Available at https://journalenrichment.com/index.php/jr/

Enrichment: Journal of Multidisciplinary Research and Development

The Use of Advanced Technology (Artificial Intelligence & Machine Learning) To Prevent the Funding of Terrorism in Indonesia

Rafi Wisesa[1], Sapto Priyanto[2], Muhamad Syauqillah[3], Athor Subroto[4]

SKSG-Universitas Indonesia, Indonesia

*Email: rafi.wisesa@gmail.com

ARTICLE INFO

Keywords: *Terrorist Financing, Artificial Intelligence, Machine Learning, Regulatory Challenges.*

ABSTRACT

The financing of terrorism in Indonesia, has become increasingly complex due to the involvement of various domestic terrorist organizations. These groups obtain funds through diverse sources such as direct donations, membership fees, self-funding, and the misuse of non-profit organizations (NPOs). This study aims to explore and analyze the potential and challenges of utilizing advanced technologies, particularly Artificial Intelligence (AI) and Machine Learning (ML), in preventing terrorist financing in Indonesia. The research employs a qualitative descriptive approach, utilizing secondary data from FATF reports and related literature. The findings indicate that AI and ML can significantly enhance the detection and investigation of suspicious financial activities, provide real-time transaction monitoring, and facilitate inter-agency collaboration. However, challenges such as data limitations, regulatory complexity, high implementation costs, and data security and privacy issues must be addressed to fully leverage these technologies. This study provides recommendations for developing a supportive regulatory framework, enhancing inter-agency cooperation, and investing in better data infrastructure to effectively utilize AI and ML in combating terrorist financing.

INTRODUCTION

Terrorism financing is one of the biggest threats to global and national security. In Indonesia, this threat is increasingly complex with the involvement of various domestic terrorist organizations such as Darul Islam and Jemaah Islamiyah. They obtain funds through a variety of sources, including direct donations, membership dues, self-funding, and the abuse of non-profit organizations (NPOs). Recent trends show the increasing use of online banking, mobile payments, and social media platforms to raise funds and facilitate donations. In an effort to counter the financing of terrorism, advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) have become critical tools. AI and ML have the ability to sift through large amounts of transaction data to identify suspicious patterns and detect anomalies that traditional methods may have missed. Machine learning algorithms can be trained to flag suspicious transactions and aid in further investigations.

The application of AI and ML not only improves detection and investigation capabilities, but also enables real-time monitoring of transactions and facilitates collaboration between national and international institutions. AI-based platforms can provide collaborative analysis tools and real-time data sharing, which is crucial in combating this evolving threat. The 2023 Reciprocal Evaluation Report by the Financial Action Task Force (FATF) highlights Indonesia's efforts in combating the financing of terrorism and emphasizes the importance of adopting this advanced technology. However, the report also identifies some challenges in the implementation of targeted financial sanctions without delay as well as the need for a better understanding of risk across all sectors, including DNFBP (*Designated Non-Financial Businesses and Professions*) and VASP (*Virtual Asset Service Providers*).

Furthermore, in the report "Opportunities and Challenges of New Technologies for AML/CFT," it is explained that AI and ML can improve risk-based surveillance and help automate and improve the accuracy of risk assessments. This allows for more effective surveillance and timely intervention. However, there are challenges

that must be faced, including data limitations, regulatory complexity, implementation costs, and data security and privacy issues. By understanding these potentials and challenges, we can develop more effective strategies to leverage AI and ML technologies in preventing the financing of terrorism. This article aims to further explore the potential and challenges in the utilization of this advanced technology to prevent the financing of terrorism in Indonesia.

The purpose of this study is to explore and analyze the potential and challenges in the use of advanced technology, especially Artificial Intelligence (AI) and Machine Learning (ML), in an effort to prevent the financing of terrorism in Indonesia. This research seeks to provide in-depth insights into how AI and ML can be used to detect, analyze, and prevent terrorism financing activities more effectively than conventional methods. Additionally, the study aims to identify the barriers and challenges faced in the implementation of this technology, including data limitations, complex regulations, and issues related to data privacy and security.

The relevance of this research for Indonesia is significant, considering that the country is often a target and base of operations for various domestic and international terrorist organizations. With the ever-evolving and increasingly complex threat landscape, an innovative, technology-based approach is needed to address these issues. This research is expected to help the Indonesian government and related agencies to understand the full potential of AI and ML in combating terrorism financing, as well as provide practical recommendations to address existing challenges. Thus, the research not only contributes to the improvement of national security but also supports global efforts in countering terrorism.

METHOD

This research uses a qualitative descriptive approach with the aim of exploring and analyzing the potential and challenges in the use of advanced AI and Machine Learning (ML) technology to prevent terrorism financing. This approach was chosen because it allows researchers to deeply understand complex and dynamic phenomena, such as the financing of terrorism and the use of advanced technology in detecting and preventing it. The main source of data in this study is the Evaluation report from the Financial Action Task Force (FATF) in 2023, as well as various related literature relevant to this topic.

Data collection is carried out through several stages. First, the researcher collected secondary data from the FATF report that provided a comprehensive overview of the terrorism financing situation in Indonesia, including the methods and strategies used by terrorist organizations, as well as government policies and efforts to address this problem. In addition, literature studies that include books, scientific journals, articles, and other research reports are also used to gain a more comprehensive understanding of the utilization of AI and ML technologies in the context of security and finance. Data from these sources is analyzed to identify relevant patterns, trends, and findings.

The data analysis method used in this study involves content analysis and thematic analysis. Content analysis is carried out to identify and categorize relevant information from FATF reports and the literature that has been collected. This process involves data coding, which is the marking of important and relevant segments of the text to the research topic. After that, thematic analysis is carried out to identify the main themes that emerge from the encoded data. These themes are then further analyzed to draw conclusions about the potential and challenges in the use of AI and ML technologies to prevent the financing of terrorism. Through this methodological approach, this research is expected to provide in-depth and thorough insights into the topic being researched.

RESULTS AND DISCUSSION

Potential in the Utilization of AI and Machine Learning

Improved Detection and Investigation

Increased detection and investigation of terrorism financing through Artificial Intelligence (AI) and Machine Learning (ML) technologies offers great potential to strengthen national security. AI and ML have the unique ability to sift through large amounts of transaction data and identify suspicious patterns, which may not be detected by traditional methods. With its deep data analysis capabilities, it can process information in real-time and generate faster and more accurate insights into suspicious activity.

Machine learning algorithms, for example, can be trained to detect anomalies in transaction data. This anomaly can be a large number of transactions that occur in a short period of time, a sudden change in transaction patterns, or activity that is inconsistent with the user's historical profile. According to the theory of Big Data and predictive analytics, put forward by Davenport and Patil (2012), the ability to analyze data at scale and apply

predictive models is essential for detecting unusual behaviors and potential threats. Machine learning algorithms can use these techniques to continuously learn and adapt to new patterns, making the system more effective over time. In addition, the *social network theory* described by Wasserman and Faust (1994) shows how social network analysis can be used to identify relationships between entities involved in terrorism financing. AI and ML can leverage this network analysis to detect suspicious patterns of interactions, such as groups of transactions that often occur between seemingly unrelated accounts but have similar patterns to terrorism financing networks.

The study from King and Walker in The Palgrave Handbook of Criminal and Terrorism Financing Law also shows that the use of AI and ML in financial detection can assist law enforcement agencies in gathering stronger evidence and detailing complex financial flows used by terrorist organizations. For example, the technology can integrate data from various sources, including banking data, financial statements, and social media, to provide a complete picture of suspicious financial activity. This approach allows for more comprehensive and effective investigations[1]. Thus, increased detection and investigation through AI and ML not only improves efficiency and accuracy in identifying threats, but also strengthens investigative capabilities to disrupt and prevent terrorism financing. The implementation of this technology within the right regulatory framework will be very beneficial for national and international security.

Real-Time Transaction Monitoring

Real-time transaction monitoring is one of the main applications of AI and Machine Learning (ML) technology in the fight against terrorism financing. By using machine learning models, transactions can be monitored in real time, allowing for the detection of suspicious activity with greater speed and accuracy. Machine learning allows the system to continuously analyze incoming transaction data, recognize normal transaction patterns, and immediately flag any activity that deviates from those patterns.

Machine learning models can be trained using historical data to understand transaction patterns that are typically associated with terrorist activities or money laundering. For example, the model can recognize large transactions that are made repeatedly over a short period of time or the transfer of funds to and from high-risk locations. For example, the *Anomaly Detection Theory* described by Chandola, Banerjee, and Kumar (2009) shows that machine learning algorithms trained with rich and diverse data can be very effective in identifying unusual or suspicious activity. The algorithm is able to update its understanding of what is considered normal over time, so it can dynamically adapt to changes in transaction patterns.

The main advantage of real-time transaction monitoring is its ability to provide a quick response to potential threats. These systems can send immediate alerts to authorities or compliance departments at financial institutions, allowing them to take swift action before the funds can be used for malicious purposes. According to the Early Warning *Systems Theory* elaborated by McKee and Shepard (2007), early detection through real-time monitoring can greatly reduce risk by providing sufficient time for proactive intervention.

A study from King and Walker in The Palgrave Handbook of Criminal and Terrorism Financing Law emphasizes that the integration of AI and ML technologies in the financial system not only improves detection capabilities but also operational efficiency. Financial institutions can reduce reliance on time-consuming and error-prone manual checks, as well as improve accuracy in identifying suspicious transactions. Thus, real-time monitoring of transactions through machine learning not only speeds up the detection process but also improves accuracy in identifying suspicious activity. The implementation of this technology in the financial sector is an important step towards more effective and responsive financial supervision in an effort to prevent the financing of terrorism.

Collaboration and Information Sharing

Collaboration and information sharing are critical elements in global efforts to prevent the financing of terrorism, and AI-based technologies offer advanced solutions to facilitate this coordination. AI-based platforms can support cooperation between various national and international institutions by providing collaborative analysis tools and effective real-time data sharing facilities. This technology enables faster and more secure exchange of information, as well as improving the ability to respond to threats in a coordinated manner.

AI platforms can integrate data from various sources, such as financial statements, transaction data, and information from law enforcement agencies, to provide a comprehensive picture of suspicious financial activity. According to the *Information Network Theory* put forward by Castells, the ability to share information quickly and

efficiently in a wide network is essential for detecting and responding to dynamic and decentralized threats. Using AI, these institutions can identify suspicious patterns that may be hidden behind large and diverse volumes of data.

The collaborative analysis tools offered by AI-based platforms allow various parties to work together in analyzing data and devising handling strategies. Inter-Agency Cooperation *Theory* emphasizes the importance of cooperation between institutions in achieving complex common goals. In this context, AI can facilitate more effective collaboration by providing an analytics dashboard that can be accessed by all relevant parties, allowing them to view the same data simultaneously and contribute to the analysis.

Additionally, real-time data sharing facilitated by AI technology allows for faster responses to potential threats. For example, if a financial institution in one country detects suspicious activity, the information can be immediately shared with law enforcement agencies or other financial institutions in another country, allowing for quick preventive action. According to the Early Warning *Systems Theory* developed by McKee and Shepard (2007), real-time information sharing is essential for early detection and rapid response to threats, so that it can significantly reduce risks.

A study from King and Walker in The Palgrave Handbook of Criminal and Terrorism Financing Law also highlights that the use of AI platforms for collaboration and information sharing can increase transparency and accountability in efforts to counter the financing of terrorism. By facilitating open access to data and collaborative analysis, the technology helps ensure that all parties are on the same page and can work together effectively to achieve common goals. Thus, the collaboration and information sharing facilitated by AI-based platforms not only improves coordination between institutions but also accelerates response to the threat of terrorism financing. The implementation of this technology is an important step in building a more effective and coordinated global framework to counter the threat of terrorist financing.

Global Case Study: The Use of AI and ML in a Global Context to Prevent the Financing of Terrorism

The use of Artificial Intelligence (AI) and Machine Learning (ML) technologies to prevent the financing of terrorism has shown significant results in different countries. Around the world, law enforcement agencies and financial intelligence agencies have begun to adopt this technology to improve their ability to detect, analyze, and disrupt the flow of terrorism funds.

One prominent example is the application of AI and ML by the Financial Intelligence Unit (FIU) in several European countries. The FIU has used machine learning algorithms to sift through and analyze large financial transaction data, helping them identify suspicious patterns and anomalies that may indicate terrorism financing. For example, in the United Kingdom, the National Crime Agency (NCA) has integrated AI into their systems to monitor transactions and detect suspicious activity in real-time. This allows them to respond to threats quickly and efficiently, reducing the risk of terrorism financing.

In the United States, the Financial Crimes Enforcement Network (FinCEN) has used AI technology to improve anti-money laundering (AML) and counter-terrorism financing (CFT) efforts. AI assists FinCEN in identifying suspicious transactions and connecting the dots between various data sources to find evidence of terrorism financing. This approach allows them to detect and disrupt terrorism financing networks more effectively than traditional methods.

In addition, in the Middle East, the Saudi Arabian government has invested heavily in AI and ML technologies to counter the financing of terrorism. The Saudi Arabian Monetary Authority (SAMA) uses this technology to monitor financial transactions and analyze data from various financial institutions. Machine learning algorithms assist them in identifying suspicious transaction patterns and send alerts to authorities for further action.

The report "Opportunities and Challenges of New Technologies for AML/CFT" by the FATF (2021) highlights that AI and ML technologies can improve data quality and simplify regulatory reporting. In the context of terrorism financing, AI and ML can be used to monitor regulatory changes in real-time, identify data anomalies, and provide report visualizations that are easier for authorities to understand. This increases efficiency and accuracy in detecting and preventing terrorism financing.

This global case study shows that the application of AI and ML in preventing the financing of terrorism not only improves efficiency and accuracy in detecting threats but also enables a faster and coordinated response. With the ability to analyze data at scale and identify suspicious patterns, the technology provides powerful tools for law enforcement agencies and financial intelligence agencies around the world to more effectively counter terrorism financing.

Challenges in the Utilization of AI and Machine Learning

Data Limitations and Data Quality

One of the main challenges in the use of AI and Machine Learning (ML) technology to prevent terrorism financing is data limitations and data quality. This challenge arises due to the difficulty of obtaining the sufficient and high-quality data needed to train machine learning algorithms effectively. The data needed to detect patterns of terrorism financing is often scattered across different institutions and countries, and is in different formats, making it difficult to collect and standardize the data.

Difficulties in aggregating data from various sources are also a significant obstacle. Financial transaction data, intelligence reports, and other relevant information are usually spread across various institutions, both national and international. Each institution has its own systems and protocols for managing data, which can differ significantly from one another. In addition, data privacy and security issues add complexity to the sharing of information across borders. According to Data *Integration Theory*, the ability to effectively combine and analyze data from multiple sources is key to identifying suspicious patterns and detecting threats more accurately.

In the context of terrorism financing, incomplete or low-quality data can lead to inaccurate analysis results, which in turn can result in inappropriate actions by the authorities. The report "Opportunities and Challenges of New Technologies for AML/CFT" by the FATF (2021) highlights that these challenges require innovative solutions, such as the development of better frameworks and standards for data collection and exchange. AI and ML technologies have the potential to address some of these challenges by providing more advanced tools for data processing and analysis, but still require quality data to function properly. Thus, to maximize the potential of AI and ML in preventing the financing of terrorism, greater efforts are needed to ensure high data availability and quality. This includes the development of better data infrastructure, closer cooperation between institutions, and the implementation of consistent data standards. Only with adequate and high-quality data, AI and ML technologies can provide accurate results and assist in effectively detecting and preventing the financing of terrorism.

Regulatory Complexity

Regulatory complexity is a significant challenge in the use of AI and Machine Learning (ML) technologies to prevent the financing of terrorism. In Indonesia, the regulations governing the financing of terrorism and money laundering involve a variety of laws and regulations that are constantly evolving. Some of them include Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, Law Number 9 of 2013 concerning the Prevention and Eradication of Terrorism Financing Crimes, and Law Number 3 of 2011 concerning Fund Transfer. In addition, other relevant regulations include Law No. 15 of 2003 concerning the Stipulation of Government Regulations in Lieu of Law No. 1 of 2002 concerning the Eradication of Terrorism Crimes and Law No. 6 of 2006 concerning the Ratification of the International Convention for the Suppression of The Financing of Terrorism, 1999.

These regulations are designed to improve financial security and prevent illegal activities, but often their complexity can be a barrier to the implementation of advanced technologies. For example, rapid and frequent regulatory changes require constant updates to technological systems, which can be a heavy burden for financial institutions and law enforcement agencies. In addition, different regulations in different jurisdictions also add a layer of complexity, especially when agencies have to comply with different rules when operating in more than one country.

The report "Opportunities and Challenges of New Technologies for AML/CFT" by the FATF (2021) highlights the need for a regulatory framework that supports technological innovation. This framework should be flexible and adaptive, allowing institutions to effectively integrate AI and ML technologies while still complying with applicable regulations. In Indonesia, the establishment of policies that support the use of technology in AML/CFT is very important. Governments and relevant authorities need to work together to create a regulatory environment that not only prioritizes security but also encourages technological innovation.

The organizational structure in handling terrorism financing in Indonesia involves many government agencies, including the Coordinating Ministry for Political, Legal, and Security Affairs, the Indonesian National Police, the National Counter-Terrorism Agency (BNPT), the Ministry of Finance through the Directorate General of Customs and Excise, the Ministry of Law and Human Rights, the Ministry of Home Affairs, the Ministry of Social Affairs, the Ministry of Religious Affairs, the Ministry of Foreign Affairs, and the Financial Transaction Reporting and Analysis Center (PPATK). With so many agencies involved, a clear coordination mechanism is needed to avoid overlap and to ensure the effectiveness of monitoring the financing of terrorism. Thus, to overcome regulatory

complexity and facilitate the implementation of AI and ML technologies in preventing the financing of terrorism, a concerted effort is needed from governments, financial institutions, and relevant authorities to develop flexible and innovative regulatory frameworks. These measures will ensure that the technology can be applied effectively, improve efficiency and accuracy in detecting threats, and maintain compliance with applicable regulations.

Implementation and Maintenance Costs

One of the main challenges in utilizing AI and Machine Learning (ML) technology to prevent terrorism financing is the high initial cost of developing and implementing these systems. The development of AI and ML technologies requires significant investments in hardware and software infrastructure, workforce training, and integration with existing systems. According to a presentation by Fithriadi Muslim in the OJK webinar on the use of new technology in the prevention and detection of money laundering and terrorism financing crimes, the cost of adopting this advanced technology is very high and can be a barrier for many institutions.

The high cost of implementation also includes the procurement of advanced hardware, analytics software, and a robust cybersecurity system. In addition, the installation and configuration process of this technology requires competent experts, which also adds to operational costs. For example, the cost of training and developing the workforce so that they can effectively use and maintain these systems is significant.

In addition to the initial cost, the maintenance and renewal of AI and ML technologies also requires ongoing investment. This technology requires regular monitoring and maintenance to ensure that the system remains functioning optimally and is able to adapt to evolving threats. According to the 2021 FATF report, challenges in digital transformation in financial intelligence units (FIUs) and law enforcement agencies (LEAs) include difficulties in securing adequate financial resources for technology maintenance and updates. This maintenance includes software updates to address new security vulnerabilities, increased data storage capacity, and adjustments to AI algorithms to address new threat patterns.

In addition, maintenance costs also include the need for data cleaning and harmonization before analysis can be performed. This process is not only time-consuming but also requires additional resources which can result in delays in decision-making and reduce the effectiveness of the system. For example, in the OJK report, it is stated that one of the main challenges is the cost and resources required to clean and harmonize data before analysis, which can reduce operational efficiency. Thus, while AI and ML technologies offer many benefits in preventing terrorism financing, the high cost of implementation and maintenance is a significant challenge. Institutions looking to adopt this technology need to consider large initial investments and ongoing costs to ensure that the system remains effective and adaptive to evolving threats.

Data Security and Privacy

Data security and privacy are critical aspects in the use of AI and Machine Learning (ML) technologies to prevent terrorism financing. The implementation of this technology involves collecting, storing, and analyzing large amounts of data, which are often highly sensitive. Data security and privacy risks are the main challenges that must be carefully managed. In the context of terrorism financing, the data processed includes financial information, banking transactions, and personal data that, if falling into the wrong hands, can be misused for illegal purposes or to the detriment of the individuals and organizations involved.

According to the OJK report on the use of new technology in the prevention and detection of money laundering and terrorism financing crimes, the risk of data leakage and privacy violations is a real threat that must be dealt with seriously. AI and ML systems, while sophisticated, are not immune to cyberattacks. Skilled hackers can exploit vulnerabilities in these systems to access sensitive data, which can then be used for financial crimes or threaten national security.

To address these risks, strong security protocols are needed to protect sensitive data. These protocols should include data encryption, strict access controls, and ongoing security monitoring and auditing. Data encryption is an important step to ensure that sensitive information remains protected, even in the event of a security breach. Strict access control ensures that only authorized individuals can access sensitive data, reducing the risk of internal leaks.

Additionally, continuous security monitoring and auditing is key to quickly detecting and responding to security threats. Intrusion detection and threat analysis systems can help identify suspicious activity and provide early warnings before greater damage occurs. According to Cybersecurity Theory, a layered approach to protecting data and information technology systems is the most effective in dealing with a variety of complex and evolving cyber threats.

In the context of regulations, governments and related institutions also need to develop policies that support data protection and privacy. A clear and comprehensive regulatory framework should include guidelines for secure data management, including requirements for security incident reporting and recovery measures. In Indonesia, regulations such as Law Number 27 of 2022 concerning Personal Data Protection are an important foundation in regulating how personal data must be managed and protected in various sectors, including in efforts to prevent terrorism financing. Thus, ensuring data security and privacy is an important step in the implementation of AI and ML technologies to prevent terrorism financing. Through robust security protocols and comprehensive regulatory policies, institutions can reduce the risk of data leakage and protect individual privacy, while harnessing the full potential of these advanced technologies to enhance national security.

CONCLUSION

This research has explored the potential and challenges in the use of advanced technologies, especially Artificial Intelligence (AI) and Machine Learning (ML), to prevent terrorism financing in Indonesia. AI and ML technologies offer various advantages in the detection and investigation of terrorism financing, real-time transaction monitoring, and collaboration and information sharing between institutions. AI and ML have the ability to sift through large amounts of data, identify suspicious patterns, and enable rapid responses to potential threats. However, there are several significant challenges that need to be overcome to maximize the potential of this technology. Data limitations and data quality, regulatory complexity, high implementation and maintenance costs, and data security and privacy risks are the main barriers that must be carefully managed. The data required to train AI algorithms is often scattered across different institutions with different formats, while rapid regulatory changes can slow down the adoption of new technologies. Additionally, the high initial cost and maintenance of AI technology, as well as the risk of data leakage and privacy breaches, add a layer of complexity to the implementation of these technologies. To address these challenges, the study recommends the development of a regulatory framework that supports technological innovation, increased inter-agency cooperation, and investment in better data infrastructure. Governments and relevant authorities need to work together to create a flexible and adaptive regulatory environment, and ensure that robust security protocols are in place to protect sensitive data. Effective implementation of AI and ML technologies will greatly benefit national and international security, as well as support global efforts to counter the financing of terrorism.

REFERENCES

Castells, Manuel. “The Network Society Revisited.” *American Behavioral Scientist* 67, no. 7 (8 Juni 2023): 940–46. https://doi.org/10.1177/00027642221092803.

Chandola, Varun, Arindam Banerjee, dan Vipin Kumar. “Anomaly Detection.” Dalam *Encyclopedia of Machine Learning and Data Mining*, 1–15. Boston, MA: Springer US, 2016. https://doi.org/10.1007/978-1-4899-7502-7_912-1.

Davenport, T. H, dan D. J Patil. “Data Scientist: The Sexiest Job of the 21st Century. Harvard Business Review,” 2012.

FATF. “Opportunities And Challenges of New Technologies For AML/CF,” 2021.

Fernandez, Karen V. “Critically Reviewing Literature: A Tutorial for New Researchers.” *Australasian Marketing Journal* 27, no. 3 (27 Agustus 2019): 187–96. https://doi.org/10.1016/j.ausmj.2019.05.001.

Financial Action Task Force (FATF). “Mutual Evaluation Report: Indonesia 2023,” 2023.

Financial Crimes Enforcement Network (FinCEN). “Annual Report on Anti-Money Laundering and Counter-Terrorism Financing,” 2023.

Fithriadi Muslim. "The Utilization of New Technologies in Preventing and Detecting Money Laundering and Terrorism Financing Crimes." OJK Webinar Presentation, 2021.

Hafezi, Nasir, Karen Jones, dan Clive Walker. “Criminal Prosecutions for Terrorism Financing in the UK.” Dalam *The Palgrave Handbook of Criminal and Terrorism Financing Law*, 967–93. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-64498-1_40.

Handayani, Linah. "Efforts to prevent and eradicate terrorism financing crimes by the banking industry, intelligence information analysis at Bank X." University of Indonesia, 2017.

King, C, C Walker, dan J Gurulé. *The Palgrave handbook of criminal and terrorism financing law*. Cham: Palgrave Macmillan, 2018.

Krippendorff, Klaus. *Content Analysis: An Introduction to Its Methodology*. 2455 Teller Road, Thousand Oaks California 91320 : SAGE Publications, Inc., 2019. https://doi.org/10.4135/9781071878781.

Leuprecht, Christian, dan Olivier Walther. "Applying Social Network Analysis to Terrorist Financing." Dalam *The Palgrave Handbook of Criminal and Terrorism Financing Law*, 945–66. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-64498-1_39.

McKee, M, dan D Shepard. "Early Warning Systems and Disaster Risk Reduction." *United Nations International Strategy for Disaster Reduction*, 2007.

Moghaddam, F. M. "The staircase to terrorism: A psychological exploration." *American Psychologist* 60, no. 1 (2006): 161–69.

Mullin, M., dan D. M. Daley. "Working with the State: Exploring Interagency Collaboration within a Federalist System." *Journal of Public Administration Research and Theory* 20, no. 4 (1 Oktober 2010): 757–78. https://doi.org/10.1093/jopart/mup029.

National Crime Agency (NCA). "Using AI to Combat Financial Crimes," 2022.

Prasetya, A. Y, A Subroto, dan A. Nurish. "Model Pendanaan Terorisme Melalui Media Cryptocurrency." *Journal of Terrorism Studies* 3, no. 1 (30 Mei 2021). https://doi.org/10.7454/jts.v3i1.1030.

Safrudin, R. "Countering Terrorism in Indonesia through the Handling of Terrorism Financing: A Case Study of Al-Jamaah Al-Islamiyah (JI)." *Journal of Defense* 3, no. 1 (2013): 113–37.

Saudi Arabian Monetary Authority (SAMA). "AI and *Machine Learning* in Financial Surveillance," 2023.

Wasserman, S, dan K Faust. *Social Network Analysis: Methods and Applications*. Cambridge University Press, 1994.