 2023). Thus, integrating cryptocurrency supervision into the national financial system through the OJK enables more adaptive law enforcement against new modes of terrorism financing that exploit the secrecy, speed, and decentralisation of blockchain technology.

In terms of expectations, the OJK is expected to strengthen its synergy with the Financial Transaction Reports and Analysis Centre (PPATK) in detecting suspicious transactions through crypto asset platforms, as well as accelerating the implementation of regulatory sandboxes and regtech technology to monitor activities in the fintech sector. This implementation is crucial considering that the PPATK in its 2023 Annual Report noted a significant increase in suspicious and high-risk cryptocurrency transactions related to TPPT, with the involvement of foreign networks (PPATK, 2024). Such inter-agency collaboration is necessary so that the surveillance system is not reactive but proactive in countering potential threats to national security.

This step will also impact stronger law enforcement against digital financial service providers (virtual asset service providers), which were previously not fully supervised. According to Shapiro and Siegel (2021), strengthening regulations and transaction reporting obligations for VASPs significantly influences reducing the pace of terrorist organisation financing, especially those based transnationally and using the dark web. Overall, the transfer of authority to the OJK represents a strategic opportunity for Indonesia to strengthen the resilience of its financial system against exploitation by terrorist groups. Through a more integrated and risk-based supervisory approach, coupled with inter-agency collaboration among the OJK, PPATK, and law enforcement agencies, Indonesia is expected to anticipate the evolving dynamics of technology-based terrorist financing.

To address these challenges, information technology is an important solution. Putri and Lisanawati (2022) highlight the role of financial technology in preventing terrorism financing, emphasising the importance of strict supervision and regulation of digital transactions to prevent misuse by terrorist groups. Additionally, a strong legal approach is needed to address money laundering and terrorism financing crimes in the era of digital banking. Ramadianto and Wicaksono (2023) suggest that a comprehensive legal approach and implementing effective AML-CFT systems in digital banking are crucial to prevent terrorism financing. Research on terrorist financing and the role of information technology in supporting and preventing such activities has grown rapidly in the last decade, both nationally and internationally. One of the main focuses is on how terrorist groups utilise technological advances, particularly in the field of digital finance, to manage and disguise their cash flows.

At the national level, Prasetya, Subroto, and Nurish (2021) assert that terrorist organisations in Indonesia, such as groups affiliated with ISIS, have utilised cryptocurrency to conceal their identities and transaction trails. Their research reveals that digital assets are used not only as a transaction tool but also as a relatively untraceable funding source, particularly due to their decentralised and anonymous nature. This is reinforced by the findings of Anggriawan and Susila (2024), who assess that weak regulation of cryptocurrency opens up opportunities for exploitation by organised crime networks, including terrorism.

In an institutional context, Putri and Lisanawati (2022) state that advances in fintech present new challenges in combating financial crime, but can also be a strategic solution. Their research shows that by strictly applying the principles of Know Your Customer (KYC) and Customer Due Diligence (CDD), financial technology service providers can narrow the scope for terrorist financing. In line with this, Ramadianto and Wicaksono (2023) highlight the importance of strengthening the Anti-Money Laundering – Counter Financing of Terrorism (AML-CFT) system in the rapidly growing digital banking sector post-COVID-19 pandemic, as a response to the increasing complexity of digital transactions that are vulnerable to abuse by terrorist groups.

On the other hand, case studies show that former terrorism convicts (napiter) in Indonesia play a significant role in terrorist financing networks. Rizky and Sari (2022) analysed former terrorists who became active again in financing the ISIS network, showing that social reintegration is not always effective without comprehensive supervision and deradicalisation strategies. They emphasise that terrorism financing is often carried out through donations, legal businesses such as plantations, and third-party accounts. Meanwhile, international literature shows similar patterns, but on a larger scale and across broader networks. Shapiro and Siegel (2021) emphasise that digital currencies such as Bitcoin have become the primary choice for terrorist groups due to their decentralised nature. This study also highlights that weak oversight of Virtual Asset Service Providers (VASPs) is critical in controlling illegal cash flows. Levi and Soudijn (2021) add that informal money transfer systems like hawala remain a favourite method for disguising cross-border transactions, especially to avoid formal reporting systems.

In Southeast Asia, Silva and Daud (2022) map the threat of terrorist financing through crowdfunding platforms and digital donations. They highlight that terrorist sympathisers in the region actively use social media and donation sites to fund travel to conflict zones or support propaganda. Reitano and Shaw (2020) also show that fragile states with weak financial oversight tend to be fertile ground for cross-border terrorist funding flows. International bodies such as the Financial Action Task Force (FATF, 2023) have also published risk-based guidelines for virtual assets and their service providers. The FATF recommends that countries integrate digital asset oversight into formal financial systems and emphasises the importance of coordination between financial authorities and law enforcement agencies to prevent the exploitation of technology by terrorists.

From these studies, it can be concluded that there is a global consensus on the importance of digital financial regulatory reform and strengthening reporting systems. In Indonesia, strategic steps such as the transfer of cryptocurrency oversight from Bappeti to OJK (Law No. 4 of 2023) are considered an appropriate response to the increasing risk of technology-based financial crime (Bappeti, 2023; OJK, 2024). However, challenges remain, particularly in closing cross-sector collaboration gaps and building a supervisory system that is adaptive to new modes of terrorism. A review of the literature and previous research shows that the issue of terrorism financing has undergone significant shifts with the development of digital technology. Based on previous studies that have been reviewed, the novelty of this research lies in important aspects that have not been comprehensively discussed in previous literature. This journal aims to: (1) identify the modes of terrorist group funding, (2) analyse the role of information technology in facilitating this crime, and (3) propose technology-based solutions for mitigation. The analysis is supported by Crime Script Analysis and Rational Choice Theory to understand the behaviour patterns of perpetrators and prevention strategies.

This research uses Crime Script Analysis (CSA) & Rational Choice Theory (RCT). CSA, developed by D.B. Cornish (1994) in his journal entitled The Procedural Analysis of Offending and Its Relevance for Situational Crime Prevention, is an approach to mapping the steps taken by perpetrators in committing crimes. In terrorism financing, CSA helps identify stages such as fund collection, transfer via cryptocurrency, and cash conversion. This approach enables authorities to intervene at critical points in the crime chain. Meanwhile, Rational Choice Theory (RCT), introduced by G.S. Becker (1968) in a political economy journal titled Crime and Punishment: An Economic Approach, assumes that criminals make rational decisions based on cost and benefit calculations. In terrorism financing, perpetrators choose technologies such as blockchain because of the low risk of detection and high efficiency. RCT explains why perpetrators utilise crypto exchanges and nominee accounts to minimise tracking. These two theories complement each other: CSA maps the crime process, while RCT explains the motivations behind perpetrators' technology choices.

2. Methodology

This study uses a qualitative approach, analyzing secondary data from reports by Interpol (2022), BSSN, the World Bank, and the World Giving Index 2024. Data was collected through a literature review and analysis of official documents related to terrorism financing and cybercrime. Analysis was conducted by applying CSA to map modus operandi and RCT to understand perpetrators' decisions.

3. Result and Discussion

3.1. Zero Modus Operandi of Terrorist Group Funding

The methods of financing terrorism have significantly transformed in the last decade, with the development of information technology and digital financial systems. The case of Mackhsun Hariry is a concrete example of how international terrorist networks utilise digital financial technology, social institutions, and surveillance loopholes to channel funds across borders in a covert and structured manner. Between 2018 and 2023, Mackhsun Hariry, an Indonesian citizen affiliated with the Majelis Mujahidin Indonesia (MMI) network and the Hay'at Tahrir al-Sham (HTS) terrorist group in Syria, was suspected of being actively involved in terrorism financing. He served as the primary intermediary for fund transfers from Indonesia to Syria at the behest of his brother-in-law, Usamah Abidullah Robbani alias Abu Royyan, who is a wanted individual (DPO) and is known to have joined the HTS network, an organisation listed as a terrorist entity under UN Security Council Resolution No. 1267.

In practice, the flow of funds was conducted through two main channels: the conventional banking system and cryptocurrency assets. Through the conventional channel, Mackhsun opened several personal accounts at Bank Mandiri and BCA, which were used to receive funds from the World Human Care (WHC) Foundation and its affiliate programme, the 'Yayasan Orang Tua Asuh (YOTA)' Foundation. This foundation collected public donations through social media such as WhatsApp, Facebook, and YouTube with humanitarian narratives for Syrian war victims. Digital posters evoked public emotional sympathy, directing funds to be transferred to the foundation's accounts. However, the funds collected, amounting to approximately Rp5.7 billion, were largely channelled to an account in the name of Abdul Mavla Alalloush in Turkey, who served as the financial coordinator for the HTS network. The transfers were carried out through structured and repetitive methods, including:

1. Chain cash transfers: Funds from WHC were transferred to the defendant's Mandiri account, then moved to the defendant's BCA account, and finally sent abroad through intermediary accounts (the defendant's university friends).
2. Diversification of third-party accounts: Due to daily transfer limits, the defendant used others' accounts to evade banking detection systems.
3. Conversion to foreign currency (USD): Funds were withdrawn in cash and deposited back in USD before being sent to overseas accounts.
4. Use of cryptocurrency exchanges: Since late 2018, the defendant began using platforms such as Indodax, Pintu, and Binance to convert rupiah into USDT (Tether). These cryptocurrency funds were transferred to various anonymous wallet addresses controlled by Abu Royyan.

In this case, cryptocurrency assets demonstrate a high level of technological adaptation by the terrorist network. USDT, as a stablecoin whose value is stable against the USD, was chosen due to its ease of conversion, wallet anonymity, and the difficulty of tracking fund flows by financial authorities. The defendant even managed several accounts on legal Indonesian exchanges, such as INDODAX, using personal and spouse identities, and utilised digital bank virtual account features for fund top-ups from conventional banks. Furthermore, the funding structure was also disguised as humanitarian activities through a social foundation, which was actually a front organisation (a cover organisation) to support the logistics of the terrorist network. The funds collected were ostensibly used to support orphaned children affected by conflict. Still, most of it was diverted to meet the operational needs of the terrorist network, including logistics on the battlefield and military training (Tadrib and Ribath).

This modus operandi reflects the digital crime script analysed through the Crime Script Analysis (CSA) approach: First, Initiation: Collection of donations in the name of humanitarianism through digital flyers. Second, Execution: Transfer funds to intermediary accounts and conversion to crypto. Third, Security: Use anonymous crypto wallets and other people's identities to avoid tracking. These findings are consistent with global reports, such as those from TRM Labs (2024) reported that the ISIS-K group uses cryptocurrencies such as stablecoins and Bitcoin, as well as anonymous wallets (unhosted wallets) and mixers to disguise cross-border terrorism financing transactions. One notable case occurred in March 2024, when ISIS-K funded an attack in Moscow using stablecoins. In June 2024, an individual in Germany was arrested for sending over USD 1,700 in Bitcoin to the network (TRM Labs, 2024).

A report from the Financial Crimes Enforcement Network (FinCEN) also confirmed that ISIS and its affiliates actively use various cryptocurrency platforms and digital wallets that do not implement strict AML-CFT systems to transfer funds from Europe to the Middle East (FinCEN, 2023). This highlights the increasing complexity of monitoring digital transactions in the context of terrorism financing. Furthermore, the Attorney General's Office of the Republic of Indonesia (2024) reported that during 2024, illegal cryptocurrency transactions amounting to Rp1.3 trillion were detected, most of which were related to money laundering activities, including money laundering suspected of being used in terrorist networks. Practices such as smurfing, mixing, and using cross-chain bridges are often employed to obscure the source of funds, underscoring the urgency of developing technology-based early detection systems (Attorney General's Office of the Republic of Indonesia, 2024).

These findings reinforce the urgency of developing technology-based AML-CFT systems. Putri and Lisanawati (2022) emphasized that oversight of fintech and digital transactions must be strengthened through strict regulations, training of fintech operators, and the involvement of security authorities in detecting suspicious transactions in the digital financial sector. Another modus operandi involves controlling energy distribution channels, particularly oil and gas. In the Idlib region of Syria, the Hay'at Tahrir al-Sham (HTS) group is known to monopolise fuel import routes from Turkey. This control enables them to generate significant profits amid military and economic pressure (Zelin, 2020).

Additionally, there is a modus operandi that often escapes public scrutiny: the misuse of charitable institutions. Funds collected for humanitarian aid or social assistance are sometimes channelled to organisations listed on the Suspected Terrorist Entities and Terrorist Organisations List (DTTOT). This modus operandi violates Law No. 9 of 2013 on the Prevention and Eradication of Terrorism Financing Crimes, which strictly prohibits channelling funds to entities affiliated with terrorism (Republic of Indonesia, 2013). In the digital age, terrorist groups exploit information technology advances to design more efficient, hidden, and difficult-to-track funding streams. This phenomenon not only represents an evolution in terrorist operational strategies but also indicates that terrorist actors are rationalising their choices based on risk and benefit calculations, as explained in Rational Choice Theory (RCT) (Cornish & Clarke, 2008). According to RCT, criminals act rationally by considering the likelihood of success, operational costs, and the possibility of being apprehended. Thus, using digital methods such as cryptocurrency, crowdfunding, and the obfuscation of digital transactions represents an efficient and low-risk adaptation from the perpetrators' perspective.

To systematically understand the operational stages of terrorism financing, Crime Script Analysis (CSA) is a highly relevant approach. CSA helps analyse the steps taken by perpetrators from planning, execution, to securing the proceeds of financing. In the context of digital financing, the crime script includes: seeking funding sources (such as online donations or fictitious charities), using digital financial platforms (PayPal, crypto, fintech), and laundering funds through e-commerce or cross-border transactions (Levi & Maguire, 2004; Maimbo & Passas, 2005). Law enforcement agencies and intelligence agencies face the challenge of detecting suspicious activities among millions of daily digital transactions. Many terrorist funding transactions are designed to appear legitimate, with small amounts and using fictitious identities (smurfing). A study by Wijayanto & Pramono (2021) shows that terrorists are now increasingly adept at exploiting digital wallets and crypto platforms due to the anonymity and decentralisation of their systems.

As a solution, information technology approaches based on Artificial Intelligence (AI) and Machine Learning (ML) have begun to be implemented by some countries to detect unusual financial patterns (FATF, 2021). Indonesia has established the Financial Transaction Reporting and Analysis Centre (PPATK), which collaborates with international institutions to strengthen the analysis of suspicious transactions in digital-based terrorism financing. These methods pose a major challenge to global efforts to break the chain of terrorism financing, especially in the digital age when funds can be disguised through new financial technologies and cross-border transactions that are difficult to trace.

3.2. Modus Operandi of Terrorism Financing in the Digital Age

The study shows that terrorist groups in Indonesia have actively utilised developments in information technology to facilitate their financing activities. Three main modes are predominantly used, namely: (1) the use of crypto assets and blockchain technology; (2) the use of nominee accounts or accounts in the name of other parties; and (3) activities through crypto exchangers as a means of disguising illegal transactions.

First, cryptocurrencies such as Bitcoin and Ethereum are used for cross-border transfers that are difficult for law enforcement agencies to track. Durrant's (2020) research shows that blockchain technology's decentralised and pseudonymous nature makes it an ideal platform for terrorists to transfer funds secretly. Platforms like INDODAX and BINANCE commonly purchase cryptocurrency before sending it to unidentified wallet addresses. Second, perpetrators often utilise nominee accounts or accounts in the name of others, either using genuine family members' identities or fake ID cards. This strategy aims to avoid detection during transaction tracing (asset tracing). Third, since 2014, there has been an increase in the use of crypto exchangers, including those operating on a peer-to-peer (P2P) basis, which allow transactions to be disguised as legal activities such as investments or remittances (Wijayanto & Pramono, 2021). These methods can be analysed using the Crime Script Analysis (CSA) approach, which divides the funding process into several stages:

1. Fund collection, through fictitious donations, online zakat, or crimes such as fraud and illegal buying and selling;
2. Fund transfer, using crypto assets purchased through exchangers;
3. Conversion, through cash withdrawals, bartering goods, or using over-the-counter (OTC) markets;
4. Distribution, i.e., operational funding to terrorist networks, such as training, logistics, and recruitment of members (Levi & Maguire, 2004).

These stages illustrate a systematic and organised structure, reflecting that perpetrators have sufficient financial and technological knowledge to exploit gaps in digital surveillance. From the Rational Choice Theory (RCT) perspective, perpetrators' choice to use blockchain and cryptocurrency is not random or emotional, but rather the result of rational consideration based on risk and benefit calculations. The perpetrators assess that operational costs are lower, anonymity is higher, and the risk of being caught is smaller than conventional methods such as bank transfers (Becker, 1976; Cornish & Clarke, 2008). Thus, information technology in terrorist financing reflects an adaptive strategy based on efficiency and instrumental logic.

3.3. Cybercrime Challenges in the Digital Age

The Interpol report (2022) presented in Global Crime Trend identifies nine major criminal threats that information technology supports, including money laundering, phishing, and financial fraud. These three modes are growing rapidly in line with the rapid advancement of digital technology and the increasing use. This aligns with the view of Thomas et al. (2021), who state that digital technology has revolutionised the criminal landscape by expanding the reach and accelerating the process of crime, thereby creating new forms of crime that are difficult for conventional legal systems to anticipate. A similar phenomenon has occurred in Indonesia, where, according to a report by the Honeynet Project (2020), the National Cyber and Cryptography Agency (BSSN) recorded a significant increase in the number of cyberattacks from 12.8 million in 2018 to 98.2 million in 2019. This surge illustrates the rapid escalation of cyber threats, expanding the scope for various criminal activities, including digital terrorism financing. According to Setiawan and Hartono (2020), the rapid development of cyberattacks in Indonesia also indicates the national cybersecurity infrastructure's lack of readiness to face increasingly sophisticated and integrated threats.

The phenomenon of increasing digital financial crime, as seen in Singapore and Southeast Asia, reflects the vulnerability of financial systems to exploitation by non-state actors, including terrorist groups. Modus operandi such as scams, romance fraud, and fake investments, which are prevalent in Singapore, not only generate massive illegal profits but also provide alternative channels for financing terrorist activities, particularly through cross-border money laundering practices (The Straits Times, 2024; 2025). Although in many of these cases the main perpetrators are criminal syndicates, the patterns and techniques used, such as the use of anonymous cryptocurrency wallets, digital money transfer platforms, and fake identities, are also adopted by terrorist groups to evade detection by financial authorities (Anggriawan & Susila, 2024; FATF, 2023).

Research by Shapiro and Siegel (2021) highlights how digital fraud schemes such as romance scams and fake investments in Southeast Asia, particularly in Singapore, provide easily transferable funds to criminal and terrorist groups through the dark web financial network. They reveal that the combination of online fraud and anonymous cryptocurrencies amplifies the risk of illegal funds infiltrating the formal

financial system. This phenomenon is reflected in a major case in Singapore involving a fake investment scheme and money laundering worth billions of Singapore dollars (The Straits Times, 2024; 2025).

Cases such as the one involving the fake Simex platform, where five US investors were defrauded of US$13.8 million through social media and dating apps, demonstrate the potential for scam proceeds to be converted and diverted for the benefit of radical groups, especially if carried out by sympathisers or cells already ideologically affiliated (The Straits Times, 2024). This is in line with the findings of the FATF (2022), which noted that global terrorist groups such as ISIS and Al-Qaeda have used a hybrid financing model, combining legal and illegal sources of funding, including proceeds from financial crimes, to finance their operations in various countries. Furthermore, according to Silke and Lia (2017), terrorist groups use a hybrid financing model that combines legal and illegal sources of funding, including proceeds from cybercrime and financial crime. The use of cryptocurrency to finance terrorism is further reinforced by the PPATK report (2023), which notes an increase in the number of suspicious transactions based on digital assets from year to year, with some of them indicating links to extremist and radicalisation activities. The report reveals that between 2022 and 2023, there were more than 1,200 digital transactions classified as high-risk, including the repeated transfer of small amounts of funds—a method known as smurfing—which was also used by former MIT members to channel funds from Syria to Indonesia (SuaraIndo. id, 2021; PPATK, 2023).

FATF (2023) also emphasises that the fintech ecosystem and digital wallets (e-wallets) have become new loopholes in the anti-money laundering and counter-terrorism financing (AML-CFT) system due to weak identity verification and limited cross-jurisdictional cooperation in tracking pseudonymous cryptocurrency assets. In the case of Singapore, for example, money laundering from scams and illegal gambling, which reached S$3 billion in 2023, also used layered transaction methods and transfers through various fintech accounts (Wikipedia, 2024), which is very similar to the funding techniques used by the Jamaah Islamiyah network in Indonesia, which divides donations into small amounts and distributes them through a network of religious figures and cooperatives (Detik.com, 2024). The case of Dwi Djoko Wiwoho, who donated more than Rp300 million to ISIS sympathisers, can also be examined from a digital economy perspective, where the use of intermediary accounts or fintech as payment channels likely served as a tool to facilitate cross-border fund transfers (The Conversation, 2020). This is where the urgency of a technology-based AML-CFT system that is adaptive to digital developments becomes very important, as suggested by Putri and Lisanawati (2022), that supervision of fintech must be strengthened with artificial intelligence systems for detecting suspicious transactions and continuously assessing user risk profiles.

Additionally, the global internet user base, which reached approximately 5 billion in 2021 according to Internet World Stats (2021), expands the scope and opportunities for international cybercrime. As Kshetri (2018) noted, the significant increase in internet penetration and digital technology has greatly expanded the cybercrime ecosystem, enabling perpetrators to cross national borders and obscure their identities easily. Technologies like blockchain, which eliminate time and geographical constraints, facilitate criminals in conducting real-time, cross-border transactions with a high degree of anonymity (Durrant, 2020). Blockchain technology enables permanent and decentralised transaction recording. Still, ironically, it also serves as an ideal medium for illicit transactions and illegal funding due to its difficulty in being monitored by authorities (Foley, Karlsen, & Putniņš, 2019).

In this context, the Crime Script Analysis (CSA) theory is highly relevant for unravelling the modus operandi of criminals. CSA helps map the criminal process sequentially and systematically, from fund collection, transaction concealment, and illicit funds distribution (Levi & Maguire, 2004). A study by van Wegberg, de Graaf, and Kleemans (2018) supports the CSA approach by showing that criminal and terrorist groups use cryptocurrency exchanges as part of a 'crime script' designed to conceal and obscure the flow of funds, thereby evading surveillance and legal action. With this understanding, the CSA approach helps law enforcement understand the funding process and opens up opportunities for intervention at critical points in the criminal chain.

Concurrently, Rational Choice Theory (RCT) provides a framework for understanding the motivations of perpetrators in choosing this technology. Perpetrators act rationally, selecting transaction routes that minimise risk and costs while maximising anonymity and the efficiency of fund transfers (Becker, 1976; Cornish & Clarke, 2008). A study by Brito and Castillo (2013) shows that in digital assets, perpetrators are more likely to use blockchain due to its transaction speed, low costs, and the difficulty of tracking by law

enforcement agencies, thereby providing strategic advantages in illegal activities, including terrorism financing.

Thus, the combination of advancements in information technology, the increase in internet users, and the adaptation of terrorism financing modus operandi as modelled in CSA and RCT highlights serious challenges in combating terrorism financing in the digital age. Supervision and regulation efforts must adopt equally advanced technologies, such as big data analysis and artificial intelligence, to effectively map and take action against these illegal financial flows (FATF, 2021).

3.4. Information Technology-Based Solutions

In the digital age, one of the main challenges law enforcement agencies face in various countries is tracing the flow of funds used to support terrorist activities. The transformation of financial transactions from conventional systems to digital forms, such as using cryptocurrencies and fintech platforms, has significantly complicated the investigation process, especially when the technology is privacy-enhancing. One concrete example of this challenge is the use of the cryptocurrency Monero by the Islamic State Khorasan Province (ISKP) in its fundraising efforts. Unlike Bitcoin, whose transactions can still be traced through the public blockchain, Monero uses privacy protocols such as ring signatures, stealth addresses, and confidential transactions that hide the identities of the sender, recipient, and transaction amount, making it nearly impossible to trace forensically by law enforcement agencies (Europol, 2022; Kethineni & Cao, 2020).

Research conducted by Carlisi and De Feo (2023) shows that international law enforcement agencies, including those in the European Union and South Asia, face significant technical challenges in mapping terrorist financing activities based on anonymous cryptocurrencies like Monero. Limited access to metadata and user information in digital transactions also poses a major obstacle to investigations, especially when perpetrators use mixers, tumblers, or transact on decentralised exchanges (DEX) not affiliated with KYC/AML regulations. The case becomes even more complex when these platforms are accessed through the dark web and combined with smurfing or layering techniques, so the trail of funds can be spread in small amounts across multiple accounts. As the FATF (2023) noted, such technology allows terrorist groups to hide their cash flows without using the formal banking system.

In the Indonesian context, similar challenges are faced by the PPATK and Densus 88 AT Polri, particularly in tracing funds collected through social media channels, anonymous digital wallets, and peer-to-peer transactions that do not go through formal reporting systems (PPATK, 2024). The absence of a cross-platform detection system, the lack of international cooperation in real-time tracing, and the slow process of mutual legal assistance (MLA) requests also exacerbate law enforcement agencies' operational challenges. To address the challenges of financing terrorism and cybercrime in the digital age, this article proposes five technology-based solutions that can improve the effectiveness of prevention and enforcement. These solutions are designed to respond to digital crime's increasingly complex and transnational dynamics.

First, applying Cyber Crime Big Data Analytics is essential for identifying suspicious financial transaction patterns. This technology can process millions of data points in a short time, extract correlations, and detect anomalies related to terrorism financing (Bellucci et al., 2021). Big data analysis has proven effective in detecting high-frequency microtransactions, which are often used to evade detection by conventional financial institutions (Chen et al., 2020). According to Clarisa Permata Hariono and Go Lisanawati (2022), financial technology can play a role in preventing terrorist financing by implementing measures that support anti-money laundering and counter-terrorist financing programmes, as well as identifying donor profiles to develop the principle of knowing the user of financial services.

Second, integrating Artificial Intelligence (AI) through the Open-Source Intelligence (OSINT) approach enables real-time monitoring of threats through social media, online forums, and the dark web. According to Moustafa et al. (2019), using AI in OSINT strengthens the predictive capacity of security agencies in anticipating radical groups' attack plans or fundraising activities. AI can also improve the detection of hate speech and extremist recruitment content that leads to financing activities.

Third, developing a Command Centre as an integrated control centre is crucial to ensure rapid coordination between agencies. In a study by Shahbaz et al. (2022), a national control centre connected to various intelligence and transaction monitoring systems has been proven to accelerate response to cyber threats and improve the effectiveness of cross-sector and cross-border enforcement.

Fourth, implementing a Data Surveillance system based on the principles of proportionality and legality can track the movement of illegal funds through various digital platforms. This technology has been used in EU projects such as FIU.net, which connects financial intelligence units to detect suspicious cross-border transactions (Ferwerda, 2019).

Fifth, developing a Data Centre as an infrastructure for data storage and processing is essential to support the entire digital security system. A robust and secure Data Centre stores financial data and metadata from various digital transactions that can serve as legal evidence. A study by Wirtz et al. (2018) emphasises the importance of a resilient information infrastructure system in addressing distributed and multi-vector cyber threats.

Sixth, an AML-CFT system based on technology that is adaptive to digital developments is crucial, as suggested by Putri and Lisanawati (2022), who argue that fintech oversight must be strengthened with artificial intelligence systems for detecting suspicious transactions and continuously assessing user risk profiles.

These solutions align with the Crime Script Analysis (CSA) approach, which emphasises the importance of intervention at every stage of the crime chain, from planning to execution (Levi & Maguire, 2004). Through CSA, technological solutions can target critical points such as fund collection, transfer, and asset conversion. Additionally, based on Rational Choice Theory (RCT), technology-based solutions also increase the costs and risks for perpetrators in committing crimes, thereby reducing the rational incentive to continue criminal activities (Cornish & Clarke, 2008). The findings of this study reveal that global and domestic terrorist groups have significantly adapted to advances in digital technology in managing their operational funding. Funding patterns no longer rely entirely on conventional methods. Still, they are increasingly shifting to digital schemes such as using crypto assets, fintech platforms, and engineering fund flows through non-profit institutions or quasi-legal activities. This reflects the increasingly complex and covert evolution of terrorist groups' financial strategies and demonstrates the rationalisation of choices based on cost-risk calculations, as explained in Rational Choice Theory (Cornish & Clarke, 2008).

The modus operandi identified includes the use of cryptocurrencies such as Bitcoin, Ethereum, and Monero, which are specifically designed to conceal the identity and amount of transactions. In Indonesia, the Attorney General's Office (2024) findings on illegal cryptocurrency transactions amounting to Rp1.3 trillion, some linked to terrorist networks, underscore the urgency of enhancing law enforcement agencies' early detection and digital capabilities. Other tactics include nominee accounts, fund fragmentation through smurfing, and using P2P cryptocurrency exchanges like INDODAX and BINANCE to obscure fund flows. In an operational context, the Crime Script Analysis (CSA) approach is highly relevant for mapping the stages of terrorism financing, from fund collection (through fictitious donations, cybercrime, or crowdfunding), fund transfers via digital assets, fund conversion into cash or logistics, to distribution for operational activities such as training, propaganda, and recruitment. This structure illustrates that terrorist actors are not only technologically adaptive but also possess financial knowledge and the ability to exploit gaps in digital surveillance systematically.

Comparisons with practices in other countries show that these challenges are global. In the United States, the financial surveillance system has been strengthened through cooperation between agencies such as FinCEN and blockchain analytics companies (e.g., Chainalysis) and the implementation of AI-based suspicious reporting. The European Union relies on the FIU.net network to connect financial intelligence units across countries, despite privacy regulations such as GDPR. Singapore takes a progressive approach by strictly regulating the fintech and crypto sectors through the Monetary Authority of Singapore (MAS) and developing regulatory sandboxes and adaptive AI investigations.

However, cross-border challenges remain a key issue, particularly in limited international cooperation, weak regulation of anonymous crypto platforms, and technical limitations in tracking transactions through decentralised exchanges (DEX), mixers, or digital wallets that do not apply Know Your Customer (KYC) principles. Several cases in Southeast Asia indicate that schemes such as fake investments, romance scams,

and cross-border transaction layering can serve as loopholes for terrorist groups to conceal the source and use of funds. This phenomenon is reinforced by the FATF report (2023) and high-profile cases such as the S$3 billion money laundering scheme in Singapore, as well as the distribution of funds by former members of an Indonesian terrorist group through smurfing methods and fake identities.

Therefore, technology-based solutions are essential in responding to these dynamics. Five strategic steps that can be implemented nationally include: (1) the application of Cyber Crime Big Data Analytics to detect transaction anomalies; (2) the integration of Artificial Intelligence and Open-Source Intelligence (OSINT) for online media monitoring; (3) the establishment of a Command Centre as a cross-agency control centre; (4) the implementation of a proportional and legally valid Data Surveillance system; and (5) the establishment of a national Data Centre to support centralised data processing and storage. This approach aligns with the CSA framework, which emphasises the importance of intervention at every stage of the crime script. RCT, which encourages increasing the costs and risks for criminals to reduce their incentives rationally.

In addition, the Anti-Money Laundering and Counter Terrorism Financing (AML-CFT) system needs to be strengthened with regulations that are adaptive to the latest technology. Fintech transactions and digital asset supervision must involve artificial intelligence-based automatic detection that can dynamically assess user risk profiles. In the Indonesian context, this can begin by strengthening the role of PPATK, Densus 88 AT Polri, and BSSN to build an integrated and responsive national framework against the threat of digital terrorism financing. Thus, the challenge of terrorism financing in the digital age is not merely about tracking technology but also about building a collaborative ecosystem across sectors, borders, and systems. Without innovations in oversight systems, enhanced institutional capacity, and stronger global cooperation, new evolving modus operandi will always remain one step ahead of conventional law enforcement systems.

4. Conclusion

This study, Terrorist Financing in the Digital Age, shows increasingly complex patterns, utilising cutting-edge technologies such as blockchain, crypto assets, and nominee accounts to conceal financial traces. These methods significantly complicate conventional tracking and law enforcement processes. In this context, the Crime Script Analysis (CSA) approach is highly relevant for mapping each stage of criminal activity, from fund collection and transfer to the use of funds by terrorist groups. Meanwhile, Rational Choice Theory (RCT) provides insight into the rational motives behind perpetrators' choice of technology, namely to optimise operational efficiency, reduce the risk of detection, and increase the likelihood of success. The increasing threat of cybercrime globally and nationally requires greater preparedness regarding information technology infrastructure and strengthening human resource capacity. The use of technologies such as Big Data Analytics, artificial intelligence (AI), and command centres can strengthen early detection systems and accelerate responses to potential terrorist financing.

Effective prevention requires strategic collaboration between government agencies, the private sector, and civil society. Long-term investment in digital technology, adaptive regulations, and financial intelligence system integration are important pillars in mitigating the threat of terrorism financing in the ever-evolving digital era. A holistic and technology-based approach is key to creating a security ecosystem that is resilient to financial infiltration by terrorist networks.

References

Abuza, Z. (2003). *Funding terrorism in Southeast Asia: The financial network of Al Qaeda and Jemaah Islamiyah*. Contemporary Southeast Asia, 25(2), 169–199. https://doi.org/10.1355/CS25-2A

Anggriawan, R., & Susila, M. E. (2024). Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations. *Novum Jus*, 18(2), 249–277. https://doi.org/10.14718/NovumJus.2024.18.2.10novumjus.ucatolica.edu.co+1journals.centeriir.org+1

Anisa, I. V., & Syauqillah, M. (2022). Strategi kontra intelijen terhadap strategi pendanaan Jamaah Islamiyah melalui lembaga amal. *Syntax Literate: Jurnal Ilmiah Indonesia*, 7(4), 1925–1935. https://doi.org/10.36418/syntax-literate.v7i4.13086

Badan Siber dan Sandi Negara (BSSN). Laporan Honeynet Project. Jakarta: BSSN, 2020.

Bappebti. (2023). *Laporan Tahunan Bappebti 2023*. Badan Pengawas Perdagangan Berjangka Komoditi.

Becker, G. S. (1976). *The Economic Approach to Human Behavior*. University of Chicago Press.

Becker, G.S. *"Crime and Punishment: An Economic Approach."* Journal of Political Economy 76, no. 2 (1968): 169–217.

Bellucci, L., Carminati, B., & Ferrari, E. (2021). Detecting financial frauds using graph databases and machine learning. *Future Generation Computer Systems*, 123, 393–403. https://doi.org/10.1016/j.future.2021.04.009

Brito, J., & Castillo, A. (2013). Bitcoin: A primer for policymakers. *Mercatus Center at George Mason University*.

Carlisi, C., & De Feo, M. (2023). Cryptocurrencies, anonymity and counter-terrorism financing: The case of Monero and ISKP. *Journal of Financial Regulation and Compliance*, 31(2), 184–198. https://doi.org/10.1108/JFRC-12-2022-0092

Charities Aid Foundation. World Giving Index 2024. London: CAF, 2024.

Chen, Y., Qin, Z., Zhang, B., & Wu, C. (2020). Big data analytics for detecting terrorist financing: A survey. *IEEE Access*, 8, 47466–47480. https://doi.org/10.1109/ACCESS.2020.2978834

Clarisa Permata Hariono & Go Lisanawati. (2022). Peran Teknologi Finansial Dalam Pencegahan Pendanaan Terorisme. *Jurnal Iustitia Omnibus*, 4(1), 71–85.

Cornish, D. B., & Clarke, R. V. (2008). The Rational Choice Perspective. In R. Wortley & L. Mazerolle (Eds.), *Environmental Criminology and Crime Analysis* (pp. 21–47). Willan Publishing.

Cornish, D.B. *"The Procedural Analysis of Offending and Its Relevance for Situational Crime Prevention."* Crime Prevention Studies 3 (1994): 151–196.

Detik.com. (2024, Januari 24). *Penggalang dana teroris di Lampung dihukum 5 tahun penjara*. https://news.detik.com/berita/d-7154171/penggalang-dana-teroris-di-lampung-dihukum-5-tahun-penjara

Durrant, R. (2020). Blockchain and cryptocurrencies: Opportunities and challenges for counter-terrorism financing. *Journal of Financial Crime*, 27(4), 1173–1186. https://doi.org/10.1108/JFC-03-2020-0044

Durrant, R. *"Blockchain and Cryptocurrencies: Opportunities and Challenges for Counter-Terrorism Financing."* Journal of Financial Crime 27, no. 4 (2020): 1123–1135.

Elliptic. (2019). *Hamas-linked wallets have received $7.7 million in cryptoassets*. Elliptic. Retrieved from https://www.elliptic.co/blog/hamas-linked-wallets-received-millions-in-cryptoassets

Europol. (2022). *Cryptocurrency laundering by terror groups: Privacy coins and forensic challenges*. European Union Agency for Law Enforcement Cooperation.

FATF. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. Financial Action Task Force. https://www.fatf-gafi.org

Ferwerda, J. (2019). The effectiveness of anti-money laundering policy: A cost-benefit approach. *Journal of Money Laundering Control*, 22(2), 210–221. https://doi.org/10.1108/JMLC-11-2017-0060

FinCEN. (2023). *Advisory on the Use of Virtual Currency for Terrorist Financing*. U.S. Department of the Treasury. https://www.fincen.gov/

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhy074

Global Relief Foundation. (2002). *Designation of the Global Relief Foundation as a financial supporter of terrorism*. U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/po3631

Honeynet Project. (2020). *Indonesia Cyber Threat Report*. https://www.honeynet.or.id

Internet World Stats. (2021). *World Internet Usage and Population Statistics*. https://www.internetworldstats.com

Internet World Stats. World Internet Usage and Population Statistics. 2021.

Interpol. (2022). *Global Crime Trend Report*. https://www.interpol.int

Kejaksaan Agung Republik Indonesia. (2024). *Laporan Tahunan Kejaksaan Agung RI: Analisis Kejahatan Siber dan Keuangan Tahun 2024*. https://www.kejaksaan.go.id/

Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, 30(3), 325–344.

Kohlmann, E. F. (2006). *Charitable organizations and terrorism financing: A war on terror status-check*. The Danish

Institute for International Studies. https://www.diis.dk/files/media/publications/import/extra/charitableorganizations_and_terrorismfinancing_ek.pdf

Kompas.com. (2017, September 27). *Dua dari 18 WNI simpatisan ISIS jadi tersangka kasus pendanaan terorisme*. https://nasional.kompas.com/read/2017/09/27/19055401/dua-dari-18-wni-simpatisan-isis-jadi-tersangka-kasus-pendanaan-terorisme

Kompas.com. (2022, Mei 11). *Dua dari lima WNI yang disanksi AS terkait pendanaan ISIS merupakan mantan narapidana teroris*. https://nasional.kompas.com/read/2022/05/11/13294211/dua-dari-lima-wni-yang-disanksi-as-terkait-pendanaan-isis-merupakan-mantan.

Kshetri, N. (2018). 1 The emerging role of big data in key development issues: Opportunities, challenges, and concerns. *Big Data for Development*, 3(1), 10–24.

Levi, M., & Maguire, M. (2004). Reducing and preventing organized crime: An evidence-based critique. *Crime, Law and Social Change*, 41(5), 397–469. https://doi.org/10.1023/B:CRIS.0000039582.04270.a4

Levitt, M. (2014). *Hezbollah: Financing Terror through Criminal Enterprise*. In J. K. Giraldo & H. A. Trinkunas (Eds.), *Terrorism Financing and State Responses*. Stanford University Press.

Maimbo, S. M., & Passas, N. (2005). *Remittances and Economic Development in Somalia*. World Bank Working Paper.

Moustafa, N., Slay, J., & Creech, G. (2019). Big data analytics for intrusion detection: A survey. *Journal of Big Data*, 6(1), 1–33. https://doi.org/10.1186/s40537-019-0192-5

OJK. (2024). *Transformasi Pengawasan OJK terhadap Inovasi Keuangan Digital*. Otoritas Jasa Keuangan.

PPATK. (2022). *Penilaian Risiko Organisasi Nirlaba dalam Pendanaan Terorisme*. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan. https://www.ppatk.go.id

PPATK. (2024). *Laporan Tahunan PPATK 2023*. Pusat Pelaporan dan Analisis Transaksi Keuangan. https://www.ppatk.go.id/

Prasetya, A. Y., Subroto, A., & Nurish, A. (2021). Model Pendanaan Terorisme Melalui Media Cryptocurrency. *Journal of Terrorism Studies*, 3(1), Article 3. https://doi.org/10.7454/jts.v3i1.1030Scholar Hub+2Scholar Hub+2Journal Portal+2

Putri, C. P. H., & Lisanawati, G. (2022). Peran Teknologi Finansial Dalam Pencegahan Pendanaan Terorisme. *Jurnal Hukum IUS QUIA IUSTUM*, 30(1), 70–90. https://doi.org/10.20885/iustum.vol30.iss1.art4Journal Portal

Ramadianto, A. R., & Wicaksono, B. A. (2023). Countering The Crimes of Money Laundering and Terrorism Financing in Indonesia Digital Banking: A Legal Approach Perspectives. *Indonesian Journal of Counter Terrorism and National Security*, 2(2). https://doi.org/10.15294/ijctns.v2i2.66841Universitas Negeri Semarang Journal

Reitano, T., & Shaw, M. (2020). Illicit financial flows and terrorism financing in fragile states. *Global Initiative Journal on Organized Crime*, *5*(1), 1–17.

Republik Indonesia. (2013). *Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme*. Lembaran Negara Republik Indonesia Tahun 2013 Nomor 87.

Rizky, F., & Sari, N. (2022). Eks-napiter dan kejahatan keuangan: Studi kasus keterlibatan dalam pendanaan ISIS. *Jurnal Ilmu Kriminologi Indonesia*, *3*(2), 118–135.

Setiawan, A., & Hartono, D. (2020). Cybersecurity readiness in Indonesia: A critical review. *Indonesian Journal of Cyber Security*, 2(1), 15–29.

Shahbaz, M., Gao, J., & Zhai, L. (2022). Role of national cybersecurity centers in combating terrorism financing. *Journal of Strategic Security*, 15(3), 35–52.

Shapiro, J., & Siegel, D. (2021). Financial crimes and cryptocurrency in Asia-Pacific: Risks and responses. *Journal of Financial Crime*, 28(4), 1169–1185. https://doi.org/10.1108/JFC-12-2020-0237.

Sirait, R. A., & Rangkuti, E. Y. (2023). Pencegahan pendanaan terorisme oleh yayasan amal di Indonesia. *Jurnal Hukum Universitas Sumatera Utara*, 11(2), 210–222. https://jurnal.usu.ac.id/jhu/article/view/11456

SuaraIndo.id. (2021, Agustus 30). *Dari koin jadi pelor: Jalur teroris menghimpun dana*.

https://www.suaraindo.id/2021/08/dari-koin-jadi-pelor-jalur-teroris-menghimpun-dana

The Conversation. (2020, Februari 28). *Yang tidak kalah penting dari isu kepulangan simpatisan ISIS: Mengawasi arus keuangan mereka*. https://theconversation.com/yang-tidak-kalah-penting-dari-isu-kepulangan-simpatisan-isis-mengawasi-arus-keuangan-mereka-132972

Thomas, D., Al-Khateeb, S., & Yu, J. (2021). Cybercrime and digital security: The evolving threat landscape. *Journal of Information Security*, 12(3), 123–137.

TRM Labs. (2024). *Crypto and Terrorism: The Rise of ISIS-K's Digital Financing*. https://www.trmlabs.com/resources/blog/terrorist-financing-six-crypto-related-trends-to-watch-in-2023.

UN Security Council. (2004). *Report of the Monitoring Group on Al-Qaeda and the Taliban* (S/2004/679). https://undocs.org/S/2004/679.

U.S. Department of Justice. (2020, August 13). *Global disruption of three terrorist financing cyber-enabled campaigns*. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-campaigns.

UU No. 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme.

van Wegberg, R., de Graaf, K., & Kleemans, E. (2018). Cryptocurrency and criminality: A research agenda. *Trends in Organized Crime*, 21(3), 270–286. https://doi.org/10.1007/s12117-018-9325-6.

Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict & Terrorism*, 44(2), 99–121. https://doi.org/10.1080/1057610X.2018.1531565

Wijayanto, S., & Pramono, A. D. (2021). Analisis Peran Fintech dalam Modus Pendanaan Terorisme Digital di Indonesia. *Jurnal Keamanan Nasional*, 7(2), 134–152.

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2018). Artificial Intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, 42(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103.

World Bank. *"Data berdasarkan International Telecommunication Union (ITU)."* 2021.

Yulianti, D., & Nachrawi, N. (2024). Analisis yuridis terhadap pendanaan terorisme oleh kelompok Jamaah Islamiyah dalam putusan No. 308/PID.SUS/2020. *Jurnal Hukum & Keamanan Nasional*, 9(1), 45–60. https://doi.org/10.31000/jhkn.v9i1.19200

Yulianti, T., & Nachrawi, G. (2022). Modus Pendanaan Terorisme oleh Jamaah Islamiyah Berdasar UU No. 5 Tahun 2018: Analisis Putusan No. 308/PID.SUS/2020/PN JKT.TIM. *IBLAM Law Review*, 4(3). https://doi.org/10.52249/ilr.v4i3.454

Zelin, A. Y. (2020). *The Jihadist Governance Dilemma: Hay'at Tahrir al-Sham and the Challenge of Local Legitimacy*. Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/jihadist-governance-dilemma