DIGITAL CARTELS: HOW NARCO-TERRORISTS LEVERAGE AND ARE COMBATED BY AI

Dr. Asmita Vaidya, Principal, Government Law College, Mumbai

Ms. Ashana Mishra, Research Scholar, Department of Law, University of Mumbai (Under the guidance of Dr. Asmita Vaidya)

ABSTRACT

This paper explores the rise of digital cartels, criminal groups involved in drug trafficking and terrorism that now use artificial intelligence and digital technologies to expand their reach. These organizations no longer rely only on physical violence or smuggling routes. Instead, they use encrypted apps to plan operations, drones to move drugs or carry out attacks, and cryptocurrency to hide money trails. Some even use artificial intelligence to analyse police patterns or manipulate social media to spread fear.

At the same time, governments and security agencies are also using AI to fight back. They use it to track online behaviour, monitor drone activity, follow money flows, and detect threats through data analysis. This has created a new kind of conflict, where both sides are using the same tools for opposite goals.

The study focuses on real-world cases, current technologies, and the risks of AI being used for harm. It also looks at the challenges law enforcement faces, such as protecting privacy while tracking criminals and keeping up with fast-changing digital tools. The paper argues that while AI offers powerful tools for safety, it can also be turned into a weapon by those who seek to do harm.

Introduction

In recent years, criminal organizations involved in drug trafficking and violence have started to operate in new ways. These groups are no longer limited to guns, cash, and hidden routes. They are now using advanced technology to expand their power and influence. When drug cartels combine their illegal activities with terrorism and digital tools, they form what we can call a "digital cartel."

A digital cartel is a criminal group that uses artificial intelligence, cyber tools, and online platforms to carry out its operations. These groups rely on encrypted messaging apps, drones, cryptocurrency, and social media to avoid detection and spread fear. At the same time, police and intelligence agencies are also using AI to monitor cartel activity, track illegal money flows, and prevent violence before it happens.

This new digital battlefield is changing the way we think about crime and security. AI is becoming a powerful tool, but it works for both sides. On one hand, it helps law enforcement stay ahead of criminal networks. On the other hand, it gives narco-terrorists new ways to grow and hide. This paper explores how digital cartels are using AI, how authorities are responding, and why this growing tech war is something the world cannot ignore.

Methodology

This research uses a qualitative approach to explore how digital cartels are using artificial intelligence and how law enforcement is responding. The study is based on open-source information, including academic literature, policy papers, government reports, news articles, and verified expert commentary. Due to the sensitive nature of organized crime and national security, much of the data comes from secondary sources that are publicly available but vetted for credibility.

The method combines case study analysis with thematic review. Cases involving specific criminal groups, such as the Sinaloa Cartel and CJNG in Mexico, are examined to understand how technology is being applied in real-world settings. These examples are used to identify broader trends in how AI is integrated into criminal activity and counter-terrorism efforts.

Themes such as communication encryption, drone deployment, money laundering, and social media manipulation are explored to build a clearer picture of the digital cartel model. Likewise,

the study evaluates how AI tools are used by authorities to detect, disrupt, and dismantle these operations.

This paper does not include interviews or field research due to safety and access limitations. Instead, it aims to offer an original synthesis of existing knowledge while identifying gaps that require deeper investigation in future research.

Theoretical and Philosophical Perspectives

The use of artificial intelligence in countering digital cartels raises fundamental questions about the nature of power, control, and responsibility in the digital age. At the heart of this issue lies the tension between state authority and individual freedom, a balance long debated in political theory. From a Foucauldian perspective, the rise of AI-powered surveillance marks an evolution in biopolitical control, where governments extend their reach into the intimate details of daily life through algorithms and data. The panoptic effect, once imagined as a prison design, now operates through networked technologies that watch without being seen. In this context, the use of AI against cartels may help enforce order, but it also risks normalizing a culture of suspicion and constant monitoring. Philosophically, this raises the question of whether the ends justify the means. Can a state preserve justice and human dignity while employing tools that inherently carry the potential for overreach and dehumanization? Moreover, the concept of justice itself is challenged when decisions are outsourced to machine learning systems that lack consciousness, empathy, or moral reasoning. From a utilitarian standpoint, the use of AI is justified if it reduces harm and saves lives. But from a deontological or rights-based perspective, the process by which security is achieved must also respect moral boundaries, regardless of outcomes. These philosophical tensions underscore the importance of not only regulating AI but also questioning the assumptions that guide its design and deployment. In the fight against digital cartels, the question is not simply how to win, but how to do so without losing sight of the values that define a just and open society.

AI Empowering Cartels

Digital cartels have moved far beyond traditional models of organized crime, which relied on violence, corruption, and manual smuggling routes. Today, they are embracing artificial intelligence and digital technologies as tools of both offense and defence. These technologies allow cartels to operate faster, more discreetly, and with greater strategic precision. By

embedding AI into their communication systems, logistics, financial transactions, and public messaging, these groups are becoming more difficult to detect and disrupt. The following subsections explain how digital cartels are actively using AI to outmanoeuvre law enforcement and extend their influence across borders.

- **Encrypted Communication and AI Monitoring-**

Encrypted messaging apps such as WhatsApp, Signal, and Telegram are now standard tools for digital cartels. These platforms offer end-to-end encryption, making it difficult for authorities to intercept or decode conversations. However, cartels have gone further by incorporating AI into their own intelligence gathering. Some groups reportedly use AI algorithms to scan large volumes of communication data, such as text messages or call records obtained through illegal access to phones or computers. This allows them to identify patterns in law enforcement activities, detect shifts in patrol routes, and spot weaknesses in border security. The integration of AI into communication and surveillance systems helps cartels not only coordinate complex operations but also avoid detection with greater accuracy than ever before.

- **Drones and Smuggling Automation-**

The use of drones by cartels is no longer experimental, it is becoming operationally routine. These drones are often equipped with GPS-guided flight paths, night-vision cameras, and AI-based navigation systems that allow them to fly without direct human control. In border regions, drones are used to deliver drug payloads across difficult terrain or evade traditional checkpoints. Some cartels have begun to automate drone deployment with pre-programmed algorithms that adapt routes based on wind, weather, or radar signals, making them less likely to be intercepted. Because these devices are cheaper and more disposable than human couriers, they reduce operational risk while increasing efficiency. AI also enables limited obstacle detection, allowing drones to navigate urban environments or avoid surveillance drones deployed by authorities.

- **Cryptocurrency and Money Laundering-**

Cartels have increasingly turned to cryptocurrencies to launder money and finance operations, taking advantage of the relative anonymity and decentralization that blockchain platforms provide. Digital currencies like Bitcoin and Monero are often used to move funds without

triggering the red flags that traditional banking transactions might raise. More sophisticated groups employ AI-driven financial tools to manage and conceal these flows. Machine learning models can break down large transactions into smaller units, distribute them across multiple digital wallets, and time transfers in ways that mimic regular market activity. AI can also help identify vulnerable crypto exchanges with weak regulatory oversight, allowing cartels to exploit gaps in international finance. The result is a deeply layered, resilient laundering structure that is far harder to trace using conventional forensic accounting methods.

- **AI-Enhanced Social Media and Propaganda-**

Digital cartels are also using AI to shape public perception and spread influence through social media. These groups have adopted generative AI tools to create manipulated images, fake videos, and deepfake recordings that either promote their dominance or intimidate rivals. Beyond creating content, cartels also rely on AI-powered bots to amplify their messages. These automated accounts flood platforms like Twitter, Facebook, and TikTok with cartel propaganda, threats, or fake news, aiming to control the narrative in regions they operate. AI allows these bots to respond in real-time, mimic local speech patterns, and engage users to create the illusion of public support or fear. This strategy helps cartels extend their control not only through violence but also through psychological warfare and information dominance, especially in territories where trust in official institutions is weak.

Surveillance and Counter-Intelligence-

Just as law enforcement agencies use AI for intelligence, so too do digital cartels. Criminal groups monitor open-source data, social media activity, and leaked law enforcement communications to anticipate raids, patrol shifts, or policy changes. AI tools enable them to mine massive datasets for keywords, time patterns, and geo-tagged content, helping them build predictive models of police behaviour. Some cartels even maintain their own informant networks and use AI to analyse tip-offs and track security forces. In regions with high levels of corruption, this digital counter-intelligence allows cartels to maintain an upper hand by staying one step ahead of official operations. By using AI defensively, cartels create a form of digital camouflage, making it harder for law enforcement to surprise or disrupt their operations effectively.

AI in Countering Digital Cartels

As digital cartels become more sophisticated in their use of technology, law enforcement agencies around the world are increasingly turning to artificial intelligence to strengthen their response. AI is now a critical part of the tools used to detect, track, and disrupt organized crime networks involved in drug trafficking and acts of terrorism. One major area of application is surveillance. AI software can now process footage from cameras placed in high-risk areas, helping authorities detect unusual behaviour, unauthorized drone flights, or hidden vehicles that may otherwise go unnoticed. This is especially useful in border zones where human monitoring is limited and drug smuggling is frequent. Financial tracking has also improved through the use of AI. By analysing patterns in banking activity and cryptocurrency transactions, investigators can follow the flow of illegal funds more effectively. AI tools can identify suspicious account behaviour and link digital wallets to organized crime, even when the money passes through multiple countries or hidden channels. Social media and open-source intelligence are also key fronts in this technological effort. Police units use AI systems equipped with natural language processing to scan digital platforms for keywords, threats, and cartel propaganda. These tools help identify coded messages and slang, allowing authorities to respond quickly to recruitment efforts or digital intimidation tactics. In some areas, predictive policing tools powered by AI are being tested to anticipate where crimes might occur. By analysing past incidents, locations, and time patterns, these systems can help law enforcement decide where to allocate resources before violence erupts. Although still controversial, this approach has shown early signs of promise in cities facing intense cartel activity. Finally, a more recent method involves the use of AI-generated digital personas that operate undercover in online cartel spaces. These virtual profiles can interact with suspects, gather intelligence, and even pose as potential recruits or buyers. When used responsibly and under supervision, such techniques offer law enforcement the ability to penetrate closed networks without putting human agents at direct risk. Together, these developments mark a significant shift in how governments are using artificial intelligence not only to catch up with digital cartels, but to anticipate and counter their next moves.

Case Studies

Understanding how artificial intelligence is shaping the fight between digital cartels and law enforcement requires a close examination of real-world events where emerging technologies

have played a significant role. These cases illustrate not only the evolving tactics of criminal organizations but also the innovative responses by state actors working to adapt their tools and strategies in a rapidly changing landscape.

One of the most striking examples of technology-driven cartel innovation is found in Mexico, where the Cartel Jalisco New Generation (CJNG) has adopted weaponized drones as part of its offensive arsenal. In recent years, the group has used modified commercial drones to drop explosives on rival gangs, civilians, and police convoys. A notable incident occurred in Michoacán, a state that has become a major battleground between competing cartels. In this attack, CJNG deployed drones equipped with fragmentation grenades, targeting law enforcement vehicles in a calculated ambush. These drones are often operated remotely and programmed to follow specific flight paths, allowing for attacks to be executed from a distance with minimal risk to cartel members. Although the level of artificial intelligence used in these drones is relatively basic, often limited to pre-programmed navigation and simple object recognition, their use marks a clear transition from conventional violence to semi-automated digital warfare. It also signals how criminal actors are repurposing off-the-shelf technology to undermine state authority in rural and urban zones alike.

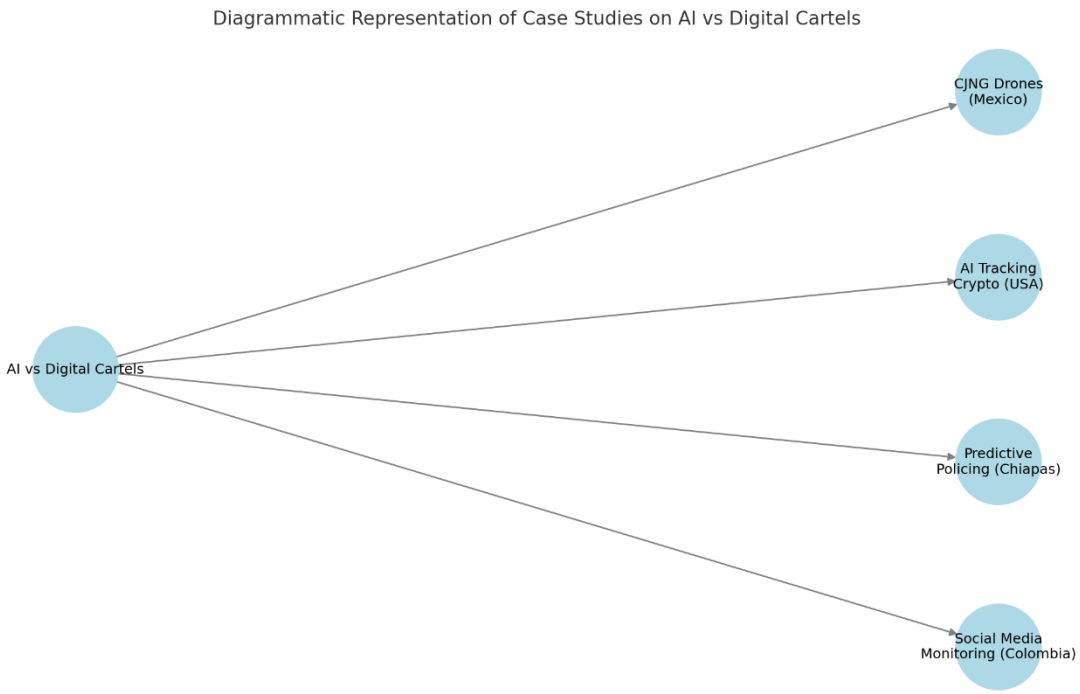
In the United States, authorities have turned to artificial intelligence as a key tool in financial investigations, particularly in the effort to dismantle the economic backbone of major drug cartels. The Sinaloa Cartel, long known for its complex and diversified revenue streams, has increasingly turned to cryptocurrencies to launder money and evade traditional financial oversight. In response, the U.S. Department of Justice and agencies such as the Internal Revenue Service and Homeland Security Investigations have employed AI-powered blockchain analysis tools to track illicit funds across digital ledgers. These tools use machine learning algorithms to identify suspicious transaction patterns, map networks of wallet addresses, and detect attempts to anonymize transactions through so-called mixers or tumblers. In one operation, investigators traced millions of dollars in Bitcoin payments linked to fentanyl sales, leading to arrests and asset seizures that would have been difficult using manual financial audits alone. This approach demonstrates the growing importance of financial intelligence powered by AI in disrupting the operational capacities of global cartels.

Another case from Mexico illustrates how law enforcement has begun integrating AI and drone technology into rural policing efforts. In the state of Chiapas, which borders Guatemala and

serves as a major transit route for drug shipments, local police forces have started using drones guided by artificial intelligence to conduct aerial surveillance of cartel activity. These drones are equipped with cameras and real-time image processing capabilities that can detect unusual patterns, such as convoys moving along back roads or gatherings in remote areas. The data collected is then analysed using AI tools that cross-reference the location, time, and movement with historical crime data to predict potential hotspots of violence or trafficking. This form of predictive policing has enabled law enforcement to carry out more targeted and timely interventions, especially in areas where geography and lack of manpower limit traditional patrols. While questions about accuracy and privacy remain, the early results in Chiapas suggest that AI-enhanced policing can serve as a force multiplier in difficult environments.

Colombia offers a different but equally revealing example of how artificial intelligence is being used to combat the digital footprint of narco-terror groups. In recent years, the Colombian government has worked with cybersecurity firms and academic institutions to develop AI systems capable of monitoring social media platforms and messaging apps for signs of cartel propaganda, threats, and recruitment activities. These systems use natural language processing to scan public posts, group chats, and metadata for patterns of communication linked to known criminal actors. For instance, slang terms, emojis, and coded language used in cartel networks are detected and flagged for review. This monitoring has proven particularly effective in identifying attempts to recruit vulnerable youth through online platforms like Facebook, Instagram, and WhatsApp. In several documented cases, authorities were able to shut down fake accounts used to lure minors into drug distribution or armed roles within criminal cells. While such efforts raise important concerns about surveillance and digital rights, they also highlight the necessity of evolving digital intelligence practices to keep pace with the modern cartel ecosystem.

Together, these case studies reflect the multidimensional nature of the conflict between digital cartels and law enforcement. They reveal how artificial intelligence is being employed on both sides of the struggle, sometimes in simple, tactical forms, and other times in highly structured and systematic ways. They also underscore the need for adaptive, well-regulated, and ethically grounded responses that can keep up with the increasingly digital nature of organized crime.



Ethical, Legal, and Operational Challenges

The integration of artificial intelligence into counter-narcotics and counter-terrorism operations raises a complex set of ethical, legal, and operational concerns that must be addressed with urgency and care. One of the most pressing issues is the potential erosion of privacy through mass surveillance. AI-driven tools such as facial recognition systems, automated license plate readers, and predictive policing platforms have the capacity to monitor not just criminal suspects but entire communities. In regions heavily affected by cartel activity, this can lead to the over-policing of marginalized populations and the collection of data without clear consent or oversight. Legally, many jurisdictions lack comprehensive frameworks to regulate the use of AI in law enforcement, resulting in a grey area where powerful technologies are deployed without transparent rules or accountability. The admissibility of AI-generated evidence in court remains inconsistent across countries, and the lack of legal standards for digital investigations can lead to failed prosecutions or human rights violations. There is also a significant risk of algorithmic bias. If AI systems are trained on data that reflect existing inequalities, they may reinforce stereotypes or disproportionately target specific racial or socioeconomic groups. This can undermine public confidence in law enforcement and fuel further instability. On the operational side, the overreliance on AI systems may create new vulnerabilities. Cartels are known to adapt quickly and may attempt to manipulate open-source data, disrupt digital evidence chains, or launch cyberattacks against investigative systems. Without skilled human

oversight, even the most advanced AI platforms can produce false positives or miss critical context. Compounding these issues is the lack of international coordination in AI governance. While digital cartels operate across multiple countries, most AI-based enforcement efforts remain isolated within national borders. A fragmented approach not only limits effectiveness but also creates loopholes that sophisticated criminal networks can exploit. Addressing these challenges requires a coordinated global response, one that blends technological innovation with robust legal and ethical safeguards.

Recommendations and Conclusion

In light of the growing threat posed by digital cartels, it is clear that artificial intelligence must be developed and deployed with both strategic intent and ethical oversight. Governments and international agencies should prioritize the creation of AI tools that are not only effective but also transparent and accountable. This means investing in systems that are regularly audited, legally compliant, and trained on diverse and accurate data to avoid reinforcing harmful biases. Law enforcement personnel must be trained to understand how AI systems work, how to interpret their outputs, and when to rely on human judgment instead. Equally important is the need for stronger legal frameworks that define the limits of AI use in policing and intelligence work, especially concerning surveillance, digital infiltration, and the handling of private data. International collaboration should be strengthened to close cross-border gaps that digital cartels frequently exploit. This includes harmonizing data protection laws, sharing technical resources, and building regional alliances to respond to threats in real time. The integration of AI into the fight against narco-terrorism is not a temporary adjustment but a permanent transformation of modern law enforcement. While the technology brings clear advantages in speed, scale, and predictive capability, it is not a solution in itself. AI must operate as a tool within a larger system of justice, guided by principles of human rights, operational discipline, and public trust. If approached thoughtfully, AI can play a decisive role in weakening the influence of digital cartels and reshaping how societies respond to organized crime in the digital age.

REFERENCES

On narco-terrorism definitions and history

Vanda Felbab-Brown, *Narcoterrorism and the Long Reach of U.S. Law Enforcement* (Brookings, Oct. 12, 2011), https://www.brookings.edu/articles/narcoterrorism-and-the-long-reach-of-u-s-law-enforcement/ btlj.orgpapers.ssrn.com+8brookings.edu+8files.ethz.ch+8.

SECI Ctr. Anti-Terrorism Task Force, *Narco-Terrorism (Global and Regional Overview)* (Turkish Nat'l Police Mar. 8, 2004), https://www.osce.org/files/f/documents/d/b/25180.pdf osce.org.

D. Tuset Varela, *Artificial Intelligence Law Through the Lens of Michel Foucault: Biopower, Surveillance, and the Reconfiguration of Legal Normativity*, 12 Open J. Soc. Sci. 189 (2024), https://doi.org/10.4236/jss.2024.1212012 scirp.org+1tandfonline.com+1.

On modern narco-terror trends and case studies

Thomas F. Deen, *The Growth of Narco-Terrorism in Mexico: Expanding the Counternarcotic Strategy with Foreign Terrorist Designation*, 2025 J. Terrorism Stud. (Mar. 2025) papers.ssrn.com+4tandfonline.com+4papers.ssrn.com+4.

The Growth of Narco-Terrorism in Mexico, supra.
Joshua N. Aston, *Narco-Terrorism: A Critical Study* (SSRN Working Paper, 2012) tandfonline.com+11papers.ssrn.com+11stars.library.ucf.edu+11.

On AI, surveillance, governmentality, and theory

Michel Foucault, *Discipline and Punish: The Birth of the Prison* 197 (Alan Sheridan trans., Vintage 1995) (1977).

See Tuset Varela, supra; Michel Foucault, *Governmentality*, in *The Foucault Effect: Studies in Governmentality* 87 (Graham Burchell, Colin Gordon & Peter Miller eds., 1991).

On AI tools and legal–ethical implications

Susan Sim et al., *Emerging Technologies and Terrorism: An American Perspective* (U.S. Army War College, 2023), https://publications.armywarcollege.edu/News/Display/Article/3747440/emerging-technologies-and-terrorism-an-american-perspective/ scirp.org.