4.1 Contours and Webs of Digital Arrest Pandemic

Sh. Aditya Hriday Upadhyay

Abstract

Digital Arrest has grown to be one of the most pressing law & order issues facing the country in the last couple of years. Execution of these crimes involves a very elaborate system whose contours stretch beyond borders and domains. Also, certain vulnerabilities of both victims and our legal enforcement system are accentuating this crime. This article analyses both sides: the contours of the system executing these arrests and our inner webs exposing us to their illicit actions. Lastly, based on recent policy responses, the article further explores potential approaches and preventive frameworks aimed at mitigating this rapidly expanding phenomenon.

Keywords

Digitization, Dark Web, Three Line System, Authority Bias, Salience Bias, Critical Thinking, Caller Name Presentation (CNAP), Cyber Forensics

Introduction

Recently, the Supreme Court of India, in a *suo moto* writ petition *titled "In Re: Victims of Digital Arrest related To Forged Documents"* expressed disbelief over the revelation that individuals across the country have collectively suffered losses amounting to nearly ₹3000 Crore due to the digital arrests scam. The occurrence of digital arrests is rising at a rate comparable to that of a pandemic. According to the Home Ministry, the cases reported on the National Cybercrime Reporting Portal have tripled between 2022 to 2024. Additionally, the total amount defrauded has surged by an astonishing 21 times during the same duration. This situation necessitates immediate action to mitigate the financial, psychological, and social damages caused by this issue. To develop and implement effective measures, we must first comprehend the contours of this crime and the inner complex webs that hinder our ability to combat this escalating threat.

Expanding Contours

The contours of this crime extend beyond borders and are quickly changing over time. A large network of scam operations is established in conflict-prone areas and special economic zones throughout Southeast Asia, particularly in Myanmar and Thailand, where government oversight is limited. Victims are enticed through deceptive job postings that promise attractive salaries and benefits, often involving travel through Bangkok, taking advantage of visa-free entry policies. These facilities serve as places where trafficked individuals are forced to engage in sophisticated scams. According to I4C, between January 2022 and March 2025, Indian authorities rescued 2,471 citizens from scam operations in Southeast Asia, where they had been deceived by false job offers and coerced into engaging in cybercrime.

Evolving *Modus Operandi*

Focusing on the methods used by offenders, these are also becoming increasingly complex and difficult to identify. The majority of scam calls utilize Voice over Internet Protocol (VoIP) technology through applications like WhatsApp and Skype. This complicates the ability to trace calls, especially when the servers are located outside of India. Fraudsters use artificial intelligence to replicate voices or generate fake video calls, convincingly impersonating officials. Recently, there has also been a notable rise in the utilization of the dark web for perpetrating these crimes. The dark web acts as a marketplace for stolen personal data, malware tools, and other illicit activities. Additionally, scammers demand payment through digital transactions such as UPI, cryptocurrency, or prepaid gift cards. The stolen funds are frequently divided into smaller amounts, funneled through numerous accounts, and ultimately transferred to offshore accounts for illegal purposes. This creates a method of easy layering, allowing them to evade law enforcement.

These Digital Arrest Scams usually have “three lines”. In the first line, a fraudster posing as an official like a bank representative contacts customers, informing them of discrepancy. The caller advises the customers to file a police complaint and offers to connect them to a higher official via WhatsApp or Skype. The fake police officials, dressed in a proper khaki uniform represent the second line. They speak in an intimidating manner and inform customers about a scam or crime committed by them. Then comes the third line involving senior level officials who inform customers of “Digital Arrest” and carry out further proceedings. Training given to the victims is based on this three-line system and performance-based incentives are also provided. With time, fraudsters are refining these methods and expanding to new domains.

Webs Impeding at Individual Level

Having seen the contours of the supply side, it is now essential to understand our inner webs which increase our vulnerability to these crimes. First, let us analyse our vulnerability at the individual citizen level. As we saw, a common aspect of these digital arrest scams is the almost constant appeal to authority: police and security forces; the judicial system and international organizations. It is this appeal to our inherent respect for authority (Authority Bias) that enhances the effectiveness of these scams. The repeated use of well-known public figures in various digital arrest scams highlights the exploitation of another cognitive bias, Salience. Victims tend to focus on a familiar name without questioning the likelihood of such a situation occurring.

Socio-economic factors also affect how vulnerable a person is to cybercrime. Individuals from disadvantaged economic backgrounds frequently do not have access to cybersecurity training and resources. This absence of cybersecurity education makes these communities more susceptible to exploitation by cybercriminals. Age is also a vulnerability that accentuates exposure to these scams. Senior citizens, especially those with minimal technological skills, are at a greater risk of falling prey to cybercrime. This demographic is frequently targeted by scams and phishing schemes because of their inadequate familiarity with technology and their increased tendency to trust online interactions.

In line with the Law of Unintended Consequences, the resounding success of Digitization in India has also given wings to these scams in various ways. In recent years, focus on digitization and consequent success has convinced a fair share of the population, especially elderly, that everything can be done electronically. Digitization especially in the Criminal Justice system has lent perceptual legitimacy to these digital arrests.

Webs Impairing the State Machinery

At the level of State, several loopholes leave us vulnerable to digital arrest. India's criminal justice system has multiple weaknesses that allow scammers to infiltrate. Currently, "digital arrest" is not a crime specifically defined under the Bharatiya Nyaya Sanhita, 2023 or the Information Technology Act, 2000. While several provisions in existing laws are used to pursue prosecutions in these cases, there isn't a specific law addressing digital arrests. This absence of specialized legislation hampers conviction rates. Additionally, most local police departments lack state of art technological tools and expertise required to investigate intricate cyber frauds. Some metropolitan authorities do possess required capacity and infrastructure but small district-level enforcement agencies are mostly poorly equipped. Even after identifying the suspects, the prosecution process is mostly delayed by complex procedural requirements, such as synchronization between states, forensic vetting, and the authentication of digital evidence. Thus, these webs at both collective and individual levels, are restricting our ability to act while empowering this rapidly growing threat.

Framework to Counter the Digital Arrest Pandemic

Having understood the contours of the perpetrators and the webs impeding the victims, we can proceed for developing strategies to combat this digital arrest issue.

- **Tackling the Individual Vulnerability**

  To begin with, it is vital to tackle psychological vulnerabilities at the individual citizen level. Initiatives to raise awareness and educate the public should be expanded through SMS, social media campaigns, the Cyber Dost initiative, the *Sanchar Sathi* portal and app, and digital displays in public areas such as metro stations and airports, emphasizing cyber safety and security. Additionally, systems should be put in place to bolster individuals' critical thinking skills when faced with potential digital arrest situations. For instance, India's telecom regulator could mandate that all communication services include a warning that appears during extended calls regarding digital arrests. From a behavioral standpoint, citizens need to overcome their natural bias toward authority and cultivate a more open mindset regarding the actions of law enforcement agencies, ensuring they verify any orders before placing their trust in them.

- **Legal and Policy Reforms**

  At the level of state, first we need to reform our legal and criminal justice architecture. The proposed Digital India Act should have elaborate provisions to tackle various intricacies of Digital Arrest Crime. Dedicated cybercrime units should be established in each district, staffed with skilled digital forensics professionals. Ongoing training and certification for law enforcement officials handling cyber-related incidents should be made compulsory. India's banking regulatory authority could implement best practices like Singapore to prevent fraudulent transactions. In Singapore, payment service providers are mandated to prevent users from attempting to withdraw over 50 percent of a customer's account balance within a 24-hour timeframe.

- **International Cooperation**

  We saw how the scope of these crimes extends beyond borders, as many scammers operate from foreign locations using infrastructure diffused across countries. Therefore, any single national effort is inadequate. Strengthening international collaboration through Interpol, partnerships with CERT, and Mutual Legal Assistance Treaties (MLATs) is essential for tracking, extraditing, and prosecuting cybercriminals operating overseas. To address the issue of international Voice over Internet Protocol (VoIP), a caller identification verification system, such as the "Caller Name Presentation (CNAP)" suggested by TRAI, is necessary to assist users in recognizing legitimate calls.

- **Technological Solutions**

  Finally, as we emphasize the need to "fight fire with fire," the solution to the digital arrest epidemic partially lies within technology itself. It is essential to create and deploy AI-powered tools like MuleHunter.AI that can monitor and detect fraudulent activities in real-time, allowing for quick responses to new dangers. We must regularly utilize and update antivirus software and firewalls to identify and eliminate threats. On a governmental level, better-equipped cyber forensic labs can enhance law enforcement's capacity to analyze digital evidence.

Conclusion

To put it together, digital arrest has transformed from a specialized crime targeting particular individuals and using niche mediums into a widespread issue that is rapidly changing and evolving at an unprecedented pace. Our shared vulnerabilities are increasingly exposing us to criminal activity. We need to recognize these challenges and take immediate action based on the aforementioned policy measures. Only coordinated efforts across all levels can halt the proliferation of this crisis and protect both the interests of innocent individuals and the governance structure of the nation as a whole.

References

i. Singh, S. (2025). *Digital Arrest: The modern-day cyber scam*. NITI Aayog. https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf

ii. Chauhan, J. (2024). *Digital arrest: An emerging cybercrime in India*. International Journal of Law, Management & Humanities. https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf
Rej, A. (2024). *India's digital arrest scams*. The Interpreter, Lowy Institute. https://www.lowyinstitute.org/the-interpreter/india-s-digital-arrestscams#:~:text=What%20is%20alarming.

iii. The Indian Express. (2025). *2,471 Indians rescued from scam centres in Southeast Asian countries during 2022–25: Govt data*.

iv. Uma. (2025). *Unmasking digital arrest: An emerging threat to modern society in India. International Journal of Law, 11(5), 45–50.*

https://www.lawjournals.org/assets/archives/2025/vol11issue5/11210.pdf

v. Business Standard. (2025). *Digital arrests: Inside India's biggest scam and how to tackle it.*

vi. The Association of Banks in Singapore. (2025). *Banks to launch enhanced safeguards from 15 Oct 2025 to better protect accounts* [Press release]. https://abs.org.sg/docs/library/banks-to-launch-enhanced-safeguards-from-15-oct-2025-to-better-protect-accounts.pdf

vii. Telecom Regulatory Authority of India. (2025). *TRAI issues advisory on digital arrest scams* [Press release]. https://www.trai.gov.in/sites/default/files/2025-10/PR_No.122of2025.pdf

viii. Ministry of Finance. (2025). *Government announces measures to counter digital arrest scams* [Press release].https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112323&reg=3&lang=2

*****

Author's Profile

Mr. Aditya Hriday Upadhyay is an Officer Trainee of the Indian Revenue Service (Income Tax), 2025 batch, who has undergone the Special Foundation Course at the National Communications Academy – Finance (NCA-F), Ghitorni, New Delhi. He holds a B.Tech. degree in Civil Engineering from the Indian Institute of Technology (IIT) Roorkee, where he demonstrated strong academic engagement and research aptitude.

He has been a recipient of the prestigious Summer Research Fellowship of the Indian Academy of Sciences, a recognition awarded for exceptional research potential and scholarly merit. His intellectual interests lie at the intersection of public policy, technology, and emerging governance models, with a focus on leveraging data-driven and technologically enabled frameworks for improved institutional effectiveness.