MP-IDSA Occasional Paper No. 67

Impact of AI on Money Laundering and Terrorist Financing

Emerging Risks And Policy Responses

Vivek Chadha

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA Occasional Paper No. 67

Impact of AI on Money Laundering and Terrorist Financing

Emerging Risks and Policy Responses

Vivek Chadha

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-81-687924-1-8

First Published: July 2026

Published by: Manohar Parrikar Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
Website: http://www.idsa.in

Cover &
Layout by: Geeta Kumari

Impact of AI on Money Laundering and Terrorist Financing: Emerging Risks and Policy Responses

Introduction

Artificial Intelligence (AI) is influencing every field of human endeavour. Its impact — both negative and positive — is likely to emerge as the most consequential factor effecting terrorist financing and money laundering. AI may not revolutionise how terrorists or launderers raise funds or clean dirty money. Yet, it will create substantive capabilities to bypass security protocols. Ironically, AI's specialist capabilities will simultaneously ease security agencies and financial institutions' task of monitoring and neutralising criminal activities.

The challenge posed by terrorist financing remains one of the persistent threats that sustains terrorism the world over. It is often referred to as the lifeblood of terrorism, given its role in sustaining terrorist organisations. If ideology and fear are two key attributes of terrorism, then terrorist financing is the third pillar that sustains it. In more cases than not, individual acts of terrorism do not require substantial amounts of money, with a few exceptions of the kind represented by 9/11 in the US and the 26/11 attack in Mumbai.[1] Yet funding remains vital for sustaining the routine activities of a terrorist organisation. This can range from paying terrorist cadres, compensation for their families to recruitment campaigns, publicity, training and procurement of weapons and equipment, supporting local

---

[1] Vipul Tamhane, 'An Account On Al-Qaeda 9/11 Terrorist Attacks Financing,' *The Defence Horizon Journal*, October 12, 2023, at https://tdhj.org/blog/post/9-11-terrorist-attacks-financing/ (Accessed April 23, 2026).

welfare initiatives and so on. From a state's perspective, it is therefore more important to drain the organisation of funds rather than focus the entire energy merely on individual acts of terrorism if terrorism itself has to be defeated.

Money laundering has different motivations than terrorist financing, yet it remains closely linked. Money laundering attempts to clean dirty money, giving sustainability to crime and generating profit. It has an economy-wide impact that ranges from sustaining black money to terrorist financing. Money laundering harms the economy by helping support a parallel, illegal financial system. 'The estimated amount of money laundered globally in one year is 2–5% of global GDP, or $800 billion–$2 trillion in current US dollars'.[2] The scale and widespread impact of money laundering does not limit its adverse effects to macroeconomics but includes the lives of common citizens on a daily basis by institutionalising corruption and crime in the society.

AI is creating new areas of exploitation for criminals and terrorists, while simultaneously reinforcing existing methods of subverting the financial system. It has given a fillip to innovative means of criminal activities by helping create false identities, identifying weaknesses in the financial system and facilitating exploiting these, and at the same time hiding the identity of law breakers.

AI's fast-evolving capabilities and a better understanding of its characteristics is raising concerns for law enforcement agencies and counter-terrorist financing and anti-money laundering organisations. As highlighted by case studies, the role of AI in criminal activities is becoming a serious cause of concern and forcing governments to seek urgent counter measures. Technological and procedural measures are also being employed by financial institutions to safeguard monetary systems and create new tools that can trace and track illegal activities.

---

[2] "Money Laundering," United Nations Office of Drugs and Crime, at https://www.unodc.org/unodc/en/money-laundering/overview.html#:~:text=Money%20Laundering,3%20Stages%20of%20Money%20Laundering, (Accessed April 21, 2026).

The paper briefly describes the characteristics and capability of AI as a technology. It explains the concept of terrorist financing and money laundering to explore the linkage between the two. These two aspects are more for readers not entirely familiar with these subjects. Others may skip this to move directly to case studies of AI's exploitation by terrorist organisations and criminals and its simultaneous employment by intelligence and law enforcement agencies attempting to remain ahead of the technological curve adopted by criminal organisations. Finally, the paper will suggest policy options to improve the adoption and implementation of AI to limit the threat from terrorist financing and money laundering.

AI as a Technology

Few technologies have led to as much debate as AI. It is already being counted among the most pathbreaking inventions, while simultaneously posing a threat of severe disruption. Google CEO Sundar Pichai said, 'AI is one of the most important things humanity is working on. It is more profound than, I dunno, electricity and fire'.[3]

Even as AI's founding fathers acknowledge its immense potential and contributions to human wellbeing, some are equally concerned about its capacity to severely disrupt the existing way of life. Geoffrey Hinton is widely regarded as the father of AI. A Nobel laureate, he is also the winner of the Turing Award. Having worked at Google, a company at the forefront of AI research, he therefore knows the technology's potential impact better than most. Hinton states, 'My big worry is, sooner or later, someone will wire into them the ability to create their own subgoals'. He adds, 'And if [AI models] are much smarter than us, they'll be very good at manipulating us. You won't realise what is going on'. And worse, 'So even if they can't pull levers, they can certainly get us to pull the levers'.[4]

---

[3] Catherine Clifford, 'Google CEO: A.I. Is More Important Than Fire or Electricity,' *CNBC*, at https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html (Accessed January 19, 2026).

[4] Sara Brown, "Why Neural Net Pioneer Geoffrey Hinton Is Sounding the Alarm on AI," MIT Management Sloan School, May 23, 2023, at https://mitsloan.mit.edu/ideas-made-to-matter/why-neural-net-pioneer-geoffrey-hinton-sounding-alarm-ai (Accessed January 20, 2026).

Hinton also discusses the ability of AI systems to self-preserve, which will make it increasingly difficult for humans to force a change in the direction of these systems or to 'kill off' the network.

Irrespective of the divided opinions on AI's constructive or destabilising impact, there is little doubt about its growing relevance. This stems from its foundational characteristics as a fast evolving and emerging technology that will profoundly change how existing systems and processes operate. AI is emerging as both an opportunity and a challenge. Nandan Nilekani, the former head of Infosys and pioneer of the Aadhar Card initiative in India focusses more on the challenges associated with AI implementation and its relationship with security. He highlights the 'deployment gap' created by the fast evolution of the technology and the inability of companies to deploy it. He has raised concerns regarding legacy systems that are not designed to take on online attacks. When this is associated with the growing capability of non-state actors to exploit AI, threats to organisations become apparent.[5]

Why is AI being viewed from contrasting perspectives, even among experts and industry leaders? This is primarily because AI, despite being increasingly prevalent, continues to remain an enigma for most. This is especially relevant to its potential and capability as a technology. AI has developed the capacity to simulate human cognition. An AI system will likely overtake an average human mind. AI's potential can be illustrated by two interesting examples. The first relates to the award of the Nobel Prize in Chemistry to a computer engineer and the second through a game called Go.

Google DeepMind pioneers Demis Hassabis and John Jumper were jointly awarded the Nobel Prize in Chemistry in 2024. According to the Nobel Prize press release, Demis and John 'developed an AI model to solve a

---

[5] Padmini Dhruvaraj, 'AI Races Ahead as Businesses Struggle with Legacy Systems: Nandan Nilekani,' *The New Indian Express,* February 17, 2026, at https://www.newindianexpress.com/business/2026/Feb/17/ai-races-ahead-as-businesses-struggle-with-legacy-systems-nandan-nilekani (Accessed April 22, 2026).

50-year-old problem: predicting proteins' complex structures'. This was achieved by creating an AI model, AlphaFold.[6] In essence, the use of AI achieved what the best of human intellect and legacy computer modelling had failed to do. This example is neither isolated nor rare. It is merely a representative expression of AI's far-reaching capabilities.

In 2016, DeepMind's AlphaGo made history by beating the best player in a best-of-five match. Go is an ancient strategy board game and is known for its complexity. It was recognised as the ultimate challenge for machines, given the possibility of 14.5 trillion moves after the first four moves.[7]

Conventional logic would suggest familiarising the algorithm with all possible moves and then letting the faster processing speed of the system and number crunching capability of the software give it an edge against even the best players. However, the competing AI algorithm was not programmed to account for all possibilities. Instead, it 'self-taught' itself to play move number 37, confounding experts. This process of self-learning was an indicator of how AI could ultimately function autonomously.[8]

This did not end the monumental changes underway. Its later version 'dispensed with any previous human knowledge', unlike the earlier system that had 'watched' 1,50,000 games. The new system self-learnt playing itself and continued to improve. It eventually reached the desired level after a day of training, indicating the scope and potential of AI-based learning in emerging systems.[9]

---

6 "Press Release," The Nobel Prize, October 9, 2024, at https://www.nobelprize.org/prizes/chemistry/2024/press-release/ (Accessed January 20, 2026).

7 "What is Artificial Intelligence," IBM, at https://www.ibm.com/think/topics/artificial-intelligence (Accessed January 21, 2026).

8 Mustafa Suleyman with Michael Bhaskar, *The Coming Wave – AI, Power and the Twenty First Century's Greatest Dilemma*, The Bodley Head, London, 2023, p. 54.

9 Ibid.

This evolution in AI can be associated with two fundamental processes: Machine Learning and Deep Learning. At a basic level, machines are 'taught' through 'supervised learning', in which human intervention trains the algorithm on inputs and their corresponding outputs. A common machine learning algorithm is called a 'neural network', which attempts to mimic the structure of the human brain. The next step in this process is to create multiple complex layers of neural networks, which helps the system reason, adapt and improve itself.

The wonders of AI are not lost on even its critics. The challenge remains in doing a better job with its implementation than those waiting to exploit its potential to disrupt the security landscape. It is evident from the contrasting perspectives on AI that the technology is poised to drive transformative change. Furthermore, even as AI will undoubtedly have a positive impact on fields such as medicine and technological innovation, there is a distinct possibility that states may lose control over the technology. This unfortunate eventuality could be accelerated or exploited by individuals or groups that do not necessarily share the government or society's perspectives on rule of law and acceptable norms of social behaviour.

Challenges Posed by AI and Its Impact

The advent of AI is likely to present challenges far beyond obvious and immediate first-order threats. However, even as the first-order threats seem more challenging to begin with, the second-order threats are likely to have more far-reaching consequences.

First-Order Threats

The first-order threats directly relate to the capabilities AI can create, especially in the hands of terrorist organisations and criminal groups. As discussed previously, AI can not only sift and interpret data at speeds that are beyond the ability of previous generation electronic systems, but it can also simulate actions and operate autonomously. Consequently, AI-driven systems can make the entire chain of terrorist financing more efficient and more effective. This is best explained with an example. An AI-powered system can do a better job of convincing people through simulated audio and visual messaging on an industrial scale to donate or talk the gullible into using fraudulent financial schemes that can accrue better returns, thereby

raising funds for the organisation. It can also be used to convince, blackmail and threaten individuals by simulating superior authority or law enforcement agencies,[10] leading to the transfer of funds or paying a ransom demand.[11]

Subsequently, this ill-gotten money can be routed through the financial system while exploiting its vulnerabilities. This exploitation of the financial channels is done by using software capable of detecting flaws in a system and exploiting these. The capability of a software like Anthropic's Mythos will be discussed later in the paper to illustrate this capability.[12]

Finally, money is distributed and disbursed through the ingenious exploitation of fake documents to open accounts, conducting multiple transfers across jurisdictions, making the task of establishing identities practically impossible for agencies. This process uses AI-enabled criminal activities to raise funds for terrorist organisations, and is equally valid for laundering funds generated through criminal acts.[13]

Digital technology-based platforms like crypto currency are emerging as a means of parking, trading and generating funds for terrorist actors. The relative obscurity provided by crypto currency compared to more traditional financial channels makes it an attractive option for terrorist groups and criminal organisations.[14]

---

10 "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes,",UNICRI and UNCCT, 2021, at https://www.un.org/counterterrorism/sites/default/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf (Accessed May 21, 2026), pp. 29–30.

11 "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes," no. 10, pp. 36–37.

12 Meghna Pradhan, "The Making of Mythos: AI-Enabled Cybersecurity and the Emerging Architecture of Access," MP-IDSA, at https://idsa.in/publisher/issuebrief/the-making-of-a-mythos-ai-enabled-cybersecurity-and-the-emerging-architecture-of-access (Accessed May 21, 2026).

13 Ibid, pp. 43–44.

14 Luis Buenaventura, 'Did ISIL Really Use Bitcoin to Fund the Paris Attacks?,' Medium, December 14, 2015, at https://medium.com/cryptonight/did-isil-really-use-bitcoin-to-fund-the-paris-attacks-1287cea605e4 (Accessed May 21, 2026).

This process-driven description of AI's employment will be illustrated through case studies in the succeeding section. At this stage, it is relevant to establish that AI's impact is likely to be felt throughout the generation, transfer and distribution chain of terrorist financing and cleaning phases of money laundering.

Second-Order Threats

The autonomous functioning of AI systems presents a potential challenge if it is programmed for destructive or regressive actions.[15] This when related to terrorist financing and money laundering raises apprehensions that warrant closer scrutiny. The emergence of AI agents underlines one such area of concern. AI agents are characterised by features like autonomy, adaptability, goal-orientation and the ability to learn from experience. This evolution is raising questions about its ethical use if users lose control or if it is programmed to undertake illegal activity. The evolving role of AI agents is likely to involve systems taking over functions independently, based on the software's agentic capacity. This is likely to reduce human monitoring and control over functions.[16]

When we co-relate AI's capability to self-learn, go beyond existing human capabilities and finally, operate autonomously as agents (often referred to as agentic AI), then its impact both as an efficient tool and a potential threat begins to emerge.

AI as a technology will have a lasting impact on all spheres of human existence. Terrorist financing and money laundering are unlikely to remain unaffected by this change. The technology will create super-intelligent machines that may work with or even without human control and supervision. AI has been progressing for decades. However, recent

---

15 "Artificial Intelligence (AI): A Simple-To-Understand Guide," Google Cloud, at https://cloud.google.com/learn/what-is-artificial-intelligence (Accessed January 27, 2026).

16 Noam Kolt, "The Challenges of Governing AI Agents," AI Frontiers, April 9, 2025, at https://ai-frontiers.org/articles/the-challenges-of-governing-ai-agents (Accessed January 27, 2026).

developments have seen it cross the tipping point. This has been accompanied by a dramatic upswing in its trajectory and growth, in some cases even exceeding the optimism of AI engineers.[17]

Nonetheless, these swift changes are not without their challenges. These challenges, while seemingly generic, are related to capability differentials among nations, varying rate of adoption and its exploitation by state and non-state inimical elements.

A brief look at the specific areas indicates AI's potential to exacerbate existing threats and challenges associated with money laundering and terrorist financing. These challenges arise from two primary factors: the technology itself and its international implementation.

AI is highly resource intensive. What is visible on the surface is a very basic exploitation of AI, even as its more intensive and impactful applications remain available to those entities that can afford it.[18] These include countries such as the US and China, which are at the forefront of AI research and patents.[19] Companies including Google, Anthropic, Microsoft, OpenAI and Nvidia are investing billions of dollars to dominate the AI ecosystem.[20] This suggests that access to AI's cutting-edge applications will be controlled by the 'AI Haves', while the 'AI Have Nots' will remain relegated to the second or even third tier of access to resource-intensive applications. In the past, terrorist groups have used easily available and open-source options

---

17 Holden Karnofsky, "AI Has Been Surprising for Years," Carnegieendowment.org, January 6, 2025, at https://carnegieendowment.org/russia-eurasia/research/2025/01/ai-has-been-surprising-for-years (Accessed February 23, 2026.

18 For a detailed estimation of AI implementation cost, "How Much Does It Cost to Develop an AI Solution? Pricing and ROI Explained?," Coherent Solutions, November 24, 2025, at https://www.coherentsolutions.com/insights/ai-development-cost-estimation-pricing-structure-roi (Accessed February 6, 2026).

19 "Key Findings and Insights," WIPO, at https://www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/en/key-findings-and-insights.html (Accessed February 23, 2026).

20 'Big Tech to Invest About $650 Billion in AI in 2026, Bridgewater Says,' *Reuters*, February 23, 2026, at https://www.reuters.com/business/big-tech-invest-about-650-billion-ai-2026-bridgewater-says-2026-02-23/ (Accessed February 25, 2026).

to augment their funding efforts. Similarly, criminals have exploited loopholes in the financial system to launder their proceeds of crime. This raises the possibility of terrorists and criminals exploiting the uneven distribution of AI implementation and targeting regions with poor implementation. The challenge that emerges from this assessment relates to the ability of criminal and terrorist groups to develop AI solutions with limited resources and use publicly available enabling AI mechanisms. Terrorists' ability to use AI resources will be further augmented by support from countries that employ these AI-based tools as instruments of state policy.[21] This will largely mitigate any resource constraints that terrorist groups may face in an AI-driven security environment.

There has been an ongoing debate around the impact of AI on society. Will it emerge as the finest tool that humanity has ever created or an autonomous agency that will render human contribution redundant over time? Consequently, this could lead to a period of social unrest due to job losses. London Business School's Dr Ekaterina Abramova has warned that 'artificial intelligence could displace workers faster than new jobs are created, raising the risk of widening inequality and social unrest'.[22] The oncoming possibility of job loss is underlined by Anthropic AI CEO Dario Amodei, who says, 'AI will disrupt 50% of entry-level white-collar jobs over 1-5 years, while also thinking we may have AI that is more capable than everyone in 1–2 years'.[23] This situation could be seen as an opportunity by criminal and terrorist organisations to exploit the interim

---

[21] "Statement by EAM Dr. S. Jaishankar on the Special Discussion in Lok Sabha on Operation Sindoor," Ministry of External Affairs, July 28, 2025, at https://www.mea.gov.in/Speeches-Statements.htm?dtl/39883/Statement_by_EAM_Dr_S_Jaishankar_on_the_special_discussion_in_Lok_Sabha_on_Operation_Sindoor (Accessed February 6, 2026).

[22] "AI Layoffs Could Outpace New Jobs, Warns Dr Abramova," London Business School, December 30, 2025, at https://www.london.edu/news/ai-and-the-future-of-work-abramova (Accessed February 6, 2026).

[23] 'Anthropic CEO Predicts 50% Entry-Level Jobs Will Be Gone in 1-5 Years as US Openings Drop to 6.5mn,' *Financial Express*, February 6, 2026, at https://www.financialexpress.com/world-news/us-news/anthropic-ceo-predicts-50-entry-level-jobs-will-be-gone-in-1-5-years-as-us-openings-drop-to-6-5mn/4132925/ (Accessed February 6, 2026).

period of uncertainty. It is as yet unclear if state and corporate haves will be able to control the adverse impact of AI in the hands of terrorists and criminals, or whether criminal and terrorist organisations will successfully exploit this interim period of flux to subvert sections of the population to fight against what might be interpreted and sold as failure of states. This will create opportunities for a pool of technically qualified and disgruntled group of people who are out of jobs and desperate to sustain themselves. While the correlation of such a group as potential recruits who may exploit the technical potential of AI for profit on behalf of criminal or terrorist organisations may seem a stretch at present, however, the role of socio-economic upheavals as a factor for rising criminal activity is an established trend.[24]

The rate and pace of technological development have created challenges for intelligence and enforcement agencies as they play catch-up with terrorist organisations and criminals who have exploited this rapid advancement before adequate controls could be created. State agencies and international bodies have struggled with technologies such as virtual currencies in the past. In 2023, only 35 jurisdictions had implemented the travel rule, by 2025, this had increased to 85.[25] The travel rule requires service providers to share user data involved in transactions, typically above a specified threshold. This should be seen in the context that weaknesses and limited implementation in a few jurisdictions can adversely affect the viability of the entire chain, thereby opening it to exploitation by criminals and terrorists. The scope of AI's exploitation extends beyond any single technological

---

[24] Hafiz Faisal Yaseen and Shuai Man, 'Criminality Trends Through Socio-Economic Factors: A Two Decade Panel ARDL Analysis of Upper-Middle-Income Nations (2000-2021),' *Crime & Delinquency*, December 13, 2025, at https://journals.sagepub.com/doi/10.1177/00111287251397995 (Accessed April 23, 2026).

[25] "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Service Providers," FATF, June 26, 2025, at https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf (Accessed February 3, 2026), p. 17. Travel rule requires service providers to share user data involved in transactions, usually above a certain threshold.

innovation like virtual currencies. This country-specific challenge will become more complex when addressing international threats. Countries continue to have varying views on AI applications, their monitoring and regulation. It will remain a challenge to frame laws that are seen as impinging on data security, citizens' freedom and their rights. This dissonance is likely to give lawbreakers the very opportunity to exploit the window of opportunity that arises during this interim period of indecision.

The implementation of existing guidelines for the regulation of laws, procedures and processes to combat terrorist financing and money laundering has demonstrated that countries, even when they seek to curb crime and terrorism, may lack the resources and capacity to undertake the recommended measures.[26] A review of the Financial Action Task Force (FATF) countries displaying weak compliance with the guidelines clearly indicates this limitation. These weaknesses are likely to amplify, given the complexities and capacity required to constrain the AI's resultant impact.

Technology companies have underscored their contribution to the great-power rivalry of the 21st century. In the context of the war in Ukraine, companies such as Starlink have been instrumental in providing vital support to Ukrainians when all else seemed to have failed. DJI drones, which have been at the forefront of the global proliferation of commercial drones, were employed in combat operations.[27] Audrey Cronin's recommendation that big corporations should be used as allies in war rather than merely as contractors, while a present-day reality, might well be superseded by these very corporations seeking influence, or worse control, over what states decide to do with the power that AI will bring.

---

[26] "FATF Grey Listing a Good Thing? Nor for Africa, Not for the Poorest," Comsure, June 9, 2024, at https://www.comsuregroup.com/news/fatf-grey-listings-a-good-thing-not-for-africa-not-for-the-poorest/#:~:text=GREYLISTING%20IMPACT,listed%20jurisdictions%20(nearly%2060%25) (Accessed February 11, 2026).

[27] Audrey Kurth Cronin, "How Private Tech Companies Are Reshaping Great Power Competition," Henry A. Kissinger Centre for Global Affairs, at https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition/ (Accessed February 11, 2026).

The growth of AI has seen the rise of private companies that are spearheading the technological revolution. This gives these companies unparalleled access to data and technological leverage. Such companies do not work for altruistic reasons and have an inherent profit motive. This creates a fundamental imbalance in the power-responsibility matrix, which could be skewed in favour of power over responsibility for AI's societal impact. When a company creates end-to-end encryption for messaging, it does not take responsibility for also providing terrorist organisations with a powerful tool to implement their designs. Nor is it at the forefront of regulating such technologies. This responsibility lies with the government. In contrast, technologies such as AI can unleash such power that they may well move beyond states' ability to regulate them.[28] According to certain expert accounts, that threshold is not far from the point at which the challenges likely to be faced by security agencies increase.

The rate and pace of AI growth indicate that 'technological innovation will continue to outpace traditional regulation'.[29] This suggests that the governance model associated with advanced technology, a proven model, is likely to be challenged. The nature and extent of the chaos in the wake of AI advances will vary according to early estimates, but the likelihood is real. This implies that terrorist organisations will seek and possibly find more ingenious ways to generate funds by manipulating information and subverting financial systems. Crime breeds freely in an environment of corruption and weak enforcement of the rule of law. Such an environment facilitates easy manipulation of the system to launder the proceeds of crime. Terrorist groups exploit existing networks of crime-laundering nexus to support their financial needs. An underregulated international environment that breeds chaos is akin to a corrupt, ungoverned space struggling to keep pace with the advancement of the AI-driven technological revolution.

---

[28] Barry Pavel, Ivana Ke, Michael Spiritas, James Ryseff, et al. "AI and Geopolitics – How Might AI Affect the Rise and Fall of Nations?," RAND, November 3, 2023, at https://www.rand.org/pubs/perspectives/PEA3034-1.html#:~:text=Big%20tech%20companies%20also%20affect,with%20one%20or%20more%20AIs (Accessed February 12, 2026).

[29] Ibid.

Understanding Terrorist Financing and Money Laundering

Having explained the characteristics of AI and the challenges it poses, the paper briefly introduces the concept of terrorist financing and money laundering to relate it to AI's impact on raising money for terrorist groups and cleansing dirty money generated through crime.

The characteristics of AI and the challenges posed through the course of its implementation are indicators of potential instability and opportunity. To understand how this phase could be exploited or used to strengthen existing law enforcement frameworks, it is important to understand the fundamental characteristics and challenges associated with money laundering and terrorist financing.

Money laundering is the conversion of 'dirty money' from illegal activities into seemingly legitimate funds, covering all stages from placement (introducing cash) to layering (complex transactions) and integration (reintroduction as clean money). For money laundering to be established, the process should involve the proceeds of crime. This suggests that money laundering falls within the scope of economic offences. However, in addition to crime, money laundering can also be associated with terrorism and its financing. This has long been established and reinforced by multinational organisations such as FATF, which provides the regulatory framework, guidance and direction for addressing these challenges. An illustrative example is FATF's report Money Laundering and Terrorist Financing in the Art and Antiquities Market.[30]

Money laundering and terrorist financing are two distinct areas of concern for states; yet despite being distinct they are related. As indicated earlier, money laundering is defined as the process of handling dirty money, or

---

[30] "Money Laundering and Terrorist Financing in the Art and Antiquities Market," FATF, February 2023, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf (Accessed January 27, 2026).

the proceeds of crime. In contrast, most money that funds terrorism need not come as proceeds of crime. In other words, it can be clean money. The primary motive of money laundering is profit from cleaning dirty money. Conversely, terrorist financing supports terrorism, which purportedly seeks to achieve a political aim. Money laundering is merely the process of converting dirty money into clean money. Terrorist financing is a key supporting element that facilitates the functioning of a terrorist organisation and, by correlation, its acts of terrorism.

Despite these differences, the potential for collaboration between these two seemingly independent activities makes the ensuing threat that much more challenging. Criminal groups create channels to move the proceeds of crime. These channels are established over time and gain a degree of reliability and robustness. For example, cross-border smuggling networks that may be associated with petty activities, such as smuggling cheaper tobacco and medicines to sell in more lucrative markets, can also be exploited to facilitate the smuggling of drugs and weapons for higher returns. Similarly, criminal groups have been employed to smuggle Fake Indian Currency Notes (FICN) across the border. While the motive of criminals will remain profit from such activities, ideologically motivated terrorist groups or their state-specific handlers, as is the case with Pakistan, are more likely to be motivated by their strategic interests.[31] Furthermore, smuggled FICN can be routed through major commercial centres in metropolitan cities to obtain clean currency, and its eventual relocation can occur through high-value assets such as gems, jewellery and property. What might seem like disconnected, disjointed individual actions can come together like pieces of a jigsaw puzzle, connecting crime, money laundering and terrorist financing.

Funding is integral to terrorism. This suggests that historically, it is as ancient as individual and collective terrorist actions. The progression of terrorism suggests an evolving roadmap and an iterative progression in perpetuating

---

[31] "Unstarred Question No. 1563," Government of India, Home Affairs, Lok Sabha, December 2, 2014, at https://eparlib.sansad.in/bitstream/123456789/710451/1/8596.pdf (Accessed April 23, 2026).

acts. With time, terrorist groups have adopted increasingly sophisticated means to fulfil their agenda. Technology has often emerged as a facilitator at one end of the spectrum, while ageless, primitive modes of funding such as cash, hundi and hawala have coexisted with equal effectiveness.[32]

The emergence of AI in general, and its impact on terrorism financing in particular, is likely to have an influence far beyond that of previous technological innovations. Even as the world struggles to keep pace with the rapid development of AI, early indicators suggest the onset of a paradigm shift in the human–machine interface.

Impact of AI on Terrorist Financing and Money Laundering

The core characteristics of AI highlight important challenges that are likely to emerge as its impact becomes more pronounced. When the key capabilities of AI are related to the means adopted by terrorist groups to raise funds and by criminals to launder their financial proceeds, future trends begin to emerge.

A brief understanding of the process involved with money laundering and terrorist financing highlighted its stages and characteristics. When this is co-related with AI, it emerges that it can create facilitating and supporting conditions for terrorist financing. It can also help with enabling mechanisms to defeat existing regulatory mechanisms in place. 'Our research predicted exactly what we're observing: terrorists deploying AI to accelerate existing activities rather than revolutionise their operational capabilities', says Adam Hadley, the founder and executive director of Tech against Terrorism, an online counter-terrorism watchdog, in an article.[33]

---

[32] "The Hawala System: A Risky Alternative to Traditional Banking," ACAMS TODAY, March 10, 2023, at https://www.acams.org/en/opinion/the-hawala-system-a-risky-alternative-to-traditional-banking (Accessed March 18, 2026).

[33] Ben Makuch, 'How Terrorist Groups Are Leveraging AI to Recruit and Finance Their Operations,' *The Guardian*, July 8, 2025, at https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence (Accessed March 18, 2026).

During the early impact of AI's development, in 2023, the FATF had noted that 'artificial intelligence-powered tools can identify prospective donors and direct them to specific funding causes they would not have otherwise been exposed to'.[34]

The technological orientation of AI as a tool suggests that its impact will be more pronounced in areas that are influenced or dominated by processes that rely heavily on technology for implementation. This suggests that the physical smuggling of cash or criminal acts like kidnapping for ransom are less likely to be influenced compared to the use of deep fakes to solicit donations or financial frauds as a means of collecting funds. In other words, wherever AI makes a commercial or technological impact on existing processes, its influence will also be seen as a facilitator for terrorist financing.

The case of Islamic State is instructive in this regard. The group received a setback after its attempts at creating a sovereign non-state geographical entity were defeated. Mohammad Taha Ali writes that the group has attempted a smooth transition from a physical to a virtual space. 'In 2024 and 2025, its propaganda teams began experimenting with generative artificial intelligence to create multilingual content, deepfake videos, and synthetic "news anchors" promoting the group's ideology'. Similarly, the strike against their hawala operations resulted in the operations being replaced by crypto wallets, decentralised exchanges and peer-to-peer trading platforms generating a 'financial ecosystem without identities'.[35]

Unlike terrorist financing, money laundering is more reliant on the financial system for cleaning proceeds of crime. In most cases, launderers will introduce money into the financial system, layer it in a way that its origins

---

[34] "Crowdfunding for Terrorism Financing," FATF, October 2023, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf (Accessed March 18, 2026), p. 27.

[35] Mohammad Taha Ali, 'Inside the Islamic State's 'AI Caliphate',' Middle East Forum Observer, November 17, 2025, at https://www.meforum.org/mef-observer/inside-the-islamic-states-ai-caliphate (Accessed April 22, 2026).

can be obfuscated and eventually integrate it as clean funds. This suggests that at each stage money will flow through the financial system with an aim to diffuse its ownership and origins. The role of AI will become more pronounced where existing systems follow a certain system of automation, analysis and predictability through electronic means. As an illustration, the process of opening an account requires the establishment of the account holder's identity through a Know Your Customer (KYC) authentication. This process is further repeated periodically. Authentication is established by processes that involve facial recognition and scanning of documents. The transfer of funds also takes place by first establishing the origin and beneficiary credentials. All these procedural measures maintain the credibility of a financial system and its accompanying procedures. AI, in the hands of experts, can assist in overcoming some of these control measures. Its role will become that much more pronounced with accompanying automation, something that does characterise most parts of the financial system.

The aforementioned comparisons and illustrative examples suggest that AI usage will be more apparent in money laundering, compared to terrorist financing. This will entail the role of technology during each stage of the money laundering process—placement, layering and integration. In contrast, terrorist financing involves a combination of technology-centric applications along with more traditional methods that continue to be used by groups and supporting countries. The printing and circulation of fake currency as a means of financing terrorism is a case in point. The circulation of FICN through existing criminal networks by Pakistani handlers has been documented in detail. This includes the printing process in state-owned and controlled Pakistani printing presses.[36]

---

[36] Rajesh Ahuja, "'Currency Number" Evidence Prove Pak Involved in Pumping Fake Indian Notes,' *Hindustan Times*, January 30, 2014, at https://www.hindustantimes.com/india/currency-number-evidence-prove-pak-involvement-in-pumping-fake-indian-notes/story-OkS7deZ5JVaqsuHmuZVk8J.html (Accessed March 18, 2026).

Hawala is yet another means of transferring value that has long since been a preferred option by terrorist groups for supporting terrorist organisations and individual acts of terrorism. This is a rudimentary system based on basic communication between *hawaladars* to transfer value for inter- and intra-state financial movement.

Terrorist financing's wide-ranging options for raising and moving funds, supported by technology and age-old, time-tested methods, make it a challenge for intelligence and enforcement agencies. The focus of this paper, however, will remain on the emerging role of AI through techniques that exploit its potential across different stages of money laundering and terrorist financing.

Money laundering's exploitation of technology deals with the proceeds of crime. However, it is equally relevant for generating funds through the exploitation of technology for criminal actions. In this regard, vishing and cyber fraud have emerged as common methods for facilitating criminal activities using AI.

Vishing Fraud

The term 'vishing' comes from a combination of the words 'voice and 'phishing'.[37] It involves criminals scamming unsuspecting individuals by pretending to represent responsible positions in law enforcement and financial institutions. They extract sensitive financial data to defraud people of their money. This can be based on fear, anxiety, trust or the immediacy of a situation. A case study illustrates the use of voice phishing software to hack into user accounts and also to pose as a financial institution employee to trick victims into sending money.[38]

---

[37] For a more detailed understanding of phishing challenges and examples of fraud see "Illicit Financial Flows from Cyber-Enabled Fraud," FATF, Interpol and Egmont Group of Financial Intelligence Units, November 2023, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf (Accessed January 28, 2026).

[38] "Illicit Financial Flows from Cyber-Enabled Fraud," FATF, Interpol and Egmont Group of Financial Intelligence Units, November 2023, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf (Accessed January 28, 2026), p. 15.

Phishing has been prevalent for some years and remains a serious concern for law enforcement agencies. The exploitation of AI can enable criminals and terrorist organisations to conduct more systematic searches for potential targets, given its capacity to process large volumes of data. Over time, this ability can be further honed by developing autonomous, agentic applications that can undertake this task independently, thereby accelerating the process, improving efficiency and enabling self-learning to enhance success rates. The early signs of text-based and voice-activated chatbots have already begun to revolutionise businesses to improve customer response systems. This progression can be tailored and tutored to replicate law enforcement officials to give a fillip to vishing operations. When this is combined with deepfake videos, carefully selected targets, especially more elderly victims, can fall prey to the growing power of AI.

In an experiment, Fabricio Toapanta, Belen Rivadeneira, Christian Tipantuna and Danny Guaman used ChatGPT and three AI-enabled applications to simulate vishing attacks. This endeavour attempted with 50 potential victims indicated success in a little more than half the cases. This is despite the predictable challenges of suspicion at the victim's end. The experiment succeeded in cloning people's voices to extract sensitive information from their relatives and friends.[39]

Cyber Crime

The advent of digital infrastructure, especially in the financial world, is considered a means of ensuring greater transparency and accountability. While this is indeed the case wherein digitisation is accompanied by a robust regulatory framework and common law enforcement mechanisms, it is rarely the case with cross-border jurisdictions, which witness varying levels of enforcement and accountability. The challenge emerging from cyber fraud underlines this anomaly. Resultantly, there has been a growth

[39] Fabricio Toapanta, Belen Rivadeneira, Christian Tipantuna and Danny Guaman, 'AI-Driven Vishing Attacks: A Practical Approach,' *Engineering Proceedings*, 77 (1), at https://www.mdpi.com/2673-4591/77/1/15 (Accessed March 24, 2026).

in cyber fraud-related crimes. This has given a fillip to the risks associated with money laundering as well. 'According to the INTERPOL Global Crime Trend Report 2022, online scams are one of the cybercrime trends most frequently perceived as posing "high" or "very high" threats globally'.[40] This trend was further reinforced in the INTERPOL Crime Trend Update For 2024.[41] The agency found online scams and frauds being interlinked with human trafficking where victims were moved to scam centres to run a criminal business model. Over time, this threat has become global, with most continents being targeted for human trafficking.

The report indicates the future trends in human trafficking for cybercrimes. It suggests that AI can transform the existing levels of cyber fraud. 'AI has been reportedly used to generate convincing fake job ads that attract human trafficking victim as well as online photos or profiles through "deepfake" technology for sextortion and romance scams, among other social engineering schemes'.[42]

INTERPOL's assessment of future trends in the exploitation of AI may also be a conservative estimate of its capabilities and potential. Further possibilities may include the complete elimination of human involvement in cyber scams, with the introduction of autonomous bots that improve upon existing capabilities. As discussed earlier, agentic applications may reinforce this trend by enabling transnational operations, given their capacity to replicate linguistic fluency and incorporate social and behavioural norms into peer-to-peer engagement.

---

40 "Illicit Financial Flows from Cyber-Enabled Fraud," FATF, Interpol and Egmont Group of Financial Intelligence Units, November 2023, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf (Accessed January 28, 2026), p. 8.

41 "Interpol Releases New Information on Globalisation of Scam Centres," INTERPOL, June 30, 2025, at https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres (Accessed January 29, 2026).

42 Ibid.

Exploitation of Crypto Currency

Crypto currency continues to remain under-regulated despite its growing prevalence. This opens the possibility to exploit its vulnerabilities and use its relative anonymity to demand as ransom, collect, store and steal the currency.

This misuse has further been aggravated by the impact of AI on crypto currency, a technology already at the forefront of technological innovation. AI has made crypto trading a challenge for regulators and law enforcement agencies to regulate and control.

Over time, indicative trends and investigations suggest an increasing incidence of crypto currency in terrorist financing. The Egmont Group, a platform for country-specific Financial Intelligence Units (FIUs), released a report in June 2023 tracing the abuse of virtual assets for terrorist financing.[43] During the period 2018–2022, 29 per cent of the respondents among member organisations of the Egmont Group identified virtual assets linked to terrorist financing. Based on their feedback, terrorist groups such as the ISIL, Al-Qaeda, Hamas and Al-Qassam Brigades were identified as being the foremost exploiters of virtual currency.[44]

An FATF update noted that the DPRK based hackers 'carried out the largest single VA theft in history, stealing $1.46 billion from the VASP ByBit'.[45] This incident may seem like a one-off; however, the challenge is more widespread due to the complexities of regulating and monitoring virtual assets.

---

[43] "Report on Abuse of Virtual Assets for Terrorist Financing Purposes," Egmont Group, June 2023, at https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf (Accessed February 17, 2026).

[44] Ibid.

[45] "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Service Providers," FATF, June 26, 2025, at https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf (Accessed February 3, 2026), p. 19.

The abuse of virtual currencies, particularly crypto, has led to tighter regulations and a crackdown on crypto-mixing websites. Europol closed Cryptomixer, a service involved in money laundering.[46]

The crackdown on crypto mixers resulted in criminals and terrorist organisations seeking AI solutions to growing challenges. They resorted to decentralising finance (DeFi) by using agentic smurfing. Agentic smurfing is an amplification of the term 'smurfing'. Smurfing is the 'practice of using multiple individuals or accounts to perform transactions so as to avoid suspicion or currency reporting requirements'.[47] The FATF notes that the term has also been referred to as cuckoo smurfing in Europe basis the cuckoo bird laying eggs in the nests of other birds. Daria Alexe notes that AI takes over this action through four phases: It generates disposable wallets with unique addresses for a single transaction. This is followed by exploiting the blockchain congestion pattern to 'optimise timing and routing' through micro transactions. Funds are introduced in small amounts below the regulatory threshold of red flagging. Finally, 'cross-chain multiple swaps across multiple blockchains' allow for minimal online evidence. This facilitates two individuals to trade without a centralised intermediary.[48] This method has been used by terrorist groups like the Islamic State-Khorasan Province (ISKP) and Hamas-affiliated groups.

---

[46] Lorenzo Franceschi-Bicchierai, "European Cops Shut Down Crypto Mixing Website That Helped Launder 1.3B Euros," Tech Crunch, December 1, 2025, at https://techcrunch.com/2025/12/01/european-cops-shut-down-crypto-mixing-website-that-helped-launder-1-3-billion-euros/ (Accessed February 18, 2026).

[47] "Concealment of Beneficial Ownership," FATF and Egmont Group, July 2018, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership.pdf (Accessed February 18, 2026), p. 82, note 70.

[48] Daria Alexe, ''Agentic Smurfing': How AI-Autonomous Micro-Laundering is Outpacing Traditional Terrorist Financing Detection,' *Global Network*, January 28, 2026, at https://gnet-research.org/2026/01/28/agentic-smurfing-how-ai-autonomous-micro-laundering-is-outpacing-traditional-terrorist-financing-detection/#:~:text=By%20Daria%20Alexe,platforms%20and%20regulatory%20authorities.%E2%80%8B (Accessed February 18, 2026).

This input suggests the coming together of terrorist financing needs and AI tech-enabled money laundering techniques. It reinforces the relevance of AI as an enabler that makes existing systems of terrorist financing and money laundering more efficient and creative, making it a challenge for law enforcement agencies.

Asha Hemrajani notes that terrorists can exploit crypto currency through a more efficient trading mechanism and its theft. 'AI-powered cryptocurrency bots can detect patterns and price trends to "offer predictions on target and breakout prices, alongside confidence levels, thus significantly enhancing decision-making processes", which is especially useful for markets with high volatility'.[49]

The international opinion on virtual assets remains divided. Countries are evaluating options regarding mainstreaming virtual currencies and their potential impact on respective economies. This has led to vastly varying approaches and predictable gaps across jurisdictions, leading to being vulnerable for exploitation by criminals, launderers and terrorist organisations alike.

This threat is amplified when AI compounds the regulatory framework's existing weaknesses. Machine learning tools are best suited to analyse the crypto exchange's relatively nascent trading experience. AI can create bots that undertake this activity, helping predict profitable options. AI tools can also be used for theft on crypto exchanges, an activity that has already been reported. 'Besides the AI used to manipulate the cryptocurrency space for financial profit, terrorists could make use of AI to facilitate the theft of cryptocurrencies from "hot wallets"'.[50]

---

[49] Asha Hemrajani, "The Use of AI in Terrorism," RSIS, August 26, 2024, at https://rsis.edu.sg/rsis-publication/rsis/the-use-of-ai-in-terrorism/#:~:text=Terrorists%20can%20leverage%20this%20ability%20to%20make%20more%20lucrative%20cryptocurrency%20trades%2C%20increasing%20their%20profits (Accessed March 18, 2026).

[50] "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes," United Nations Office of Counter-Terrorism and United Nations Interregional Crime and Justice Research Institute, 2021, at https://www.un.org/counterterrorism/sites/default/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf (Accessed February 3, 2026), p. 39.

Assessment of Case Studies

AI is improving existing techniques for generating proceeds of crime and laundering assets. From vishing fraud to fooling the existing KYC norms, and from identifying vulnerable targets to spreading misinformation, AI can make automated systems intelligent. This value add is evident from the techniques applied and their illustrative examples cited above.

When these activities are more specifically related to money laundering, each of the techniques—vishing, KYC fraud and exploiting crypto currency—become relevant to the linkage between crime and money laundering. The underlying capability of AI systems enables them to simulate legitimate financial flows and patterns. Furthermore, this ability is reinforced by automation, rather than by agents executing each transaction to *place* and *layer* small amounts of money as part of the larger money-laundering process.

The placement of money into the financial system by any individual or institution is validated by regulatory procedures such as the KYC norms. This includes confirming an individual's identity through an authenticating system such as biometric checks, facial identification and documentary evidence. Advanced AI systems have been successfully employed to create fake biometric or facial identity and documents. In 2024, an employee of a multinational company in Hong Kong paid $25 million to scammers on a video call posing as company employees, including as its chief financial officer.[51] This example is indicative of AI's ability to create fake yet believable identities that can be used to authenticate and validate systemic requirements.

In contrast, AI is also employed to counter fake identities by digitally validating inputs through systemic checks and balances. In 2021, Revealense was founded with the assistance of experts in varied fields such as

---

[51] Heather Chen and Kathleen Magramo, 'Finance Worker Pays Out $25 Million after Video Call with Deepfake 'Chief Financial Officer",' *CNN World*, February 4, 2024, at https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk (Accessed February 27, 2026).

psychology, neuropsychology, nonverbal and cultural-pattern specialists to analyse voice and video communication to decipher and decode AI-generated content.[52] This is not the only initiative, several others followed. However, the rate and pace of change in AI tools suggest that criminals and government agencies will remain engaged in this competitive desire to seek an advantage over the other. By correlation, this is likely to keep the threat emanating from the exploitation of AI-based technology alive in the foreseeable future.

The aforementioned case studies illustrate the exploitation of AI in different ways. As diverse as these might seem, given the distinct means of adoption, the underlying exploitation of AI's capabilities becomes evident. In each case, an attempt to offset the limitations that terrorist organisations and criminal groups faced through AI's inherent capability comes to the fore. This desire to eliminate existing limitations and create new opportunities involves AI's ability to 'understand' the financial system's functioning, 'monitor' it and 'identify' trends to 'exploit' its weaknesses, making it an ideal tool for sidestepping the existing security safeguards. This is achieved by accurately recreating 'reliability', 'relevance', 'replication', 'repeatability' and 'reinforcing' weaknesses. AI's distinct characteristics lend themselves to augmenting the capabilities of terrorist organisations and money launderers.

The FATF's assessment of potential vulnerabilities reinforces emerging money laundering and terrorist financing trends. It speaks of 'discriminative/predictive models' that can detect patterns and assist criminals bypass these automated systems by selecting alternative options. Generative AI has fast developed the ability of creating content that is becoming difficult to distinguish from the original. This facilitates deceptive actions to establish identity and authenticity for exploiting a financial system. Finally, AI Agents

---

[52] Gil Press, 'Detecting Deepfakes: Fighting AI with AI,' *Forbes*, August 6, 2024, at https://www.forbes.com/sites/gilpress/2024/08/06/detecting-deepfakes-fighting-ai-with-ai/ (Accessed March 2, 2026).

create a level of automation and decentralisation that brings greater efficiency to financial manipulation of a system.[53]

The process of money laundering is closely linked with predicate offences, which generate proceeds of crime. AI has created alternative and advanced means of undertaking this process. AI's ability to create fake identities, documents and automate transactions is well-suited to enhancing criminals' capacity to launder funds.

Terrorist organisations face the threat of law enforcement agencies creating and following digital trails. 'Follow the money' is an established practice for assisting investigations. AI assists terrorist groups in hiding their identity, automating processes with the least intervention and creating fake documents and identities to facilitate their operations.

AI as an Enabler

The aforementioned examples might suggest that the role of AI is likely to be limited to the exploitation of technology by lawbreakers through activities such as money laundering and terrorist financing. AI's potential, its characteristics and its control by a few also suggest that states and corporate organisations, working in consultation with governments, will seek to create a capability differential against criminals and terrorists. The state's ability to take a deeper dive, both through direct control over algorithms and autonomous agents, will empower more than constrain if the technology is not completely democratised.

As an illustration, the US Treasury's Financial Crimes Enforcement Network (FinCEN) released guidance to assist identify frauds and deepfake content using GenAI. It not only explains typologies associated with the crime,

---

[53] "Horizon Scan: Artificial Intelligence and Deepfakes – Impacts on Money Laundering, Terrorist Financing and Proliferation Financing," FATF, at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Horizon%20Scan%20AI%20and%20Deepfakes.pdf.coredownload.inline.pdf (Accessed April 1, 2026), p. 10.

but also 'provides red flag indicators to assist with identifying and reporting related suspicious activity'.[54]

In yet another case, the FATF reports that a financial institution used AI to identify suspicious transactions based on 'heavy volumes, timings, and amounts'. AI was able to detect anomalies in the documents provided by detecting 'that the background elements of the photo of the company's storefront and interior bore a strong resemblance to a counterfeit document from a customer previously identified as high risk'.[55]

Fake Currency

The global experience in general and India's experience in particular indicates a gradual increase in the sophistication of techniques by state and non-state actors to create counterfeit currency. This leads to a systematic process of analysing fake currency for all its elements of production from the type of paper used, inks, printing technologies, creating fake security measures, colour gradations and texture. Based on this in-depth assessment, mechanical, electronic and physical guidelines are disseminated to identify fake notes. This is a time consuming and laborious procedure that comes with its own time lag between detection, dissemination and implementation of safety measures. Additionally, the implementation of these measures could remain uneven given the sheer logistics of the process involved. Further, there are cost implications for the provision of electronic equipment and training, especially for small private businesses.

It is in light of these challenges that AI-based solutions can prove to be useful for a larger section of the financial and business community. Zar Ni Aung, Sa Kaung Min Htet and Hlaing Htake Khaung Tin indicate the approach for the use of AI and machine learning to identify fake currencies.

---

[54] "FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions," U.S. Treasury Financial Crimes Enforcement Network, November 13, 2024, at https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf (Accessed February 5, 2026).

[55] "Artificial Intelligence and Deepfakes: Impacts on Money Laundering, Terrorist Financing and Proliferation Financing,"no.53 (Accessed February 5, 2026).

Based on a large dataset, AI-based solutions can be updated, disseminated and shared with ease. Their accuracy levels are much higher than traditional methods like physical inspection and ultraviolet verification. The authors place this variation at 75 per cent for visual inspection and 97 per cent in the case of Convolutional Neural Networks (CNNs).[56] Presently, the use of AI also comes with the challenge of costs for creating the dataset and limited computational resources. This indicates the potential use of a hybrid method to exploit the best of both options depending on the availability of resources and access to AI-based technology tools.

AI-powered Forensic Tools

AI's computational and analytical power gives it the natural ability to emerge as a powerful tool for law enforcement. AI can analyse datasets to discern patterns and equally dissimilarities and deviations from this as well. This gives it the ability to detect and raise red flags during different stages of the money laundering process.

Amongst the multiple tasks that can be done better with AI is the ability to monitor transactions for anomalies. 'AI algorithms analyse vast volumes of transaction data in real-time, identifying suspicious patterns like unusual wire transfers, large cash transactions and activities deviating from usual customer behaviour'.[57] Similar automation can be brought in for customer due diligence (CDD). AI can create patterns based on customer financial behaviour to help detect better risk assessment and identification of threats

---

[56] Tun Zar Ni Aung, Sa Kaung Min Htet and Hliang Htake Khaung Tin 'Artificial Intelligence and Machine Learning Approaches for Identifying Fake Currency: An Analysis,' *AVE Trends in Intelligent Computer Letters*, December 2025, 1 (3), 161–169, at https://www.researchgate.net/publication/400668386_Artificial_Intelligence_and_Machine_Learning_Approaches_for_Identifying_Fake_Currency_A_Review/references (Accessed March 24, 2026), p. 164.

[57] "AI-Powered Anti-Money Laundering (AML) Solutions: Leveraging AI and Machine Learning to Detect and Prevent Suspicious Transactions in Real-Time," Infosys BPM, June 26, 2025, at https://www.infosysbpm.com/blogs/financial-crime-compliance/ai-powered-anti-money-laundering-solutions.html (Accessed March 27, 2026).

to allow greater focus and attention. AI is also a useful tool for financial forensics to facilitate fast and efficient investigation of cases.[58]

AI tools can work unsupervised through raw data to detect patterns and linkages that can raise behavioural anomalies. These tools point out deviations in actions either from existing rules or past customer records.

AI-based Anti-Money Laundering (AML) Controls

Existing financial systems are based on customer due diligence and KYC guidelines that are driven by customers providing their information and data. The reliability of this information is based on customer inputs and authenticity of documentary evidence made available. Banks attempt to analyse customer behaviour based on transactions, including attempts to break down larger amounts into smaller ones to hide the scale and scope of the transactions. Attempts are also made to use jurisdictions that have weaker controls.[59]

Banks on their part attempt to balance compliance with efficiency. There is a simultaneous need for raising red flags based on suspicious transactions while ensuring that it does not overburden the system, which may lead to rising costs and delays in the execution of procedures. AI is able to limit the instances of false red flags and simultaneously hasten the execution process, reducing the load on the staff that would have otherwise been involved in a time-consuming process of checks and balances.

Preventive Investigation—Dark Web

AI can also serve as an enabler to constrain the exploitation of technological advancements by criminals and terrorist groups. Recent years have seen

---

[58] "AI-Powered Anti-Money Laundering (AML) Solutions: Leveraging AI and Machine Learning to Detect and Prevent Suspicious Transactions in Real-Time," no. 57.

[59] Aaron Ricadela, "Anti-Money Laundering AI Explained," Oracle India, August 28, 2024, at https://www.oracle.com/in/financial-services/aml-ai/ (Accessed April 2, 2026).

the exploitation of cyber spaces characterised by restricted accessibility. The dark web has been one such example exploited by terrorist organisations for terrorist financing.

Ying Zhang et al. argue that AI can be used to change the existing 'passive response' to 'proactive early warning'. 'AI systems based on natural language processing (NLP) technology can not only identify common terrorism-related keywords but also understand their synonyms, near-synonyms, implied semantics and related context. Additionally, AI-driven web crawlers have more powerful extraction capabilities. They simulate human browsing behavior and automatically adjust the extraction frequency and scope based on preset rules and strategies to avoid being intercepted by the target website's anti-crawling mechanism'.[60] This is ideal for scouring the dark web for sensitive data, verifying, collating and structuring it for systematic evaluation.

In India, the importance of AI to counter terrorism is gaining relevance. The Ministry of Home Affairs has confirmed the use of 'AI-based tools to monitor the dark web, scam websites and fraud networks for tracking cybercrime discussions, phishing campaigns and suspicious financial transactions'.[61]

Digital Currencies

The proliferation of digital currencies has opened a vast alternate space for the manipulation of currencies and transferring value. The use of

---

[60] Ying Zhang, X. Zhang, N. Wei, Y. Luo, et al. "Research on the Development and Utilization of AI-Driven Open-Source Intelligence on Terrorism", in Siarry, P., Cheung, S.K.S., Jabbar, M.A., Li, X. (eds), *Proceedings of the 2024 International Conference on Wireless Communications, Networking and Applications*, WCNA 2024, Lecture Notes in Electrical Engineering, vol 1550. Springer, Singapore, at https://link.springer.com/chapter/10.1007/978-981-95-6946-5_43#citeas (Accessed April 2, 2026), p. 424.

[61] Mukesh Ranjan, 'MHA Employs AI Tools for Dark Web Monitoring,' *The New Indian Express*, March 31, 2026, at https://www.newindianexpress.com/nation/2026/Mar/31/mha-employs-ai-tools-for-dark-web-monitoring (Accessed April 2, 2026).

stablecoins has assisted in the illicit flow of money, fuelling terrorist finance and money laundering. AI is increasingly being used to recognise patterns to reinforce human intervention by providing scale. 'The effect on investigations is simple: machines take on the role of scanning and sorting, allowing human investigators to focus on context, judgement, and strategy'.[62]

Policy Options to Counter Money Laundering and Terrorist Financing

An overview of AI as a technology, characteristics of money laundering and terrorist financing and the likely impact of AI on these threats reinforce the emerging challenges posed. Despite AI being an evolving technology, its growing influence is evident from the case studies discussed. It is seen that terrorist organisations and criminal groups are leveraging AI's unique capabilities to improve the existing models of raising and cleaning dirty money. It can be argued that any attempt to formulate a strategic framework to combat the role of AI in money laundering and terrorist financing may be premature. On the contrary, any delay in such an endeavour could create and reinforce the existing opportunities that are already available to terrorist and criminal organisations. This suggests a periodic review of the strategic framework to evaluate the threats emerging from the use of AI on money laundering and terrorist financing.

The importance and relevance of taking an 'AI initiative' becomes imperative against non-state actors, terrorist organisations and criminal groups, especially when the advances being made by the technology are rapid and any lag in implementing guidelines can have severe effects. This is reinforced by a decision by Anthropic with its latest AI iteration called Mythos. This new generation update can locate vulnerabilities in existing software systems

---

[62] Adam Rousselle, "Closing the Enforcement Gap: AI, Illicit Liquidity, and the Next Phase of Counter-Terrorist Finance," Global Network on Extremism and Technology, October 24, 2025, at https://gnet-research.org/2025/10/24/closing-the-enforcement-gap-ai-illicit-liquidity-and-the-next-phase-of-counter-terrorist-finance/ (Accessed April 22, 2026).

that humans are unable to detect despite years of testing. This implies that if such a software is made available to the wider audience, its misuse cannot be obviated. In this case, Anthropic has decided to stall the open release of the model and limit access to a few major companies and governments in an attempt to detect vulnerabilities in systems and harden them to future attacks and exploitation.[63]

AI advancements of the Mythos kind could open new avenues in the cat-and-mouse game between law enforcement agencies and law breakers. This suggests the need for agencies to firstly, remain aware and informed of the newest developments in the industry and their implications on security. Secondly, AI is progressing at a pace that is unprecedented in any previous technological domain. This implies not only keeping pace with frequent upgrades and advancements, but also adopting newer models that allow government agencies to remain ahead of AI's potential exploitation for breaching financial systems and tools. This could include close tie-ups with industry leaders and partnerships with companies that remain at the cutting edge of AI research and development. Thirdly, existing procurement cycles that have a long gestation period cannot work in an environment wherein new updates will come midway into the procurement procedure. Alternative options like long-term contracts that include automatic upgrades to newer systems may provide a better option for ensuring that critical systems remain at the forefront of AI advancement.

The fast-evolving impact of AI to support terrorist financing and money laundering is throwing up a growing variety of case studies both at the international level and within India. It is important to collate these case studies through a close private–public partnership to develop emerging typologies. The state initiative to share the threat emanating from digital arrests is a useful example that can be emulated to spread awareness and limit the challenges associated with AI.

---

[63] Kevin Roose, 'Anthropic Claims its New AI Model, Mythos is a Cyber Security 'Reckoning',' *New York Times*, April 7, 2026, at https://www.nytimes.com/2026/04/07/technology/anthropic-claims-its-new-ai-model-mythos-is-a-cybersecurity-reckoning.html (Accessed April 9, 2026).

In this regard, the impact of advancements represented by software like Mythos is not lost on the Indian government. It has asked the concerned departments to study its implications — a step in the right direction.[64]

The Indian government carried out a detailed risk assessment for money laundering and terrorist finance preceding the 2024 mutual evaluation.[65] The FATF duly acknowledged Indian authorities having a 'strong understanding of ML (money laundering) risks' and a 'sophisticated understanding of TF (terrorist financing) risks as reflected in the 2022 NRA … Consistent with the risks identified in the NRA, India has implemented a broad range of policy, operational and legislative measures to mitigate these risks'.[66]

The FATF notes several areas that merit greater attention. However, understandably, the impact of AI in risk assessment and strategy development remains limited to 'analysis of suspicious transactions and case creation'.[67] As highlighted earlier, the fast-paced development, impact of AI and its adoption by terrorist groups and criminal organisations demands an urgent updating of the existing risk assessment, particularly in relation to the impact of the technology. This includes the percentage

---

64 Aroon Deep, 'IT industry, Govt. Examine Cybersecurity Implications of Anthropic's Mythos Model,' *The Hindu*, April 9, 2026, at https://www.thehindu.com/sci-tech/technology/it-industry-govt-examine-cybersecurity-implications-of-anthropics-mythos-model/article70842640.ece (Accessed April 13, 2026).

65 The Financial Action Task Force, a multinational body undertakes country specific evaluation to analyse the 'implementation and effectiveness of measures to combat money laundering, terrorist financing and proliferation financing'. This is a thorough assessment of respective countries indicating the adequacy of existing FATF guidelines and areas that need improvement.

66 "Anti-money laundering and counter-terrorist financing measures: Mutual Evaluation Report India," Financial Action Task Force and Asia Pacific Group, September 2024, at https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/India-MER-2024.pdf.coredownload.inline.pdf (Accessed April 13, 2026), p. 5. Explanatory text in parenthesis by author.

growth in AI usage, which, in turn, will govern the allocation of resources that need to be apportioned for blocking the threat.

It is equally relevant for open-source strategy documents like the National Counter-Terrorism and Policy document PRAHAAR to underline the emerging challenges stemming from AI-based exploitation of technology by terrorist groups.[68] The context and scope of PRAHAAR does not allow a detailed scrutiny of specific threats. However, it can help stakeholders by providing access to specialised sources accessible for specific guidance on the threats emanating due to the impact of AI, emerging typologies and suggested measures to improve responses.

The private sector-led AI initiatives and development of security tools are likely to find faster introduction within the commercial environment including the financial sector. The potential grave repercussions of AI-based threats to these systems will witness early adoption, especially when compared to state structures. Studies already suggest that AI-based systems are improving security and reducing costs.[69]

The security and profit-driven initiatives will be led by major financial institutions. However, the inherent interconnectivity of the financial structures implies that it is the more vulnerable, less profitable and smaller institutions like cooperative banks that could become potential targets. A similar challenge can be faced by Designated Non-Financial Businesses and Professions (DNFBPs), an area that has already been flagged by the FATF

---

67 Ibid, p. 73.

68 "National Counter Terrorism Policy and Strategy," Ministry of Home Affairs, at https://www.mha.gov.in/sites/default/files/PRAHAAREng_23022026.pdf (Accessed April 22, 2026).

69 Dr Kostis Chlouverakis, "How Artificial Intelligence Is Reshaping the Financial Services Industry," EY, April 26, 2024, at https://www.ey.com/en_gr/insights/financial-services/how-artificial-intelligence-is-reshaping-the-financial-services-industry#:~:text=%5B1%5D%20For%20instance%2C%20JPMC,%5B4%5D (Accessed April 13, 2026).

as a potential for improvement.[70] These institutions do not have as well-instituted processes and procedures for establishing and reporting violations of laid down guidelines. This emerges from the varied capacities of businesses that form a part of the DNFBPs and challenges associated with implementing the existing guidance across the board for a diverse set of entities.

India's mutual evaluation report mentions the counter-terrorism strategy. This document also includes the 2023 Action Plan for countering terrorist finance and money laundering strategies based on the 2022 National Risk Assessment.[71] Despite successfully strengthening the national effort, the strategy 'does not adequately focus on guiding the improvement of resources and expertise of the State police to be able to conduct TF investigations to support national CT strategies and investigations'.[72] This limitation is an indicator of gaps within the wider national counter-terrorism structure and processes. When this is related to the challenges associated with the emergence of AI as a threat, these very gaps can become potential lacunae for an effective strategy for fighting AI's innate ability to exploit weaknesses in structures and procedures.

India's 2023 strategy document focusses on six areas as part of the 2023 Action Plan. These include, prevention, detection, investigations, capacity building, cooperation and outreach. The FATF felt that the action plan 'does not identify key focus areas where resources are more critical than in others'.[73] Further, it does not focus on the emerging influence of AI on existing or developing challenges. The action plan is designed for a five-year period from 2023–2028.[74] AI's emerging threats and challenges suggest the need for a mid-term evaluation and reassessment of the action plan.

---

70 "Anti-money laundering and counter-terrorist financing measures: Mutual Evaluation Report India," no. 66, p. 115.

71 Ibid, p. 125.

72 Ibid, p. 126.

73 Ibid, p. 50.

74 Ibid, p. 240.

This could be undertaken by a task force that not only gives suggestions for incorporating AI-related inputs, but also monitors its fast-paced evolution and emerging areas of exploitation by terrorist groups and criminal organisations.

Conclusion

AI is here to stay, as are the threats emerging from terrorist financing and money laundering. Past experience suggests that states and multinational organisations facing these challenges have had to play catch up with terrorist groups and criminal organisations remaining ahead of the curve. Despite the advantage of a nimbler adversary, states did succeed in erecting barriers through structural changes, establishment of processes and procedures that improved the effectiveness of intelligence and enforcement agencies. Over time, there was improvement in international cooperation and coordination with agencies. While not perfect, states did eventually limit the manoeuvre space available to exploit the financial system and terrorist's funding capacity.

The emergence of AI changes the existing paradigm significantly. The gap between terrorists and criminals at one end and state agencies on the other had been reduced in the past. AI has provided an opportunity to reopen it yet again. This paper reinforces AI's significant role in the ability of law breakers and law enforcers to pursue their exclusive objectives. For now, AI will enhance the capability of terrorist organisations to employ crime to raise funds and shield themselves from intelligence organisations. Similarly, criminal groups will benefit from AI's capabilities to commit crime and place, layer and integrate their ill-gotten wealth.

Simultaneously, the paper highlights the initiatives being taken by governments and companies that are closely associated with them to reduce the cost of due diligence and concurrently improve effectiveness by improving the ability to study anomalies in patterns and trends, which were until now beyond the capability of existing systems.

It is also evident that an interconnected world allows terrorist groups and criminals to exploit the weakest or attempt to sidestep stronger guardrails. This will remain a challenge in an emerging AI world where resources and capacity building will likely remain uneven across nationalities. Conversely,

terrorists and profiteering money laundering operations will find ways and means to navigate the cost–benefit balance to their advantage.

AI presents challenges that raise uncomfortable questions regarding free and democratic accessibility for all. While AI will benefit those with limited resources to improve efficiency, it may also provide access to others keen on exploiting it for criminal purposes. The converse is equally perplexing. Limiting access will strengthen governments but deny others of cutting-edge benefits.

The answers, as difficult as these might be, are best deliberated upon through a collective effort that attempts to bridge rather than divide. The FATF is a fine example of such an endeavour in the past. Even as states strive to utilise AI and limit its adverse impact, the onus of building a cohesive and collective effort must come from the FATF. The organisation is funded adequately, supported widely and has proven capability to create consensus despite obvious geopolitical pulls and pressures. The advent of AI will probably test individual nations and collective endeavours alike to ensure that technology remains a blessing and does not emerge as a curse in the future.

Terrorist financing and money laundering remain serious international challenges. These seemingly distinct threats are interlinked and feed off each other, thereby reinforcing the challenge they pose individually. The advent of Artificial Intelligence (AI) is revolutionising every field of human endeavour. Early indicators suggest that terrorist financing and money laundering have also been impacted by it. AI functions as a catalyst. It may not change the counters of the threat, yet, it has the ability to enhance it if suitable measures are not instituted by organisations, countries and the wider international community. This paper briefly describes the characteristics and capability of AI as a technology. It explains the concept of terrorist financing and money laundering to explore the linkage between the two. It analyses case studies of AI's exploitation by terrorist organisations and criminals and its simultaneous employment by intelligence and law enforcement agencies attempting to remain ahead of the technological curve. Finally, the paper suggests policy options to improve the adoption and implementation of AI to limit the threat from terrorist financing and money laundering.

Col Vivek Chadha (Retd), served in the Indian Army for 22 years prior to taking premature retirement to pursue research. He joined the Manohar Parrikar Institute for Defence Studies and Analyses in November 2011 and is a Senior Fellow at the Military Affairs Centre. Colonel Chadha's areas of research are counter terrorism, military and indigenous studies. He was part of the team that wrote the Indian Army's first *Sub Conventional Doctrine* in 2006. His single author books on counter terrorism include *Low Intensity Conflicts in India: An Analysis; Lifeblood of Terrorism: Countering Terrorism Finance and Company Commander in Low Intensity Conflicts.* His single author books on military subjects include, *Even if Ain't Broke Yet, Do Fix It: Enhancing Effectiveness Through Military Change; Kargil: Past Perfect: Future Uncertain; CDS and Beyond: Integration of the Indian Armed Forces and Mahabharata's Strategic Insights: Navigating the Dharmic Compass*.

His current area of research focusses on the strategic lessons of the Mahabharata. He is the Managing Editor of the *Journal of Defence Studies*.

MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Manohar Parrikar Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
Website: http://www.idsa.in