8th International Scientific Conference ITEMA 2024 – Conference Proceedings
DOI: https://doi.org/10.31410/ITEMA.2024.473

# AI vs. Transnational Crime: Harnessing Intelligent Technologies to Disrupt Global Criminal Networks

Carlos Imbrosio Filho[1]

Received: November 4, 2024
Accepted: January 24, 2025
Published: June 2, 2025

**Keywords:**
Artificial intelligence;
Transnational organized crime;
Machine learning;
Predictive analytics;
Data privacy;
International cooperation;
Law enforcement;
Anti-money laundering (AML);
Cybersecurity;
Ethical concerns

**Abstract:** *Transnational organized crime (TOC) poses severe threats to global security, economies, and human rights, with criminal networks leveraging technology and financial systems to engage in activities like drug trafficking, money laundering, and cybercrime. Traditional methods struggle to keep pace, but artificial intelligence (AI) offers powerful tools to combat TOC. This article explores AI technologies such as machine learning and predictive analytics by enabling real-time data analysis, enhancing the detection of suspicious activities, and acting as threat prediction. Additionally, AI enhances international cooperation by facilitating intelligence sharing and improving anti-money laundering efforts. However, challenges like data privacy, ethical concerns, and AI bias must be addressed. Criminals also exploit AI, requiring law enforcement to stay ahead. A multi-stakeholder approach involving governments, law enforcement, and academia is crucial for developing ethical, effective AI solutions to disrupt and prosecute TOC.*

## 1. INTRODUCTION

Transnational organized crime (TOC) poses an increasing threat to global security, economic stability, and human rights. Criminal networks exploit technological advancements to enhance illicit activities such as drug trafficking, human trafficking, money laundering, and cybercrime, crossing borders and defying traditional law enforcement methods (Interpol, 2020). As these networks grow more complex and sophisticated, new tools are needed to counter them effectively. Artificial intelligence (AI) has emerged as a transformative tool in this fight, offering unprecedented capabilities for detecting, disrupting, and preventing TOC activities, even though criminals have also benefited from its advancements.

The present article explores the role of AI in combating TOC, focusing on how intelligent technologies such as machine learning, natural language processing (NLP), and predictive analytics are reshaping law enforcement strategies. It also discusses the challenges and ethical considerations of AI use, the importance of international cooperation, and how AI can help governments and institutions strengthen their anti-money laundering (AML) measures.

## 2. STATISTICAL EVIDENCE SUPPORTING AI IN COMBATING INTERNATIONAL CRIME

AI technologies such as machine learning, natural language processing (NLP), and predictive analytics allow law enforcement agencies to analyze vast amounts of data in real-time, detect

[1] University Autónoma de Lisboa, Rua de Santa Marta, 47, 1169-023, Lisbon, Portugal

suspicious activities, and predict emerging criminal trends. Interpol (2020) reports that AI-driven crime analytics could improve crime detection rates by as much as 30%, particularly in cybercrime, human trafficking, and financial crimes. This improvement is due to AI's ability to process large datasets and identify patterns that might be missed by human investigators, reducing the manual burden and increasing the accuracy of law enforcement responses.

A report deployed by Europol (2020) also provides compelling evidence of AI's role in disrupting criminal organizations, particularly in the areas of drug trafficking and financial crime. AI applications in data analysis, pattern recognition, and threat prediction have increased the efficiency of cross-border operations, with Europol estimating that AI can reduce investigation times by 40%, allowing faster responses to criminal activities. The use of AI in predictive policing, for instance, has allowed law enforcement agencies to preempt criminal activities by identifying and disrupting drug trafficking routes before criminal organizations can fully establish them.

Furthermore, the United Nations Office on Drugs and Crime (UNODC, 2021) highlights AI's potential in anti-money laundering (AML) efforts. AI technologies can analyze financial data at unprecedented scales, identifying suspicious patterns of financial transactions that are indicative of money laundering. According to the UNODC, the implementation of AI in AML systems has led to a 15–20% increase in the detection of illicit financial flows. In the case of human trafficking networks, AI has been instrumental in mapping criminal organizations by analyzing social media, online communication, and dark web activity, allowing law enforcement agencies to uncover hidden connections between actors and dismantle trafficking rings.

Besides all the above-mentioned reports, a study led by PwC (2020) emphasizes that the adoption of AI in law enforcement could lead to a reduction in international crime incidents by 15–20% by 2030 (enhacing potential), with significant impacts on border security, cybercrime prevention, and the disruption of illicit trade and smuggling networks. PwC's projections are based on the increasing use of AI-powered surveillance technologies, which can monitor and analyze vast amounts of digital communications, as well as the growing capabilities of AI-driven systems to predict and counter criminal strategies. These advancements enable a proactive approach to law enforcement, where AI is used not only to respond to crimes after they occur but also to prevent them from happening.

With that said, we definitely have set the grounds for the current research, where we will dedicate this first phase of the study to defining the main tools and mechanisms applicable to both police and judicial activity.

## 3. THE ROLE OF AI IN COMBATING TRANSNATIONAL ORGANIZED CRIME

### 3.1. Machine Learning and Predictive Analytics

AI technologies, particularly machine learning and predictive analytics, have revolutionized the detection and prevention of criminal activities. Machine learning algorithms can process vast amounts of data in real-time, identifying patterns and connections that human investigators might overlook. For example, AI systems are used to detect suspicious financial transactions, helping to uncover money laundering schemes and track the flow of funds through international networks (UNODC, 2021).

Predictive analytics further enhance law enforcement capabilities by forecasting emerging threats. These models analyze historical crime data and real-time intelligence to anticipate the movements of criminal organizations, allowing authorities to proactively target networks before they execute their operations. The effectiveness of these tools is already visible in cases where AI has been used to disrupt major drug trafficking and human trafficking rings (Europol, 2022).

Therefore, machine learning (ML) and predictive analytics have become critical tools in combating transnational crime by enhancing data processing, threat identification, and crime forecasting. Based on the Europol's report (Europol, 2020) data we were able to acknowledge that predictive analytics could improve law enforcement's ability to anticipate criminal activities, reducing response times by up to 40% and preventing crimes in high-risk areas by 25%. Moreover, machine learning algorithms would play a crucial role in helping the analysis of financial transactions, identifying and isolating up to 15% more suspicious activities linked to money laundering and illicit financial flows (UNODC, 2021). In addition to that, (Campedelli et al., 2020) highlighted that ML models can detect hidden patterns in crime networks, contributing to faster dismantling of organized crime rings, especially in drug and human trafficking. These statistics illustrate the growing significance of ML and predictive analytics in modern law enforcement strategies.

### 3.2. Enhancing International Cooperation and Intelligence Sharing

TOC networks operate across borders, making international cooperation essential for effective crime prevention. AI can facilitate the sharing of intelligence between nations, enhancing the ability of law enforcement agencies to track and dismantle cross-border criminal organizations. By leveraging AI-powered platforms, countries can share real-time data on suspicious transactions, cybercrime activities, and trafficking routes, improving coordination in global investigations (Interpol, 2020).

AI can also automate legal and regulatory compliance processes, helping governments and businesses detect and prevent illicit financial flows. This is particularly relevant in anti-money laundering efforts, where AI systems can identify potential violations and ensure that AML measures are implemented efficiently (PwC, 2020).

We take for granted that beyond the inellingence sharing as a *modus operandi*, another main aspect to validate is the international cooperation in police and judicial data sharing as a crucial *systematization* in addressing the complex and cross-border nature of transnational crime. Through initiatives such as Europol's *Secure Information Exchange Network Application (SIENA)* and Interpol's *I-24/7* communication system, law enforcement agencies are able to share intelligence in real-time, improving the coordination of investigations and the apprehension of criminals operating across jurisdictions. Judicial cooperation, facilitated by networks like Eurojust and the International Criminal Court (ICC), further enhances the ability to prosecute transnational criminals by harmonizing legal frameworks and ensuring the timely exchange of evidence. This collaboration has proven essential in tackling organized crime, human trafficking, and cybercrime, as it enables faster and more comprehensive responses to global criminal threats.

States need to prioritize cooperative public policies within their national police and judicial bodies when addressing transnational crime. By fostering collaboration and enhancing data sharing, national agencies can contribute valuable intelligence that accelerates the resolution of criminal cases and improves the accuracy of investigations. This cooperation not only strengthens law enforcement capabilities but also aligns efforts across borders, helping dismantle criminal networks that operate internationally. States that invest in such coordinated approaches ensure that their judicial and policing frameworks are better equipped to tackle complex crimes like human trafficking, drug smuggling, and cybercrime, which no single nation can effectively combat alone.

### 3.3. AI as a Tool for Crime Prediction and Threat Prevention

Predictive analytics, powered by AI, allows law enforcement agencies to anticipate criminal activities and proactively target criminal networks before they execute their operations. AI-driven models, trained on historical crime data and real-time intelligence inputs, can predict future hotspots of criminal activity and alert authorities to emerging threats. Interpol (2020) estimates that the use of predictive policing models could reduce crime rates in high-risk areas by up to 25%, particularly in regions with high levels of organized crime. This predictive capability is essential in identifying smuggling routes, criminal hideouts, and potential areas of conflict before they escalate into full-blown criminal operations.

For instance, Europol (2020) has utilized predictive analytics to anticipate trends in drug trafficking across Europe, allowing law enforcement to intervene in key smuggling corridors and reduce the influx of narcotics into major cities. Similarly, AI systems have been deployed to predict cyberattacks, allowing cybersecurity teams to reinforce defenses before criminal organizations can launch coordinated attacks on critical infrastructure.

## 4. CHALLENGES IN THE USE OF AI FOR LAW ENFORCEMENT

While AI offers significant advantages in combating TOC, several challenges must be addressed. One primary concern is regarding the issue of data privacy. The use of AI for surveillance and monitoring raises ethical questions about the balance between security and individual privacy rights. AI systems must operate within the bounds of national and international privacy laws to avoid infringing on civil liberties.

Another major concern is the potential for bias in AI algorithms. AI systems are only as good as the data they are trained on, and if that data is biased, the outcomes could lead to discriminatory practices in law enforcement. For example, biased algorithms might disproportionately target certain ethnic or social groups, leading to unjustified surveillance or arrests. As UNODC (2021) points out, addressing bias in AI is critical to ensuring that law enforcement practices remain fair and just.

Furthermore, as criminals increasingly adopt AI to enhance their operations—such as automating cyberattacks or using AI to evade law enforcement—governments must continuously innovate to stay ahead of these developments. Criminal organizations are already using AI to shield their activities, making it more difficult for authorities to track and disrupt them. Law enforcement agencies need to invest in advanced AI systems and training programs to ensure they can effectively counter the use of AI by criminal groups (Europol, 2020).

## 5. CHALLENGES AND ETHICAL CONSIDERATIONS

Despite the potential benefits, the use of AI in combating TOC raises several challenges. One key concern is data privacy, especially when AI is used for surveillance and monitoring purposes. Ensuring that AI systems respect individual privacy while maintaining security is a delicate balance that must be addressed through stringent data protection regulations (GDPR and Right to Privacy).

Another issue is the risk of bias in AI algorithms. If not properly managed, AI systems can produce biased outcomes, leading to false positives or disproportionately targeting certain groups (UNODC, 2021). This is particularly problematic in criminal justice, where biased algorithms could contribute to unfair treatment or wrongful accusations (inaccuracy factor).

Moreover, criminals are increasingly adopting AI to enhance their operations. From automating cyberattacks to using AI tools to evade detection, organized crime groups are leveraging the same technologies intended to stop them. Law enforcement agencies must stay ahead of these developments, investing in research and training to counter the use of AI by criminal networks (Europol, 2020).

Lastly, it is well-known that artificial intelligence (AI) and robotics are advancing rapidly in their ability to replicate human skills, with the potential to fundamentally reshape the workforce in the coming decades (LEAs and Police activity included). These technological developments could significantly impact the current role of education in fostering skill development and preparing students for future employment. As highlighted by the OECD's Artificial Intelligence and the Future of Skills initiative (OECD, 2021), the evolving nature of AI demands that educational systems adapt to ensure learners are equipped with the necessary skills to thrive in increasingly automated and technology-driven industries, but most important, on how to drive these technologies for the sake of society maintenance.

## 6. THE FUTURE OF AI IN COMBATING TOC

To maximize the effectiveness of AI in the fight against TOC, a comprehensive, multi-stakeholder approach is essential. Governments, law enforcement agencies, the private sector, and academia must collaborate to develop AI tools that are both effective and ethically sound. Investment in technological infrastructure, cross-border intelligence sharing, and training programs will be crucial in fully realizing AI's potential in combating TOC (Europol, 2022; OECD, 2021).

The benefits of AI in crime prevention are evident in its ability to process massive amounts of data, identify hidden connections, and predict emerging threats. However, without proper safeguards, AI could also exacerbate existing issues such as privacy violations, discrimination, and the misuse of technology by criminal groups.

## 7. FUTURE RESEARCH DIRECTIONS

A compelling future research direction for the current matter could focus on the promising integration of AI-driven predictive analytics and blockchain technologies to enhance international cooperation and transparency in disrupting illicit financial flows.

As a matter of fact, the technology advancement and all the cross tech-tools could offer our police forces the ability to apply advanced AI algorithms, such as machine learning and neural networks, to enhance predictive models for identifying and preventing emerging criminal threats, particularly in areas like human trafficking, drug smuggling, and cybercrime. This research could explore the use of AI to detect patterns of criminal behavior across borders in real-time, allowing law enforcement agencies to act proactively (currently entitled by scientists and theorists as *Predictive Analytics for Crime Prevention*).

Beyond that, a second scope of this insightful research would aim at how AI and blockchain can work together to trace and disrupt the financial networks that fuel global crime. By integrating AI with blockchain, authorities could create immutable and transparent records of financial transactions that allow for better monitoring of cross-border money laundering and the funding of criminal activities. This aspect could also highlight the challenges and benefits of anonymization in blockchain versus the need for transparency in law enforcement. The blockchain for transparency in financial transactions would depend directly on the state public will to reduce printed currencies in the market that could enhance the financial transactions monitoring, as well as the continuous oversight in cross activities such as private luxury goods purchases (*e.g.* yachties, sports cars, private aircraft, etc.), business agreements and real estate investments.

As a tradeoff agreement, civil society shall stay flexible and open for the sake of public security, as another challenge that will arise in dealing with all the AI ethics and privacy implications in law enforcement. In this sense, a future research direction could investigate the ethical implications of using AI to monitor criminal networks. Research must analyze how to balance the use of surveillance technologies with protecting civil liberties and privacy, ensuring AI systems are employed responsibly and do not lead to overreach by authorities (boundaries of public security over the right to privacy and GDPR).

Lastly, a research path might address the need for harmonizing international legal frameworks to govern the use of AI in transnational crime prevention. This could explore how different countries' legal systems can cooperate in creating standardized protocols and how AI can be adapted to respect jurisdictional boundaries while fostering global law enforcement cooperation.

## 8. CONCLUSION

Artificial intelligence offers a powerful tool in the global fight against transnational organized crime. By harnessing AI technologies such as machine learning, predictive analytics, and natural language processing, law enforcement agencies can enhance their ability to detect, disrupt, and prevent criminal activities. At the same time, the challenges and ethical considerations surrounding AI use must be carefully managed to ensure that these technologies are used responsibly and effectively.

The application of AI in law enforcement offers transformative potential in combating crime and enhancing public safety, but it must be carefully balanced with respect for privacy to uphold democratic values and fundamental rights. By implementing AI systems within clear legal frameworks that prioritize data protection, transparency, and accountability, law enforcement agencies can effectively utilize intelligent technologies without infringing on individual liberties. This balance is essential to maintain public trust and ensure that technological advancements serve to strengthen, rather than undermine, the principles of democracy and the protection of human rights.

International cooperation and collaboration between multiple sectors will be key to ensuring AI's success in combating TOC. With the right investments in technology, training, and regulation, AI has the potential to be a game-changer in the fight against global criminal networks.

## References

Campedelli, G. M., Favarin, S., & Malleson, N. (2020). Machine learning for spatial crime analysis: Review, critique, and future directions. *Computers, Environment and Urban Systems, 81*, 101477. https://doi.org/10.1016/j.compenvurbsys.2020.101477

Europol. (2020). How AI is revolutionizing law enforcement in the fight against organized crime. Europol.

Europol. (2022). AI innovation and security: Optimizing law enforcement operations against criminal organizations. European Union Agency for Law Enforcement Cooperation.

Europol. (2022). Data sharing and international cooperation in law enforcement. Europol.

Interpol. (2020). Artificial intelligence and law enforcement: The emerging AI frontier for global security. Interpol.

Interpol. (2020). International cooperation in police intelligence: I-24/7 global communication system. Interpol.

OECD. (2021). Artificial intelligence and the future of skills. https://www.oecd.org/en/about/projects/artificial-intelligence-and-future-of-skills.html

PwC. (2020). Global AI report: The economic impact of artificial intelligence on crime prevention. PricewaterhouseCoopers.

United Nations Office on Drugs and Crime (UNODC). (2021). Artificial intelligence and robotics: Challenges and opportunities for law enforcement. UNODC.

## Additional reading

Brantingham, P. J., & Brantingham, P. L. (2019). Predictive policing and artificial intelligence: Examining the promise and perils of data-driven law enforcement. *Journal of Criminal Justice, 62*, 34-45. https://doi.org/10.1016/j.jcrimjus.2019.04.002

Chawki, M. (2021). Artificial intelligence and big data: A blueprint for combating transnational organized crime and cybercrime. In M. Chawki (Ed.), Cybercrime, Digital Forensics, and Jurisdiction (pp. 125-145). Springer. https://doi.org/10.1007/978-3-319-76681-8_

Elmaghraby, A. S., & Losavio, M. M. (2021). Cybersecurity challenges in smart cities: Safety, security, and privacy. *Journal of Advanced Research, 5*(4), 491-497. https://doi.org/10.1016/j.jare.2019.01.011

Eurojust. (2021). Strengthening judicial cooperation across borders. Eurojust.

McQuade, S. C. (2019). Artificial intelligence and the law: Criminal justice applications for addressing cybercrime and transnational criminal organizations. *AI & Society, 34*(1), 67-79. https://doi.org/10.1007/s00146-018-0857-9