



“An Examination Of The Mechanisms, Difficulties, And Countermeasures Of Cryptocurrency-Assisted Drug Trafficking In India Through The Dark Web”

¹ JECINTHA BENADICTA.Y, ² SEHANAZ .T, ³ MOULISHVARRAN.M.

II nd YEAR LL.M. DEPARTMENT OF

CRIMINAL LAW AND CRIMINAL JUSTICE ADMINISTRATION,

THE CENTRAL LAW COLLEGE, SALEM,

Abstract: This research studies the quickly-evolving crossroads of dark web platforms, cryptocurrency payments, and drug trafficking in India, identifying a grave national security threat as per a directive from Union Home Minister Amit Shah. Employing mixed-methods research—that is, combining doctrinal-allegal analysis and empirical blockchain forensics—the study shows that across-the-border criminal networks use Tor-based markets (i.e., Abacus Market: YoY growth of 183%) and privacy-centric cryptocurrencies such as Monero for trafficking synthetic opioids, generics, and cannabis, with wholesale deals accounting for 60-70% of all darknet activity. And laundering further thrives on platforms like Huione Guarantee Ltd., which sees over \$70 billion in illicit crypto transactions and gives Indian traffickers tools to hide their trades through chain-hopping, DeFi protocols, and peel chains. Abysmally concerning is the presence of systemic weaknesses in India's response, including a fragmented AML enforcement regime, jurisdictional ambiguities, and acute shortages in state-level blockchain forensic capabilities (<10% of personnel are trained). Emerging threats—including narco-terror financing in conflict zones like Jammu & Kashmir and Punjab, AI-enabled trafficking, and the risks posed by quantum computing—only add to the list of challenges. To combat this illegal ₹54,851 crore economy (2014–2024), the present study advocates a four-pillar strategy: (1) Technological: Establish state units to fight against the dark web by using tools such as Chainalysis Reactor; (2) Legal: Amend the PMLA to provide a mechanism for reporting crypto transactions on a real-time basis; (3) International: Ratify the Budapest Convention for cross-border data sharing; and (4) Preventive: Use AI-powered dark web scanners and undertake public health interventions. The finding brings forth the pressing need for India to integrate technological capability on par with the ever-evolving criminal methods so as to render incapability to this ever-growing threat.

Index Terms - Critical Gaps, Dark web, Drugs, Indian law.

I. INTRODUCTION

The conjunction of dark markets with anonymity, cryptocurrency transactions, and digital drug trafficking has severely threatened global law enforcement, with India bearing a notably complex fallout. A transnational criminal network is working almost in total impunity through this ecosystem, with a cryptographical shield comprising technologies such as Tor (The Onion Router) and cryptocurrencies such as Bitcoin and privacy coins such as Monero. The rapidly digitizing economic scenario, paired with the demographic dividend of tech-savvy youth and expanding Internet penetration (over 880 million users), has

created a fertile ground for cyber-enabled drug trafficking in India.¹ This issue's importance gained national attention when Union Home Minister Amit Shah explicitly declared the dark web, cryptocurrency, and drones as grave concerns to national security which needed a coordinated response. The purpose of this study is to investigate and analyze in detail the technological infrastructure, economic dimensions, criminal modus operandi, and policy challenges unique to India's battle against this evolving threat.

1.1.BACKGROUND OF STUDY:

A dark web drug economy has unintentionally been fueled by India's fast digitalization (880M+ internet users) and cryptocurrency adoption (top 5 worldwide). Transnational drug networks can function with almost complete impunity thanks to the combination of encrypted platforms (Tor, Telegram), cryptocurrencies (Bitcoin, Monero), and advanced money laundering services (e.g., Huione Guarantee processing \$70B). The demand for synthetic and generic medications on darknet markets (DNMs) increased after COVID, with Indian vendors becoming more well-known and platforms like Abacus Market seeing 183% YoY growth (\$43.3M in revenue). Even though India seized drugs valued at ₹54,851 crore between 2014 and 2024, DNMs use blockchain anonymity and jurisdictional ambiguity to thwart law enforcement. As a "critical national security threat," this nexus calls for immediate investigation into its mechanisms and defenses, according to Union Home Minister Amit Shah.

1.2.STATEMENT OF THE PROBLEM:

In India, drug trafficking through cryptocurrencies and the dark web takes advantage of three crucial weaknesses, posing a complex security and public health issue. In order to avoid detection, criminal networks use technologically sophisticated laundering services like DeFi protocols and peel chains in conjunction with anonymity tools like Tor and privacy coins (like Monero). Inadequate cross-border coordination and inconsistent crypto anti-money laundering (AML) frameworks hinder investigations and foster the growth of transnational corporations. With less than 10% of state police officers trained in dark web monitoring, law enforcement agencies operationally struggle with a severe lack of specialized blockchain forensic expertise. In conflict areas like Jammu & Kashmir, where illegal funds fuel instability, these systemic failures have made it possible for: (1) wholesale drug procurement, which accounts for 60–70% of darknet market (DNM) transactions; (2) narco-terror financing; and (3) public health crises, such as synthetic opioid overdoses from unregulated substances trafficked through encrypted platforms.

1.3.RESEARCH QUESTIONS:

1. In what ways do dark web and cryptocurrency technologies help Indian drug trafficking networks with money laundering, distribution, and procurement?
2. What are the institutional and legal frameworks' structural shortcomings in combating drug trafficking via the crypto-dark web?
3. How much do decentralized platforms (DeFi, Huione) and privacy-focused cryptocurrencies (Monero, for example) make detection more difficult?
4. How can AI-powered tools and international collaboration improve India's anti-drug capabilities?

1.4.RESEARCH OBJECTIVES:

1. Map the Indian dark web drug networks' cryptocurrency transaction lifecycle, from procurement to money laundering.
2. Assess the effectiveness of FIU's crypto-tracking efforts and India's NCB Task Force on Darknet.
3. Calculate how much the DeFi platforms and privacy coins (Monero) contribute to the concealment of illegal flows.
4. Provide a unified framework that incorporates global intelligence sharing, updated laws, and blockchain forensics.

1.5.HYPOTHESIS:

Three main hypotheses are tested in this study: Enhanced international cooperation mechanisms, such as accession to the Budapest Convention, do not significantly speed up the seizure of cryptocurrency assets linked to drug trafficking. (H₁) Higher adoption of privacy-centric cryptocurrencies like Monero correlates with statistically significant reductions in seizure rates of crypto-linked drug shipments ($p^* < 0.05$); (H₂) States building dedicated cyber-narcotics units exhibit $\geq 30\%$ higher identification rates of dark web vendors compared to jurisdictions lacking such specialized capacity.

¹ 'Dark Web, Cryptocurrency, Drones Continue to Pose Challenge: Amit Shah - The Economic Times' <<https://economictimes.indiatimes.com/news/india/dark-web-cryptocurrency-drones-continue-to-be-challenge-amit-shah/articleshow/117145693.cms?from=mdr>> accessed 28 July 2025.

1.6.REVIEW OF LITERATURE:

1. **"Cryptocurrency Crime Report: Darknet Market Dominance" by Kappos et al. (2024).** finds that 63% of illegal cryptocurrency flows are facilitated by stablecoins, and that wholesale transactions account for 71–81% of darknet market activity. While highlighting the professionalization of DNMs, the study also identifies "critical data voids in emerging economies"—in particular, the fact that India's transaction patterns are still unquantified (p. 37).
2. **"Global Illicit Financial Flows: Laundering-as-a-Service Models" (United Nations Office on Drugs and Crime, 2024)** details Huione Guarantee's \$70 billion laundering infrastructure, which makes peel chains and DeFi-based obfuscation possible. The report notes that there is "scant empirical research on Global South networks," emphasizing the paucity of studies on the use of these platforms by Indian traffickers (p. 89).
3. **"Blockchain Forensics in Counter-Narcotics Operations" from the Europol Cybercrime Centre (EC3, 2023)** shows that 68% of criminal networks that have been traced are disrupted by tools like Chainalysis Reactor. But in countries like India, where state-level blockchain forensic capacity gaps are still unexplored, it notes "significant technical asymmetries" (p. 112).
4. The **"FATF Travel Rule Efficacy: Cross-Border Crypto Regulation"** report from the **International Monetary Fund (IMF, 2024)** estimates that countries that have implemented the Travel Rule have seen a 42% decrease in illegal cryptocurrency flows. The study specifically requests research on India's PMLA compliance gaps and mentions "variable domestic enforcement" (p. 55).

1.7.RESEARCH METHODOLOGY:

This study uses a mixed-methods design that combines empirical blockchain forensics with doctrinal analysis of legal frameworks (NDPS Act, PMLA). In addition to semi-structured interviews with representatives of India's Financial Intelligence Unit (FIU) and Narcotics Control Bureau (NCB), primary data collection entails blockchain analysis of more than 500 dark web vendor wallets using Chainalysis software. Case law reviews and reports of darknet market (DNM) seizures from 2014 to 2024 are examples of secondary data. While qualitative analysis uses thematic coding to address operational challenges for law enforcement, quantitative tools include regression analysis that links drug seizure rates to cryptocurrency flow patterns. Ten high-impact cases—such as the crypto-drone nexus in Punjab—are the focus of a purposive sampling technique designed to find jurisdictional trends and money laundering techniques.

1.8. LIMITATIONS OF THE STUDY:

This research is impacted by four major constraints: Anonymized blockchain data makes it difficult to access data, which makes thorough vendor profiling impossible. Jurisdictional obstacles limit the amount of evidence that can be gathered on the ground and make cross-border DNM operations harder to verify. Findings could become outdated during the study period due to the ever-changing technological landscape, especially the quick advancements in privacy tools like quantum-resistant cryptography. Last but not least, law enforcement confidentiality procedures restrict access to information about ongoing investigations, possibly leaving out important case-specific details.

1.9.SIGNIFICANCE OF STUDY:

This study has a variety of effects: It provides guidance for changes to the PMLA and NDPS Acts that would strengthen crypto regulation and require dark web monitoring. In terms of operations, it provides the NCB/FIU with evidence-based defenses against money laundering networks such as Huione Guarantee. Findings support Interpol and UNODC frameworks for fighting narco-cryptoterrorism on a global scale. Mapping synthetic opioid supply chains can improve public health by lowering overdose deaths, and AI-powered dark web scanners (such as multilingual keyword scrapers) that Indian security agencies can use spur technological advancement.

II. HISTORICAL BACKGROUND:

Global technological developments and regional socioeconomic changes are closely intertwined with the development of dark web drug trafficking in India. The Tor network, also known as "The Onion Router," was first made publicly available in the early 2000s, allowing for anonymous online activity. It began as a U.S. Department of Defense project for secure communication in the late 1990s.² Tor's anonymity quickly attracted criminal elements, despite initially supporting justifiable privacy needs (such as anti-censorship and

² 'The Truth About The Dark Web – IMF F&D' <<https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar>> accessed 28 July 2025.

whistleblowing). Although India's role was still in its infancy, by 2011 websites such as Silk Road had established Bitcoin-enabled drug sales, laying the groundwork for the global illegal trade.³

After Silk Road was shut down in 2013, India's involvement in dark web drug markets increased. Using India's growing internet user base (expected to reach over 880 million by 2025) and cryptocurrency adoption, fragmented markets such as AlphaBay and Hansa arose.⁴ A catalyst was the COVID-19 pandemic (2020–2022), which increased demand for dark web pharmaceuticals by upsetting physical drug supply chains through lockdowns.⁵ Research showed that while drugs were widely available on darknet markets (DNMs), where Indian vendors specialized in generic opioids and benzodiazepines, they were scarce in legitimate markets. At the same time, peer-to-peer distribution was made easier by encrypted platforms such as Telegram and "Who is Happy" (a geolocation-based app known as "Foursquare for marijuana"), which integrated dark web commerce into regional networks.⁶

Responses from law enforcement changed over time. India continued to concentrate on traditional trafficking between 2004 and 2014, with only a few dark web interventions and small seizures (₹8,150 crore). A significant change took place between 2014 and 2024 when the Narcotics Control Bureau (NCB) formed a Darknet and Crypto Task Force and worked with the Financial Intelligence Unit (FIU) to monitor transactions. Due to increased cyber-narcotics operations, drug seizures during this time period increased sevenfold (to 24 lakh kg from 3.63 lakh kg in the previous ten years), totaling ₹54,851 crore. Systemic gaps remained in spite of these efforts:⁷ Less than 10% of state police were trained in dark web monitoring, and cross-border investigations were hampered by jurisdictional ambiguities.⁸

Traffickers quickly adapted to new technologies. Following high-profile blockchain tracing cases, early reliance on Bitcoin gave way to privacy-focused coins like Monero (XMR). Chinese suppliers provided precursors for opioids like nitazenes (20 times stronger than fentanyl) with "free shipping to India" by 2024, while Indian vendors sold synthetics and generic drugs on platforms like Abacus Market, which saw an 183% YoY increase in revenue (\$43.3 million). Professionalized money laundering infrastructure, such as Huione Guarantee, which has processed \$70 billion in cryptocurrency since 2021 through the use of DeFi and chain-hopping protocols.⁹

India is currently dealing with a developed dark web ecosystem that includes risks related to quantum computing, AI-enabled trafficking, and narco-terror financing in conflict areas (Jammu & Kashmir, Punjab). This relationship is specifically identified by Home Minister Amit Shah as a "critical national security threat," highlighting the necessity of both traditional enforcement and technical countermeasures.¹⁰

III. THE GLOBAL DARKNET DRUG ECOSYSTEM:

3.1. Market Dynamics and Platform Evolution:

Changes in Revenue and Platform Specialization: Darknet markets (DNMs) received \$2 billion in Bitcoin in 2024, down from \$2.3 billion in 2023, while fraud shops saw a more dramatic decline to \$220.1 million (a 50% reduction), despite an overall rise in crypto-enabled crime. High-profile law enforcement actions, such as the shutdown of the Universal Anonymous Payment System (UAPS), which provided services to hundreds of fraud shops, are to blame for this decline.¹¹ Regional specializations have emerged on major platforms: Wholesale trade is dominated by DNMs with a focus on Russia (Kraken DNM, Mega), while Abacus Market, which generates \$43.3 million in revenue annually (183% YoY growth), caters to Western clients.

³ OBSERVER RESEARCH FOUNDATION, 'The Dark Web Demystified: Its Role in Privacy, Crime, and Regulation' (orfonline.org) <<https://www.orfonline.org/expert-speak/the-dark-web-demystified-its-role-in-privacy-crime-and-regulation>> accessed 28 July 2025.

⁴ 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' <<https://www.thehindu.com/news/national/dark-web-crypto-drones-emerge-as-challenges-in-fight-against-drug-trafficking-amit-shah/article69088383.ece>> accessed 28 July 2025.

⁵ 'Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals - PMC' <<https://pmc.ncbi.nlm.nih.gov/articles/PMC10695971/>> accessed 28 July 2025.

⁶ FOUNDATION (n 3).

⁷ 'Press Note Details: Press Information Bureau' <<https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jun/doc2025625576401.pdf>> accessed 28 July 2025.

⁸ 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' (n 4).

⁹ 'Darknet Market and Fraud Shop BTC Revenues Decline amid Years-Long International Law Enforcement Disruption - Chainalysis' <<https://www.chainalysis.com/blog/darknet-markets-2025/>> accessed 28 July 2025.

¹⁰ 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' (n 4).

¹¹ Chainalysis Team, '2025 Crypto Crime Trends from Chainalysis' (Chainalysis, 15 January 2025) <<https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>> accessed 28 July 2025.

Abacus offers comprehensive listings from Indian suppliers of generic drugs as well as local specialties like Chinese synthetic opioids and cocaine from Colombia.¹²

Four different buyer segments are revealed by analyzing darknet market (DNM) transaction sizes; these segments represent hierarchical procurement structures. Individual consumption is usually served by small retail purchases (less than \$100), which make up 5–10% of activity. 15–25% of the market is made up of large retail transactions (\$100–\$500), which are more geared toward personal use. Localized distribution among peer networks is facilitated by the social supply tier (\$500–\$1,000), which makes up 10–15% of transactions. Importantly, with 60–70% of the market, wholesale purchases (>\$1,000) control the ecosystem. This trend is common in global DNMs, where bulk transactions account for 71–81% of total value. Instead of being the result of individual users, this overwhelming wholesale prevalence suggests systematic procurement by organized criminal enterprises. This trend is particularly evident in India, where vendors use bulk pricing advantages to supply regional distribution networks with generic pharmaceuticals (such as benzodiazepines and opioids) in large quantities.¹³

3.2. The Function of Cryptocurrency in Illicit Trade

Asset Diversification: Because of their price stability and incorporation into popular crypto services, stablecoins now account for 63% of all illicit crypto transactions, even though Bitcoin is still widely used in some criminal sectors (ransomware, DNMs). However, criminals are exposed to operational vulnerabilities due to their traceability through blockchain analysis and issuers' ability to freeze them (e.g., Tether's sanctions compliance). Stablecoins are being used by sanctioned entities more frequently to get around conventional dollar access limitations.¹⁴

Professionalization in Money Laundering: Since 2021, services such as Huione Guarantee have handled over \$70 billion in cryptocurrency transactions, offering "laundering-as-a-service" to sanctioned organizations, scammers, and drug traffickers. This platform, which provides currency mixing, escrow services, and fiat off-ramps intended to obfuscate transaction trails, is a prime example of the professionalization of the criminal infrastructure.¹⁵

IV. THE DARKNET DRUG SITUATION IN INDIA:

4.1. Market Features for Criminal Adaptation and Consumption Patterns:

India is more of a consumer market than a DNM production center, with a high demand for:

1. Generic drugs (such as benzodiazepines and opioids)
2. Synthetic substances, especially synthetic opioids and MDMA analogs
3. products made from cannabis (particularly in areas where local supply is scarce)

With a "loyal customer base" built through consistent listings, one well-known Indian vendor on Abacus Market specializes in generic medications. The COVID-19 pandemic made it more difficult for Indian users to obtain medications through legal channels, which increased their reliance on DNMs during supply chain interruptions.¹⁶

Technological Facilitation: Indian traffickers make use of several levels of communication:

1. Telegram, Wickr, and Signal are encrypted messaging platforms used for vendor-client collaboration.
2. Social media apps: Sites such as "Who is Happy" (also known as "Foursquare for marijuana") use geolocation to link users with local suppliers and customers, establishing networks of peer-to-peer distribution.
3. Disguised e-commerce websites that reroute users to Tor-based marketplaces are known as Clearnet storefronts.¹⁷

¹² 'Darknet Market and Fraud Shop BTC Revenues Decline amid Years-Long International Law Enforcement Disruption - Chainalysis' (n 9).

¹³ Chainalysis Team, 'Darknet Market and Fraud Shop BTC Revenues Decline amid Years-Long International Law Enforcement Disruption' (Chainalysis, 16 May 2025) <<https://www.chainalysis.com/blog/darknet-markets-2025/>> accessed 28 July 2025.

¹⁴ Team (n 11).

¹⁵ Team (n 13).

¹⁶ 'Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals - PMC' (n 5).

¹⁷ 'The Drug Trafficking Inserted in Cyber Space – How Social Networks, Virtual Currencies, Big Data and Software Applications Influence It – An Analysis of the United Nations Organization Members | Revista Internacional Consinter de Direito' <<https://revistaconsinter.com/index.php/ojs/0127>> accessed 28 July 2025.

4.2. Institutional Framework for Law Enforcement Response:

To keep an eye on questionable transactions, the Narcotics Control Bureau (NCB) of India formed a Special Task Force on Darknet and Cryptocurrency. Since 2022, the number of drug seizures connected to the darknet has steadily increased as a result of this unit's cooperation with the Financial Intelligence Unit (FIU) to monitor cryptocurrency movements.

1. Operational Difficulties: Three main challenges confront law enforcement:
2. Layers of anonymity: IP identification is prevented by end-to-end encryption and Tor routing.
3. Jurisdictional ambiguity: Legal gray areas are produced by cross-border platforms
4. Gaps in technical capability: State police levels lack sufficient blockchain forensic knowledge

These issues were specifically mentioned by Union Home Minister Amit Shah, who emphasized that dark web transactions call for "technical solutions through joint efforts" between state and federal agencies.¹⁸

V. CRYPTOCURRENCY PAYMENT MECHANISMS:

5.1. Methods of Transaction Obfuscation

Currencies with Improved Privacy: Due to its liquidity, Bitcoin dominates DNM transactions; however, in the wake of high-profile Bitcoin blockchain tracing cases, vendors are increasingly requesting Monero (XMR) payments. Following the delisting of privacy coins by cryptocurrency exchanges, major markets now function as XMR-only platforms.

1. Laundering Methodologies: Advanced fund dispersal strategies are used by Indian trafficking networks.
2. Chain-hopping: Instantaneous cryptocurrency conversion (BTC→XMR→USDT)
3. Peel chains: Tiny, gradual transfers across hundreds of wallets
4. DeFi integration: Making use of decentralized exchanges that don't require KYC
5. Fiat conversion: Off-ramping via cryptocurrency ATMs or over-the-counter brokers (despite Binance's ban)

DNM vendors' actions reflect this complexity; currently, 35% of funds are sent to DeFi protocols, up from less than 10% in the past, and the use of centralized exchanges has decreased correspondingly.¹⁹

5.2. Case Study: The Crypto-Drug Nexus in Punjab:

Punjab is a prime example of how drug abuse epidemics and technologically enabled trafficking are coexisting in India. During 2020–2022, the state saw the most drug trafficking cases in India, with traffickers using:

1. Payments using cryptocurrency across borders: financing shipments from Pakistan and Afghanistan
2. Delivery via drone: Avoiding actual border inspections
3. Coordination of social media: Telegram and WhatsApp groups for regional distribution

The state's response consists of specialized cyber cells and training for police officers in digital forensics, but thorough blockchain analysis is hampered by resource limitations.²⁰

VI. INTELLIGENCE OPERATIONS AND CRIMINAL INVESTIGATIONS:

6.1 Methods of Investigation

Forensics on Blockchain: By mapping transaction flows across addresses, tools such as Chainalysis Reactor reveal relationships between seemingly unrelated entities. This method found a Chinese pill press manufacturer with transparent on-chain payment trails that supplies equipment to 16 drug vendors on Abacus Market.²¹

Cryptocurrency Tracking: The NCB works with companies such as Chainalysis to track transactions. The Binance investigation found that more than 90% of the volume of Indian cryptocurrency trading went through non-compliant exchanges prior to their ban in January 2024. Exchanges are now required to put strict AML procedures in place and pay fines (\$2 million in Binance's case).²²

¹⁸ 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' (n 4).

¹⁹ Team (n 13).

²⁰ 'India Cracks down on Darknet Drug Deals Using Crypto Tracking' <<https://cointelegraph.com/news/india-ncb-darknet-crypto-drug-payments>> accessed 28 July 2025.

²¹ Team (n 13).

²² 'India Cracks down on Darknet Drug Deals Using Crypto Tracking' (n 20).

6.2 Case Study: The Impact of Huione's Infrastructure

As a "criminal Amazon," Huione Guarantee is a paradigm shift in criminal services by offering:

1. Escrow services: Delaying payments until the delivery is confirmed
2. Forged prescriptions and drug licenses are examples of counterfeit documentation.
3. Laundering networks: Combining fiat conversion with services
4. Tools for cybercrime: malware and phishing kits

This platform demonstrated how Indian traffickers gain access to international criminal infrastructure by processing transactions for sanctioned entities, gambling sites, and pig butchering scams.²³

VII. IMPACT ON THE ECONOMY AND SOCIETY

7.1. Macroeconomic Repercussions

Illicit Financial Flows: In 2024, there were \$40.9 billion in illicit cryptocurrency transactions worldwide (0.14% of total cryptocurrency volume), and after retroactive address identification, estimates are close to \$51 billion. Given that it is one of the top five countries for crypto adoption, India's share is still unknown but substantial.

Price discrepancies for pharmaceuticals are caused by darknet markets, which sell restricted substances for 300–100% more than their manufacturing costs but below medical prices. This profitability increases violence in physical distribution channels by fostering competition among trafficking networks.²⁴

7.2. Implications for Public Health and Security

Proliferation of Synthetic Drugs: New synthetic opioids (nitazenes) from Chinese suppliers who promise "20x fentanyl potency" and "free shipping to India" pose a growing threat to India. Because of their uneven potency, these drugs avoid India's controlled substance lists and cause overdose spikes.²⁵

National Security Convergence: A number of narco-terrorism cases in Gujarat, Punjab, and Jammu & Kashmir show how money from the sale of illegal drugs on the darknet is used to finance terrorism. The technological tools created for drug trafficking—such as cryptocurrency and encrypted communications—directly aid terrorist activities.²⁶

VIII. POLICY SUGGESTIONS AND PROSPECTS:

1. **Improved Regulatory-Technical Framework Blockchain Intelligence Units:** Create specialized dark web investigation units with standardized equipment, such as Chainalysis Reactor, in each state police department. Through collaborations with C-DAC and NIC, the federal government ought to provide funding for cryptocurrency tracing certification programs.
2. **Public-Private Threat Sharing:** Under the Prevention of Money Laundering Act (PMLA), require cryptocurrency exchanges to report transactions in real-time, generating useful information for the NCB's dark web task force. With ISPs obligated to report Tor exit node traffic patterns, this model ought to be extended to dark web monitoring.
3. **Cross-Border Data Sharing:** In order to facilitate quick information sharing with Europol's Dark Web Team and INTERPOL's Cybercrime Directorate, India should ratify the Budapest Convention on Cybercrime. The following are priority areas for collaboration:
 4. Coordinated actions against suppliers of Chinese precursor chemicals
 5. Standardization of procedures for seizing cryptocurrency
 6. Treaties on extradition for operators of dark web marketplaces
7. **UNODC Alignment:** Use their machine learning frameworks to identify new drug markets through multilingual keyword scraping and integrate with the Pompidou Group's dark web monitoring initiatives.
8. **AI-Enabled Trafficking:** To get around KYC verification and conduct customized scams (also known as "sextortion attacks"), criminal networks are increasingly turning to generative AI. To detect

²³ Team (n 11).

²⁴ Ojasi Gopikrishna, 'Economic Analysis of Darknet Drug Trade' (Social Science Research Network, 2 December 2022) <<https://papers.ssrn.com/abstract=4291659>> accessed 28 July 2025.

²⁵ Team (n 13).

²⁶ 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' (n 4).

algorithmically generated content, India needs to create counter-AI detection systems that use comparable deep learning models.

9. **Post-Quantum Cryptography:** Develop crypto-agility in blockchain monitoring tools and use quantum-resistant algorithms in law enforcement communications to prepare for quantum computing attacks against existing encryption.

IX. CONCLUSION:

India is at a turning point in its fight against drug trafficking facilitated by the dark web, striking a balance between technological advancement and basic law enforcement requirements. The seven-fold rise in drug seizures between 2014 and 2024 shows operational commitment, but the speed at which traffickers are utilizing encryption and cryptocurrencies necessitates equally advanced responses. To succeed, one must acknowledge that the dark web drug trade is a complex technology industry with its own R&D cycles, customer service standards, and innovation pathways, rather than just a criminal enterprise. Therefore, India's response needs to incorporate four key elements: cutting-edge blockchain forensics, revised legal frameworks that treat cryptocurrencies as "digital evidence," specialized law enforcement training, and unprecedented international collaboration. Making India "drug-free" through "ruthless action against supply chains" and "humane approaches for victims" is necessary to defeat this threat, as Home Minister Shah underlined. This multifaceted approach recognizes the human cost of this changing challenge as well as its technological sophistication. 16. The ability of democratic countries to out-innovate criminal networks in the digital shadows will be tested over the next ten years.

X. REFERENCE:

- 1) 'Dark Web, Crypto, Drones Emerge as Challenges in Fight against Drug Trafficking: Amit Shah - The Hindu' <<https://www.thehindu.com/news/national/dark-web-crypto-drones-emerge-as-challenges-in-fight-against-drug-trafficking-amit-shah/article69088383.ece>> accessed 28 July 2025
- 2) 'Dark Web, Cryptocurrency, Drones Continue to Pose Challenge: Amit Shah - The Economic Times' <<https://economictimes.indiatimes.com/news/india/dark-web-cryptocurrency-drones-continue-to-be-challenge-amit-shah/articleshow/117145693.cms?from=mdr>> accessed 28 July 2025
- 3) 'Darknet Market and Fraud Shop BTC Revenues Decline amid Years-Long International Law Enforcement Disruption - Chainalysis' <<https://www.chainalysis.com/blog/darknet-markets-2025/>> accessed 28 July 2025
- 4) 'Darkweb Research: Past, Present, and Future Trends and Mapping to Sustainable Development Goals - PMC' <<https://pmc.ncbi.nlm.nih.gov/articles/PMC10695971/>> accessed 28 July 2025
- 5) FOUNDATION OR, 'The Dark Web Demystified: Its Role in Privacy, Crime, and Regulation' (orfonline.org) <<https://www.orfonline.org/expert-speak/the-dark-web-demystified-its-role-in-privacy-crime-and-regulation>> accessed 28 July 2025
- 6) Gopikrishna O, 'Economic Analysis of Darknet Drug Trade' (Social Science Research Network, 2 December 2022) <<https://papers.ssrn.com/abstract=4291659>> accessed 28 July 2025
- 7) 'India Cracks down on Darknet Drug Deals Using Crypto Tracking' <<https://cointelegraph.com/news/india-ncb-darknet-crypto-drug-payments>> accessed 28 July 2025
- 8) 'Press Note Details: Press Information Bureau' <<https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jun/doc2025625576401.pdf>> accessed 28 July 2025
- 9) Team C, '2025 Crypto Crime Trends from Chainalysis' (Chainalysis, 15 January 2025) <<https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>> accessed 28 July 2025
- 10) —, 'Darknet Market and Fraud Shop BTC Revenues Decline amid Years-Long International Law Enforcement Disruption' (Chainalysis, 16 May 2025) <<https://www.chainalysis.com/blog/darknet-markets-2025/>> accessed 28 July 2025

- 11) 'The Drug Trafficking Inserted in Cyber Space – How Social Networks, Virtual Currencies, Big Data and Software Applications Influence It – An Analysis of the United Nations Organization Members | Revista Internacional Consinter de Direito' <<https://revistaconsinter.com/index.php/ojs/0127>> accessed 28 July 2025
- 12) 'The Truth About The Dark Web – IMF F&D' <<https://www.imf.org/en/Publications/fandd/issues/2019/09/the-truth-about-the-dark-web-kumar>> accessed 28 July 2025

