ISSN 2395 2733

# Sardar Vallabhbhai Patel National Police Academy Journal



Vol. LXXV, No. 1
JUNE, 2026

## ABOUT THE ACADEMY

Sardar Vallabhbhai Patel National Police Academy is a premier training institute of the country which trains officers of the Indian Police Service. The Academy conducts Basic Training, mandatory Mid Career Training Programmes & a host of In-Service Courses.

The Academy trains officers of other Central Services i.e., IRS, IFoS, etc., as well as Police Officers of friendly neighboring countries. The Academy also promotes research in Police subjects.

***



To order or subscribe, please contact :
The Deputy Director (Publications), SVP National Police Academy, Shivarampally,
Hyderabad - 500 052 Phone ; 91-40-24015151 to 58, 91-40-24235999
Fax: 91-40-24015179, E-mail: publicationsec@svpnpa.gov.in

# *SVP National Police Academy*

# *Journal*

*June, 2026*

Vol. LXXV, No. 1

*Published by*
SVP National Police Academy
Hyderabad

ISSN 2395 2733

# *SVP NPA Journal*

*June, 2026*

## EDITORIAL BOARD

Volume 75 Number 1, June 2025

# Contents

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol.& LXXV No.1, (P. 1-14)

# 'Detecting Deception' in Criminal Investigations – Need to evolve 'Structured Interrogation Methods'

Venkataraman G* & Venkatesh Balasubramanian**

***Abstract:***

*Criminal investigations substantially involve, collecting the evidences from the scene of crime, identifying the suspects/accused, and linking the evidences beyond reasonable doubt to prove that the accused only had committed the offence. 'Eliciting' information from witnesses is a major part of the investigation, and the most difficult part is to elicit the information which is only within the knowledge of the suspect/accused, who have legal protections that they need not share the information which is self-incriminatory. The investigator is expected to be an 'expert' interrogator, adept at detecting 'lies/deception' by the witnesses/ suspects/accused and at the same time is also expected to be skilful in eliciting the 'truth' from them. This requires the development of 'Structured Interrogation Methods'.*

***Key Words****:*

*Lie-detection, Detecting deception, Criminal investigation, Interrogation, Structured Interrogation Methods*

*Indian Police Service Officer of 1994 Batch, belonging to Tamil Nadu Cadre (presently serving as Director General of Police, Administration).

**Professor, Department of Engineering Design, Indian Institute of Technology, Madras.

## 1. Introduction:

Investigating a crime is both a science and an art.

It is a 'science', because whatever evidence, especially the material objects like the weapon used in the crime, blood stains, DNA, hair follicles, bones, etc., collected during the investigation should meet the rigorous standards of scientific proof so that the courts can conclude safely that the accused had committed the crime 'beyond reasonable doubt' and that no one else could have done that in the given circumstances. As a pre-requisite, the Investigating Officer needs to satisfy himself/herself that the evidence is in fact what he/she believes it to be, and he/she can rest assured of it only with the opinion of a Forensic Scientist or an expert in the field, who is going to depose before the court and convince the court, the nature of evidence based on sound and accepted principles of scientific theory.

Investigation is also equally an 'art', because of the 'human factor' involved. Even to identify the relevant material objects implicating a 'suspect', the information is mostly elicited from the various witnesses who could have witnessed it, or who had been around the scene of the crime in and around the given time, etc. It becomes further complicated when the Investigating Officer cannot discriminate who a 'suspect' is amongst the many 'witnesses' with whom he/she is interacting with. It involves a lot of creativity, communication skills, and innovativeness to make witnesses speak and come out with all that they know. It is further compounded in many instances where there are no witnesses at all, and the Investigating Officer is straight-away looking for suspects.

Investigation substantially involves collecting the evidence from the scene of the crime, identifying the suspects/accused, and linking the evidence beyond a reasonable doubt to prove that the accused only had committed the offense. Many a time, even the witnesses/victims may not be forthcoming to share all the information they have and it is entirely on the persuasive skills of the investigator that he/she succeeds in collecting the maximum possible information from them. In this endeavor, the most difficult part is to elicit the information which is only within the knowledge of the suspect/accused. There are legal protections that ensure that he/she need not share information that is self-incriminatory. Even if the accused

'confesses to committing the crime', the same could not be used as 'evidence' except when it is made 'voluntarily' and leads to the discovery of material facts which corroborate his/her 'confession'.

'Eliciting' information from witnesses is a major part of the investigation. Many further courses (lines) of investigation emanate from the information (clues) provided by the witnesses. Similarly, concerning the information which is exclusively within the knowledge of the 'suspect/accused', there is no means of verifying the same from any other source, and the 'missing piece of evidence' to complete the investigation is fully dependent on his/her revelation. The investigator is left with no choice but to 'believe' what he/she says. But it is natural to expect that the 'suspects/accused' may not always reveal the truth and may attempt to conceal, partly reveal, deny or even deceive the investigator. The investigator is expected to be adept at detecting 'lies/deception' by the witnesses/suspects/accused and at the same time is also expected to be skilful in eliciting the 'truth' from them. To achieve the same, he/she needs to be an 'expert' interrogator.

Though several studies have been done on 'lie-detection' and many scientific theories have been developed, about the practical utility of the same, much is left to be desired. Almost all of them were done in laboratory settings (with mostly college students as subjects) and lacked the credibility of 'field studies'. There are tools such as polygraphs, brain mapping, narco-analysis, etc., which have been developed to detect 'lies' and the same could be administered on the subjects (suspects) only by 'experts' in a formal laboratory/hospital setting, and not in a regular day-to-day policing environment. Also, the success of such tools depends to a great extent on the 'questionnaire' developed in coordination with the 'experts' who conduct the tests. Even with such tests, one can detect 'lies', but positive 'elicitation of truth' is still dependent on the 'interrogation' skills of the investigator. It is generally believed that 'experienced' investigators are better than 'novice' investigators in detecting lies and eliciting truth and that they have better 'interrogation' skills. However, there is no research work to prove the same.

## 2. Literature Review:

### 2.1Theories on Deception:

One important theory on deception is that it is accompanied by emotional processes, specifically, negative emotions such as guilt (about the act the liar is trying to cover up and possibly about the act of lying itself), fear (that the lie might be uncovered), and anxiety (Ekman, 1969). However, positive emotions are also possible during lying, as liars may experience glee at the prospect of deceiving the interrogator. This emotional theory of deception is closely linked to the leakage hypothesis, which states that cues to an underlying emotion may leak, as non-verbal signs of the emotion the liar is attempting to suppress (Ekman P. , 2009)**.**

Cognitive Load theory is another important theory on deception, according to which, lying is cognitively more taxing and more mentally demanding than speaking the truth (Zuckerman, 1981). According to the Cognitive Load theory, cognitive processes may involve cold cognition wherein the processes are rational and deliberate, and also hot cognition, where the processes are emotional. Studies have also indicated that cues to cognitive load are not always easy to define. Some cues are rigid body language which could also indicate tension and stress, making more speech errors, taking longer pauses before questions, and a general decrease in body movements, especially the peripheral parts like arms, fingers, feet, legs, etc. It is also associated with a decrease in the frequency of eye blinks (Leal, 2008). Lying involves the creation of a plausible story with suppression of truth, which requires extra focus to ensure credibility and acceptance, and thus cognitively more demanding as compared to telling the truth (Vrij, 2011).

According to the theory of human social interaction, people behave like actors on the stage as if life is a theatre, and they are typically motivated to control the impressions others have of them, to come across in desirable ways (Goffman, 1959). This led to the development of the theory of self-presentation perspective on deception (De Paulo, 2003), according to which both truth-tellers and liars have the same intention of giving an impression of being ‘honest’; but the liars claim to honesty is illegitimate; that they display ‘deception discrepancy’, the difference between their

claims and reality; and that they might experience a higher degree of mental busyness and deliberateness (De Paulo, 2003, p. 78).

### 2.2 Lie Detection Tools:

The existing literature on lie detection techniques broadly falls into three broad categories, viz., observations of behaviour, analysis of verbal elements (including the content of the speech), and measurement of psychophysiological measures, mainly polygraph. Given the lack of reliable cues, poor accuracy rates in studies, and difficulties in assessing them, tools based on the observations of behaviour are not practically viable.

### Verbal Lie Detection Techniques:

Scientific Content Analysis (SCAN): It is a verbal lie-detection technique developed by a former Israeli police lieutenant and polygraph examiner Avioam Sapir in which the subject is asked to write down in his/her hand-writing details of all that he/she did during the period in question and then by an expert would analyze the same based on pre-determined criteria regarding use of certain words or phrases, which would reveal whether the subject is lying. (Sapir, 1987/2000). The tool has been criticized for lack of any theoretical framework, not being scientific, and lacking empirical evidence (Porter, 1996).

Statement Validity Analysis (SVA) is another lie-detection tool. It is based on cues relating to cognitive load and impression management. It is a comprehensive framework for establishing the veracity of statements. It consists of a case-file analysis, a semi-structured interview, and a Criteria Based Content Analysis (CBCA) to assess the quality of the transcribed interviews and their evaluation with a Validity Checklist (Vrij A. , 2008). CBCA is built on the theory, according to which reports of events arising out of one's self-experience are likely to be different in many ways from those that are based on imagination, and that lies and truths differ in their verbal characteristics (Undeutsch, 1982). According to critics, the assumption that CBCA criteria like unusual details, superfluous details, reproduction of speech, spontaneous corrections, admitting lack of

memory, etc. are indicative of truth, is not supported by any underlying theory and that there is no link between the Undeutsch hypothesis and the criteria of CBCA (Vrij A. , 2005).

Reality Monitoring is another verbal lie detection tool based on social cognitive theory and memory theory according to which the reports of imagined events (lies) are different from the reports of experienced events which are based on real memories (Johnson, 1981). Real experiences will have memories of two types of information, viz., perceptual information and contextual information. Perceptual information consists of visual details, touch, taste, smell, sound, etc. Contextual information includes those of time and space. The perceptual and contextual information will be clear and vivid, as compared to the imagined ones (Johnson K. R., 1998). It involves the application of certain criteria to the written statements to classify them as truthful or deceptive and requires trained coding.

Verifiable Details is another verbal lie detection tool exploiting the conflicting motivations of the liars who try to include a lot of details in their statement to create an impression of being 'honest' and at the same time avoid details that would make them get caught, whereby liars provide more unverifiable details than truth tellers (Nahari, 2012b).

## Psychophysiological Lie Detection Techniques:

**Polygraph** is the most popular psychophysiological lie detection tool. It is based on the principle that when there is a conscious attempt to deceive or conceal any information, the fear of detection will cause heightened levels of arousal and thus significant physiological changes in electro-dermal (Galvanic Skin Resistance) responses, respiration, pulse rate, and blood pressure, which are controlled by Autonomous Nervous System and is involuntary (Podlesny, 1978).

Anxiety based Polygraph tests include Relevant-Irrelevant Test (RIT) based on the principle that answers to the Relevant Questions show more psychophysiological changes because of the anxiety of detection and the Comparison Question Test based on the principle that guilty people show more psychophysiological changes to both the Relevant Questions and

Comparison Questions than the truth-tellers who need not deceive in answering the Relevant Questions (Raskin, 2002).

Recognition-based Polygraph tests are based on the principle of psychophysiological response to personally stimulating stimuli based on the theories of Pavlov. The Concealed Information Test is one such polygraph test that is based on the principle of orienting reflexes wherein whenever the guilty person recognizes specific details of the crime, he will be affected by orienting reflexes (Sokolov, 1963 Vol 25) and thus it will lead to heightened arousals and psychophysiological indicators.

The success of the polygraph tests depends on the framing of questions. There are criticisms against polygraph tests. It is not validated based on a theory. The procedures for administering it are not standardized. It is not accepted as evidence in courts, and is primarily a tool for investigation, that too, only with the willing participation of the suspect/accused. Also, it has been misused by law enforcement officers to obtain false confessions from the accused (Garrett, 2011).

**P-300 as a Lie Detector:** When a subject is exposed to a stimulus, whether verbal or non-verbal like visual, MERMERs (Memory and encoding related multi-faceted electroencephalographic responses) were elicited only with regard to the 'probe stimuli' if he/she was involved or participated in the event corresponding to the stimuli, and that no such response was elicited to irrelevant stimuli (Farwell, 2001).

### 2.3 Importance of Interviewing/Interrogation in Detecting Deception:

Though it is generally believed that detection can be detected from the leakage of cues by the liar, there is not much literature to support it. According to one theory, it is more of an interactive enterprise wherein during managing the conversations, the lie-catchers play an important part in eliciting appropriate responses from the subject (Hartwig, 2005). During interrogations, the liars while striving to strike a balance between withholding incriminating information and providing enough information to appear credible, make choices to admit what is not incriminating, and adopt an avoidance strategy or escape strategy to avoid giving critical information. To find deception, investigators must ask well-thought-out,

systemic and strategic questions that could differentiate and elicit different responses from those telling the truth and liars (Levine, 2010) (Vrij A. a., 2012).

The Asymmetric Information Management Technique helps elicit truth by encouraging forthcoming verbal strategies from subjects and leads to a withholding strategy by liars, as they would avoid forthcoming with the information to avoid getting exposed (Cody Normitta Porter, 2020) and also, because it is cognitively more demanding to add any information especially when they have to create a story to fit in their lies.

Increasing the Cognitive Load on the liars increases the lie-detection accuracy levels (Vrij A. R., 2015). Asking the subjects to state their versions of the events in a reverse order increases their cognitive load more than that it would cause on truth-tellers (Gilbert, 2006). Cognitive Load is also increased when the subjects are asked to keep eye contact with the interviewer (Doherty-Sneddon, 2005). Even though liars may plan and prepare well to look credible when they lie, it would be difficult to be fully prepared for every possible question, and thus if unanticipated questions are asked, they would be exposed to a higher cognitive load (Granhag, 2008).

One of the latest developments in the field of interrogation is the concept of Strategic Use of Evidence (SUE). It is founded upon the psychological theory of Self-Regulation according to which individuals control their behaviour in such a way as to steer away from undesirable outcomes and move towards a favourable outcome (Forgas, 2009). The truth-tellers and liars adopt different strategies to create a favourable impression. While liars try to conceal information because of the threat of getting exposed, the truth-tellers try to reveal as much on the apprehension that his/her truth may not be believed. The liars are not aware of the nature of the information, and the amount of information, the interviewer has. Hence, the interviewer withholding the potentially incriminating evidence and using it in pieces to elicit the truth will lead to increased cognitive load and the liars will adopt a strategy of avoidance and escape/denial, which will be reflected in their verbal responses (Granhag P. M., 2015). A tool based on the SUE framework is Evidence Framing Matrix (EFM), which

helps to plan, structure and pose questions during the interrogation by strategically disclosing pieces of information with differing degrees of specificity of the information and the source of it, in such a way that because of the increased cognitive load, the subject exudes cues to deception, which brings out 'statement-evidence inconsistencies' in the statements of the subject (Granhag P. L., 2013).

### 2.4 Interrogation Techniques:

In Scharff Technique named after Hanns Scharff, the German Air Force pilot during the Second World War, who had invented this technique, information is collected from the subjects in a friendly conversational way, making them believe that the interrogator knows much more and that what they reveal is already in his/her knowledge, and thus they are not revealing anything. This presupposes that the interrogator has got some information to make the suspect believe in that manner. Though it is not based on any scientific theory, a meta-analysis of experimental tests shows that it is effective (Luke, 2021)

The Reid Technique is widely used in the United States. It is a tool for 'Interviewing and Interrogation'. It was developed by John E. Reid, a former police officer. In this technique, first a 'factual analysis' is made about the available information about the crime and the probable suspect, including his/her bio-social data, to form an opinion on whether the suspect could be proceeded against. In the second stage, the suspect is 'interviewed' using the tools of 'Behaviour Analysis Interview'. It is a non-accusatory one. It involves standard investigative questions. It also includes 'behaviour-provoking' questions. These questions help in eliciting symptoms of deception. In the third stage, the suspect is treated as an accused, and the interview becomes interrogation in an accusatorial manner, seeking specific answers to pointed evidences. This stage involves positive confrontation with the available evidences, development of a theme about the crime, countering the denials by the accused, overcoming the objections raised by the accused, continued interrogation and retention of his/her attention for eliciting further details even while dealing with his/her passive mood, posing alternatives to his/her defenses/alibi, asking

the suspect to narrate the complete details of the offense, and converting the same to a written confession (Kassin, 2007).

PEACE method of interrogation is another technique. It is in practice in United Kingdom. This, Preparation and Planning, Engage and Explain, Account, Closure and Evaluate (PEACE), method has been developed as an alternative to accusatorial approach of the Reid's Technique. It is less confrontational and does not start with the assumption that the suspect is the accused or guilty. It is designed to build a conducive environment of rapport with the subjects or suspects, encouraging them to fully state their version without interruption and elicit more information through open-ended questions (Bull, 2004), thereby avoiding the scope for 'confirmation bias' which could be present in the Reid Technique (Scherr, 2020).

### 2.5 Importance of Baselining in Lie-detection Tests:

People's behaviour, physiological responses, speech, body movements, etc., are not uniform across individuals (DePaulo, 1998). It is not feasible to benchmark any standard reading as a baseline to compare people's behaviours when subjected to various lie-detection tests like Comparison Question Test, Concealed Information Test, etc. Hence, it is important to do 'baselining' within the subjects, i.e., arriving at the 'baseline' for that particular subject about his/her normal 'readings' so that his/her readings when subjected to the critical elements of 'lie-detection' are comparable. Also, questions must be properly framed to bring out this 'within-subject' comparisons clearly in the lie-detection tests (Ben-Shakar, 2008) (Grubin, 2008) (Vrij A. , 2008). People behave differently in different situations on a relative level amongst different individuals. Similarly, individuals too behave differently in different situations at the individual level. Any baselining without considering the differences in situational factors may lead to the 'fundamental attribution error' wherein the effect of situations is overlooked in evaluating the response of the subject (Ross, 1977).

## 3. Present Scenario:

The average accuracy of finding lie-detection is 54% which is no better than the chance rate of 50%, though it is generally felt that it may not be

true for those professionals who make judgements of truth or lie as part of their official works, like police officers, etc. (Vrij A. , 2008). Contrary to common belief, lie-detection accuracy rates of presumed 'experts', mostly police officers, do not significantly outperform the success rates of laypeople (Meissner, 2002) (Bond, 2006). The possible reasons for poor accuracy rates in lie detection are that practitioners rely on behaviours which are not actually indicative of deception (wrong subjective cue hypothesis) or that the cues themselves are so weak (weak objective cue hypothesis) (Hartwig M. C., 2011).

In the entire investigation process, the most difficult component is eliciting the 'truth' from the suspect/accused, especially in cases where the said 'truth' is only within the knowledge of that person, and nobody else. In such cases, there is no other way, but to rely on his/her 'confession', which is 'obtained' after prolonged iterative process of interrogations. It is possible that under certain circumstances, the said 'confessions' may not be the 'ground truth', and there is no proven way to approve or disprove the same. The courts just decide whether the evidences are proved beyond reasonable doubt or not.

## 4. Conclusion:

In this background, improving the capabilities of the Investigating Officers in the area of interrogation is crucial not only to detect lies, but also to fully unravel the truth. Also, given the poor conviction rates in criminal cases, it is necessary to improve the quality of investigation, which is contingent on the interrogation skills of the investigators.

Similar is the belief that experienced investigators will be better than novice investigators in detecting lies. When the police officers' performance as compared to lay people, in detecting lies, is not significantly different, the common belief that experienced investigators will be better than novice investigators in detecting lies, cannot be taken as granted.

Hence, it is essential that 'structured interrogation methods' are designed incorporating the findings of various theories on 'detecting deception' and 'eliciting information' in a multi-disciplinary approach

involving criminology, psychology, sociology, anthropology, communications, linguistics, etc., and the investigators are properly trained on the same.

This will foster scientific thoughts in the investigative processes, improve the quality of investigation, and the experience of witnesses/suspects in their interactions with the investigating officers. Eventually, it will further the interests of justice and result in better administration of the Criminal Justice System.

## Statements and Declarations:

**Ethical Considerations :** Not applicable.

**Consent to Participate** : Not applicable.

**Consent for Publication :** Not applicable.

**Declaration of Conflict of Interest:** The author(s) declared no potential conflicts of interest with regard to the research, authorship, and/or publication of this article.

**Funding Statement:** The author(s) received no financial support for the research, authorship, and/or publication of this article**.**

## References

1. *Ben-Shakar, G. (2008). The case against the use of polygraph examination to monitor post-conviction sex offenders. Legal and Criminological Psychology, 13, 191-207.*
2. *Bond, C. a. (2006). Accuracy of Deception Judgements. Personality and Social Psychology Review, Vol.10, No.3: 214-234.*
3. *Bull, R. &. (2004). Conversation Management. In R. M. Bull, Investigative Interviewing: Psychology and Practice. Wiley.*
4. *Cody Normitta Porter, E. M. (2020). Lie-Detection by Strategy Manipuraltion: Developing an Asymmetric Information Management Technique. Journal of Applied Research in Memory and Cognition, 232-241.*
5. *De Paulo, B. L. (2003). Cues to deception. Psychological Bulletin, 124, 74-118.*
6. *DePaulo, B. &. (1998). Nonverbal Communication. In S. F. D.T. Gilbert, The Handbook of Social Psychology (pp. 3-40). Boston, MA: McGraw-Hill.*
7. *Doherty-Sneddon, G. P. (2005). Gave aversion: a response to cognitive or social difficulty? Memory and Cognition, 33, 727-733.*
8. *Ekman, P. (2009). Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage. New York: W W Norton & Co.*

9. *Ekman, P. F. (1969). Nonverbal leakage and clues to deception. Psychiatry, 88-106.*
10. *Farwell, L. a. (2001). Using Brain MERMER Testing to Detect Concealed Knowledge Despite Efforts to Conceal. Journal of Forensic Sciences, 1-9.*
11. *Forgas, J. B. (2009). They psychology of self-regulation: an introductory review. In J. B. Forgas, Psychology of Self-Regulation: Cognitive, Affective, and Motivational Processes (pp. 1-17). New Yokr: Psychology Press.*
12. *Garrett, B. (2011). Convicting the Innocent: Where Criminal Prosecutions Go Wrong. Cambridge, MA: Harvard University Press.*
13. *Gilbert, J. F. (2006). The effects of varied retrieval cues on reminiscence in eyewitness memory. Applied Cognitive Psychology, 20, 723-739.*
14. *Goffman, E. (1959). The Presentation of Self in Everyday Life. New York: Anchor.*
15. *Granhag, P. a. (2008). A New Theoretical Perspective on Deception Detection: On the Psychology of Instrumental Mind Reading. Psychology, Crime and Law, Vo.14, No.3: 189-200.*
16. *Granhag, P. L. (2013). Eliciting Cues to Deception by Tactical Disclosure of Evidence: The First Test of the Evidence Framing Matrix. Legal and Criminological Psychology, Vol. 18, 341-355.*
17. *Granhag, P. M. (2015). The Strategic Use of Evidence (SUE) Technique: A Conceptual Overview. In A. V. P.A. Granhag, Deception Detection: Current Challenges and New Directions. Chichester, UK: Wiley.*
18. *Grubin, D. (2008). The case for polygraph testing of sex offenders. Legal and Criminological Psychology, 13, 177-189.*
19. *Hartwig, M. C. (2011). Why Do Lie-Catchers Fail? A Lens Model Meta-Analysis of Human Lie Judgments. Psychological Bulletin, Vol.137, No. 4: 643-659.*
20. *Hartwig, M. P. (2005). Deception Detection via Strategic Disclosure of Evidence. Law and Human Behaviour, Vol 29, 469-484.*
21. *Johnson, K. R. (1998). False Memories and confabulation. Trends in Cognitive Sciences, 2, 137-146.*
22. *Johnson, M. R. (1981). Reality Monitoring. Psychological Review , 88, 67-85.*
23. *Kassin, S. S. (2007). Police Interviewing and Interrogation: A Self-Report Survey of Police Practices and Beliefs. Law and Human Behaviour, Vol. 31: 381-400.*
24. *Leal, S. a. (2008). Blinking during and after Lying. Journal of Nonverbal behaviour, Vol.32, 187-194.*
25. *Levine, T. A. (2010). Increasing Deception Detection Accuracy with Strategic Questioning. Human Communication Research, Vol 36, 216-231.*
26. *Luke, T. J. (2021). A meta-analytic review of experimental tests of the interrogation technique of Hanns Joachim Scharff. Applied Congitive Psychology, 35: 360-373.*
27. *Meissner, C. a. (2002). "He is Guilty! Investigator Bias in Judgements of Truth and Deception". Law and Human Behaviour, Vol. 26, 469-480.*
28. *Nahari, G. V. (2012b). Exploiting liars' verbal strategies by examining the verifiability of details. Legal and Criminological Psychology .*
29. *Podlesny, J. R. (1978). Effectiveness of techniques and physiological measures in the detection of deception. Psychophysiology, 15, 344-358.*
30. *Porter, S. Y. (1996). The langueage of deceit: an investigation of the verbal clues to deception in the interrogation context. Law and Human Behaviour, 443-459.*
31. *Raskin, D. H. (2002). The omparison question test. In M. Kleiner, Handbook of Polygraph Testing (pp. 1-47). San Diego, CA: Academic Press.*

32. *Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. In L. Berkowitz, Advances in Experimental Psychology (pp. 174-221). New York: Academic Press.*
33. *Sapir, A. (1987/2000). The LSI Course on Scientific Content Analysis. Phoenix: Laboratory for Scientific Interrogation.*
34. *Scherr, K. R. (2020). Cumulative disadvantage: A psychological framework for understanding how innocence can lead to confession, wrongful conviction, and beyond. Psychological Science, 15, 353-383.*
35. *Sokolov, E. (1963 Vol 25). Higher Nervous Functions: The Orienting Reflex. Annual Review of Physiology, 545-580.*
36. *Undeutsch, U. (1982). Statement reality Analysis. In A. Trankell, Reconstructing the Past: The Role of Psychologists in Criminal Trials (pp. 27-56). Deventer: Kluwer.*
37. *Vrij, A. (2005). Criteria Based Content Analysis: A Qualitative Review of the First 37 studies. Psychology, Public Policy, and Law, Vol. 11, 3-41.*
38. *Vrij, A. (2008). Detecting Lies and Deceit: Pitfalls and Opportunities. New York: John Wiley & Sons Ltd.*
39. *Vrij, A. a. (2012). Eliciting Cues to Deception and Truth: What Matters are the Questions Asked. Journal of Applied Research in Memory and Cognition, Vol. 1, 110-117.*
40. *Vrij, A. G. (2011). Outsmarting the liars: towards a cognitive lie detection approach. Current Directions in Psychological Science, 20, 28-32.*
41. *Vrij, A. R. (2015). A Cognitive Approach to Lie Detection: A Meta-Analysis. Legal and Criminological Psychology.*
42. *Zuckerman, M. D. (1981). Verbal and nonverbal communication of deception. Advances in Experimental Social Psychology, Vol. 14, 1-57.*

**Author's Profile:**

1. Mr. Venkataraman G, an Indian Police Service Officer of 1994 Batch, belonging to Tamil Nadu Cadre (presently serving as Director General of Police, Administration).
   Email: venkatips@gmail.com
2. Mr. Venkatesh Balasubramanian, Professor, Department of Engineering Design, Indian Institute of Technology, Madras.
   Email: chanakya@iitm.ac.in

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 15-28)

# A Study on Brain Mapping, Polygraphy, and Narco Analysis Tests in India: Legal and Scientific Perspectives

Dr. Divya Raviya Jadeja*

***Abstract:***

*It has become clear in the process of investigation of crime that truth seeking is becoming increasingly mixed with developments in neuroscience and psychophysiology. Of these investigative techniques, brain mapping, polygraph and narco would be those that stand out most in terms of detecting deception, memory recognition and the obtaining of information from suspects. Brain mapping uses a technique called electroencephalography (EEG) or functional magnetic resonance imaging (fMRI) to discover involuntary neural reactions that occur when exposed to information related to crime. Lying is detected through physiological changes such as heart rate, respiration and skin conductivity that may relate to deceptive responses, in a test called "polygraphy". Narco analysis involves administering drugs to trigger a semi-conscious state to the aim of lowering inhibitions and promoting disclosures. These methods have a great investigatory potential but are not entirely scientifically sound and have not been legally accepted. Brain mapping is still experimental, and is difficult to interpret due to variability from person to person. The rate of failure to detect deception is extremely high, as is also the rate for errors that are interpreted as "deception" when in reality they are triggered by factors other than deception and have to do with emotional*

*Deputy Superintendent of Police (DSP) currently posted at the Headquarters in Kheda-Nadiad District, Gujarat

*state. The dangers of false memory and suggestibility with the use of narco analysis make it an ethically dubious technique. Legally, all three techniques instantly infringe an individual's right to not incriminate themselves when used without their knowledge or consent and hence their use in obtaining results is entirely inadmissible in court so long as there is no corroboration through independent evidence, as held by the Supreme Court of India in Selvi v. State of Karnataka (2010). Though these methods have some drawbacks, they are still used in investigations in cold cases, pre-employment screening, in terrorism investigations, and in cognitive research. Their use serves as a stark reminder of the importance of balancing innovation in science with key human rights considerations. The adoption will need to be accompanied by strong ethical protections, free consent, medical monitoring and continuous scientific validation. This article thoroughly examines the scientific development, legal provisions, application and limitations of brain mapping, polygraphy and narco analysis, and makes information available for all stakeholders—including law enforcement, legal professionals and researchers— confronted by the complicated and evolving landscape of science and the law.*

***Keywords:***
*Brain Mapping, Polygraphy, Narco Analysis, Legal Admissibility, Forensic Investigation*

## 1. Introduction:

In recent years the criminal justice system has made significant changes, reflecting changes in science, technology and psychology. Although eye evidence, physical evidence, and forensic analysis are still recognized as key foundational aspects of investigations, innovative approaches, supported by technology, are being introduced to aid investigations to increase the accuracy, efficiency and breadth of investigations. Of these developing technology options, brain mapping, polygraphy and ‘narcology’ tests have received considerable publicity for revealing the

hidden truth, identifying dishonesty and revealing the thoughts in mind of suspects.[1]

Brain mapping uses a neurophysiological technique to analyse brain pattern and looks for brain recognition or familiarity with information that the suspect may be unable and unwilling to report, including information relating to a crime. The lie detector test (polygraphy) is the common name for measuring involuntary, physiological arousal like heartrate, blood pressure, and galvanic skin response (GSR) that occurs during questioning due to stress or deception. In contrast, within narco analysis they are fed drugs or chemical agents that have a sedating or psychoactive effect, which is supposed to make it easier for them to give out information than if they were awake.[2]

These methods are not designed to take the place of traditional investigative methods, but are additional tools that can be used to provide investigative leads, confirm other evidence, or clarify and reconstruct actions during investigational procedures in complex cases. But their use is not unproblematic. There are great variations in the reliability of these techniques: brain mapping is a scientific technique with potential while psychophysiological is psychologically and physiologically liable to variation while narco gives rise to serious doubts on suggestibility and memory formation of false memories.[3]

In addition to scientific issues, these techniques raise critical legal and ethical questions, such as the admissibility of the results in court, the principle against self-incrimination, informed consent, the protection of human rights, and many others. The potential benefits of these technologies for policing must be weighed against concerns for their constitutionality and ethical implications, as the deployment of these tools

---

[1] *Farah, M. J., & Heberlein, A. S. (2007). "Brain Imaging and Memory Recognition: Scientific and Legal Perspectives." Nature Reviews Neuroscience, 8, 108–118.*

[2] *National Research Council (2003). The Polygraph and Lie Detection. Washington DC: National Academies Press.*

[3] *Inbau, F. E., Reid, J. E., Buckley, J. P., & Jayne, B. C. (2013). Criminal Interrogation and Confessions, 5th Edition.*

brings multiple scientific and legal challenges for law enforcement, legal professionals and policymakers.[4]

## 2. Scientific Evolution:

Brain mapping, polygraphy, and narco analysis are three examples of the merging of three domains (neuroscience, physiology, psychology) in the field of forensic investigation. Although there are some different methods behind the techniques, they all serve the purpose of helping investigators find truth, understand how their participant is thinking, and assess the credibility of the words of their suspect.[5]

### 2.1 Brain Mapping:

Brain mapping is the systematic use of advanced neuroimaging studies and tests (specifically but not limited to Electroencephalography (EEG), Functional Magnetic Resonance Imaging (fMRI), and Quantitative EEG (QEEG)) to study the brain's activity. Brain mapping is used to match a brain pattern to a recognition of the stimuli involved in a crime in forensic applications, of course. The scientific underpinning of brain mapping studies can be traced back to the 1960s and 1970s when investigations focused on the link between measures of brain activity and memory and cognition. The technique has undergone major development over the last few decades and easy detection of P-300 waves is now used in many forensic's applications – for example, in which the brain produces different signals when viewing familiar or meaningful stimuli. The scientific basis for brain mapping is that the brain will react automatically to stimuli it recognizes, even if the person denies knowing what the stimuli is. These involuntary movements are those that are recorded with the hope of obtaining objective information about recognition or knowledge, which can be used to reconstruct events and/or the facts of which the movements are involuntary have been attested. Even though it has the potential to

---

[4] *Saxena, A. K., & Singh, J. (2015). "Narcoanalysis and Legal Implications in India." Indian Journal of Legal Medicine, 42(2), 54–62.*

[5] *Meijer, E. H., Verschuere, B., Merckelbach, H., & Ben-Shakhar, G. (2017). "Cognitive Forensics: Brain-Based Techniques for Criminal Investigation." Trends in Cognitive Sciences, 21(7), 525–537.*

succeed, brain mapping has not yet been sufficiently approved in large scale use to warrant its interpretation with great certainty, which relies greatly on the accuracy of the technology and the skill of the brain mapping expert.[6]

### 2.2 Polygraphy:

The polygraph, also referred to as the lie detector exam, measures involuntary physiological reactions, including blood pressure, heart rate, respiration, and galvanic skin response (GSR). The approach relies on the premise that untrustworthy persons will have autonomic nervous system reactions to deception, which may be documented and analyzed to ascertain the presence of deceit. The polygraph's history traces back to the early 1900s, when John Augustus Larson developed the first modern polygraph, which was later enhanced for accuracy and use by Leonard Keeler. The polygraph began its ascent as a rapid and non-invasive investigation instrument. The scientific advantages are not acknowledged, since physiological changes may result from a stimulus rather than deceit, including fear, anxiety, physical conditions, or environmental stress. Consequently, although polygraph exams may provide investigative insights and assist in interrogations, they cannot be considered definitive evidence of deceit.[7]

### 2.3 Narco Analysis:

Narco analysis is a process of administering sedative or psychoactive chemicals, primarily sodium pentothal, to a subject so that they are reduced in their inhibitions and then responses are "called forth" from them that are assumed to be "true" as opposed to "false." The beginnings of the use of narco analyse could be found in psychiatric practices in the early 20th century when physicians experimented with the administration of drugs to facilitate disclosures during therapy. Writer, film, and television journalist Carl Lachman elaborated on it within the 1940s and 1960s when

---

[6] *State of Maharashtra v. Praful B. Desai, (2003) 4 SCC 601. – Discusses evidence admissibility and forensic tests in Indian courts.*

[7] *Narayanan, P., & Gangadhar, B. N. (2012). "Event-Related Potentials and Brain Mapping in Forensic Investigations." Indian Journal of Psychiatry, 54(1), 12–18.*

investigators started to use it to get information from suspects who weren't engaged in cooperation. As the person/people are being questioned about the crime or other events, they are under medical supervision and in a semi-conscious state. Narco analysis has led at times to confessions or police leads, but it is regarded as very dubious evidence. There are serious ethical and scientific implications with the technique due to its suggestibility, formation of false memories and inducing coercion. Furthermore, it is subjective and so strictly reliant on the ability of the examiner and the psychological state of the examined person that it has a restricted use as a definite investigative tool.[8]

## 3. Legal Evolution and Status:

However, brain mapping, polygraphy and narco analysis in criminal investigations have also been influenced by human rights issues, as well as changing legal standards. International laws exhibit healthy skepticism, given concerns about technique's reliability, its potential for abuse, and protection of individual rights.

### 3.1 International Perspective:

The use of such methods is highly variable throughout the world for investigative purposes. Polygraphs are not admissible as evidence in the U.S. courts based on both the history of the United States Supreme Court (Inverness in the landmark case of *Frye v. United States*[9] in 1923 and later Daubert in the 1990s) and the general rule in the United States that strictly scientific methods are required for tests to be admitted as evidence. However, polygraphy is still used in investigative settings, pre-employment screenings, and parole monitoring, where there are situations where the information about the exam could influence law enforcement and/or organizational choices without being presented in formal court

---

[8] *National Human Rights Commission of India (NHRC). (2011). Report on the Use of Narco Analysis and Brain Mapping in Criminal Investigations. New Delhi: NHRC.*

[9] *Giannelli, P. C. (1980). The admissibility of novel scientific evidence: Frye v. United States, a half-century later. Colum. L. Rev., 80, 1197.*

settings. In European countries, polygraph examinations are also limited and never used as a primary means of gathering evidence, but rather confirmation of evidence.[10]

The nature of narco analysis, with its obvious coerciveness and suggesting quality, is of course limited in use, internationally speaking. It is not commonplace in court, but rather more widely used in the context of intelligence agencies and controlled interrogations. It has not been widely accepted due to worries about false confessions, manipulation, and infringements of personal autonomy. Brain mapping is largely experimental–only a few precedence cases in which it has been recognised or embraced by the judiciary. Neuro-imaging methods like fMRI and EEG provide some exciting potential clues about recognition and memory, but have not yet been adopted, even in the courts, and accepted as routine evidence. There are questions about how standard and reproducible batteries of measurements are, whether they are legally acceptable, and how the measurements are to be interpreted.

### 3.2 Indian Legal Context:

The critical interface between law, science and human rights in India is a clear case study. In *Selvi v. State of Karnataka (2010)*[11] the Supreme Court of India gave its decision on the usage of Narco analysis, Polygraphy and brain mapping in criminal investigation. The Court ruled that such tests made without informed consent infringed the constitutional rights to protection from self-incrimination (art. 20(3)) and personal liberty (Art. 21). Whilst these processes might be useful for investigations purposes, they can be imposed coercively only on the same principle as offends fundamental rights, and can imperil the integrity of the criminal justice system, the judgment stated.

---

[10] *United Nations Office on Drugs and Crime (UNODC). (2010). Manual on Human Rights and Criminal Justice for Investigators: Narco Analysis, Polygraph, and Brain Mapping. Vienna: UNODC.*

[11] *AIR 2010 SUPREME COURT 1974*

Under this post-Selvi framework, such techniques can be used voluntarily to obtain investigative leads which may be used in court if and only if backed by independent evidence such as forensic tests, witnesses etc, or another type of legally acceptable evidence. Throughout its history, the courts have stressed the importance of medical supervision, voluntary consent and safeguard against coercion, making sure that application of these does not militate against human dignity or against the code of ethics. Further, any findings derived from the use of these tools should be taken with a pinch of salt; and the police are allowed to use them only as an investigative tool and not as a conclusive proof of any kind.[12]

## 4. Real-Life Applications:

Although the science and law of these procedures constrain the potential uses of brain mapping, polygraphy, and narco analysis, they have been successfully used in criminal investigations, forensics research, and the intelligence community. The techniques are mostly used to aid investigations with existing evidence, to offer investigative leads when a case has not been resolved, and to, in general, help law enforcement in suspect behaviour understanding.

In situations, where investigators want to see if a suspect recognizes crime related information, the brain mapping techniques have been used, especially to detect P-300 waves. It's been employed in scenarios ranging from theft, to homicide to terrorism, where very subtle neural responses can help to distinguish a person who has direct knowledge of a crime from one who hasn't. Apart from investigative contexts brain mapping is being used in forensic psychology research to investigate cognitive patterns, memory recall, the neurological correlates of deception and the profiling processes, which will, in turn, improve the understanding of criminal behaviour.[13]

---

[12] *Verma, S., & Gupta, A. (2018). "Emerging Role of Neuroimaging in Forensic Investigations in India." Journal of Forensic Sciences India, 7(1), 15–28.*

[13] *Sharma, P., & Singh, M. (2015). "Ethical Concerns and Human Rights Issues in Forensic Psychophysiology in India." Indian Journal of Legal Studies, 6(1), 23–38.*

Despite less-than-ideal legal admissibility, polygraph devices are still in widespread use across the world, especially in pre-employment hiring screenings, probation evaluations and investigative interrogations. Polygraph tests may also be employed in order to cut down on suspects in main or complex cases, including financial fraud or serial crimes. Polygraphy is also helpful in intelligence operations for the assessment of the credibility of informants and/or people in sensitive positions; results are not considered to be conclusive. The ease of use and relatively low cost of the polygraph have helped sustain it as an easy investigative tool, especially in regions such as the United States and India where it is not used invasively.[14]

In a few cases in India, particularly in cases of terrorism, organised crime and kidnap, the only way to interrogate these suspects for information was by using narco analysis. The hope is to achieve a semi-conscious state that will help investigators obtain information about accomplices, crime scenes, or potential threats. The use of narco analysis is strictly monitored, under medical supervision and legal guidelines, and can be useful in producing actionable intelligence; however, the process is still extremely controversial because of the possibility for a "confession" to a crime to be false from a variety of reasons, such as suggestibility. Its use was used to show the conflict between the usefulness of the investigation and ethical issues, results must be taken with a grain of salt and verified with other independent evidence.[15]

| Parameter | Brain Mapping | Polygraphy | Narco Analysis |
|---|---|---|---|
| Scientific Basis | Measures brain activity (EEG, fMRI, P-300 wave) linked to recognition of stimuli | Measures autonomic nervous responses (heart rate, respiration, skin conductivity) during questioning | Uses sedatives (e.g., sodium pentothal) to lower inhibitions and facilitate responses |

[14] *Gangadhar, B. N., & Subbakrishna, D. K. (2002). "Brain-Based Techniques for Deception Detection: Indian Perspectives." Indian Journal of Psychiatry, 44(2), 85–92.*

[15] *R. Rajagopal v. State of Tamil Nadu, (2013) Mad HC – Highlights procedural safeguards for investigative testing.*

| Parameter | Brain Mapping | Polygraphy | Narco Analysis |
|---|---|---|---|
| Accuracy / Reliability | Experimental; moderately reliable for recognition, but not full truth verification | Controversial; affected by stress, anxiety, medical conditions; not fully reliable | Low reliability; results influenced by suggestibility, false memories, and drug effects |
| Legal Admissibility | Inadmissible in Indian courts (Selvi v. State of Karnataka, 2010); mainly investigative | Inadmissible as evidence in most courts worldwide; may guide investigation | Inadmissible in Indian courts without consent; internationally limited to intelligence use |
| Consent Requirement | Mandatory for ethical/legal use; involuntary testing is prohibited | Voluntary consent recommended; coercion violates rights | Mandatory informed consent; coercion violates constitutional rights |
| Practical Applications | Identifying recognition of crime-related stimuli; research; cognitive profiling | Pre-employment screening; investigative leads; interrogation support | Investigative leads in serious crimes/terrorism; intelligence gathering |
| Ethical Concerns | Privacy, cognitive autonomy, potential misuse | Psychological stress, coercion, privacy invasion | Risk of false confessions, psychological harm, human rights violations |
| Cost & Technical Requirement | High; requires specialized neuroimaging equipment and trained personnel | Moderate; requires polygraph machine and trained examiner | Moderate to high; requires medical supervision, drugs, and controlled environment |
| Advantages | Can detect subconscious recognition; non-invasive; potential | Quick, non-invasive, widely known method; easy to administer | Can elicit information from uncooperative subjects; useful for intelligence purposes |

| Parameter | Brain Mapping | Polygraphy | Narco Analysis |
|---|---|---|---|
| | for scientific validation | | |
| Limitations | Still experimental; individual brain variability; interpretation complex | High false positive/negative rates; influenced by emotions unrelated to deception | Unreliable due to drug effects; ethical/legal issues; suggestibility risk |

## 5. Challenges and Limitations:

Although brain mapping, polygraphy and narco analysis are fascinating avenues of scientific exploration, their deployment in a criminal investigation is fraught with substantial uncertainty and limitations, making it an unreliable, inapplicable and legally dubious tool. The first thing on everyone's mind is the scientific reliability. Autonomic nervous system (ANS) measures, which are used by the polygraph, have false-positive and false-negative rates because individuals may experience physiological reactions from fear, anxiety or medical causes other than the deceptive response. Likewise, when responses come from the user during narco analysis, they are subject to suggestion and induction of false memories, often due to the use of psychoactive substances (drugs) to incite dissociation and reduce inhibitions. Brain mapping techniques, as sophisticated as they are, have been utilized in a relatively experimental way, and interpretation of such brain imaging data (P-300 waves, etc. or fMRI scan data) although quite technical, and extremely variable, between individuals, may be less suitable for general use.[16]

These techniques are highly restricted from a legal viewpoint in terms of admissibility in our courts. However, judicial systems, including the Indian judiciary following the *Selvi v. State of Karnataka case (2010)*, tend to expect corroborating evidence to be obtained using other means in order to ensure findings based on brain mapping, polygraphy or narco analysis

[16] *Farah, M. J., & Heberlein, A. S. (2007). "Brain Imaging and Memory Recognition: Scientific and Legal Perspectives." Nature Reviews Neuroscience, 8, 108–118.*

are not solely the result of brainworming. The results themselves are not usually considered conclusive evidence – thus allowing them to be used to help investigate a crime.

The application of such methods complicates ethical issues also. Issues of coercion, informed consent, potential psychological harm, and violation of fundamental human rights are important ones, especially in the use of "narco" analysis and "polygraphy." Subjects might suffer from inappropriate stress or trauma, leaving moral and legal issues as to the appropriateness of improper stress or trauma.[17]

However, the tools are not widely used, due to practical limitations. Both brain mapping and narco analysis require sophisticated, specialized imaging technology and trained staff, and are both costly. Polygraphy is somewhat simpler but does need the administration of skilled examiners for proper execution. Lastly, there is a certain amount of cultural and individual variability and differences in physiologic patterns, neuronal functioning and cognitive reactions make it difficult to standardize results and thus to interpret the results across various populations.[18]

## 6. Conclusion:

The growing use of technology in criminal investigations is exemplified in the use of brain mapping, polygraphy and narco analysis, which is the field where neuroscience, physiology and law enforcement intersect. These are some of the latest and most innovative ways to test deceptive behaviors, to reconstruct events, and to assess the credibility of suspects, which are all important investigative leads that can assist traditional evidence. But the scientific and ethical and/or legal protections mean that these are used with caution and regulation. These practices are not to supersede or interfere with independent evidence and must be carried out with the free will of the

---

[17] *Agarwal, A., & Kaur, J. (2020). "Legal and Ethical Dimensions of Narco Analysis, Brain Mapping, and Polygraph Tests in India." Indian Journal of Criminology and Criminal Justice, 15(2), 45–63.*

[18] *Ministry of Home Affairs, India. (2013). Guidelines on the Use of Narco Analysis, Brain Mapping, and Polygraph Tests in Investigation. Government of India.*

participants, medical oversight, and respecting human rights, such as those courts have upheld in India and elsewhere.[19]

The change of the investigative methods reveals a major sociological and legal dilemma between modern highlighting and respect for basic rights. To fill the potential, it is essential that strict regulation, moral codes and scientific validation of the abilities are developed continually. When used properly, all of these techniques can increase the efficiency and accuracy of criminal investigations while maintaining constitutional and moral boundaries. In the future, the fine balance between investigative value and individual rights will be crucial to the success or failure of brain mapping, polygraphy and narco analysis as reliable, ethical and lawful tools in the armory for justice.[20]

## References:


1) *Agarwal, A., & Kaur, J. (2020). "Legal and Ethical Dimensions of Narco Analysis, Brain Mapping, and Polygraph Tests in India." Indian Journal of Criminology and Criminal Justice, 15(2), 45–63.*
2) *Choudhary, A., & Saxena, V. (2017). "Polygraphy in Indian Investigations: Limitations and Prospects." Indian Police Science Review, 55(3), 67–79.*
3) *Farah, M. J., & Heberlein, A. S. (2007). "Brain Imaging and Memory Recognition: Scientific and Legal Perspectives." Nature Reviews Neuroscience, 8, 108–118.*
4) *Gangadhar, B. N., & Subbakrishna, D. K. (2002). "Brain-Based Techniques for Deception Detection: Indian Perspectives." Indian Journal of Psychiatry, 44(2), 85–92.*
5) *Inbau, F. E., Reid, J. E., Buckley, J. P., & Jayne, B. C. (2013). Criminal Interrogation and Confessions, 5th Edition.*
6) *Krishnamurthy, V. (2016). "Polygraph Tests and Their Use in Indian Legal System." Indian Police Journal, 63(2), 45–58.*
7) *Meijer, E. H., Verschuere, B., Merckelbach, H., & Ben-Shakhar, G. (2017). "Cognitive Forensics: Brain-Based Techniques for Criminal Investigation." Trends in Cognitive Sciences, 21(7), 525–537.*


---

[19] *Suresh, R., & Verma, A. (2014). "Scientific and Legal Issues in Narco Analysis in India." Journal of Indian Law and Society, 5, 98–112.*

[20] *Choudhary, A., & Saxena, V. (2017). "Polygraphy in Indian Investigations: Limitations and Prospects." Indian Police Science Review, 55(3), 67–79.*

8) *Ministry of Home Affairs, India. (2013). Guidelines on the Use of Narco Analysis, Brain Mapping, and Polygraph Tests in Investigation. Government of India.*
9) *Narayanan, P., & Gangadhar, B. N. (2012). "Event-Related Potentials and Brain Mapping in Forensic Investigations." Indian Journal of Psychiatry, 54(1), 12–18.*
10) *National Human Rights Commission of India (NHRC). (2011). Report on the Use of Narco Analysis and Brain Mapping in Criminal Investigations. New Delhi: NHRC.*
11) *National Research Council (2003). The Polygraph and Lie Detection. Washington DC: National Academies Press.*
12) *R. Rajagopal v. State of Tamil Nadu, (2013) Mad HC – Highlights procedural safeguards for investigative testing.*
13) *R. v. South Wales Police (1999) UKHL – Comparative case on polygraphy admissibility.*
14) *Saxena, A. K., & Singh, J. (2015). "Narcoanalysis and Legal Implications in India." Indian Journal of Legal Medicine, 42(2), 54–62.*
15) *Selvi v. State of Karnataka, (2010) 7 SCC 263.*
16) *Sharma, P., & Singh, M. (2015). "Ethical Concerns and Human Rights Issues in Forensic Psychophysiology in India." Indian Journal of Legal Studies, 6(1), 23–38.*
17) *State of Maharashtra v. Praful B. Desai, (2003) 4 SCC 601. – Discusses evidence admissibility and forensic tests in Indian courts.*
18) *Suresh, R., & Verma, A. (2014). "Scientific and Legal Issues in Narco Analysis in India." Journal of Indian Law and Society, 5, 98–112.*
19) *United Nations Office on Drugs and Crime (UNODC). (2010). Manual on Human Rights and Criminal Justice for Investigators: Narco Analysis, Polygraph, and Brain Mapping. Vienna: UNODC.*
20) *Verma, S., & Gupta, A. (2018). "Emerging Role of Neuroimaging in Forensic Investigations in India." Journal of Forensic Sciences India, 7(1), 15–28.*

## Author's Profile:

***Dr. Divya Raviya Jadeja*** is a Deputy Superintendent of Police (DSP) currently posted at the Headquarters in Kheda-Nadiad District, Gujarat. She holds a Bachelor of Science (B.Sc.), an MBA in Human Resources (MBA-HR), a Bachelor of Laws (LLB), a Master of Laws (LLM), and a Ph.D. in "Administration of Criminal Justice System: Role of Police and Prosecution" from Gujarat University.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 29-44)

# Re-articulating Cyber Fraud Governance: Towards a Multi stakeholder Security Architecture in India

Harmeet Singh, IPS*

*"In the network society, the space of flows dissolves time by disordering the sequence of events and making them simultaneous in the communication networks, thus installing society in structural ephemerality; being cancels becoming"*
*(Manuel Castells, The Rise of the Network Society: The Information Age: Economy, Society and Culture, 1996)*

***Abstract:***

*Cyber enabled fraud (CEF), globally and in India is evolving into a systemic risk. It is entrenched within the country's speedily expanding digital public infrastructure and is marked not only by soaring speed and scale but also global complexities, making it a jurisdiction-less and a decentralised crime. This paper makes an attempt to highlight that there is a fundamental structural asymmetry existing between the rapid pace of cyber fraud on the one hand and the bracketed and siloed institutional response to these frauds on the other, thus rendering traditional enforcement-oriented approaches inadequate. This article attempts to locate the key gaps in India's existing framework -response systems which are reactive, non-integrated data ecosystems, and accountability mechanisms that need synergy. Cyber enabled fraud should therefore be reconceptualised as risks to the entire digital public infrastructure, making*

*Director General of Police, Assam.

*it an ecosystem risk. The paper conceptualises a multi stakeholder governance architecture through shared accountability, real-time collaboration, and agile legal responses, thus marking a shift from mere coordination-based responses. This article also hinges on an integrated and collaborative governance model centred on prevention of cyber fraud. Such a model can efficiently address the asymmetry between cyber offence and state response.*

***Keywords:***
*Cybercrime, Cyber Security Governance in India, Digital Public Infrastructure, Institutional Coordination vs Governance, Legal Agility, Multi Stakeholder Approach.*

## Introduction:

Cyber fraud, a mind boggling and perplexing crime for the common citizen, has today transitioned from peripheral risks relegated to the margins to a systemic threat embedded within the country's digital transformation. While on one hand, the story of rapid expansion of digital public infrastructure—financial inclusion through Jan Dhan accounts, real-time payments via UPI, mobile connectivity across nook and corner, and identity integration through Aadhaar—has created an unprecedented economic opportunity; on the other hand, it has generated totally new vectors of vulnerability.

**1.**Cyber fraud is no longer only episodic or opportunistic; it is organised, scalable, and increasingly transnational in character**.** Analyses of the recent trends by the Reserve Bank of India are indicative of exponential growth in formal reporting of complaints and humongous financial losses. The regulatory mechanisms also point out the sophistication of attack vectors that signal a structural crisis rather than a cyclical anomaly (RBI, 2023; NCRB, 2022).

**2.** There is a fundamental asymmetry that exists at the core of this crisis: the scale and the pace of cybercriminal operations far outperform the response mechanism of the existing institutional and legal framework. Whereas cyber enabled fraud is executed within no time, whether by

leveraging spoofed identities, social engineering or through multi-layered financial transactions, it may require several days or even months of investigation and coordination amongst agencies to unravel and detect the crimes. This asymmetry is further heightened by the mushrooming industrialisation of cybercrime. Criminal ecosystems have started mirroring legitimate digital markets, offering 'as-a-service' models such as phishing kits and malware subscriptions and mule-account networks. Since the entry barrier has effectively collapsed, it has become enabling for even very low-skilled actors to orchestrate complex frauds through modular, outsourced components (Europol, 2023).

**3.** Artificial Intelligence has deepened the entire threat landscape. As noted by EUROPOL "As AI tools become more accessible, cybercriminals are able to lower the barrier to entry, scale operations more effectively, and increasingly commit crimes without direct involvement in the operations. This evolution means that criminals will likely minimise the time needed to launch attacks, while increasing both their scale and personalisation." (IOCTA,2026) Deepfake technologies and AI-augmented social engineering tools have turned the scale of deception even more monstrous. While generating synthetic content is now extremely fast and inexpensive, detecting and proving with evidence about such manipulation remains resource-intensive and time-consuming. This widening technological gap between offences brings to fore the inadequacies of conventional deterrence-based approaches, which rely on the probability and severity of punishment. This Europol terms as the 'Velocity Gap' [1](IOCTA,2026) that is the gap which the Law Enforcement Agencies (LEAs) experience in foiling cyber frauds, because of its accelerated pace in execution. In cybercrime, when one analyses the patterns, detection remains uncertain, attribution is complex, and jurisdictional boundaries often shield perpetrators from enforcement.

**4.** This paper advances the central argument that cyber fraud cannot be effectively addressed through siloed and bracketed institutional responses. Neither policing, nor banking regulation or telecom oversight in isolation

[1]*Velocity gap is defined as the widening gap between CEF operationalisation and the intervention of LEAs by Europol-IOCTA,2026.*

can contain a phenomenon that inherently spills over all these domains simultaneously. Instead**,** cyber frauds must be reconceptualised as a shared ecosystem risk, requiring a coordinated, multi stakeholder governance framework. The effectiveness of such a framework lies not merely in cooperation, but in clearly defined, enforceable, and proportionate accountability across all actors embedded in the digital ecosystem. To understand the multi stakeholder governance framework and its effectiveness in dealing with cybercrime risks, let us analyse how cybercrime is being handled at organisational levels in India at present.

**5.** Despite significant progress in digital governance, several structural gaps continue to undermine/plague India's ability to effectively address cyber fraud:

**(i)** The current mechanisms of LEAs in India are mostly complaint-driven, with very limited capacity for proactive detection and prevention. Most of the action taken is reaction driven, only after reporting by the victim. This delays intervention at a stage, when most needed and when funds are already dissipated through multi-layered transactions. As very recently observed by EUROPOL, "The widespread criminal use of end-to-end encryption (E2EE) platforms, coupled with complex jurisdictional and technical barriers, creates significant investigative blind spots. These obstacles hinder the identification of suspects and the corroboration of evidence, ultimately slowing down investigations and weakening preventive actions against imminent threats." (IOCTA, 2026). In this regard, FATF notes that fraud related financial flows are often rapidly transferred through multiple accounts, reducing the likelihood of recovery when intervention is delayed" (FATF, 2022). On a similar note, the RBI also highlights the delays in reporting can significantly reduce recovery rates indicating the absence of preventive transaction monitoring at scale (RBI, 2023). Moreover, real-time fraud interdiction systems are unevenly implemented across institutions.

**(ii) Data Ecosystems are not fully integrated**-In India, in most cases data sharing is not simultaneous rather it is sequential, leading to critical time lags in response. The real-time data-sharing architecture that enables seamless exchange of actionable intelligence across banks, telecom providers, platforms, and law enforcement is still at a nascent stage. Platforms such as the Indian Cyber Crime Coordination Centre (I4C) have improved such coordination to a great extent. Data sharing across banks, telecom operators, and law enforcement is yet to be real-time, seamless and fully integrated. "LEAs are often hampered by restrictive or inadequate data retention policies. By the time investigators request access to relevant data, it is often no longer available, impairing their ability to track suspects or disrupt criminal operations", as highlighted by EUROPOL (IOCTA, 2026) points to the fragmented data sharing between LEAs and digital service providers is a case in point. It is further highlighted recently by EUROPOL, "The alignment of data retention policies across digital service providers, not just in terms of retention duration but also regarding which data is kept, would significantly enhance LE capabilities" (IOCTA, 2026) and can go a long way to effectively address CEF. The FATF emphasizes upon this structural issue and underscores that effective disruption of cyber-enabled fraud requires timely information sharing between financial institutions, law enforcement, and other stakeholders. (FATF, 2022)

**(iii) Weak Regulation of Enabling Infrastructure leads to a plethora of mule accounts ecosystem: KYC weaknesses remain –**Globally and India's CEF landscape is marred with widespread use of mule accounts. Weak enforcement of Know Your Customer (KYC) norms and identity verification along with the complicity of those manning these systems enable large-scale laundering. The FATF explicitly identifies these risks and flags off how Money Mules are a key enabler of fraud schemes, allowing criminals to distance themselves from illicit proceeds. In Illicit Financial Flows from Cyber-Enabled Fraud (FATF/Interpol/Egmont,2023), it is

mentioned how CEF-proceeds are rapidly laundered through a network of accounts, which can get complex by extending across multiple borders and financial institutions, although this may vary based on the criminal group's level of sophistication. This IFFCEF report (2023) categorises CEF enabled ML accounts as individual mules and also legal entities, shell companies too. Indian banking data also show recurring patterns of accounts misuse despite regulatory safeguards (RBI, 2023). Hence it can be observed that mule accounts, fraudulent SIM cards, and digital identities continue to proliferate due to gaps in KYC enforcement, monitoring, and accountability.

**(iv) In the domain of telecommunication-** **"**While CaaS and technology advancements continue to lower entry barriers for scammers, the primary operational evolution is the deployment of more sophisticated telecommunications infrastructure, to bypass KYC protocols and disrupt traditional evidence chains, as commonly seen in phishing and account takeover (ATO) campaigns. A rise in the use of IMSI catchers (and SMS blasters, also enabled to send SMS messages) points to the adoption of interception technology by criminal networks." (EUROPOL, IOCTA 2026). This excerpt rightly connotes the vulnerabilities of the telecommunication domain and the leverage that it provides to the CEF. One is already aware how spoofed calls, SIM-based fraud and bulk messaging continue to be breeding grounds for CEF. While regulatory steps have been taken, enforcement gaps persist. These are compounded by the TSPs' customer bases.

**(v) Forensic capabilities are limitedly digitised or at nascent stage of digitisation and its impact on Investigative Capacity -** Cybercrime investigation requires specialised skills in digital forensics, block chain imaging and tracing and also AI-enabled fraud detection. It is witnessed that capacity constraints, both in terms of manpower and technology continue to limit effectiveness in enforcement.

(vi) **Jurisdictional constraints, legal Delays cause operational issues**– International cooperation remains a critical challenge in cyber-enabled fraud cases due to jurisdictional fragmentation and legal differences amongst various countries as underscored by the FATF. Domestically also it is witnessed that procedural requirements often impede timely intervention. A significant proportion of cyber fraud operations have transnational linkages which complicates investigation and prosecution. Interpol points out, "A more concerted approach is also called for to combat financial crime and corruption, particularly money laundering, which ultimately sustains and empowers organized crime. It has been estimated that countries intercept and/or recover less than one per cent of global illicit financial flows. The proceeds of crime are often rapidly moved beyond borders through multiple jurisdictions, rendering the process of asset recovery complex and highly dependent on effective international cooperation. (Global Crime Trend Summary Report,2022). India's Mutual Evaluation Report similarly emphasises the need for faster cross-border information exchange (FATF, 2024)

(vii) **Platform accountability is very inconsistent which** means digital intermediaries vary in their responsive capacity to fraud related requests, and therefore the proactive detection mechanisms remain laggard. Digital platforms, social media, messaging services, and online marketplaces have come to play a critical role in enabling fraud vectors. Thus, it is witnessed that accountability frameworks remain underdeveloped. World Economic Forum has for the fact of matter taken note of how platforms and social media must move from passive intermediaries to active risk managers within the digital ecosystem.

(viii) **Issues arising out of low user awareness** -The regulatory platforms like the FATF, RBI have time and again noted that customer awareness remains a key pillar in preventing digital payment frauds. Behavioural vulnerabilities among users are

exploited at a massive scale and this indicates the need for more targeted and sustained awareness strategies. Cyber fraud exploits human behaviour as much as it does technological gaps. Despite awareness campaigns, behavioural vulnerabilities persist so rampantly and on it thrives CEF. Citing reference to the role of Enforcement Directorate (ED), the IFFCEF[2] (FATF, 2026) highlights its ML operations which revealed a large-scale criminal conspiracy involving shell company operations mainly duping and playing on the 'gullibility' of people. In this context, it can be stated how pig-butchering[3] continues to be a favourite genre of modus operandi for this organised crime.

In addition to the issues enlisted above, this paper also observes that the governance metrics have to be outcome oriented focussed on fraud prevention rates and recovery efficiency. The current evaluation frameworks focus heavily on inputs, say for example- the number of FIRs, arrests, advisories rather than outcomes. This is reflective of a deeper governance gap pointing sharply to the lack of measurable accountability across stakeholders.

## 6. The Limits of Siloed and bracketed Institutional Responses:

Traditional governance structures are organised along sectoral lines with clearly demarcated responsibilities assigned to LEAs, financial regulators, and telecom authorities. While these models have/are functioned(ing) effectively in addressing conventional crimes in yesteryears, it is fundamentally not in tune with the architecture of cyber fraud.

Lifecycle of a cyber fraud transaction spills over multiple domains.First, it originates through telecom networks (spoofed calls or SMS), gets facilitated through digital platforms (social media or messaging applications), extracts value via banking and payment systems, and

---

[2] *See the cited report, it carries a special section on role of Indian Police in CEF*

[3] *Pig butchering is defined as a combination of romance scam and investment fraud. Please see (IOCTA, Europol, 2023)*

subsequently gets laundered proceeds through layered financial transactions. It is to be noted that each stage falls under a different regulatory or institutional jurisdiction. Nevertheless, no single entity has end-to-end visibility, grasp or accountability over the entire transaction chain. This fragmentation creates systemic blind spots, allowing criminals to exploit the layers between institutions.

As already highlighted in the earlier section of the paper, empirical studies and policy reports have consistently highlighted this lacuna of seamless co-ordination among different organisations i.e.. inter organisational platform to address cyber-crimes. In this context, the RBI (2023) has underscored the need for stronger inter-bank coordination and real-time fraud monitoring systems. Similarly, the NCRB (2022) data reveal significant delays not only in reporting and but in investigation too. At the global level, analyses by the Financial Action Task Force (FATF, 2022) underline the growing role of mule accounts and cross-border financial flows in enabling CEF, thus pointing to the regulatory fragmentation as a key vulnerability.

Taking cue from the above, relying only on post-facto or reactive enforcement is inadequate and may not yield productive outcome in a time bound manner. In respect of the LEAs, the procedural requirements for investigation and the time taken for evidence collection and prosecution are disproportionate to the speed with which cyber fraud is committed and monetised. In a nutshell, these enforcement-heavy approaches are reactive, resource-intensive, and ultimately ineffective in reducing incidence at scale. In this context, this paper tries to negotiate a working definition of ‘multi stakeholder approach’ at institutional level to approach CEF and related ML.

## 7. Working definition of Multi stakeholder Approach to CEF:

A multi stakeholder approach to CEF and related ML can be defined as a governance model in which all platforms/institutions that constitute the digital ecosystem share responsibility for its security commensurate to their role, capabilities and risk exposure. This approach visualises a structured

framework of shared accountability, real-time collaboration, and integrated response mechanisms and not mere ad-hoc co-ordination. The World Economic Forum visualises this as a collaborative model where governments, private sector entities, and civil society share responsibility for managing cyber risks (WEF, 2023). This article hinges on the concept of 'correct hands'[4] as the theoretical underpin of its definition of multi stakeholder approach to CEF. Premised on the concept of 'correct hands', the rationale for a multi stakeholder approach is not only inter-agency collective action domestically but also inclusive of joining hands with the international platforms, given the decentralised nature of CEF and related ML. In principle, therefore multi stakeholder framework encompasses:

- Law Enforcement Organisations/Agencies
- Financial Institutions and Payment Gateways
- Telecom Service Providers
- Digital Platforms and Social Media
- Policymakers and Regulatory Mechanisms
- Cyber security Firms/ Technology Providers/ Private Partners (PPP)
- Civil Society Organisations
- International FIs – Multilateral and Regional Collaboration

"The cybercrime landscape will continue to present LEAs with an array of evolving challenges, making a proactive and strategic approach more necessary than ever. In the coming years, law enforcement's ability to tackle cybercrime will depend on its capacity to harness innovative technologies, to be able to lawfully access critical data, and to collaborate more closely with the private sector" (IOCTA,2026). A deeper reflection

[4] *As taken up by FATF (IFFCEF, 2023), multi-lateral programmes aim to do two things: collect the minimum level of information required for law enforcement action and pass that information into the "correct hands". To ensure effective cross-border response, all nodes of the multi-lateral networks also agree on governance rules and procedures. The concept of 'safe hands' is used for multi-lateral networks are usually global in nature, regional initiatives may also be useful to mitigate challenges by building upon already established regional collaboration.*

on the above observation underscores the urgent necessity of creating a resilient, participative and collaborative platform amongst the aforementioned stakeholders. This aligns with global best practices in cyber security governance, where collaborative frameworks, such as public-private partnerships like European Union Agency for Cyber security and information-sharing alliances like Financial Services Information Sharing and Analysis Center and the Forum of Incident Response and Security Teams—have demonstrated greater effectiveness in managing complex cyber threats (World Economic Forum, 2023).

## 8. The Indian case:

**i)** India already has multiple coordination platforms and mechanisms- inter-agency meetings, advisories, helplines for handling CEF. Nevertheless, reiterating, not mere co-ordination but a resilient **governance** model necessitates that there is a, fully functional governance architecture in place that is a unified command-and-control architecture for cyber fraud response. As encapsulated in IFFCEF (2026), "Given the cross-cutting nature of CEF, there is a clear need for strong domestic co-ordination across agencies. Some jurisdictions have approached co-ordination through a whole-of-government strategic approach that guides a jurisdiction's CEF related policies. This involves an overarching cross-functional body, comprised of key ministries across judicial, enforcement, regulatory and info-communications sectors. The co-ordinated approach allows jurisdictions to identify key vulnerabilities and devise holistic policy responses across the key sectors." [5](IFFCEF,2023).

In the view of this observation regarding a cross- functional body, operating nationally, the Indian Cyber Crime Coordination Centre (I4C), established by the Ministry of Home Affairs is a glaring example. I4C provides a 'national framework' and 'eco-system' for LEA s and to act as the nodal point for cybercrime response. The National Cybercrime

[5] *This edition of IFFCEF, 2023 carries a detailed section on the domestic level co-operation amongst competent authorities and the best practices to be adopted nationally and at multilateral levels for CEF.*

Reporting Portal -the 1930 helpline, the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), Joint Cyber Coordination Teams, and the National Cyber Forensic Laboratory speak volumes of the co-ordination amongst various agencies that are helping India move beyond the police station centric model.

Nevertheless, these mechanisms still largely function as coordination platforms, not as a unified command architecture for CEF and related ML. These institutions exchange information, issue alerts, hold timely meetings, and respond after a complaint is received. Governance, on the other hand, requires clear authority with defined responsibility - binding protocols, escalation chains, measurable timelines, and enforceable accountability across the lifecycle of CEF and related ML.

A typical lifecycle of a CEF involves-telecom operator issuing SIM; a social media interface, mule account and UPI transactions, a payment aggregator, and eventually laundered through virtual assets. In the entire chain, each stakeholder sees its own part- Police see the complaint; banks looking into the transaction; telecom companies overseeing the communication layer; digital platforms see the digital contact point. Unless one architecture integrates these partial views into a real-time response system, cyber fraud remains nobody's complete responsibility.

Indian institutional evolution demonstrates gradual progress, which needs to be further worked on. The I4C war room has in its ambit -banks, payment aggregators, telecom service providers and State/UT police for real-time monitoring and coordinated action against CEF. This is enabling-verified complaints are shared with banks for tracing & freezing funds, mule accounts to be tracked, and supporting law enforcement with money trails and evidences. While this is an important movement towards governance, the larger national system still needs stronger legal backing, as well as operational so that response is not dependent only on institutional goodwill and post-complaint reactionary escalation. Therefore, the need of the hour is conversion of coordination into command responsibility[6] .

---

[6] *Similar to centralised response centres and the concept of safe hands as observed by FATF.*

As rightly noted by FATF, "Developing communication channels among FIUs, police, and prosecutors to ensure centralised reporting, streamlined information and evidence exchange, as well as instructions to freeze and seize assets. This may also include the use of automated data triage to assist in identifying possible matters of interest and quickly identify an appropriate LEA for investigation. Such co-ordination also mitigates duplicity of law enforcement efforts as CEF criminals can target victims across various parts of a jurisdiction" (IFFCEF, 2023), a mature Indian CEF governance model requires **a) A single operational doctrine** for cyber financial fraud which defines what must happen within the first 15 minutes, 1 hour and so on after reporting. **b) Binding obligations** on banks, payment intermediaries, telecom operator to act on validated fraud signals. **c) Real-time interoperability of (suspicious) data** visible across the eco system. **d) Accountability metrics** on percentage of funds saved, repeat use of mule accounts, compliances by platforms and prosecution outcomes. **e) operational partnerships with private sector (PPP) model** to collaborate with private sector so as to improve detection efforts, identify hidden ML networks through tactical information exchange.[7]

**ii) Legal agility and the Indian cyber governance:**

The FATF's[8] work on CEF is noteworthy as it treats cyber fraud not merely as a technology offence, but as a fast-moving decentralised financial crime that generates illicit proceeds spanning jurisdictions. FATF has very rightly noted that CEF has not only grown exponentially in both volume and global spread, but its proceeds are often transferred across jurisdictions in no time.

As discussed earlier, multi stakeholder efforts also foresee international co-operation. From this vantage point, 'Legal agility' is defined as the ability of law and regulation to respond at the speed of the offence. CEF is not defeated only by criminalising conduct. It requires laws and protocols that allow rapid preservation of data and freezing of accounts, sharing of

---

[7] *Please see the entire section on models of domestic co-operation and collaboration by different countries (IFFCEF, 2023). The best practices can be adopted for developing an indigenous model.*

[8] *Ibid.*

fraud intelligence, cross-border cooperation, attribution of digital evidence, and recovery of proceeds. As observed by FATF, "Formal co-operation, including mutual legal assistance, typically takes a long time. Given the rapid nature of digital crimes and associated ML activities (where evidence could be quickly dissipated if not preserved), relying on formal co-operation may therefore be significantly less effective. To remain nimble in rendering cross-border assistance to successfully curb CEF criminal activity, competent authorities are increasingly relying on informal co-operation mechanisms by sharing information directly with their foreign counterparts. This can occur at a law enforcement or FIU level through various channels, including the Egmont Secure Web, INTERPOL's I-24/7 as well as other informal networks such as the Camden Asset Recovery Inter-Agency Network (CARIN) and regional Asset Recovery Inter-Agency Networks (ARINs)." (IFFCEF,2023)[9]

India has created reporting and response channels such as 1930, NCRP and CFCFRMS, but the criminal tracking process remains gentler than the fraud cycle. If freezing powers, data access are delayed by sequential procedures after the fraudsters have started laundering through multiple accounts, it is witnessed that the legal system becomes more reactive in its delivery. Taking cue from the observation of FATF highlighted in this paper, emergency freezing and payment-suspension protocols, time-bound data preservation duties, clear legal standards for sharing fraud intelligence, recognition of cyber fraud as a proceeds-generating organised crime including faster international cooperation come in the realm of legal agility, because many frauds proceeds and digital evidences are transnational in character.

---

[9] *It is in this context the report comprehensively addresses the issue of international cooperation in handling CEF. It notes multilateral informal arrangements; regional forums rather than bilateral can help better in addressing CEFs. Collecting minimum level of information and passing it to the correct hands remain the underlying principle of such multilateral legal assistance.*

If one carefully analyses FATF's 2024 Mutual Evaluation of India, it is apparent that India needs a substantial framework for AML/CFT and international cooperation. A system may be formally compliant, yet operationally slow. Cyber fraud governance requires not only legality, but speed, interoperability and enforceable response timelines.

In the light of the above discussion, it can be put forth that India's next reform frontier is not simply stronger punishment of the offence, which is important but also simultaneous agile lawful action. The objective should be to compress the institutional response time so that the legal system can intervene before the proceeds disappear. In cyber fraud, delay is not merely procedural inconvenience; it is a substantive failure of governance.

**References:**


1. *EUROPOL. (2023). Internet Organised Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.*
2. *EUROPOL. (2026). Internet Organised Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.*
3. *Financial Action Task Force. FATF/OECD. (2023). Illicit Financial Flows from Cyber -Enabled Frauds. FATF, Interpol and Egmont Group of Financial Intelligence Units.*
4. *Financial Action Task Force. (2018). Professional Money Laundering*
5. *INTERPOL. (2022). Global Crime Trend Summary Report. INTERPOL General Secretariat.*
6. *National Crime Records Bureau (NCRB). (2022). Crime in India 2022. Ministry of Home Affairs, Government of India.*
7. *Reserve Bank of India (RBI). (2023). Annual report 2022–23. RBI.*
8. *Reserve Bank of India (RBI). (2023). Annual report 2025–26. RBI.*
9. *World Economic Forum. (2023). Global Cybersecurity Outlook 2023. WEF.*


**Author's Profile:**

Shri Harmeet Singh, an officer of the 1992 batch of the Indian Police Service from the Assam–Meghalaya cadre, is currently serving as the Director General of Police, Assam. Over a distinguished career spanning more than three decades, he has combined operational excellence with a strong academic and research orientation. He began his policing career in Assam, serving in key field assignments including Superintendent of

Police, Nagaon, before proceeding on central deputation, during which he served in various theatres.

Shri Singh has developed domain expertise in areas such as conflict resolution, counter-terrorism, counter-radicalisation, cybersecurity, infrastructure security, disaster management, child protection and citizen-centric interfaces. He is widely recognised for conceptualising innovative, technology-driven policing initiatives and creating both soft and hard infrastructure to enhance service delivery systems. He has also conceptualised Nagarik Mitra, the Assam Police Smart Social Media Centre, and Shishu Mitra, a child-friendly policing initiative, run in collaboration with UNICEF and Utsah.

An accomplished scholar-practitioner, Shri Singh's research and writings have been published by premier institutions such as the Sardar Vallabhbhai Patel National Police Academy and the Rajasthan Police Academy. He is a regular columnist and a sought-after speaker at academic institutions, technology forums, and policy platforms. He also serves as Emeritus Faculty at Rashtriya Raksha University, contributing to national security education. His academic engagements, including lectures on child protection and digital rights, reflect a sustained commitment to bridging field experience with scholarship in contemporary policing.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 46-59)

# Personal Financial Management

Seju P Kuruvilla, IPS*

***Abstract:***

*Financial stability is a cornerstone of the Safety Needs (Second Level) in Maslow's hierarchy of needs. It encompasses job security, stable income, safety net, savings, and growth providing the individual with the capacity to manage daily finance, absorb economic shocks, and ensure future security. Since financial management is not taught in schools and colleges it is imperative for individuals to learn on their own. A series of surveys conducted for government service officers between 2021-2026 revealed significant gaps in awareness regarding insurance, emergency funds, retirement planning and long-term investing. Out of 2,644 officers who participated in the survey only 1044 (40%) had an emergency fund in place, 1043 (40%) had a life insurance policy, out of whom only 214 (20%) had adequate cover. The survey results highlight the need for a structured personal financial management model for government service officers. In addition, financial discipline not only strengthens personal security but also contributes to professional independence, ethical resilience, and peace of mind in public service. This article is written from the perspective of IPS recruits and in-service officers, whose careers involve stable income streams and have limited time for active financial management. The views expressed are for educational purposes only and should not be construed as individualized financial advice.*

* *Deputy Director NTRO*

## Introduction:

Along with my batchmates I too got my first salary in September 2007 during our Foundation Course at Lal Bahadur Shastri National Academy of Administration, Mussoorie. It was a historic event in our lives, as we were earning for the first time. During the next couple of weeks, the body and the mind were conspiring to find out the best ways to spend the hard-earned money. All plans executed with perfection and within couple of weeks I was successful in spending all the money in my new SB account and eagerly waiting for the next salary which would arrive on the last working day of the month. This cycle of monthly salary flowing into the bank account and the hard-earned money flowing out to the restaurants and shopkeepers on the Mall road, to the telecom operators, towards mess bill, to Ganga Dhaba, and to the Taxi Wala continued like a well-oiled system.

From Mussoorie I moved to Sardar Vallabhbhai Patel National Police Academy in December 2007. After completing a year-long Basic Course Phase-I training along with my other batchmates we moved to our respective cadre for District Practical Training. Shortly after reaching Bihar, I moved to East Champaran District. The cycle of salary inflow and outflow continued in the same fashion except that the location and the beneficiaries changed. The bank account base branch shifted from Mussoorie to Shivrampally and to Motihari and it is here where I met my first financial advisor in the form of the SBI Branch Manager (and an LIC Agent). It was fiscal year closing (February/March), and I received my first free financial advice to open an LIC policy (Jeevan Anand: Life Cover of Rs 5 lakh; Premium of Rs 27,000/-) to save tax.

The story would be the same for many of my batchmates and the larger civil service/government service community. Financial Management is neither taught as regular subject to students in Schools /Colleges/ Universities nor to the regular employee in Training Institutions. It is neither a topic of academic discussion in family circles nor in friends' circles in India thereby leaving a huge vacuum. Luckily for me except for the initial misdirection in the form of LIC Policy (an Endowment Plan), I was fortunate to have colleagues/friends/family members who guided me towards a disciplined and process driven model of financial management.

Keeping the same spirit alive, this article attempts to provide a *simplified, easy to understand and practical model*, covering all aspects of Personal Financial Management, for a Government Service Officer who is expected to spend the remaining part of his/her life (till retirement) dedicated to the service of the nation. Before you read further it is advised to participate in a baseline survey. The baseline survey is intended to help you identify your savings and investment patterns and habits.

## Why do we need a model?

The financial market resembles an amusement park where the rides are becoming increasingly complex, having no age/height restrictions and with no one to guide you even though you need not participate in all rides and need not be fastest in all. To navigate such a complex and volatile situation and to effectively utilize the growth opportunity offered by the financial market we need to *simplify things,* have a *set of rules,* and *automate* the process.

## The SIP Model:

The **Safety Investment Protocol (SIP)** model of PFM has emanated from a series of discussions and deliberations at the National Police Academy during the period from 2020 to 2022. The model is based on traditional wisdom from authors of financial management books and articles suitably tailored for Civil Service Officers incorporating practical experience. As the name suggests, the model has three basic components: (i) Safety, (ii) Savings & Investments, (iii) Protocols.

## The SIP Matrix

| Safety | Investments | Protocols |
|---|---|---|
| **Life Cover** | **Goals** | **Habits** |
| **Medical Cover** | **Savings** | **Automation** |
| **Emergency Cover** | **Investments** | **Review** |

We will now discuss each of the components one by one in detail.

### Safety First:

In this volatile, uncertain, complex, and ambiguous world in which we are living, safety assumes paramount importance as it helps in reducing the risks involved and thereby providing protective cover. Like any other field we need to have multi-layered safety protocols to protect our hard-earned money. The model recommends a 3-layer safety strategy with the following 3 Protective Covers: (i) Life Cover, (ii) Medical Cover, (iii) Emergency Cover.

### Life Cover:

The concept of life cover (Life Insurance) is to provide financial stability to the family (dependents) in case of a sudden death of the earning member. Here the basic idea is to have sufficient income from the Insurance corpus for the dependents to continue their life without changing their existing lifestyle.

Life Insurance is income risk protection i.e., protecting the income source even after death. When it comes to taking a life insurance Policy, we need to have a much deeper understanding of life insurance as an

instrument and in the process, we need to address many questions like: When to start? Till when? How much? Type of insurance? Which company?

The answers to most of these questions come from the basic understanding of the *underlying need* for life insurance, i.e., income protection for the dependents to maintain their lifestyle.

Since the whole idea of taking life insurance is to provide income for the dependents, the *starting point* should be as soon as you have a financial dependent and the *stop point* should be when the last dependent person becomes financially independent of you.

As far as the sum assured is concerned, it should be sufficient to help your dependents maintain their current and future lifestyle requirements. The global rule of thumb says the assured amount should be around fifteen times your annual income.

Insurance plans can be divided into two broad categories (i) Term Insurance and (ii) Money Back/ULIP/Endowment Policy. The former is a pure insurance policy whereas the latter is a combination of insurance and investing. Most agents push to sell Money Back/Endowment/ULIP policies as they get huge commissions for the sales of each policy. These are extremely inefficient in terms of providing sufficient life cover as only an extremely low percentage of the annual premium amount is kept aside for insurance and the remaining is utilized to invest in some financial instruments (Debt/Equity). As mentioned earlier, I have experienced this and similarly many in my generation and previous generations of civil servants must have too.

For example, with an annual premium of Rs 27,000/- under the Endowment Plan I am only insured for Rs 5,00,000 which is grossly insufficient for my dependents in case of my sudden death. Whereas as per the rule of thumb I should be insured to a tune of 15 Y i.e., 2 Cr. Only Term Insurance Policies which are pure insurance can provide 15 Y coverage at a reasonable annual premium.

Hence *Term Insurance* is the most efficient form of life cover.

Coming to the company, it is important to associate yourself with the most reliable one available in the market as it is going to be a long-term association, a lifetime partner. The claim settlement ratio of the company gives a fair idea of the performance of the company.

### Medical Cover:

Health insurance is essential to protect your savings from high medical costs and ensure access to quality health care. It acts as a safety net against unexpected accidents or serious illnesses, covering hospitalization, treatments, and medicines. Being government employees, we are covered by either State Government or Central Government health schemes. However, many a time it is found that the govt schemes are not available in all locations, not covering all aspects of treatment or the entire expense, etc. Even though all governments are continuously improving the health schemes, there will always be limitations. Hence, it is recommended to go for private medical insurance (base plan) or Top-up medical insurance depending upon the gaps in the current available government schemes.

### Emergency Cover:

To meet any emergency needs which may arise due to any unforeseen situations it is recommended to have a dedicated fund (emergency fund) which is readily available at any given point in time.

This fund should be *highly liquid* and *stable* and hence should be in the form of fixed deposits, ultra-short-term debt funds, gold, or cash.

The Emergency Fund should be at least 6 to 8 times of the monthly living expenses and can be set up over a period of time.

### Savings:

Savings is the money left over after subtracting expenses and spending from earnings over a given period. The reinvestment of this surplus results in creation of assets. Wealth is the accumulation of these assets and the income generated from these assets. We all know: Savings = Income – Expenditure.

The expenditure can be controlled by adopting some of the best practices like questioning each spending, avoiding impulse buying, delaying gratification, having a check on lifestyle inflation and through monthly budgeting. Income can be increased by having passive income sources. This can be done by investing the savings in income-generating assets.

But treating savings as the leftover, after making all the expenses from the monthly income, may not be the best way for building savings. The alternate approach is to *decide in advance* how much is to be saved each month. Let us say 20% of the monthly income (as per the NWS Rule). Accordingly, income, expenditure and savings equation can be re-written as:

**Expenditure = Income - Savings**

*Wealth can be generated without a high income, but there is no chance of building wealth without a high saving rate.* Hence, Savings form the foundation block for all wealth generation.


### Lifestyle Inflation:

Lifestyle inflation is the tendency of individuals to increase their spending in response to an increase in income, which can hinder their ability to save and achieve financial goals. Lifestyle inflation can cause people to get stuck in a cycle of living between salary days, where they have just enough money to pay the monthly bills. It is important to understand that *market inflation is beyond our control whereas lifestyle inflation is within our control.*

### Investment:

The primary reason for investing money is to save for future, to preserve money against inflation and to replace human capital with financial capital as we age. The ultimate objective is to increase the total wealth of an

individual, enabling him/her to have freedom of choice throughout his/her life.

The ideal path to investment will be to first identify goals, then classify them into short/medium/long term, create savings and invest the money accordingly. This is easier said than done as most of us will not go beyond short-term goals. The alternative method is to save a fixed percentage of the income every month and invest the amount from a long-term perspective.

### Investment Options:

The investment world is constantly evolving with a vast array of financial instruments ranging from traditional deposits to complex derivatives, some of which are speculative in nature. The fundamental question every investor faces is to select the type of instrument. In personal finance the instruments have multiple characteristics, but the objective of our investments is that they should give reasonable returns, provide liquidity during time of need and mitigate risks throughout our lifespan. Hence risk, return and liquidity form the core characteristics of any financial instrument. In addition, we should also have a fair idea of expenses involved in acquiring/disposing/storing, tax liabilities and the amount of hassle associated with the instruments.

### Investment Instruments:

| Sl No | Instruments | Risk | Return | Liquidity | Expenses | Tax | Hassle |
|---|---|---|---|---|---|---|---|
| 1 | Fixed Deposit | VL | L | Yes | - | Yes | - |
| 2 | PPF/SSY | VL | M | No | - | - | - |
| 3 | Bonds/Debentures | L/M | L/M | Yes | - | Yes | - |
| 4 | Equity | H | H | Yes | Yes | Yes | - |
| 5 | Gold | M | M | Yes | Yes | Yes | Yes |
| 6 | Property | H | V | No | Yes | Yes | Yes |

Very Low (VL); Low (L); Medium (M); High (H); Variable (V)

The above financial instruments can be broadly classified into Debt and Equity. Debt instruments like FD/PF/bonds/debentures are income generating assets whereas Equity Shares/Mutual funds/property are wealth creating assets. The selection of financial instruments for short-term/medium-term/long-term goals will depend on the core characteristics of the instruments, i.e., risk, return and liquidity.

**Short Term Investment** requires *low risk* and *high liquidity*. Hence fixed deposits, recurring deposits, ultra short term and short-term debt funds are preferred for short-term investments as they are low risk, high liquidity income generating assets. Investment in Property/PPF/equity is not suited for short-term owing to illiquidity and volatility, respectively.

**Long Term Investment** aims at *high growth*. This can be achieved through investing in high return wealth creating assets. But all high return instruments are in the high-risk category and are characterized by high volatility. Equity shares/equity mutual funds and PPF are instruments which can be opted for long term investment owing to high growth potential of equity markets and annual compounding and tax benefits of PPF. Academic research has consistently found that the equity market gives high returns over rolling periods of 10-, 20-, and 30- year periods. In his studies, Professor Jeremy J Siegel found that stocks fetched returns at least 5 percent higher than inflation and higher than cash or bonds in 99.4 percent of rolling 30-year periods from 1802 to 2001.

### Investing in Equity Shares:

The equity market consists of shares of thousands of big and small companies, some of which may grow exponentially, and some may significantly underperform or fail. The market is extremely volatile and the valuations of the shares of the companies are linked to both intrinsic aspects of the company and the extrinsic aspects of the market like government policies, emotions and sentiments of the investors, national, regional, and global events, etc. Under such circumstances where experts find it difficult to identify and select stocks with full confidence, it is extremely difficult for a police officer/government employee to be able to select stocks of companies which have great prospect of future growth.

Some fun facts about equity market:

- Neither can you time the market nor consistently beat the market.
- Equity investment is filled with risks, expenses, and emotions.
- The more the managers and brokers take, the less the investors get.
- Aiming for average is the best shot for finishing above average.

Considering these basic facts of equity market, it is advised to *be part of the market as a passive investor* wherein we buy a part of the whole market, rather than buying specific individual stocks. This can be done easily through something called Index Funds.

### Index Funds:

Index funds mirror the performance of benchmarks like NIFTY 50 and other stock market indices by mimicking their makeup. Index funds invest in the same assets using the same weights as the target index, typically stocks or bonds. Index funds provide broad market exposure and diversification across various sectors and asset classes.

Academic research has consistently found that most active investors (stock pickers) within a given market segment underperform the relevant index after fees and taxes when the number of years of investment extends to a decade or more. Investors do not need to spend their precious time analyzing various stocks. Investors, academicians, and various authors such as Benjamin Graham, Warren Buffet, John C Bogle, Paul Samuelson, et al have long been strong proponents of index funds. Beyond wealth creation, retirement planning and tax efficiency form the next critical pillars of long-term financial management.

### Retirement: (NPS/UPS)

Retirement is an inevitable stage of life for all government officers and is filled with uncertainties of longevity, health and fitness conditions, future inflation, post-retirement lifestyle, and income streams. Hence, it is necessary to plan and prepare ourselves physically, mentally, emotionally, and financially to live through the second innings of our life.

Investment in retirement is a long-term investment and will include selection of retirement options (NPS/UPS) and schemes. It will be futile to decide whether to opt for NPS/UPS purely based on financial calculations

like Net Present Value (NPV) or Internal Rate of Return (IRR) as we are clueless regarding our individual life expectancy i.e., the time of death. Hence, decision should be taken only after evaluating all the features like assured income; inflation protection; corpus withdrawal; family pension; death, VRS & other premature exit options; continuation and deferment options; withholding of pension; freedom and flexibility offered. *You are choosing your lifetime partner (NPS/UPS), it should suit your personality, so choose wisely.*

As far as schemes are concerned it is critical to understand the available schemes (Default, Scheme G, LC 25, LC 50, and LC 75). New recruits should opt for LC 75 as it provides maximum equity exposure, which will eventually form the foundation for high growth over the long term.

### Tax-efficient Investing:

The table (Investment Instruments) shows that most of the instruments have a tax component. The tax rates vary from instrument to instrument and from time to time as per the changing government policies and the evolving tax landscape. The most tax efficient instruments are "Exempt-Exempt-Exempt" (EEE) in which the investments are tax-free at all three stages: investment (contribution), accumulation (interest earned), and withdrawal (maturity). It offers maximum tax efficiency, allowing your money to grow tax-free. For example, PPF and SSY are EEE instruments; In ULIP plans the maturity proceeds are tax-exempt under section 10(10D) of IT Act. In equity there is a provision for tax harvesting under section 112A of IT Act. The tax laws keep changing very often and hence be aware and take advantage of these benefits by calculating *after tax returns* for each instrument and then investing accordingly.

### Protocols:

Using the SIP model I have tried to simplify all aspects of financial management and to establish a set of rules for safety, savings, and investments. Now, to bind things together and to ensure consistency, it is necessary to have a set of protocols in place. This includes habit formation, automation, and review.

### Habit Formation:

*Personal finance is more behavioral than mathematical* and hence habit formation assumes paramount importance. Safety, savings, and investments are built over a period by continuously engaging in these activities until they become a habit. The habits will further become part of the individual's personality and become his/her culture.

### Automation:

Process automation is one of the most critical aspects of protocol as it eases out the investors' mental faculty and reduces decision fatigue. This is done through the process of Systematic Investment Plans (SIPs) and Systematic Withdrawal Plans (SWPs).

### Systematic Investment Plans (SIPs):

A Systematic Investment Plan works on a simple principle by investing a fixed amount of money at regular intervals into a specific fund. The process is typically automated, with the amount being debited directly from the investor's bank account. The primary benefit being Rupee cost averaging. This strategy frees the investor from the challenge of timing the market. The investments channelized through these SIPs need to be stepped up over the years. The Pay Raise Rule provides the foundation for stepping up SIPs on a regular and sustainable basis.

### Systematic Withdrawal Plans (SWPs):

A systematic withdrawal plan (SWP) is a scheduled investment withdrawal plan which is mostly used for retirement but can also be used for various other payout needs. Systematic withdrawal plans can be set up for withdrawals from most of the investment instruments available in the market.

### Review & Rebalance:

All aspects of the SIP matrix should be monitored and reviewed on a yearly basis. During the review process, the short-term, medium-term, and

long-term goals need to be reassessed, and the asset allocation should be rebalanced as per the revised position.

**SIP Matrix – Reloaded:**

**Some Common Mistakes:**

- Delaying investing
- Chasing hot stocks
- Fear of missing out
- Excessive EMI burden
- Untamed lifestyle inflation
- Lack of nominations/will
- Indiscipline, impulse buying
- Missing tax-efficient investing
- Buying insurance as an investment
- Having inadequate emergency fund
- Non timely submission of property returns to government

| Emergency Cover | Goals | Habits |
|---|---|---|
| • 6 x Monthly Expenses<br>• Liquid Fund | • Long/Medium/ Short Term Financial Goals | • Build Positive Habits<br>• Consistency<br>• Discipline |
| **Life Cover** | **Savings** | **Automation** |
| • Term Policy<br>• 15 x Annual Income<br>• As soon as you have dependents<br>• Up to ___years | • Pay Yourself First<br>• Minimum 20%<br>• Conscious Spending<br>• Lifestyle Inflation | • Investment Account<br>• Monthly Budgeting<br>• SIPs<br>• SWPs |
| **Medical Cover** | **Investments** | **Review** |
| • Top Up Plan | • Invest in Self<br>• Index Fund<br>• Asset Allocation<br>• Risk Mitigation | • Annually |

## Rules of Thumb:

| Sl No | Rule | Value | Remarks |
|---|---|---|---|
| 1. | **Emergency Fund Rule** | **6X** | Equal to six times monthly expenditure |
| 2. | **Insurance Rule** | **15Y** | Sum Assured should be fifteen times annual income |
| 3. | **EMI Rule** | **< 40%** | The EMI of all loans combined should not be more than 40% of the monthly income |
| 4. | **NWS Rule** | **50:30:20** | Needs-50%; Wants-30%; Savings-20% |
| 5. | **Investment Rule** | **100-Age** | Invest (100-Age) % of your monthly savings in Equity and the remaining in Debt. |
| 6. | **Pay Raise Rule** | **50%** | Save 50% of every pay raise |
| 7. | **Splurge Rule** | **2X** | For every Rs X splurged on something invest the same amount. |
| 8. | **Retirement Fund Rule** | **3Y@40; 6Y@50; 8Y@60** | The total retirement corpus should be three times annual income at 40 years, six times at 50 years and eight times at retirement. |

NB: These are indicative rules and should vary depending on individuals' financial circumstances and risk appetite.

## Conclusion:

The first and the foremost is to invest in self through education, skill upgradation and saving 15-20% of your in-hand salary. The savings need to be immediately invested in appropriate financial instruments with debt and equity allocation as per your age & risk appetite. The entire process of savings and investment needs to be automated through a separate investment account and through SIPs with diversified low-cost index funds forming the core of the equity portfolio. In the times ahead invest time and energy in learning more about asset allocation, risk mitigation, global diversification, tax harvesting and the ever-evolving lexicon in the

financial world. Once you get a broad understanding of these aspects you will be able to create a unique portfolio tailored exclusively for you as per your personality, ambitions, and financial situation. Do not forget to get term insurance, a medical top-up plan and to set up an emergency fund the triple safety cover to protect you in times of emergencies. Have a regular check on lifestyle inflation and review the components of the SIP model on a yearly basis and let time and money do the hard work of increasing your wealth to give you freedom of choice throughout your life.

## References and Further Readings:


1. *Benjamin Graham. The Intelligent Investor*
2. *Darren Hardy. The Compound Effect*
3. *Jeremy J Siegel. Stocks for the Long Run: The Definitive Guide to Financial Market Returns & Long-Term Investment Strategies*
4. *Morgan Housel. The Psychology of Money, The Art of Spending Money: Simple Choices for a Richer Life*
5. *Monika Halan. Let's Talk Money: You've Worked Hard for It, Now Make It Work for You, Let's Talk Mutual Funds: Building Wealth in a Smart Swift Manner*
6. *Nick Maggiulli. Just Keep Buying: Proven Ways to Save Money and Build Your Wealth*
7. *Mark Mobius. The Book of Wealth: A Young Investor's Guide to Wealth and Happiness*
8. *James Clear. Atomic Habits*
9. *Bill Perkins. Die with Zero: Getting All You Can from Your Money and Your Life*
10. *Sahil Bloom. The 5 Types of Wealth: A Transformative Guide to Design Your Dream Life*


**Author's Profile:**
Seju P Kuruvila, IPS Deputy Director NTRO

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 60-78)

# Roadmap to Bring Back Indian Fugitives Based Abroad

Daljeet Singh, IPS*

***Abstract:***

*With the ever-growing economic activities across the globe and glocalization of criminal activities (like, cybercrimes, economic and financial crimes including money laundering and frauds, trans-national organized crimes, including drug trafficking and human trafficking etc.), the need for international co-operation in investigation, trial and asset recovery in criminal matters has increased exponentially globally. With the digital revolution, extensive penetration of internet and ever increasing boundaryless nature of offences, the need for international cooperation is being felt more anxiously than ever before. Extradition and deportation of fugitives based abroad is an inexplicable part of international co-operation in such matters. This paper critically examines the available tools to bring back the Indian fugitives based abroad and suggests a road map to expedite the process of their extradition, including changes in the legal and procedural framework, strategic mechanism to harness the diplomatic channels, inter-agency cooperation, capacity building of Law Enforcement Agencies and use of technology.*

## Introduction:

Every sovereign country makes laws, rules and regulations for its citizens to follow, so that order is maintained in their society. Any citizen violating

*Second in command Ops Directorate, FHQ, BSF Block-X, CGO Complex Lodi Road, New Delhi-110003.

the statutory provisions of the law of the land is liable for it. The general tendency of the offenders is to avoid the due process of law in their country and if they find it difficult to avoid the legal process in their own country, they try to find some safe haven abroad, which are out of bounds of the domestic laws of their own country.

With the ever-growing globalization and interconnectivity, it has become easier for the offenders to escape to the foreign jurisdictions to avoid prosecution in their own country. In such scenario, the importance of international cooperation in bringing these offenders before the jurisdictional courts are beyond any iota of doubt. Extradition of fugitives is an important arm of such international cooperation in criminal matters.

### International Extradition Jurisprudence:

The foundation of international extradition jurisprudence is laid on the Latin principle of "aut dedere aut judicare" (either extradite or punish), which was propounded by Hugo Grotius, the great Dutch jurist of 16th Century. International Law Commission (ILC) set up by the United Nations (2014, pp. 141-142) mentioned in its Report as follows:

> *"The role the obligation to extradite or prosecute plays in supporting international cooperation to fight impunity has been recognized at least since the time of Hugo Grotius, who postulated the principle of aut dedere aut punire (either extradite or punish): "When appealed to, a State should either punish the guilty person as he deserves, or it should entrust him to the discretion of the party making the appeal." The modern terminology replaces "punishment" with "prosecution" [aut dedere aut judicare] as the alternative to extradition in order to reflect better the possibility that an alleged offender may be found not guilty."*

Thus, under the international extradition jurisprudence, the paradigm has gradually shifted from punishment to prosecution of the fugitive offender.

Recognizing the need for international cooperation in criminal matters, "Model Treaty on Extradition" was adopted by the UN General Assembly

Resolution 45/116, which was amended by the UN General Assembly Resolution 52/88 (UNODC, 1990). Subsequently, Article 16 of the "United Nations Convention against Transnational Organized Crime" (UNOTC), 2000 provided for "extradition" in the offences covered by the Convention. These model treaties and convention provide a road map for any country to promulgate extradition laws in their jurisdictions and enter into extradition treaties, agreements or arrangements with other countries, whether bilateral or multilateral.

The international extradition jurisprudence is anchored on certain fundamental doctrinal principles, such as reciprocity, dual criminality, specialty, double jeopardy, human rights consideration, fair trial, proportional punishment, political & military offense exceptions, equivalence and limitation etc.; and it is shaped by treaties, bilateral agreements, and evolving case laws across jurisdictions. In Abu Salem Abdul Qayoom Ansari vs. State of Maharashtra (2010 INSC 602), Hon'ble Supreme Court of India has also recognized the five substantive ingredients of extradition, as follows: "Doctrinally speaking, extradition has five substantive ingredients. They are: (a) reciprocity, (b) double criminality, (c) extraditable offences, (d) specialty and (e) non inquiry."

The specific terms governing extradition depends heavily on bilateral or multilateral treaties, supplemented by domestic statutory laws and due process requirements. These principles collectively ensure that the extradition of fugitives is properly regulated and honour the sovereignty of both states and individual rights, in tune with the basic fundamental principles of international cooperation and human rights protection.

## Legislative Framework for Extradition Under Indian Jurisprudence:

"The Extradition Act, 1962" of India (hereinafter called "the Act of 1962"), as amended in 1993 provides the legislative framework for extradition of fugitive criminals from India. For the extradition of a fugitive criminal from India, a bilateral arrangement or agreement or extradition treaty or a suitable multilateral convention is required, which provides for extradition in offences covered by that particular multilateral

convention, provided that both the requesting State and India are parties to it.

No comprehensive reliable database of the fugitives for which the extradition request has been submitted by India to a foreign country or the fugitives extradited by foreign countries to India is available publicly online. One of the basic reasons behind this may be the privacy rights of the offenders. The only reliable and authentic resource throwing some light on the issue of the fugitives, is the replies given by the Government of India on the floor of Parliament.

As per the information culled out of the replies to the various questions raised on the floor of the Parliament of India, during the period of five years (2019-2024), only 23 persons were successfully extradited to India as against 178 extradition requests made to different countries. Thus, the success rate of extraditions request has been less than 8%. About 1/3rd of the total extradition requests made by India are pending in the USA only (MHA, 2024).

### Extradition Law of India Needs a Fresh Energy:

The Extradition Act, 1962 of India is more than 6 decades old. Although, some amendments were made in this Act in the year 1993, yet, the Act seems to be devoid of the legal requirements in view of the changed circumstances during last couple of decades. The digital revolution, extensive penetration of Internet, exponential rise of cybercrimes, ever growing economy, new nature of economic and financial crimes, trans-national organized crimes and promulgation of plethora of new domestic and international laws and treaties etc. are some of the factors, which necessitates a relook into the provisions of the Extradition Act, 1962.

Some of the issues concerning the Extradition Act, 1962 of India are being discussed hereinbelow:

(i) The Act of 1962 does not define the term "extradition" in the definition section (2) of the Act. Following the doctrine of "aut dedere aut judicare" (either extradite or prosecute), the term "extradition" needs to be clearly defined in the Act on the lines of the "UNODC Model Law on Extradition".

(ii) Section 2(c) of the Act of 1962 defines the "extradition offence" as

follows: "(c) "extradition offence" means—

a. in relation to a foreign State, being a treaty State, an offence provided for in the extradition treaty with that State;
b. in relation to a foreign State other than a treaty State an offence punishable with imprisonment for a term which shall not be less than one year under the laws of India or of a foreign State and includes a composite offence;"

The definition given in Section 2(c)(ii) above needs a relook, especially on the ground (of quantum of punishment) that whether the efforts put in for extradition of a fugitive are commensurate with the punishment prescribed in this sub section. The minimum punishment prescribed for the "extradition offence" may be revisited to make it commensurate with the efforts likely to be made for the extradition of fugitive.

(iii) A plain reading of the Section 2(f) of the Act of 1962 of India gives the impression that the term "fugitive criminal" has been defined in respect of the extradition offence in a foreign State, whereas there seems a black hole with respect to the definition of "fugitive criminal" or "fugitive offender" committing the extradition offence in India but settled in a foreign country.

(iv) It may be noted that Section 2(f) of The Fugitive Economic Offenders Act, 2018 defines the term "fugitive economic offender", but this definition is restricted to the "Scheduled Offences" specified in the Schedule appended to this Act only. It does not cater to the needs of the Extradition Act.

(v) Fast Track Exclusive Courts for Extradition Matters: Extradition is a very specialized and complex field. The legal process involved in extradition consumes a big chunk of time of the Courts. Moreover, adjudicating extradition matters require in depth understanding of the International Laws, Treaties and judicial pronouncements. Thus, there is a need to set up Fast Track Exclusive Court for Extradition Matters under the Extradition Act of India. This exclusive Court would be in a better position to understand the nuances of extradition and reduce the judicial delays in the extradition matters.

(vi) Joint Investigation Teams (JITs): Sometimes, investigation of the cases involving fugitives may be very complex and any domestic LEA conducting that investigation may have to face innumerable

challenges due to jurisdictional issues. Thus, possibility of formation of joint investigation teams (JITs) involving suitable officers from the Indian as well as foreign LEAs may be explored in the complex matters, where the extradition of fugitive seems a remote possibility. Such mechanism should be given legal backing through the Extradition Act.

(vii) Principle of Dual Criminality is one of the fundamental doctrinal principles of extradition under the international jurisprudence. As per this doctrine, the alleged act, for which extradition request is made, must be a punishable offence in both requested and requesting countries. If it is not so, extradition will likely be denied. Fugitives deliberately flee to jurisdictions where their actions are not considered crimes, complicating extradition and causing long delays.

Although, the collective reading of the definitions of "composite offence" and "extradition offence" given in Section 2(a) and 2(c) respectively along with Section 34 of the Act of 1962 suggests that the principle of dual criminality has been indirectly recognized in this Act. However, to avoid any ambiguity, this principle should be explicitly spelt out in the Act.

(viii) Principle of Double Jeopardy is another fundamental doctrinal principle of extradition, wherein a person cannot be extradited for the same crime if they have already been tried and punished for the same crime in either country, reflecting the principle of "non bis in idem". This prevents multiple prosecutions for the same crime and foreign courts can block or delay extradition on these grounds.

Although, this principle can be problematic in certain cases. For example, David Headley, an American terrorist, involved in the death of about 140 Indian nationals in 26/11 Mumbai attacks, was not extradited by the US to India, as he had already been sentenced to imprisonment by US courts, for killing six Americans.

Thus, the elements of Principle of Double Jeopardy and the conditions of their applicability should be clearly spelt out in the Act itself. This would be possible only if the ingredients of "extradition offences" are brought in conformity with the international standards.

(ix) To make "The Extradition Act, 1962" more effective and commensurate with the emerging needs of the criminal justice

administration, a list of specific acts of omission and commission under the various Indian Laws and Acts needs to be appended to the Extradition Act in the form of a Schedule conforming to the fundamental doctrinal principles of international extradition jurisprudence. Although, this list of scheduled extradition offences shall be a subject matter of negotiation for execution of Extradition Arrangements or Treaties with foreign States and finally, only those scheduled extradition offences shall be appended to the Treaty, which are mutually agreed upon between the States.

(x) "Sovereign Assurances": One of the major concerns cited by many countries, while rejecting the extradition request from India, is the provision of death penalty for some offences. In such matters, sometimes Sovereign Assurances are given by India to the requested country. For example, in case of Abu Salem, Government of India gave sovereign assurance to the Government of Portugal that he will not be awarded the death penalty.

Although, Section 34C of the Act of 1962 has made provision of life imprisonment for death penalty, however, the Act is silent on the concept of "sovereign assurances" in such matters.

Thus, the "Sovereign Assurances" and conditions thereof should be explicitly spelt out in the Act itself. It will embolden the confidence of the prospective foreign countries likely to enter the Extradition Treaty or Arrangement with India.

(xi) Protection Against Political and Military Offenses: Extradition is often refused by the foreign countries if the offense is deemed to be political or military in nature to prevent persecution for political beliefs or military actions. Many a time, fugitive accused argue before the Court that prosecution is politically motivated, which stalls or blocks extradition requests.

Although, Section 31(2) the Act of 1962 primarily acknowledges the "political character" exception of certain offences specified in the Schedule appended to the Act of 1962, however, a plain reading of this Schedule clearly suggests that it only enumerates the list of some "offences which are not to be regarded as offences of a political character". It may be noted that many of the offences mentioned in this list have been repealed or

omitted. Besides, over a period of time, many new offences have come up, which are not mentioned in this list.

Furthermore, the "political offences" have not been categorically defined in the "extradition offence" under section 2(c) of the Act of 1962. Thus, the vagueness in the definition of "political offences" leaves scope for different interpretations by the Courts. It ultimately helps the fugitive offender to argue in his favour that he may be prosecuted for the political reasons and consequently it may delay the extradition process. Similarly, the "military offences" have also not been defined in the Act of 1962.

Thus, there is a need to clearly define the "political offences" and "military offences" in the Act itself, so as to overcome the ambiguity and bring certainty in the outcome of the process of extradition.

(xii) Although, Section 34B of the Act of 1962 mentions about the "provisional arrest", however, the meaning of "provisional arrest" has not been explained in the definition section to distinguish it from the "arrest" as prescribed in the Code of Criminal Procedure (Cr.PC), 1973 as amended from time to time.

(xiii) With the advent of the three New Criminal Laws (NCLs), i.e. Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Surakha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, the list of Extradition Offences as well as the Offences mentioned in the Schedule appended to the Act, need a relook. Apart from this, procedural provisions of Extradition Act also need to be recast to make it in tune with the NCLs.

(xiv) The Extradition Act, 1962 prescribes procedures for handling both extradition requests being sent to foreign countries as well as the extradition requests received from different countries.

Any Extradition Treaty is notified either under Chapter-II or Chapter III of the Extradition Act, 1962. The procedure for extradition of a fugitive criminal under Chapter-II of the Act is more stringent and requires a "prima facie case" against the fugitive in India whereas, the extradition procedure for a fugitive criminal under Chapter-III of the Act is comparatively swifter. Here, establishing the identity of the fugitive and the issuance of a warrant of arrest is sufficient and the need for a "prima

facie case" against the accused is not required. However, the provisions of Chapter-IV regarding the return or surrender of Indian fugitives from foreign countries are not so elaborate and explanatory as the provisions given in Chapter-II and Chapter-III of the Act.

It is suggested that without prejudice to any treaty obligations, the substantive conditions for extradition as well as refusal for extradition of fugitives from India must be explicitly enumerated in the Act itself. It will reinforce the faith of the States during the negotiation process for the Extradition Treaty or Bilateral Treaty.

By making these changes in the extradition legislation, India can strengthen its legal apparatus, enhance its ability to combat trans-national crimes, and hold fugitive offenders accountable for their acts.

### Trial in Absentia:

Section 355 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 makes provisions for "inquiries and trial being held in absence of accused in certain cases". Similarly, Section 356 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 makes provisions for "inquiry, trial or judgment in absentia of proclaimed offender" and prescribes a procedure thereof.

These provisions may be used for prosecution of fugitive offenders, even if they are abroad. It will facilitate the international cooperation in extradition of the fugitive. Because, if the fugitive offender is convicted, it will support the "principle of sufficient evidence" against fugitive and will ultimately buttress the claim of India in extradition of the fugitive.

However, this provision should be used with a great caution, because in case of conviction in absentia, the fugitive may claim that he may not get a fair chance of trial in India, thereby violating his basic human rights. However, this claim of the fugitive can again be rebutted by India by claiming that the fugitive has right to appeal against the conviction in the High Court and thereafter in Supreme Court of India.

### Deportation vs. Extradition:

It may be noted that extradition is a formal and treaty-based process, which requires compliance with the stringent provisions of the Extradition Treaty,

whereas deportation can be faster via administrative action, especially when extradition treaties are not present. Diplomatic channels and immigration mechanism may be harnessed to explore the possibility of deportation of fugitives through administrative arrangements, without resorting to the complex extradition process.

## Harnessing the diplomatic channels:

### Need for Extradition Treaties or Arrangements with more countries:

So far, India has signed Extradition Treaties with only 48 countries/territories and entered into extradition arrangements with only 12 countries, which collectively makes only 30% of the 196 INTERPOL member countries (MHA, 2024). In other words, about 70% of the INTERPOL member countries, with which India has no extradition arrangement or treaty, are safe havens for the Indian fugitives.

Under the international jurisprudence, extradition is governed by the bilateral or multilateral treaties, based on the principle of "nulla poena sine lege" (no punishment without a law) (UN, 2014). As per this maxim, a law should be in place if some fugitive has to be extradited.

The last Extradition Treaty signed by India was nine years ago with Afghanistan (2016) and the last Extradition Arrangement made by India was six years ago with Armenia (2019) (MHA, 2024). Thus, no Extradition Treaty and no Extradition Arrangement during last nine years and six years respectively is a matter of deep concern for Indian Criminal Jurisprudence.

Thus, there is a dire need for the Government of India to make diplomatic efforts to conclude Extradition Treaties or Arrangements and Mutual Legal Assistance Treaties (MLATs) with many more countries, which are presumed to be the safe haven. While expanding the extradition treaties, focus should be laid on the key countries with significant number of Indian fugitives. It'll ensure that fugitive criminals are brought to face the criminal justice system.

Summit diplomacy and the visits of high-level dignitaries should be used to emphasize the need of extradition cooperation in the bilateral relations. Pending extradition matters should receive sustained political

attention during these high-level summits and visits. Diplomats should be sufficiently trained in the minute nuances of the extradition matters, so that they may negotiate with their counterparts before such high-level summits and visits.

The countries like, Canada, United Arab Emirates (UAE), United Kingdom (UK) and United States of America (USA) are known as safe havens for Indian fugitives. Further, extradition treaty with some of the countries is very old and does not capture the essence of the emerging challenges. Simultaneously, over a period of time, some new strategic partners of India have also come up, with which extradition treaty needs to be executed. Thus, diplomats dealing with these countries must pay special attention to extradition matters connected with these countries.

Besides, the concept of Most Favoured Nation (MFN) should not be restricted to the field of economis only and may be harnessed in the extradition matters also. Although, while negotiating Extradition Treaties and Arrangements, the basic fundamental doctrinal principles under the international extradition jurisprudence should be given the due consideration.

### Principle of Reciprocity:

Extradition usually operates on reciprocal arrangements, where countries agree for mutual cooperation through treaties, wherein countries agree to extradite fugitives based on mutual cooperation and reciprocity. Absence of a treaty leads to non-obligation on the part of States to extradite the fugitives. Maintaining strong bilateral and multi-lateral relations and diplomatic ties will increase the cooperation and reciprocity in extradition matters, thereby expediting the processes.

### Principle of Specialty:

The doctrine of specialty limits post-extradition prosecutions by requiring that the extradited person is prosecuted, detained, or punished only for specific offenses for which the fugitive was extradited, and not for any other offences committed by him before the extradition was granted. This

restriction shields individuals from facing charges for other offenses after surrender.

Section 21 of the Act of 1962 (as amended in 1993) essentially endorses the principle of specialty. Hon'ble Supreme Court of India has also upheld this view in "Daya Singh Lahoria vs. Union of India and Ors" (2001 INSC 212) and in "Abu Salem Abdul Qayoom Ansari vs. State of Maharashtra" (2010 INSC 602).

Section 21 of the Act of 1962 should be highlighted through diplomatic channels while negotiating Extraditions Treaty or Arrangement with the other States. It will help the foreign countries to easily grasp the nuances of the Indian Extradition Jurisprudence and come forward to enter into treaty or arrangement, whichever is applicable.

### Human Rights Considerations:

Many states deny extradition if the individual risks being subjected to torture, inhumane treatment in prisons, or unfair trial in the requesting country. International extradition law lay emphasis on human rights safeguards, blocking extradition where a person may face threats to basic rights may bar extradition in accordance with international conventions. Fugitives use these human rights concerns or poor detention conditions in India to delay or block extradition proceedings in foreign courts. The case of extradition of Vijay Mallya from UK is an important recent case law in this regard.

In the Abu Salem (Supra) case, Hon'ble Supreme Court of India also laid emphasis on the human rights concerns and held that:

> *"In the context of extradition law, which is based on international treaty obligations, we must keep in mind the emerging Human Rights movements in the post-World War II scenario and at the same time the need to curb transnational and international crime. The conflict between these two divergent trends is sought to be resolved by expanding the network of bilateral and multilateral treaties to outlaw transnational crime on the basis of mutual treaty obligation. In such a situation there is obviously a demand for inclusion of Human Rights concerns in the extradition process and at the same*

*time garnering more international support and awareness for suppression of crime. A fair balance has to be struck between Human Rights norms and the need to tackle transnational crime."*

To strike the balance between the human rights concerns of the fugitives and the control on the transnational crimes, it is the need of the hour to improve the domestic prison conditions and make it to meet international safeguards and human rights standards. For this, a model of the prison cell or detention facility may be prepared, which should conform to all the international standards of human rights and circulate to all States/UTs India. Efforts should be made to have at least one such prison or detention facility in the capital cities of all the States/UTs. Visits by the foreign diplomats may also be facilitated to visit such model prisons or detention facilities. It will help in mitigating the objections from foreign courts on the ground of poor prison conditions.

Similarly, the law enforcement agencies must be trained and sensitize to ensure that all the established legal procedures must be followed while dealing with any offender, so that the news of human rights violations, including false implication, torture, arbitrary executions, enforced disappearance, arbitrary detention, inhumane treatment, unfair trials, unfair judicial processes and other human rights violations etc. do not appear in the media unnecessarily. These news clippings are potential tools in the hands of the fugitive offenders to block the extradition proceedings against him or her.

Further diplomatic engagements may be used to provide assurances regarding the prison conditions and other human rights issues in India. It will help in mobilizing opinion of the international fraternity in support of the standards of human rights concerns in India.

### Nationality Exception:

Some states refuse to extradite their nationals, often using constitutional provisions or treaty exceptions as grounds. On the other hand, some countries, instead of extraditing their own nationals, offer domestic prosecution instead. This can delay extradition, particularly with countries that assert strong sovereignty over their citizens. This nationality-based

refusal is often rooted in sovereignty and personal jurisdiction principles, with such countries opting to prosecute their nationals domestically rather than extradite. Some of countries using this nationality exception in extradition matters are: China, France, Italy, Russia, Saudi Arabia, United Arab Emirates (UAE) etc.

India faces challenges with these countries where nationality grounds are strong legal barriers to extradition. Thus, India needs to use its diplomatic channels to influence these States to waive off this nationality exception on a bilateral reciprocity basis. It will help in increasing the chances of expeditious extradition of fugitives based in these countries.

### Establishment of dedicated institutional mechanism for extradition matters:

India needs to establish a dedicated institutional mechanism in the form of a special extradition unit, which will help in expediting the process of extradition of fugitives. Since Central Bureau of Investigation (CBI) is the National Central Bureau (NCB) for India for the purpose of INTERPOL, therefore a separate Extradition Zone or International Police Cooperation Zone headed by an officer not below the rank of Joint Director and assisted by appropriate numbers of other rank officers may be set up within CBI. If need be, their regional offices may also be set up in the major countries having significant population of Indian fugitives.

The Extradition Zone of CBI may be given the responsibility of compilation, maintaining and regularly updating the database of all fugitive offenders, for which extradition process is going on. If need be, Director, CBI may be given the liberty to associate domain experts from other agencies with the Extradition Zone of CBI on need basis. Apart from this, this Zone shall also study the objections raised by the foreign countries in various extradition matters on case-to-case basis and compile, update and disseminate the list of learning points for the benefit of all other law enforcement officers.

### Extensive Use of INTERPOL Channels, BHARATPOL and other Technological Tools:

Law enforcement agencies need to extensively use the appropriate INTERPOL channels, like Red Notices for international assistance in locating and restricting the movement of fugitives. Strategic efforts should be made to convert INTERPOL Blue Notices (for tracing the location of fugitives) to Red Notices (for provisional arrest, arrest and extradition of fugitives). It will disrupt the overseas network supporting the fugitives. Apart from this, optimum use of the "Diffusion" tool of INTERPOL should also be made by the LEAs through NCB, Delhi to the NCB of the concerned Country.

The Bharatpol portal, launched by the Central Bureau of Investigation (CBI), integrates the central and state LEAs to streamline international cooperation, Interpol notices, and real-time tracking of fugitive requests. The CBI's Global Operations Centre and Interpol's I-24/7 coordinates with the police forces and other LEAs across the globe for swift extradition efforts. Optimum use of these facilities and tools should be made by the LEAs for international cooperation in investigation of cases related to the fugitives.

Apart from the above, open-source intelligence (OSINT) tools and cyber-enabled surveillance tools may be used to locate the fugitives, while complying with all the privacy protocols and legal procedures.

### Inter-Agency Coordination:

Various law enforcement agencies, like, Ministry of External Affairs (MEA), Bureau of Immigration (BOI), Central Bureau of Investigation (CBI), Enforcement Directorate (ED), Narcotics Control Bureau (NCB) and National Investigation Agency (NIA) etc. may strive for greater inter-agency coordination.

MEA is the Central Authority for the purposes of Extradition matters in India. MEA handles the diplomatic requests, extradition treaties, and consular channels and coordinates with the foreign governments. BOI executes the deportation or administrative actions at the points of entry and exit and maintains the watchlists and passenger data checks. CBI leads the

complex process of extradition of fugitives and the investigations related thereto, disseminates relevant INTERPOL notices across the globe, coordinates with foreign counterparts, runs international operations hubs, and tracks fugitives across borders. ED targets the money laundering, proceeds of crime, and asset tracking and coordinates with the foreign financial institutions and regulators. NCB is involved in investigation of big-ticket cases involving drugs and cross border organized crime.

There is a dire need to develop a secure blockchain based technology-driven platform, which will support the financial trail mapping, communication analysis, and darknet analysis. This platform will share minute details about the fugitives and will help in locating and monitoring the fugitives worldwide. This network should preferably be used for mutual communication among the stakeholders.

Various ministries and government departments maintain structured national databases on the points related to their mandate, which may be interconnected to the above platform and be used for background checks before passport issuance as well as detecting and cancelling travel documents of fugitives. This platform should maintain updated database of fugitives, ensure timely escalation of high-risk cases, and track responses from foreign authorities. Passport data, immigration flags, criminal records, and ongoing extradition requests should be integrated to this platform with an auditable trail.

This platform should also provide real-time communications with foreign counterparts, including secure channels for urgent requests, document and evidence sharing, and status updates. There should be a system of automatic pop-up or alert in the above platform, whenever any suspicious activity is observed by any of the stakeholders. For example, whenever a Red Notice is issued against any fugitive, an automatic alarm or alert in the above platform will sound the stakeholders of the above network, so that they may take necessary action in their respective jurisdiction in respect of this fugitive.

Regular inter-agency briefings would be required among the stakeholder agencies, so that the security and sanctity of the above platform is maintained.

## Capacity Building of Law Enforcement Agencies (LEAs):

Drafting for any type of international cooperation in criminal matters, for example LR, MLAT Request, INTERPOL Notices etc. and in particular, Extradition Requests requires a set of certain special skills, which are acquired through rigorous training and continuous practice. Preparation of Extradition Dossier of fugitive is also a herculean task, which requires special training.

It has been a general presumption among some law enforcement agencies (LEAs), that this drafting is not their cup of tea and it is the unconquered fort of Central LEAs, especially the CBI. This myth needs to be rebutted, if the extradition of fugitives has to be expedited.

With the ever-increasing cybercrimes and transnational nature of other organized crimes, this has become more important than ever before that all the stakeholders are properly trained in the extradition matters. Because, undue delay and mistakes in drafting the extradition requests, may warrant avoidable objections from the Courts of requested countries. Sometimes, this process may linger on and the fugitive may get benefit of "principle of limitation" and may become immune from prosecution.

Thus, extensive and regular training sessions of LEAs are required for their capacity building. Joint training exercises may also be planned, involving the international experts on extradition procedures, asset recovery, INTERPOL notices, and cross-border surveillance etc.

On the one hand, it will reduce the burden on the CBI and on the other hand, it will help in expediting the extradition process of fugitives, as the time span to draft a proper extradition request and preparation of extradition dossier in conformity with the international standards will be reduced significantly.

## Conclusion:

India's extradition laws, though robust, face several challenges in addressing the growing complexity of transnational crimes. The current legal framework requires significant amendments to keep pace with the evolving nature of crimes and the international jurisprudence dealing with such crimes. Key reforms should focus on codification of extradition

offences, setting up Exclusive Fast Track Courts to deal with the extradition matters and ensuring that the basic doctrinal principles of international extradition jurisprudence are clearly spelt out in letter and spirit through amendment in the legislation.

Harnessing the diplomatic channels to enter into Extradition Treaties or Arrangements with as many as countries as possible, considering to accord Most Favoured Nation (MFN) status to the countries, which are willing to enter Extradition Treaty with India, garnering international cooperation in deportation of fugitives from the countries having no Extradition Treaty with India, addressing human rights concerns, improving prison conditions to bring it to international standards, establishment of dedicated institutional mechanism (like Extradition Zone in CBI) for extradition matters, extensive use of INTERPOL channels, BHARATPOL and other technological tools, inter-agency coordination, capacity building of Law Enforcement Agencies (LEAs) are some of the sine-qua-non in ensuring the timely and effective extradition of fugitives based abroad.

The above multi-faceted and structured approach may help India to bring back the fugitives hiding abroad into the country. The Standing Focus Group on Enhancing Cooperation to Track and Apprehend Fugitives Abroad (SFG-ECTAFA) set up by the Government of India may be given the task to examine the above suggestions and make appropriate recommendations to the Government for consideration.

## References:


1. *Government of India, 1962. The Extradition Act, 1962. [Online] Available at:<https://www.indiacode.nic.in/bitstream/123456789/1440/1/196234.pdf>.[Ac c essed on 6th November, 2025].*
2. *Government of India, 2018. The Fugitive Economic Offenders Act, 2018.[Online] Available at:< https://www.indiacode.nic.in/bitstream/123456789/4035/1/A2018-17.pdf>.[Accessed on 6th November, 2025].*
3. *Government of India, 2023. Bhartiya Nagarik Suraksha Sanhita (BNSS), 2023. [Online] Available at:<https://www.indiacode.nic.in/handle/123456789/20099>.[Accessed on 6th November, 2025].*
4. *Ministry of Home Affairs (MHA), Government of India, 2024. Reply to Lok Sabha unstarred question no. 2440. [Online] Available at: <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-*

*pdfs/LS10122024/2440.pdf> [Accessed on 6th November, 2025].*

5. *Supreme Court of India, 2001. Daya Singh Lahoria vs. Union of India and Ors. (2001 INSC 212). [Online] Available at:<https://api.sci.gov.in/jonew/judis/17725.pdf>.[Accessed on 6th November, 2025].*
6. *Supreme Court of India, 2010. Abu Salem Abdul Qayoom Ansari vs. State of Maharashtra (2010 INSC 602). [Online] Available at:<https://api.sci.gov.in/jonew/judis/36830.pdf>.[Accessed on 6th November, 2025].*
7. *United Nations (UN), 2014. Report of the International Law Commission. Sixty-sixth Session. General Assembly Official Records. Supplement No. 10 (A/69/10). [Online] Available at:<https://documents.un.org/doc/undoc/gen/g14/134/72/pdf/g1413472.pdf>.[Accessed on 6th November, 2025].*
8. *UNODC, 1990. Model treaty on extradition. [Online] Available at:<www.unodc.org/documents/congress//background-information/International_Cooperation_CM/Model_Treaty_Extradition_EN.pdf>.[Acce ssed on 6th November, 2025].*
9. *UNODC, 2000. United Nations Convention against Transnational Organized Crime. [Online] Available at:<https://www.unodc.org/unodc/en/organized-crime/intro /UNTOC.html>. [Accessed on 6th November, 2025].*
10. *UNODC, 2004. Model law on extradition. [Online] Available at:<https://www.unodc.org/documents/legal-tools/model_law_extradition.pdf>.[Accessed on 6th November, 2025].*

**Author's Profile:**

Second in command Ops Directorate, FHQ, BSF Block-X, CGO Complex Lodi Road, New Delhi-110003.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 79-94)

# Leveraging Artificial Intelligence to Prevent Misuse of the Dark Web

Sudipta Das, IPS*

## *Abstract:*

*The Dark Web harbours a criminal ecosystem enabling drug trafficking, arms trade, child sexual abuse material, terrorist propaganda, ransomware distribution and stolen credentials. Standard law enforcement tools have proven inadequate against its decentralised architecture, anonymising communications, encryption protocols, cryptocurrency transactions and multinational character. Darknet narcotics trafficking represents a potent national security threat to India. This article examines how Artificial Intelligence (AI) can be leveraged to detect, monitor, infiltrate, and disrupt Dark Web criminality, with a special emphasis on AI-powered narcotics interdiction. It advances the hypothesis that AI-driven adaptive encryption systems, dynamically calibrated through real-time NLP threat analysis and post-quantum cryptographic standards, can raise operational barriers for criminals while preserving the anonymity essential to journalists, dissidents, and legitimate users.*

## *Keywords:*

*Dark Web, Artificial Intelligence, NLP, darknet markets, OPSEC, cryptocurrency forensics, threat hunter, adaptive encryption, post-quantum cryptography, anti-narcotics.*

* *Sector HQrs, SSB Bongaigaon Chaprakata, District Chirang, Assam 783380.*

## Introduction:

The Internet's architecture encompasses concealed layers that are invisible to conventional search engines. Beyond the indexed surface web lies the Deep Web, comprising authenticated content, academic databases and private portals behind password-protected paywalls and firewalls. Deeper still lies the Dark Web, accessible only through specialised software such as The Onion Router (Tor), I2P, and Freenet. By routeing traffic through a layered system of encrypted relays, these networks confer near-complete anonymity upon their users, rendering identification of actors and their locations technically formidable. Although this anonymised architecture is legitimate for journalists, dissidents, whistleblowers, and privacy advocates operating under repressive regimes, it has produced one of the most prolific criminal marketplaces in history. Europol's Internet Organised Crime Threat Assessment (IOCTA) 2026[1] considers the Dark Web as a critical enabler within the global cybercrime ecosystem, providing operational infrastructure, services and anonymity.

Artificial Intelligence (AI), a transformative technology that has become the buzzword of modern times, is catalysing innovation and attracting millions of users. A Large Language Model (LLM) derives its ability to predict the next token by consuming information from myriad sources, which support the accrual and reinforcement of its knowledge base. LLMs enable both structured and unstructured data to be extracted and quality-controlled in real time, in ways that were not possible before. The latest frontier AI models are adept at 'thinking' and efficiently simulating sapient traits like deliberation, planning, multi-step problem-solving and memory retention. Being a dual-use capability that could either amplify malicious intent or mitigate it, AI is opening up new frontiers and practical use cases for law enforcement agencies (LEAs).

With each evolutionary model iteration, Generative AI is becoming more autonomous and adaptable to complex real-world factors. However, GenAI, being a value-neutral entity, is vulnerable to being weaponised for launching social engineering attacks, accelerating online fraud schemes, and producing child sexual abuse material (CSAM) at an industrial scale. At the same time, AI systems that are trained on vast datasets, and capable

of processing unstructured data at lightning speed, can crawl hidden services, scan forums for subversive patterns, classify illicit content across multiple languages, de-anonymise cryptocurrency flows, maintain synthetic undercover personas over extended periods, and autonomously assess emerging threats in real-time. These capabilities have already led to coordinated, multi-agency operational successes, such as the February 2024 dismantling of the ransomware group LockBit, the May 2025 disruption of major drug supply networks through Operation RapTor, and the identification of CSAM distribution rings.

### Dark Web's criminal ecosystem:

To understand how AI can prevent Dark Web misuse, it is necessary to characterise the ecosystem being countered. The Dark Web hosts several overlapping unlawful and immoral forums, each demanding distinct AI-enabled responses. Darknet markets (DNMs) operate through***.*** ***Onion*** domains and offer drug trafficking, weapon sales, counterfeit currency, ransomware, unlicensed betting, banned sexual activities, stolen financial credentials, and fraudulent identification documents. These platforms mimic legitimate e-commerce websites, featuring vendor ratings, escrow services, and customer reviews, and often permit referral-only or invitation-only registration. Since the emergence of Silk Road in 2011 as a DNM that pioneered the use of Bitcoin for illicit drug sales, successive markets have generated billions in black-market revenues. The aggregate cryptocurrency flows on the Dark Web have reached nearly US$2.6 billion in 2025[2], about 60% of it contributed by illegal drug transactions, and the rest by clearinghouses for identity theft, fraud shops, and malware.

Apart from narcotics, CSAM represents one of the most egregious categories of Dark Web harm. The Internet Watch Foundation's AI CSAM Report 2026[3] mentioned 8029 AI-generated images and videos as showing realistic child sexual abuse in 2025. AI has garnered significant interest in clandestine discussion forums, where members are debating the use of commercial AI models, dedicated jailbreak services, or locally hosted open-source models[4]. The Dark Web, paired with end-to-end encrypted messaging applications, functions as a strategic virtual infrastructure for

jihadist and extremist operations, propaganda and fundraising. The Dark Web also hosts a mature Cybercrime-as-a-Service (CaaS) economy through which malicious tools, ransomware kits, and criminal expertise are rented or sold with minimal technical prerequisites. With cybercriminals integrating AI tools into ransomware attack strategies, Cybersecurity Ventures has predicted the global costs from ransomware damage to increase from US$74 billion in 2026 to US$276 billion by 2031[5].

Despite the LEA actions, DNMs are highly resilient, with namesake markets emerging within days and weeks of a successful takedown operation. Moreover, since defrauded victims on the Dark Web have voluntarily entered these loosely monitored virtual spaces, presumably to circumvent mainstream legal provisions or to access prohibited services, self-reporting of cybercrimes is negligible. Anonymity of buyers and sellers makes it very difficult to perform usual statistical profiling and segmentation of DNM members and visitors. As a result, LEAs need to continuously monitor the Dark Web to detect new modus operandi and innovative but devious applications of technology, and even partake in forbidden activities to gain genuinely actionable insights. The crux is that time-honoured law enforcement methods simply cannot match the velocity, anonymity, and global reach of Dark Web criminality.

**OSINT to detect OPSEC lapses:**

Not every breakthrough in Dark Web investigations relies on sophisticated technology. Often, it is the criminal's own mistake that reveals their identity. Operational Security, commonly abbreviated OPSEC, encompasses the disciplined practices that are supposed to keep an online offender's digital persona entirely insulated from his true identity. But, time and again, major DNM operators have been exposed by bad OPSEC. For example, Ross Ulbricht, the founder of drug DNM Silk Road, was unmasked because he had reused his nickname and email address from surface web forums in the early promotions of Silk Road on the Dark Web. Similarly, Alexander Cazes, the founder of AlphaBay market, used his personal email bearing his real name to send automated welcome messages to newly registered AlphaBay users. The broader investigative lesson is clear, that a significant

number of Dark Web busts start with an OPSEC failure rather than breaking cryptographic systems.

LEAs, which actively mine data from forums, social media, data leaks, and archived posts in search of suspects having reused a username, email or an encryption key, can boost their capabilities by harnessing AI, which can gather every fragment of a suspect's digital footprint[6]. AI can efficiently use techniques like linguistic analysis, which involves comparing writing styles and vocabulary preferences across pseudonymous accounts, and metadata analysis for extracting timestamp data embedded in documents or location from GPS-tagged images. AI can support the efforts of Open Source Intelligence (OSINT) specialists by making their analysis and reports more comprehensive and instantaneous.

### Enhanced Surveillance and Pattern Recognition:

The sheer scale of Dark Web activities, which span millions of forum posts, marketplace listings, and chatroom exchanges, generated daily across hundreds of hidden services, renders manual human analysis structurally impossible. AI-powered surveillance systems are capable of automated pattern recognition, can operate continuously without investigator fatigue, and thus extract actionable intelligence from the overwhelming data environment of the Dark Web. Since Tor's onion-routing architecture does not expose link indices, Dark Web crawling poses unique technical challenges. Hidden services must be discovered through recursive link traversal, seeding from known. ***Onion*** addresses and following internal hyperlinks. A recursive crawling study processing approximately 1.49 million Dark Web URLs identified roughly 100,000 accessible subdomains returning active content, reflecting both the breadth and the difficulty of systematic coverage[7]. Unlike established surface web crawlers that struggle to penetrate encrypted and obfuscated layers of the Deep and Dark Webs, AI-enhanced Dark Web crawlers can decipher complex encryption methods and anonymising techniques[8]. The SpyDark crawler[9] deployed pre-trained NLP models to compute relevance scores for content classification, thus enabling selective harvesting of high-value intelligence.

Platform fragmentation occurs when underground communities migrate from a dismantled DNM to encrypted messaging platforms (particularly Telegram) and decentralised applications beyond Tor's ***.onion*** ecosystem. LEAs require AI that can extend monitoring across multiple platforms, and correlate identities across fragmented criminal environments. The adaptive, domain-change-resilient crawler integrated with AI-based content classifiers represents the necessary architectural response to this perpetual adaptation challenge.

Criminal actors continuously evolve linguistic practices to defeat detection, by substituting numerals for letters, employing coded terminology, switching languages mid-transaction, or migrating to platforms beyond current crawler reach. AI surveillance systems must maintain continuously updated lexicons through adversarial training. The models should be specifically calibrated against known obfuscation patterns, and regularly retrained as new patterns emerge.

Beyond crawling, AI can also construct the behavioural profiles of individual Dark Web actors, and map the relational networks connecting them. Posting patterns, linguistic fingerprinting (such as use of idiosyncratic vocabulary, persistent syntax preferences, characteristic spelling patterns), and platform activity timings correlated with time-zone inferences constitute dimensions of profiling that remain consistent even when an actor changes pseudonyms. This enables re-identification of known perpetrators migrating from one marketplace to another. Even sophisticated actors, who meticulously maintain separate Dark Web personas, frequently reuse contact information across distributed sites, thus enabling cross-site attribution. Social network analysis of Dark Web communities, combining named entity recognition, sentiment analysis, and topic modelling, is a proven intelligence methodology for mapping criminal supply chains[10]. Detection of drug trafficking on the Dark Web in the Indian context using machine learning (ML) classification demonstrated the operational applicability of NLP surveillance across diverse geographic and linguistic environments[11].

### Cryptocurrency Forensics:

Cryptocurrencies, particularly privacy-oriented coins like Monero and Zcash, constitute a foundational pillar of Dark Web anonymity. Monero's ring signature and stealth address mechanisms are specifically designed to defeat on-chain analysis. However, AI forensic tools are combining on-chain pattern analysis and off-chain behavioural intelligence. Graph Neural Networks (GNNs) can model blockchain transaction networks and identify cluster patterns that link multiple pseudonymous addresses to a single actor[12]. By combining heuristic analysis with network topology, ML models can uncover mixing services, chain-hopping, and layering strategies that are used to launder drug sales proceeds[13].

Commercial platforms are operationalising these AI approaches. Globally, LEAs are deploying AI-driven blockchain analytics provided by platforms like Chainalysis, Elliptic, and TRM Labs. By using AI-assisted blockchain analytics, Europol and the Australian Federal Police could dismantle LockBit in 2024, seizing 34 servers and freezing more than 200 cryptocurrency accounts. AI forensic tools are exploring opportunities for de-anonymisation at the point of cash-out rather than within the transaction chain itself, by increasingly targeting the fiat on-ramps and off-ramps, which are services that facilitate the exchange of government-issued currencies for cryptocurrencies and vice versa. This technique, when combined with corroborative intelligence from seized DNM servers that provide associations of crypto wallet addresses, has proven decisive in multiple high-profile operations.

### Threat-Hunter Bot for Automated Threat Assessment and Response:

Traditional cybersecurity investigations and countermeasures are activated by system alerts, and are typically undertaken in the form of a reactive mechanism, after malicious activities and system intrusions have been detected. As a result, they are unable to handle tactics, techniques and procedures of clever adversaries. On the other hand, threat hunting is a form of proactive defence that deals with emerging and unseen threats, detecting and eliminating potential cyberattacks that have just penetrated

(or about to penetrate) the environment without raising alarms[14]. In short, a threat hunter is designed for discovering and uncovering new threats.

LEAs should consider deployment of a Threat-Hunter Bot in the Dark Web, which can operate as an adaptive system that keeps optimising and updating its response strategies, with minimal manual reconfiguration. It may be considered an AI-powered version of a SOAR platform (Security Orchestration, Automation and Response), a cybersecurity approach (similar to that used by large private organisations) which improves response time, reduces human errors, ensures consistent execution of incident response processes, facilitates collaboration among security teams and tools, and integrates threat intelligence for better decision-making[15]. A five-stage closed-loop framework is being suggested below:

i. **Sense**: NLP crawlers will continuously analyse the raw content from Dark Web forums, marketplace listings, encrypted messaging archives and paste sites (i.e. sites which publicly post leaked data, compromised credentials, proprietary code and sensitive information).
ii. **Assess**: ML models will evaluate signals against pre-specified categories of threats, such as credentials trafficking, ransomware coordination, weapons brokering, narcotics distribution, terror financing, etc.
iii. **Score**: The Bot will generate and dynamically update threat actor-level composite risk metrics in the form of indices.
iv. **Respond**: When indices exceed pre-defined thresholds, the Bot will respond in a phased manner. At low thresholds, the Bot will generate and share structured intelligence packages for human review. At intermediate thresholds, the Bot will initiate technical countermeasures autonomously, such as blocking flagged Tor circuit identifiers or redirecting traffic to LEA-controlled honeypot mirrors.
v. **Escalate**: At the highest thresholds, the Bot will automatically generate a structured law enforcement notification package containing case summary, actor profiles and jurisdiction-appropriate referral documentation.

### Adaptive Encryption:

There exists a perpetual tension between security priorities and civil liberties in darknet regulation. Adaptive encryption offers a technical architecture that advances both simultaneously, rather than forcing a binary trade-off. Since the Dark Web is overwhelmingly text-based producing volumes of content in multiple languages and criminal slangs, the mechanism being proposed involves an AI-powered encryption system that would continuously perform NLP analysis of Dark Web communications, identify potential threat vectors where benign discussions start transitioning towards criminal activity, and dynamically adapt its cryptographic protocols in proportion to the detected threat level.

In this context, DarkBERT, a transformer-based LLM developed by South Korean researchers, merits LEA consideration. Trained on 2.2 terabytes of Dark Web data, the model understands the complex jargon used by DNM members and hackers. It can identify cyber threats, fraudulent transaction discussions and emerging malware campaigns with significantly higher accuracy than other domain-agnostic models. Being the most domain-adapted model currently available[16], DarkBERT can classify conversational content with high accuracy, identifying the semantic shift from benign chat to criminal planning. A forum thread beginning with privacy advocacy chat may progressively incorporate drug vendor recruitment language, escrow coordination, or discussion on shipping. These are precisely the contextual drifts that regular keyword detection algorithms would miss, but a transformer-based contextual analysis would capture.

The AI will monitor such transitions continuously, assigning a dynamic Threat Score to individual conversation threads, channels, and user sessions. The Threat Score will function as the primary input to the encryption adaptation engine across three operational tiers:

- **Tier 1 (Low Threat Score)**: Standard Tor-grade encryption will operate, and this is sufficient for journalists, researchers, and whistleblowers conducting legitimate anonymous communication.
- **Tier 2 (Elevated Threat Score)**: The system will escalate to hybrid post-quantum cryptographic protocols, adding quantum-resistant key

encapsulation alongside classical algorithms, and will impose enhanced authentication requirements. The NIST 2024 post-quantum cryptography standards will provide the cryptographic foundation for this adaptive architecture.

- **Tier 3 (High Threat Score)**: Full post-quantum cryptographic suites will be activated, maximising the complexity of encryption, while simultaneously flagging the session for LEA monitoring through the Threat-Hunter Bot pipeline discussed in the previous section.

Crucially, the escalation logic would protect rather than expose legitimate users. When a researcher's session is incorrectly elevated, the result would be a stronger encryption protecting their anonymity. Only when criminal intent is confirmed at the highest confidence threshold, would the Tier 3 pathway converge with law enforcement notification; and even then, human review would be mandatory for taking any action. Integration with Tor's onion-routing architecture, particularly the HybridOR protocol that is resistant to future quantum computing attacks, should be the subject of active cryptographic research.

The proposed adaptive encryption system would add an extra layer of complexity that would deter all but the most determined and technically skilled actors. The system would not seek to eliminate Dark Web's anonymity, but would invert the economic logic of criminal operations. As criminal activity intensifies, the operational environment would become more complex, less predictable, and progressively less hospitable.

### Anti-narcotics Enforcement:

The illicit trade in narcotics represents one of the most direct and consequential manifestations of Dark Web criminality within India's national security apparatus. The Union Home Minister, Shri Amit Shah, while chairing a conference on "*Drug Trafficking and National Security*" on 11 January 2025, explicitly identified the use of the Dark Web, cryptocurrency, online marketplace and drones as challenges to curb drug trafficking[17]. The Narcotics Control Bureau already has a Darknet Task Force, which coordinates with Financial Intelligence Unit, international agencies and cybersecurity professionals, resulting in successful

takedowns of drug trafficking syndicates such as the DNMs Team Kalki[18] in 2026, Ketamelon in 2025[19] and Zambada Cartel[20] in 2023. AI-based monitoring is required to maintain continuous situational awareness of international DNMs serving Indian buyers, and India-based DNMs.

DNM vendors construct layered anonymity through coded language. Products are listed by slang, abbreviated chemical notation, and regionally specific euphemisms, which are intelligible to experienced users, but opaque to conventional keyword-matching filters. For example, heroin can appear as "brown sugar", "smack", "horse", or "desi"; methamphetamine as "crystal", "glass" or "ice"; cocaine as "snow", "charlie" or "blow"; new psychoactive substances as alphanumeric codes "4-MMC" or "M-CAT". Pricing structures can encode transaction volume through quantity abbreviations and bulk discount schedules that signal organised distribution rather than individual use; while delivery instructions will convey dead-drop coordinates, trusted courier networks, and steganographic communication channels. These constitute operational intelligence of the highest value to anti-narcotics enforcement.

The challenge demands not keyword detection, but a semantic understanding of evolving criminal communication. Transformer-based NLP architecture can capture contextual dependencies and nuanced semantics that overcome deliberate language manipulation. If applied to narcotics surveillance, DarkBERT-class models can identify the contextual transition from general pharmaceutical discussion to vendor solicitation, complete with pricing schedules and delivery logistics, even when the transition employs substitution ciphers or newly emerged slang that defeats static keyword lists. AI can identify not just individual transactions but market-level shifts, for instance, new narcotics entering regional supply chains, novel delivery obfuscation methods, or the migration of established vendor networks from disrupted DNMs to successor platforms.

### Undercover Personas for Covert Infiltration of Criminal Networks:

AI can assist LEAs in constructing synthetic undercover personas capable of actively engaging with criminal networks over extended periods. LLMs,

that have been trained on Dark Web linguistic registers, could generate and maintain credible undercover profiles that respond authentically, accumulate transaction histories, and build reputations without experiencing the fatigue and psychological strain such covert activities could impose on human operatives. Unlike mortal law enforcement agents, AI personas can simultaneously sustain multiple identities across forums and markets, operate continuously across time zones, and maintain perfect recall of every prior interaction. As a persona accumulates social capital within the Dark Web's reputation economy, it gains access to deeper intelligence, such as supplier networks, distribution logistics, co-conspirators, and operational vulnerabilities.

For example, an AI vendor persona embedded within a drug supply network could map entire distribution chains; within arms trafficking forums, it could trace procurement channels; within terrorist financing networks, it could chart cryptocurrency flows connecting funders and operatives. Conversely, an AI narcotics buyer persona can identify suppliers, extract product quality and supply-chain intelligence, and capture delivery logistics, while avoiding the physical risk that human undercover purchasers incur. The evidence trail generated by transaction records, shipping address databases, communication logs, cryptocurrency wallet associations, would constitute case-ready material for prosecution under the NDPS Act.

Operation Bayonet in 2017 provides a landmark digital precedent in which the Dutch police seized covert control of Hansa, then Europe's largest drug DNM, and operated it for nearly a month, collecting vendor IP addresses and passing approximately 10000 international buyer delivery addresses to Europol[21]. Throughout the operation, investigators impersonated platform administrators and mediated disputes while extracting intelligence.

Entrapment, where individuals get induced to commit crimes they would not have committed independently, is a major legal concern. To address this, there needs to be top leadership endorsement and authorisation before AI deployment, clear documentation of AI decision-making, defined operational boundaries that prevent AI-initiated unlawful

transactions, and continuous human oversight[22]. The Hansa operation avoided this because police allowed the market to function exactly as criminals had designed it, observing and logging rather than inducing criminal behaviour.

## Conclusion:

AI represents a categorical improvement to existing law enforcement countermeasures in the Dark Web, which presents one of the most operationally complex environments in the digital age. The AI advantage is not a permanent feature and must be continuously validated through adversarial training regimes, specifically designed around known patterns of obfuscation, and regularly retrained as malicious AI capabilities evolve. The blackbox nature of LLMs makes it difficult for investigators and prosecutors to explain algorithmic findings in a court of law. The chain of custody for AI-derived intelligence has not been settled legally, and requires urgent cross-jurisdictional legislative attention. Leveraging AI to prevent Dark Web misuse is not a purely technical problem, but is a governance challenge that impacts privacy rights, democratic accountability, international law, and resets the ethical limits of state surveillance in digital spaces. A consequential challenge facing today's security policymakers, researchers, and legal scholars is how to strike the right balance between exploiting AI's extraordinary power and simultaneously preserving the civil liberties it might threaten.

## References:

1. *Europol (2026). The evolving threat landscape: How encryption, proxies and AI are expanding cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf*
2. *Chainalysis (2026, February 19). From Fentanyl to Fraud: On-Chain Activity Highlights Illicit Market Evolution. https://www.chainalysis.com/blog/crypto-drug-sales-darknet-markets-2026/*
3. *Internet Watch Foundation (2026). AI CSAM Report 2026. https://admin.iwf.org.uk/media/hl1nvdti/iwf-ai-csam-report-2026.pdf*
4. *Check Point Research (2026, May 26). AI Threat Landscape Digest March-April 2026. https://research.checkpoint.com/2026/ai-threat-landscape-digest-march-april-2026/*

5. *Cybersecurity Ventures (2025). Global Ransomware Damage Cost Predictions. https://cybersecurityventures.com/wp-content/uploads/2023/11/RansomwareCost.pdf*
6. *Khalil, M. (2026, May 13). How law enforcement tracks criminals on the Dark Web. https://deepstrike.io/blog/how-law-enforcement-tracks-criminals-on-the-dark-web*
7. *Alaidi, A. H. M., Al_airaji, R. M., Alrikabi, H.T., Aljazaery, I.A., & Abbood, S.H. (2022). Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques. International Journal of Interactive Mobile Technologies (iJIM), 16(10), pp. 122–139. https://doi.org/10.3991/ijim.v16i10.30209*
8. *Jegan, R., Rajavarman, V., & Geetha, S. (2024). AI-enhanced Dark Web Crawler for Cybersecurity Monitoring. Journal of Propulsion Technology. https://www.propulsiontechjournal.com/index.php/journal/article/view/6660/4348*
9. *Dalvi, A., Kadam, S., Vinayak, A., Salunke, S., & Rathod, D. (2021). SpyDark: Surface and Dark Web crawler. In Proceedings of ICSCCC 2021 (pp. 45-49). IEEE. https://doi.org/10.1109/ICSCCC51823.2021.9478115*
10. *Singh, S. K., Singh, A., Pandey, H. M., & Kumar, V. (2023). Towards safe cyber practices: Developing a proactive cyber-threat intelligence system for Dark Web forum content. Information, 14(6), 349. https://doi.org/10.3390/info14060349*
11. *Purohit, P., Purohit, A., & Soni, N. (2025). Drug site detection on Dark Web: Convergence of machine learning to address online drug trafficking in India. In K. K. Awasthi et al. (Eds.), The Green Revolution: Building Sustainable Solutions. Springer. https://doi.org/10.1007/978-3-031-93444-5_147*
12. *Harlev, M. A., Sun Yin, H., Langenheldt, K. C., Mukkamala, R., & Vatrapu, R. (2018). Breaking bad: De-anonymising entity types on the Bitcoin blockchain using supervised machine learning. Proceedings of the 51st Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2018.443*
13. *El-Kady, R. (2025). Leveraging artificial intelligence for enhanced detection and mitigation of illicit activities on the Dark Web. International Cybersecurity Law Review. https://doi.org/10.1365/s43439-025-00145-5*
14. *Hillier, C., & Karroubi, T. (2022). Turning the Hunted into the Hunter via Threat Hunting: Life Cycle, Ecosystem, Challenges and the Great Promise of AI. https://vsis-www.informatik.uni-hamburg.de/getDoc.php/publications/666/2204.11076.pdf*
15. *Darktrace (2024). What is SOAR? https://www.darktrace.com/cyber-ai-glossary/soar-security-orchestration-automation-and-response*
16. *Jin, S., Kim, S., Jang, J., Cho, H., Shin, J., Jin, S., & Kim, B. (2023). DarkBERT: A language model for the dark side of the internet. Proceedings of ACL 2023. https://doi.org/10.18653/v1/2023.acl-long.415*
17. *Press Information Bureau (2025). Union Home Minister and Minister of Cooperation, Shri Amit Shah, chairs a regional conference on 'Drug Trafficking and National Security in New Delhi.*

*https://www.pib.gov.in/PressReleasePage.aspx?PRID=2092097&reg=3&lang=1*

18. *Narcotics Control Bureau (2026, March 8). NCB Busts Pan-India Darknet Drug Network "Team Kalki". https://narcoticsindia.nic.in/pressrelease/08_03_2026_team_kalki.pdf*
19. *NCB (2025, July 1). NCB Busts Top Darknet Drug Vendor "Ketamelon" in Operation Melon. https://narcoticsindia.nic.in/pressrelease/01_07_25_hq_cochin_darknet.pdf*
20. *News On AIR (2023, August 1). Narcotics Control Bureau Busts Country's Biggest Dark-Net LSD Cartel. https://newsonair.gov.in/narcotics-control-bureau-busts-countrys-biggest-dark-net-lsd-cartel/*
21. *Temple-Raston, D., & Jarvis, W. (2023, September 13). The 'game-changing' attitude behind a very creative Dark Web takedown. The Record. https://therecord.media*
22. *Blanchard, A., & Taddeo, M. (2023). The ethics of artificial intelligence for intelligence analysis. Digital Society, 2(1), Article 36. https://doi.org/10.1007/s44206-023-00036-4*

## Author's Profile:

Sudipta Das is a 2012 batch IPS officer of Tripura cadre, currently serving as DIG Sashastra Seema Bal, Sector HQr Bongaigaon. Previously, he had served as Group Commander of NSG's elite counter-terrorism unit, 11 Special Rangers Group. During his NSG tenure, the officer led a Task Force for counter-terror operations during the Maha Kumbh Mela 2025 in Prayagraj, Uttar Pradesh. He also served in various capacities in Tripura Police as District Superintendent of Police, in Crime Branch and at Police HQ.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 94-112)

# A Study on Application-Based Mule Account Operations and Cryptocurrency Conversion in Cyber Enabled Financial Frauds

Shahnaz I, IPS*

***Abstract:***

*The rapid growth of digital banking, Unified Payments Interface (UPI) ecosystems, online gaming and gambling platforms, and cryptocurrency-based payment mechanisms has significantly transformed the landscape of Cyber-Enabled Financial (CEF) fraud. Organised cybercrime syndicates increasingly employ large-scale mule account networks, coordinated through mobile and web-based applications, to facilitate the laundering and movement of illicit proceeds. These operations rely on systematic fund layering across intermediary bank accounts and UPI IDs, using techniques such as burst transactions, temporary account activation, rapid multi-layer routing, and decentralised coordination mechanisms to obscure financial trails and evade detection.*

*This paper examines the operational architecture of application-based mule account ecosystems, including mule account categorisation, transaction-routing methodologies, commission management systems, and cryptocurrency conversion workflows. Particular emphasis is placed on the convergence between Cyber-Enabled Financial fraud and illegal gaming/gambling payment infrastructures, which act as significant leakage points for transferring illicit proceeds from the regulated banking system into unregulated cryptocurrency ecosystems. The study further*

*2021-Batch IPS Officer of the Tamil Nadu cadre

*analyses the role of APK and web-based applications in automating mule account management, enabling cryptocurrency conversion into assets such as Tether (USDT), and facilitating cross-border laundering through decentralised wallet applications. Additionally, the paper presents observations from APK and network traffic analysis of mule-management applications, discusses investigative challenges arising from offshore hosting infrastructure and fragmented transaction trails, and proposes preventive and investigative measures to strengthen financial monitoring, cryptocurrency tracing, inter-agency cooperation, and regulatory oversight against organised Cyber-Enabled Financial crime.*

***Keywords:***
*Cyber Fraud, Mule Accounts, UPI Fraud, Cryptocurrency Laundering, USDT, TronLink, Financial Cybercrime, Burst Transactions, Layering, Digital Payments, Blockchain Investigation, Organised Fraud Networks.*

## 1. Introduction:

Cybercrime has emerged as one of the most significant threats to financial systems worldwide, driven by rapid digitisation and the proliferation of online financial services. Among various forms of cybercrime, Cyber-Enabled Financial (CEF) fraud has become particularly prevalent, exploiting technological advancements to orchestrate complex, large-scale operations targeting individuals, businesses, and financial institutions.

CEF frauds now operate through organised networks using thousands of mule accounts. Deliberate fund layering across banking and UPI platforms fragments and hides the money trail. This multi-layered routing obscures the origin and movement of stolen funds, making detection and recovery extremely difficult for investigators and financial institutions.

Mobile applications enable decentralised layering, sieving, and asset obfuscation, making mule account operations more sophisticated. These apps and web-based systems coordinate large-scale credential sharing, account activation, fund routing, and conversion to cryptocurrencies. This increases the scale, speed, and complexity of laundering, especially as crypto assets like USDT make tracing illicit funds harder.

## 2. Mule Accounts in Cyber Financial Crimes:

### 2.1 Definition of Mule Accounts:

A mule account is a bank or UPI-linked account used as an intermediary to receive, transfer, or withdraw proceeds of cyber-enabled financial frauds. These accounts may be operated knowingly or unknowingly by individuals deceived into sharing credentials or offered commission to rent their accounts. Mule accounts are central to obscuring the money trail between victims and cyber scam fraudsters.

### 2.2 Organised Mule Networks:

The mule network syndicates maintain structured mule account networks consisting of:

- Account suppliers,
- Mule account aggregators and agents,
- ATM withdrawal operators,
- Cryptocurrency exchangers,
- Coordinators operating communication applications.

These networks are designed to rapidly disperse funds across multiple accounts, thereby concealing the financial trail.

### 2.3 Categories of Mule Accounts:

Mule accounts are categorised into several types based on their use in the layered obfuscation of the proceeds of Cyber-Enabled Financial (CEF)Fraud. They can be categorised into:

a. First Layer Mule Accounts.
b. Middle Layer.
    i. Burst Transaction Mule Accounts.
    ii.Onward Transaction Mule Accounts.
c. End Point Mule Accounts.

**a. First Layer Mule Accounts**: These accounts are directly involved in cyber fraud, receiving funds transferred by victims. They typically have higher transaction limits and are most often current accounts.

**b. Middle Layer Mule Accounts**: These accounts further obfuscate the money trail by transferring funds through layers and distributing them down the layering hierarchy.

**i. Burst Transaction Mule Accounts**: These accounts are primarily observed in cases involving gaming or gambling applications. They serve as payout accounts for users of gaming or gambling apps. Comprehensive applications for managing fund movement, messaging, and coordinating pay-in and pay-out accounts are observed in such mule account operations. This is one of the leakage points from the banking system to Cryptocurrency and is discussed in detail later in this paper.

**ii. Onward Transaction Mule Accounts**: These accounts serve to transfer funds to additional layers, further complicating the investigation and tracing of the financial flows.

**c. End Point Mule Accounts**: Typically used for the conversion of funds into cryptocurrency or for cash withdrawal via ATM or cheque. These accounts represent the exit points before the illicit proceeds leave the traditional banking system.

**2.4 Management of Mule Accounts in Cyber-Enabled Financial (CEF)Fraud:**

Based on the type of bank account—for instance, savings or current account—the mule account is selected to serve as either a first-layer or an endpoint mule account. Mobile or web-based applications are used in the leakage-point management during the mule account obfuscation process.

### 2.4.1 Endpoint Mule Accounts Transaction:

Endpoint mule accounts do not require high transaction limits. They are primarily used to withdraw money from ATMs/cheques for cryptocurrency exchanges. Typically, a large number of endpoint mule accounts are required because CEF fraud originating from first-layer Mule accounts is split into smaller denominations, each convenient for withdrawal, across numerous endpoint mule accounts. As a result, managing these numerous endpoint mule accounts manually becomes cumbersome and time-consuming. Therefore, it is noted that international

cyber crime syndicates automate and manage such operations through mobile applications.

### 2.4.2 Burst Transaction:

A notable pattern observed in the middle-layer mule account operations is the use of burst transactions. The recipients of such transactions are general public users of illegal gaming and gambling applications or websites like 1XBet, Rabet, etc.

In this methodology:

- Large numbers of transactions to the tune of thousands are executed within a few minutes.
- Funds are fragmented into multiple smaller transfers to multiple UPI IDs or bank accounts almost simultaneously.

This clearly points out the nexus of illegal gaming or gambling applications and the International cyber scam compounds. Based on the interrogation reports of various cyber slavery repatriates from Southeast Asian countries, it is to be noted that many illegal Gaming and Gambling companies operate in the same Casinos as the cyber scam companies. Such quid pro quo arrangements between illegal operations are facilitated by web and mobile-based applications. This pattern creates substantial complexity in financial tracing and delays investigation.

### 2.4.3 Enabling Mule Accounts:

The crypto conversion application allows agents to activate or deactivate mule accounts as needed, providing direct control over which accounts are operational at any given time. This capability enables fraud networks to swiftly adjust account usage, complicating the tracking and recovery of illicit funds by investigators.

## 2.5 Mule Accounts in Leaking CEF Fraud Proceeds from Banking System to Crypto ecosystem:

Although the illicit proceeds are initially routed through the formal banking system, they are ultimately removed from it and converted into unregulated digital assets. Investigations reveal that such leaks often occur

through cheque withdrawals, ATM withdrawals, and gaming or gambling application payout accounts, as mentioned above. Mule account aggregators associated with endpoint mule account handlers increasingly use mobile and web-based applications to convert the proceeds of CEF fraud into cryptocurrency, after taking a commission. The applications are hosted outside India and are unregulated. This creates a vacuum in tracing the proceeds of crime and breaks the continuity of tracing them to higher-level coordinators or kingpins. Thus, the role and functionality of such applications need to be analyzed to conduct a comprehensive investigation into CEF fraud and trace international kingpins.

## 3. Application-Based Mule Account Ecosystem:

Given the wide array of mule accounts in use for a single CEF Fraud, there is increasing automation in the management of mule account operations through mobile-based and web-based applications. Such sophistication has facilitated almost real-time layering and filtering of proceeds of CEF Fraud. This can be seen as a major reason for the defeat of the golden hours of reporting in CEF Fraud. These applications are used by the endpoint mule account aggregator and illegal gaming/gambling mule account aggregators.

### 3.1 Functional Components of Application-Based Mule Account Ecosystem:

The ecosystem supporting CEF fraud operations is designed to streamline and automate several critical processes. Typically, these applications are designed to support various stages of the illicit operation, including:

- **Mule account management:**

  It enables the systematic enrolment of mule account credentials for fraudulent activities and facilitates real-time tracking of inflows and outflows of defrauded funds. Additionally, the application enables hassle-free activation and deactivation of mule accounts to support day-to-day CEF fraud operations. This infrastructure also ensures the efficient routing and rapid transfer of fraudulent proceeds across

multiple intermediary accounts, thereby complicating efforts to trace and recover illicit assets.

- **Commission management:**

Applications used in these networks enable real-time tracking and distribution of commissions to mule account aggregators, based on the volume and value of transactions processed. The system also calculates fines for non-compliance with operational requirements or failure to meet assigned targets. A comprehensive tally sheet is maintained, recording the total amount from CEF fraud-related operations and providing a detailed breakdown of commissions per account. This structured approach ensures efficient financial oversight and incentivizes continued participation by aggregators.

- **Banking system to Cryptocurrency conversion:**

Mule account aggregators are typically assigned unhosted cryptocurrency wallets, which allow them to manage digital assets outside the regulatory oversight of financial institutions. The application is used to link the unregulated crypto wallet to a mule account aggregator user account, thereby facilitating the crucial leakage point. These wallets enable the receipt, storage, and transfer of cryptocurrencies. Additionally, the application offers features for real-time display and balance checking, enabling aggregators to efficiently monitor their cryptocurrency holdings and transactions.

### 3.2 Procurement of APK file:

Although these applications are readily available on communication platforms such as Telegram, one cannot create a user account without a referral from the APK supplier. User accounts can be created only by local suppliers who have direct contact with international cyber scam compound operators.

Before account creation, local suppliers instruct users on several operational rules. Operators and handlers must meet daily transaction targets or incur fines. Preference is given to banks that allow large-value transactions with minimal scrutiny. Users are required to maintain multiple linked bank accounts and UPI IDs to bypass transaction limits and

restrictions, and are encouraged to regularly add or replace mule accounts to evade detection and maintain uninterrupted fund transfers.

Mule account aggregators are charged by the local APK supplier for each user account created. It is to be noted that, based on the utility and daily limit, charges range from 1 Lakh to 10 Lakh. APK files used for illegal gaming or gambling operations are charged at a higher rate than those used for CEF fraud-related operations. This is because the mule accounts involved in CEF frauds are frozen under the robust mechanism for cybercrime reporting at cybercrime.gov.in and the 1930 helpline. In the absence of such reporting and freezing mechanism for the illegal gaming/gambling operations, the mule account used run for longer period without glitch except when there is a burst transaction related to CEF fraud as mentioned earlier.

### 3.3 Safety and Obscuring Measures in the Applications:

To register on applications like P2P (Paytoplay), users must submit a video stating their name and purpose, and hold their PAN card, to the local APK supplier for verification by international cyber scam operators. Once registration is accepted, credentials for login are provided. Login requires two-factor authentication, usually via time-based OTPs from authenticator apps set up through QR code. If access to the authenticator app is lost, the agent must contact the local supplier to regain entry. Some apps also use messaging platforms or chatbots to send OTPs for authentication and transaction approval. This will be explained further under the heading "The Nexus of Applications for Illegal Gaming/Gambling." As a safeguard mechanism, if suspicious activity is detected, the app will remotely delete stored data and suspend the user account.

### 3.5 Nexus of Application for Gaming or Gambling operations:

Multiple mobile and web-based applications operate in tandem, particularly in the management of pay-in and pay-out activities associated with illegal gaming and gambling operations. Burst transaction patterns frequently reveal a convergence of cyber-enabled financial (CEF) fraud proceeds with funds directed to illegal gaming and gambling users.

Applications managing these transactions often feature compartmentalised functionalities with significant interdependencies, enabling coordinated and efficient operation. Additionally, offshore gaming and betting platforms facilitate cross-border fund transfers and the settlement of illicit proceeds, further complicating regulatory oversight and enforcement.


Fig. 3.1. Chatbot in Reddy application that guides the user – Trust-based verification.

## 4. Operational Workflow of Mule Account Applications (APK and Weblink-based):

These laundering networks use a commission-based model, assigning roles to individuals who move illicit funds through decentralised mule accounts across multiple banks to hide the money trail and avoid detection. They use APK-based applications (e.g., Cocopay, HK Pay, Done Pay) to manage inter-account transfers, as well as cryptocurrency exchange applications (e.g., P2P Expert) to convert fraudulent proceeds into digital assets.

### 4.1 Addition and Activation of Mule Accounts:

In the application, the mule agents can add multiple bank accounts, configure IFSC codes, integrate multiple UPI IDs, and enable or disable accounts dynamically.

The operation includes adding multiple mule bank accounts at once, enabling the accounts, and carrying out burst transactions involving rapid fund transfers across multiple layers. Such layered routing mechanisms are intentionally designed to confuse Investigating Officers (IOs) and conceal the money trail.

Approval for activating UPI IDs or bank accounts is generally controlled centrally through coordinators.

### 4.2 Transaction Routing Mechanism:

Once the accounts are activated, fraud proceeds are credited into first-layer mule accounts. The mule agents receive routing instructions through coordination applications such as Telegram, Reddy Application. Funds are rapidly transferred to subsequent mule accounts via UPI or banking channels. The process is repeated across several layers within short durations.

The mule agent may temporarily disable the bank account or UPI ID on the application once the maximum transaction limit is reached.

#### 4.3.1 Transaction Pattern in Organised Mule Account Operations:

Analysis of transaction records reveals a repetitive pattern: multiple UPI credits from accounts over a short period, rapid accumulation of balances (₹40,000–₹50,000) and withdrawals up to ATM limits (about ₹40,000 per day). Rapid multiple outgoing transactions to split the received amount to multiple accounts. Withdrawn cash is handed to cryptocurrency exchangers, and this cycle is repeated daily using the same or new mule accounts.

| S No. | Acknowledgement No. | Account No./ (Wallet /PG/PA) Id | Bank/FIs | Layer | Account No | Ifsc Code | Transaction Date | Transaction Amount | Disputed Amount | Action Taken By bank |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 22912250106****** | 407311422*** | Axis Bank | 1 | 92402002069**** | UTIB0002771 | 13/11/2025 02:31:26 PM | 3,50,000.00 | 3,50,000.00 | State Bank of India |
| 2 | 22912250106****** | 92402002069**** | City Union Bank | 2 | 50010101373**** | CIUB0000175 | 13/11/2025 12:00:00 AM | 29,310.00 | 29,310.00 | Axis Bank |
| 3 | 22912250106****** | 92402002069**** | State Bank of India | 2 | 40388354**** | SBIN0012988 | 13/11/2025 12:00:00 AM | 29,250.00 | 29,250.00 | Axis Bank |
| 4 | 22912250106****** | 92402002069**** | Tamilnad Mercantile Bank Ltd. | 2 | 521005031**** | TMBL0000052 | 13/11/2025 12:00:00 AM | 28,250.00 | 28,250.00 | Axis Bank |
| 5 | 22912250106****** | 92402002069**** | Indian Overseas Bank | 2 | 138010000**** | IOBA0000138 | 13/11/2025 12:00:00 AM | 28,000.00 | 28,000.00 | Axis Bank |
| 6 | 22912250106****** | 92402002069**** | TAMIL NADU STATE APEX COOP BANK | 2 | 719898**** | TNSC0011000 | 13/11/2025 12:00:00 AM | 27,830.00 | 27,830.00 | Axis Bank |
| 7 | 22912250106****** | 92402002069**** | State Bank of India | 2 | 4427716**** | SBIN0011064 | 13/11/2025 12:00:00 AM | 27,650.00 | 27,650.00 | Axis Bank |
| 8 | 22912250106****** | 92402002069**** | Indian Overseas Bank | 2 | 138010000**** | IOBA0000138 | 13/11/2025 12:00:00 AM | 27,650.00 | 27,650.00 | Axis Bank |
| 9 | 22912250106****** | 92402002069**** | Tamil Nadu Grama Bank | 2 | 1005883**** | IDIB0PLB001 | 13/11/2025 12:00:00 AM | 27,510.00 | 27,510.00 | Axis Bank |
| 10 | 22912250106****** | 92402002069**** | State Bank of India | 2 | 3800047**** | SBIN0002268 | 13/11/2025 12:00:00 AM | 27,500.00 | 27,500.00 | Axis Bank |
| 11 | 22912250106****** | 92402002069**** | Bank of Baroda | 2 | 5169010**** | BARB0RAMANA | 13/11/2025 12:00:00 AM | 27,260.00 | 27,260.00 | Axis Bank |
| 12 | 22912250106****** | 92402002069**** | Tamilnad Mercantile Bank Ltd. | 2 | 3331000506**** | TMBL0000333 | 13/11/2025 12:00:00 AM | 27,250.00 | 27,250.00 | Axis Bank |
| 13 | 22912250106****** | 92402002069**** | City Union Bank | 2 | 2760010021**** | CIUB0000276 | 13/11/2025 12:00:00 AM | 27,160.00 | 27,160.00 | Axis Bank |
| 14 | 22912250106****** | 92402002069**** | TAMIL NADU STATE APEX COOP BANK | 2 | 71985**** | TNSC0011000 | 13/11/2025 12:00:00 AM | 27,000.00 | 15,380.00 | Axis Bank |

Fig 4.1 shows the multiple outgoing transactions to split the received amount to multiple accounts.

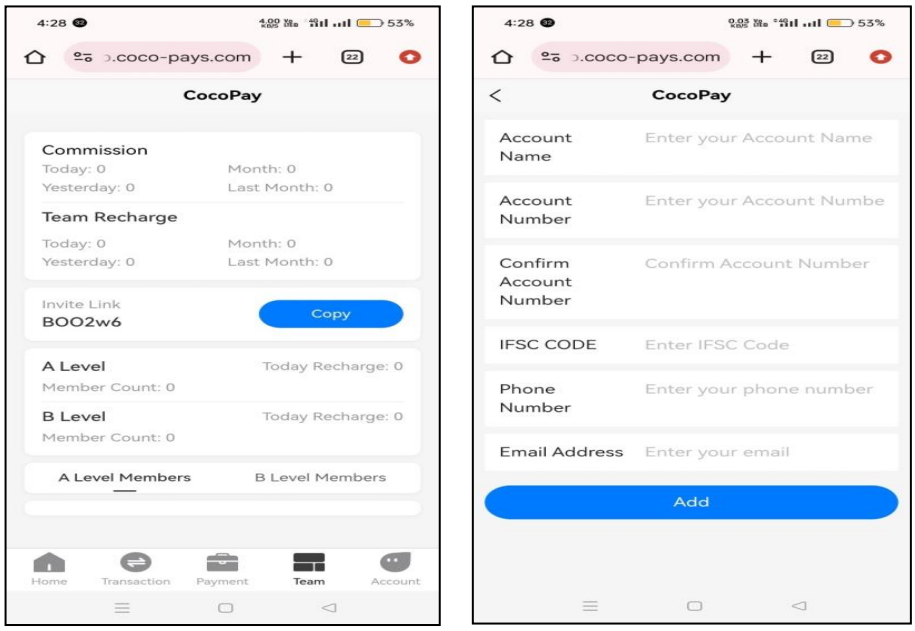



Fig. 4.2. Screenshot from an APK-based application where bank accounts are added for fund management.

## 5. Comparison of Cyber-Enabled Financial (CEF) Fraud and Illegal Gaming / Gambling APK:

APK files are widely used in the Money Laundering Ecosystem in:

- Cyber-Enabled Financial (CEF)Fraud
- Illegal Gaming / Gambling

The detailed comparison is listed below:

| **Aspect** | **Cyber-Enabled Financial (CEF)Fraud APK Ecosystem** | **Illegal Gaming / Gambling APK Ecosystem** |
|---|---|---|
| Nature of Transactions | Fraud proceeds originating from cyber frauds such as investment scams, impersonation scams, phishing, task frauds, etc. | Transactions linked with illegal online gaming, gambling, or gaming-linked payment ecosystems. |
| Commission Structure | Commission for routing transactions of ₹1 lakh is reportedly around 5.5%. | Commission for routing transactions of ₹1 lakh is comparatively higher, generally ranging between 8% and 9%. |
| Operational Risk | Higher risk of immediate detection, account freeze, or hold by banks and financial institutions. | Comparatively lower immediate detection and delayed freezing/holding of mule accounts. |
| APK/Application Cost | Operational APK costs are comparatively lower. | APK platforms and operational infrastructure generally involve higher costs. |
| Sustainability of Mule Accounts | Mule accounts are more frequently flagged or frozen after suspicious transactions. | Mule accounts reportedly remain active for longer durations, enabling sustained routing operations. |
| Transaction Monitoring by Banks | Suspicious transaction patterns are more rapidly identified due to direct linkage with fraud complaints. | Only burst transactions involving Cyber Crime is reported and monitored. |
| Fund Routing Pattern | Rapid payment from Array of CEF fraud | Continuous layered routing and aggregation mechanisms are more |

| | | |
|---|---|---|
| | funds. Payout through the App in the crypto transaction. Thus the application is creating an Air Gap between Payin and Payout accounts. | commonly observed. |
| Investigative Complexity | Difficulty in financial tracing due to Air Gap in transaction flow due to Crypto Conversion. | Increased complexity in tracing due to delayed account restrictions and integration with gaming payment ecosystems. |

Fig 5.1 – Comparison of Cyber-Enabled Financial Fraud and Illegal Gaming / Gambling Ecosystem.

## 6. The Operation of P2P Expert Application:

The application requires users to authenticate by entering their credentials and completing a two-factor authentication process, as illustrated in Fig. 6.a to 6.d. Upon successful login, the dashboard displays the wallet balance and the list of mule bank accounts added by the user (Fig. 6.e). The interface, as depicted in Fig. 6.f and 6.g, enables agents to add bank accounts designated for mule account operations. Fig. 6.h presents the cryptocurrency wallet address to which agents transfer USDT to recharge the wallet. Fig. 6.i illustrates the interface for the sale of USDT, facilitating the conversion of available USDT balance to INR, which can then be credited to the linked bank accounts.

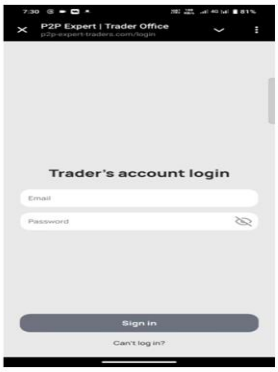



Fig (6.a)

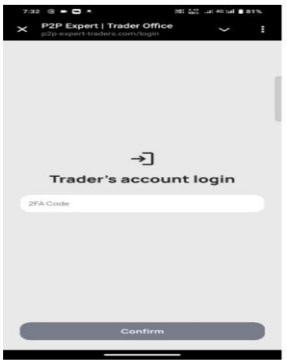



Fig (6.b)

Fig (6.c)

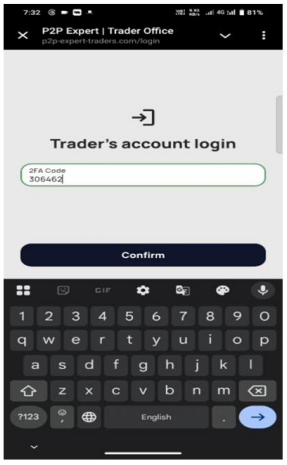



Fig (6.d)

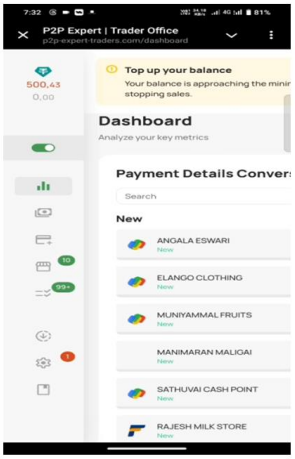



Fig (6.e)

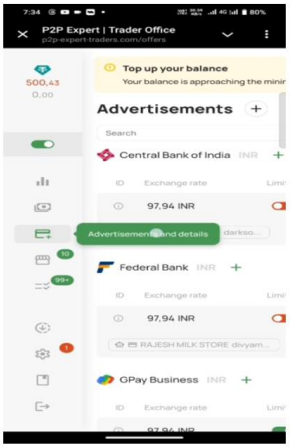



Fig (6.f)

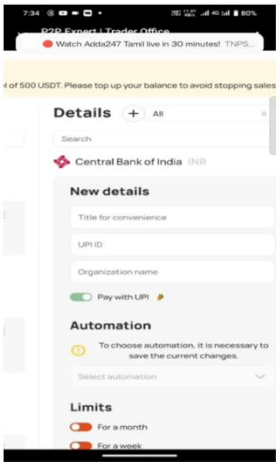



Fig (6.g)

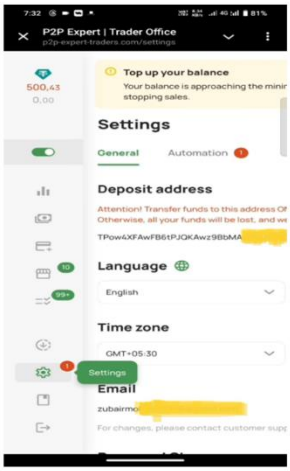



Fig (6.h)

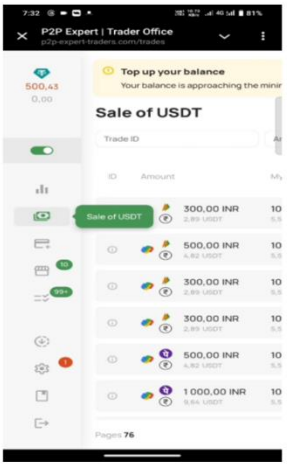
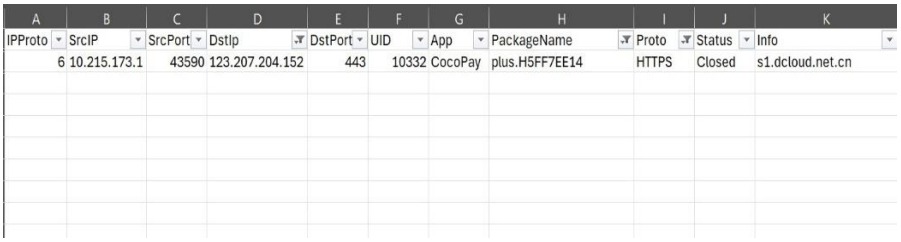



Fig (6.i)

## 7. APK Analysis of CocoPay Application:

The APK file of an application named CocoPay was collected and analysed. The APK file was installed and executed in a controlled environment, wherein all network traffic generated by the application was captured, recorded, and examined. Based on traffic analysis of the CocoPay application, it was observed that the application was communicating with infrastructure hosted by a China-based provider.



| A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|
| IPProto | SrcIP | SrcPort | DstIp | DstPort | UID | App | PackageName | Proto | Status | Info |
| 6 | 10.215.173.1 | 43590 | 123.207.204.152 | 443 | 10332 | CocoPay | plus.H5FF7EE14 | HTTPS | Closed | s1.dcloud.net.cn |

Fig 7.1 Packet capture showing the Network traffic communication to the Destination IP.

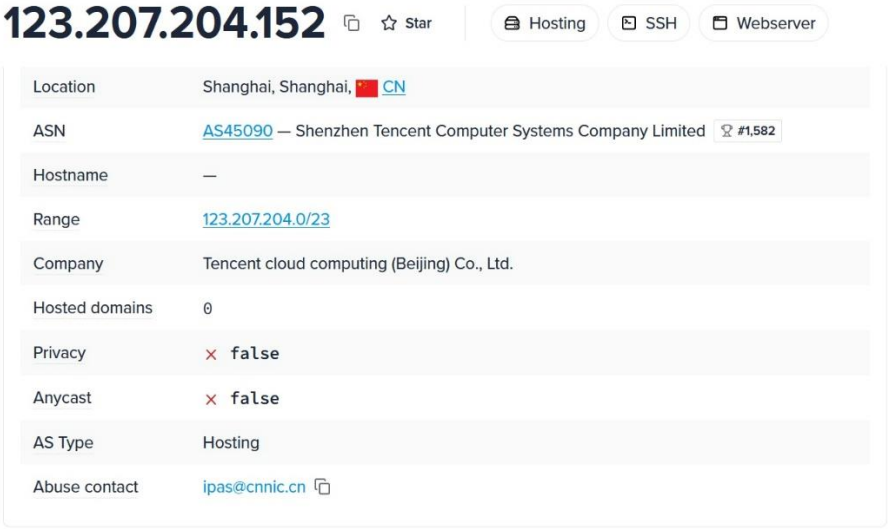



Fig 7.2 IP lookup of the Capture network traffic.

Due to the data-centre nature of the identified IP infrastructure, the associated network monitoring revealed communication with multiple destination IP addresses, indicating the use of dynamically allocated or distributed hosting services.

## 8. Cryptocurrency Conversion and USDT Laundering:

### 8.1 Use of Cryptocurrency in Laundering:

Cybercrime syndicates use cryptocurrencies to launder and transfer proceeds from financial frauds. Cryptocurrencies enable cross-border asset transfers without banks, conceal ownership with pseudonymous wallets, allow rapid fund movement, complicate tracing with layered transactions, evade traditional monitoring, and store illicit gains in decentralised systems.

Cryptocurrency-based laundering mechanisms are often integrated with peer-to-peer (P2P) trading systems, decentralised wallet applications, and third-party exchange accounts, enabling fraudsters to transfer assets rapidly across jurisdictions while minimising direct linkage to verified identities.
One of the commonly utilised digital assets in such operations is Tether (USDT), a stablecoin generally pegged to the US Dollar.

Based on the analysis of the mule account operations, it is found that USDT is commonly favored by cybercriminal networks due to its stability, high liquidity, broad exchange support, ease of peer-to-peer transfer, compatibility with decentralized wallets, and ability to facilitate cross-border transactions. These characteristics allow for rapid conversion and movement of illicit funds without significant value fluctuation or regulatory oversight. As a result, fraudulent proceeds are often aggregated and converted into USDT through various exchanges or facilitators, then dispersed across multiple wallets to further obscure the transaction trail.

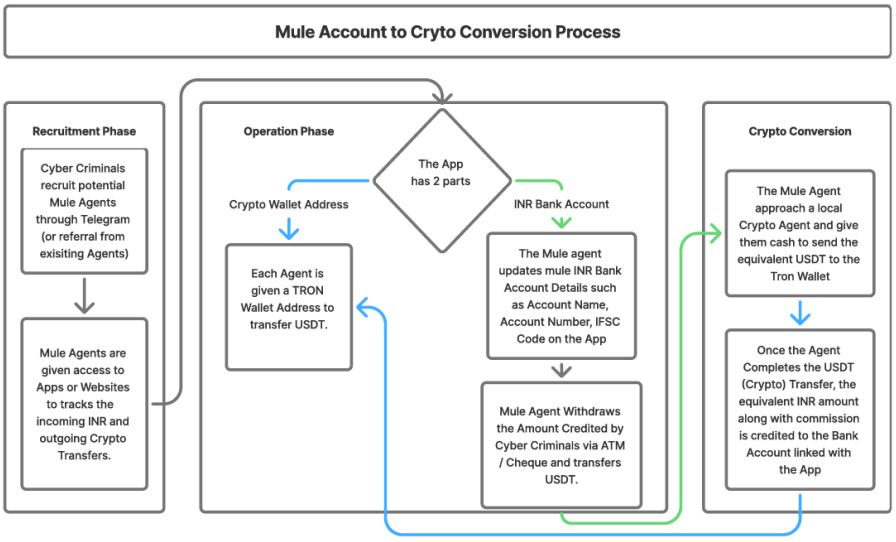



Fig. 8.1. Entire workflow of the fund layering and crypto conversion

## 8.2 Use of Decentralised Wallet Applications:

USDT transactions often use decentralised wallets like TronLink, which are popular because they do not require KYC verification. These wallets enable users to create multiple addresses, rapidly transfer USDT across borders, and layer transactions to reduce links to real identities. The lack of KYC checks significantly increases the difficulty of tracing transactions and attributing wallet ownership to specific individuals.

## 9. Challenges Faced by Investigating Agencies:

Cyber-Enabled Financial frauds increasingly exploit digital banking, UPI platforms, and cryptocurrencies through complex, organised networks of mule accounts managed via dedicated applications. These operations involve the rapid movement and layering of illicit funds across numerous bank and UPI accounts, obfuscating money trails and complicating detection. Mobile and web-based applications automate the enrolment, activation, and management of mule accounts, facilitate commission distribution, and enable seamless conversion of stolen funds into cryptocurrencies like USDT. These applications are hosted in non-cooperative jurisdictions, thus making it cumbersome to investigate the

key controller in this operation. The transfer of funds to unregulated wallets and the use of illegal web-based applications for cryptocurrency conversion create an air gap in the transaction flow, disrupting the fund trail and making it significantly more difficult to trace the movement of funds. Such methods obscure transaction origins, facilitate layering of transactions across multiple wallets or platforms, and significantly reduce the ability of investigators to identify the ultimate beneficiaries or determine the original source and destination of the assets. The convergence of cyber-enabled frauds with illegal gaming and gambling operations has led to the freezing of multiple accounts, resulting in significant strain on human and investigative resources. The account holders of the various layers of mule accounts are geographically far away and typically from various states, thus hindering the on-field operations.

## 10. Preventive and Investigative Measures:

Mitigating these threats requires:

- Enhancing KYC verification, suspicious transaction monitoring, and analysis of abnormal UPI activities.
- Strict regulation and banning P2P-based cryptocurrency transactions, along with stronger regulatory oversight of cryptocurrency transactions.
- Enhanced coordination and cooperation with cryptocurrency exchanges, blockchain analytics providers, and international agencies for seamless and timely sharing of data.
- Monitoring the usage of illegal mule agent applications at the network level and blacklisting associated IP addresses to prevent illegal fund flow.
- Conducting public awareness programmes on the risks and legal consequences of mule account operations and cryptocurrency-linked frauds.

## 11. Conclusion:

Application-based mule account operations represent a sophisticated evolution in cyber-enabled financial crimes. Organised fraud syndicates

increasingly employ dedicated applications, automated coordination systems, layered transaction-routing mechanisms, burst-transaction methodologies, decentralised wallet applications, and cryptocurrency conversion processes to launder fraudulent proceeds while concealing the money trail.

The simultaneous activation of multiple mule bank accounts, rapid routing of funds through layered UPI transactions, and conversion into cryptocurrencies such as Tether (USDT) through decentralised wallet applications like TronLink significantly complicate investigation and recovery efforts.

Addressing these emerging threats requires coordinated efforts among law enforcement agencies, financial institutions, cybersecurity experts, cryptocurrency monitoring entities, and regulatory authorities to strengthen detection, tracing, prevention, and enforcement mechanisms.

**Author's Profile:**

Shahnaz I, IPS

Shahnaz Ilyas is a 2021-batch IPS officer of the Tamil Nadu cadre with a background in Electronics and Communication Engineering and prior experience in the Information Technology industry. During her service, she has served as Assistant Superintendent of Police, Orathanadu Sub-Division in Thanjavur District, and Superintendent of Police in the Cyber Crime Wing, where she headed the State Cyber Crime Investigation Centre and the State Cyber Command Centre.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 113-127)

# The Interoperable Criminal Justice System (ICJS): Revolutionising India's Justice Delivery

R. Arulmozhiselvi*

***Abstract:***

*The criminal justice system in India is undergoing a structural digital transition. While earlier technology initiatives improved individual institutions such as courts, police stations and prisons, the Interoperable Criminal Justice System (ICJS) seeks to go a step further by connecting the principal pillars of criminal justice into a shared information architecture. ICJS enables secure, authorised and near real-time exchange of information among police, courts, prisons, prosecution and forensic laboratories. Its central promise is the principle of "one data, one entry", under which information entered once by the competent agency can travel across connected systems without repeated manual entry. This paper explains the concept, architecture, implementation status, impact, challenges and future roadmap of ICJS, and situates it within the broader movement towards a more efficient, transparent, accountable and citizen-centric justice delivery system.*

***Keywords:***

*Interoperable Criminal Justice System, ICJS, e-Courts, CCTNS, e-Prisons, e-Prosecution, e-Forensics, Digital Justice.*

* *District Judge (Tamil Nadu cadre, 2003 Batch); formerly on deputation as OSD (Registrar), Training Cell and Member (Human Resources), eCommittee, Supreme Court of India*

## 1. Introduction:

India's justice institutions have, over the last two decades, moved steadily from paper-based functioning to digital processes. This transition has not been confined to courts alone. The e-Courts Mission Mode Project strengthened the digital functioning of courts; the Crime and Criminal Tracking Network and Systems (CCTNS) digitised police-station records; and the e-Prisons initiative created a digital framework for prison administration [1], [2], [3]. These initiatives form the foundational layer on which a larger and more integrated criminal justice ecosystem is being built.

The purpose of this digital shift is not merely administrative convenience. Its broader objective is to improve the quality and speed of justice delivery, reduce avoidable procedural delay, enhance transparency and accountability, and make justice services more accessible and cost-effective for citizens [1], [4], [6]. Criminal cases, however, require the coordinated functioning of several institutions. A police investigation, a remand order, a forensic report, a charge-sheet, a prosecution decision, a bail order or a release order cannot be treated as isolated events. Each depends on timely and accurate information flowing from one institution to another.

It is in this context that the Interoperable Criminal Justice System (ICJS) assumes significance. ICJS is a national platform conceptualised and implemented by the Ministry of Home Affairs to enable seamless data exchange among the five principal pillars of the criminal justice system: police, courts, prisons, prosecution and forensic science laboratories [4], [5]. It attempts to transform fragmented digitisation into institutional interoperability.

## 2. What is the Interoperable Criminal Justice System (ICJS) ?

ICJS may be understood as a digital ecosystem that allows authorised stakeholders in the criminal justice system to share, receive and act upon relevant case information through connected databases and applications. Its function is to bridge the communication gaps that traditionally existed between police stations, courts, prisons, forensic laboratories and

prosecution departments. In the earlier paper-based environment, these institutions often functioned in silos. Documents had to be physically transmitted, records were repeatedly entered by different departments, and delay in one institution affected the progress of the entire case.

The system therefore serves three connected purposes. First, it reduces duplication of data entry. Secondly, it enables faster exchange of verified information. Thirdly, it creates a common digital view of the criminal case for authorised agencies. For example, when an FIR is registered in the police system, the relevant information can be digitally made available to the court system. When a court remands an accused to judicial custody or passes a bail or release order, the concerned prison can receive the information digitally instead of waiting for manual transmission of papers.

The defining principle of ICJS is "one data, one entry". This principle means that a data point should be entered only once by the agency that creates or verifies it, after which it should become available to other connected systems according to legal and administrative permissions. The principle reduces clerical repetition, minimises human error, strengthens data integrity and accelerates criminal case movement across institutions.

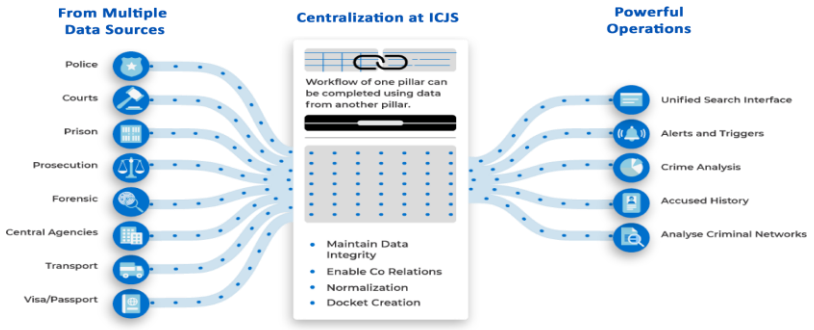



*Figure 1: ICJS as a centralised interoperability platform connecting multiple data sources and justice-sector operations.*

## 3. Digital Interventions Across the Criminal Case Journey:

Digital transformation is visible at almost every stage of the criminal case journey. A person may seek legal assistance through online legal aid portals; a case may enter the formal system through digital filing or digital

police records; pre-trial proceedings may be supported by video conferencing and electronic transmission of orders; and judgments, release orders and case-status information may be made available through connected platforms. ICJS does not replace all these tools. Rather, it gives them a common integration framework wherever criminal justice information must travel between institutions.

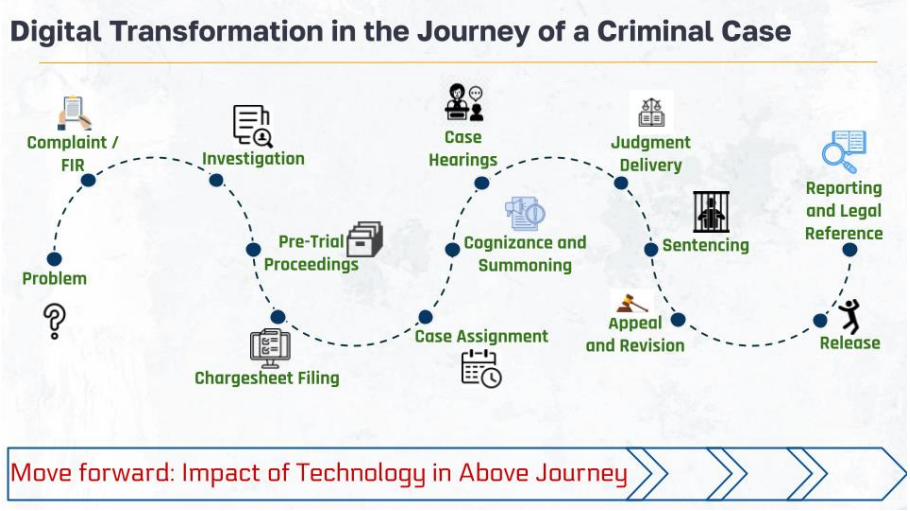



*Figure 2: Digital transformation in the journey of a criminal case.*

| ***Stage of Case*** | ***Digital Intervention / Technology*** | ***Key Features / Benefits*** |
|---|---|---|
| ***Problem / Dispute Arises*** | *Online Legal Aid Portals [4], [6]* | *Access to legal information and assistance through NALSA, SLSA and SCLSC* |
| ***FIR / Charge Filing*** | • *e-Filing (eFiling 3.0) [1]*<br>• *eSewa Kendras [1]* | • *Digital submission of documents*<br>• *Assistance for users*<br>• *Bilingual templates*<br>• *Online vakalat*<br>• *E-signing*<br>• *Oath recording* |
| ***Pre-Trial Proceedings/ Investigation*** | • *Virtual Hearings (VC) [7]*<br>• *e-Filing* | • *Remote bail and remand hearings*<br>• *Online bail applications* |

| ***Stage of Case*** | ***Digital Intervention / Technology*** | ***Key Features / Benefits*** |
|---|---|---|
| | • *Court calendar integration*<br>• *FASTER 2.0* | • *Automated scheduling*<br>• *Secure transmission of bail and release orders* |
| ***Charge-sheet Filing*** | *ICJS Portal* | • *Online submission of charge-sheets*<br>• *Mandatory digital acknowledgement through CNR numbers* |
| ***e-Payments*** | *Online Payment Portal* | *Digital payment of court fees, fines and penalties* |
| ***Case Assignment*** | *Case Information System (CIS) [1]* | *Assists in assigning cases based on availability and workload* |
| ***Hearing Scheduling*** | • *Online appearance through VC*<br>• *Online appearance-slip filing* | *Remote appearances and improved scheduling discipline* |
| ***Issuing Summons / Notices*** | *NSTEP (National Service and Tracking of Electronic Processes)* | • *Real-time tracking of summons and notices*<br>• *Electronic service through SMS and email* |
| ***Case Hearings [6]*** | • *Video conferencing*<br>• *Live streaming*<br>•*Real-time voice transcription*<br>• *SUPACE* | • *Remote hearings*<br>• *Public viewing*<br>• *AI-driven transcription*<br>• *AI-enabled legal research* |
| ***Judgment Delivery*** | • *AI in judgment summarisation [6]*<br>• *FASTER [7]*<br>• *Virtual Courts* | • *AI-generated summaries and digital transmission of judgments*<br>• *Online adjudication of petty offences* |
| ***Sentencing*** | • *e-Prisons Portal*<br>• *Digital warrants* | • *Tracks prisoner status*<br>• *Manages sentences*<br>• *Supports faster execution of sentences* |
| ***Research and*** | *National Judicial Data* | • *Tracks case disposals* |

| *Stage of Case* | *Digital Intervention / Technology* | *Key Features / Benefits* |
|---|---|---|
| ***Development*** | *Grid (NJDG) [12]* | • *Supports data analytics for crime trends and judicial efficiency* |
| ***Release*** | • *e-Prisons Portal*<br>• *Automated flaggers* | • *Tracks release status*<br>• *Maintains accurate records of property and custody details* |
| ***Reporting and Legal Reference [6]*** | • *eSCR*<br>• *Judgment search portal*<br>• *RTI Online Portal*<br>• *Open APIs*<br>• *Neutral Citation System* | • *Searchable Supreme Court judgments and free download*<br>• *Searchable High Court judgments and free download*<br>• *Case tracking for institutional litigants*<br>• *Standardised legal references* |

*Table 1: Digital interventions across the case journey.*

## 4. ICJS: Seamless Integration Across Criminal Justice Pillars

The ICJS framework is built around the interconnection of five core pillars. These are: (i) Police through CCTNS; (ii) Courts through e-Courts and the Case Information System; (iii) Prisons through e-Prisons; (iv) Prosecution through e-Prosecution; and (v) Forensics through e-Forensics. The design recognises that criminal justice delivery cannot be improved only by digitising one institution. A digital court record becomes more effective when it can receive investigation information, transmit court orders to prisons, and make relevant status updates available to the police and prosecutors.


*Figure 3: Core and possible future pillars connected through ICJS.*

### 4.1 Police: CCTNS

CCTNS is the principal police-side system. It supports the digitisation of police-station functioning and enables the sharing of FIR and charge-sheet

data with e-Courts applications [2]. This is particularly important because the criminal case begins with investigative records. When these records are digitally available to the court system, the chances of delay caused by manual transmission and repeated entry are reduced.

### 4.2 Courts: e-Courts and CIS

The e-Courts system and the Case Information System provide the court-side digital interface. Through ICJS, courts can receive FIR and charge-sheet data from CCTNS and share CNR numbers and case-status updates with the police system [1], [5]. This creates a reciprocal flow of information: the court receives case material from the police, while the police receive authenticated case-status information from the court.

### 4.3 Prisons: e-Prisons

The e-Prisons system supports the management of prisoner information, custody status, parole, bail and release-related processes [3]. Its integration with court systems is crucial because delays in communication of release or bail orders can directly affect personal liberty. Automated digital alerts and real-time updates can reduce the risk of overstay and improve coordination between courts, prisons and police.

### 4.4 Forensics: e-Forensics

Forensic reports often have a decisive role in criminal investigation and trial. e-Forensics enables online interaction between police stations and forensic laboratories, supports digital workflow management, and aims to make forensic information available to authorised stakeholders in a timely manner [8]. Faster and more reliable movement of forensic reports can reduce avoidable adjournments and improve the quality of investigation.

### 4.5 Prosecution: e-Prosecution

e-Prosecution is intended to streamline the work of prosecutors by giving them timely access to FIRs, charge-sheets, forensic reports and case-status information [9]. Prosecution decisions require complete and updated case information. ICJS can therefore improve the ability of prosecutors to

prepare for hearings, respond to court queries and coordinate with investigating agencies.

### 4.6 Integration with Other Systems:

ICJS also reflects a broader ecosystem approach. The Case Information System is being integrated, wherever relevant, with systems such as land records, e-Challan, the Ministry of Corporate Affairs portal, Common Service Centres and litigation-management platforms [5]. This wider integration is significant because criminal cases often intersect with other domains such as property records, transport violations, corporate offences and government litigation. Interoperability therefore supports not only individual case processing but also institutional decision-making.

| ***Pillar Name*** | ***Corresponding IT System*** | ***Key Data Shared / Received*** | ***Impact on Interoperability and Data Management*** |
|---|---|---|---|
| ***Police*** | *CCTNS (Crime and Criminal Tracking Network and Systems) [2]* | *• Shares FIR and charge-sheet data with e-Courts*<br>*• Receives CNR and case-status updates from e-Courts* | *• Reduces duplication*<br>*• Enables real-time investigation updates*<br>*• Facilitates nationwide searches for criminal records* |
| ***Courts*** | *e-Courts [1]* | *• Shares CNR and case updates with CCTNS*<br>*• Receives FIR and charge-sheet data from CCTNS*<br>*• Integrates with e-Prisons, e-Challan, Land Records, MCA Portal and CSCs* | *• Minimises data re-entry*<br>*• Ensures real-time access to investigation details*<br>*• Streamlines judicial processes*<br>*• Enables comprehensive case management* |
| ***Prisons*** | *e-Prisons [3]* | *• Updates custody details in real time*<br>*• Receives* | *• Reduces prisoner overstay*<br>*• Improves* |

| | | | |
|---|---|---|---|
| | | *automated alerts for bail, parole and release orders* | *communication between prisons, courts and police*<br>*• Facilitates timely intervention for under-trials* |
| ***Prosecution*** | *e-Prosecution [8]* | *Accesses case information, FIRs, charge-sheets and forensic reports from other pillars* | *• Streamlines prosecution workflow*<br>*• Ensures public prosecutors have timely access to case information for trials* |
| ***Forensics*** | *e-Forensics [9]* | *• Provides forensic reports to police and courts*<br>*• Supports digital chain-of-custody management* | *• Automates forensic workflow*<br>*• Supports secure evidence handling*<br>*• Speeds up the investigation process* |

*Table 2: ICJS pillars and their interoperability.*

## 5. Transformative Impact on Justice Delivery:

The significance of ICJS lies in its capacity to address recurring systemic problems rather than isolated administrative errors. Many delays in criminal cases arise not because a single institution is inactive, but because information does not move in time between institutions. A missing forensic report, a delayed custody update, an uncommunicated release order, or an incomplete police record can each slow down the justice process. ICJS attempts to respond to these bottlenecks by creating a secure and traceable data-sharing environment.

The impact may be seen in at least seven areas: police investigations, judicial delay, prison management, inter-State coordination, accountability, socio-legal efficiency and policy planning. In each of these areas, the common theme is that reliable data, shared in time, allows institutions to act earlier and with greater accuracy.

| *Area of Impact* | *Historical Issues* | *ICJS Solutions* | *Illustrative Example* |
|---|---|---|---|
| ***Police Investigations*** | • *Loss of FIRs*<br>• *Incomplete information*<br>• *Duplicate data*<br>• *Delayed forensic reports* | • *Centralised digital database for FIRs*<br>• *Real-time evidence sharing*<br>• *Cross-domain verification* | *Helps avoid wrongful action based on duplicate or incomplete records by displaying available prior records* |
| ***Judicial Delays*** | • *Missing documents and misplaced case records*<br>• *Lack of synchronisation between pillars* | • *Automated alerts for pending reports*<br>• *Transparent scheduling*<br>• *Real-time CIS integration* | *Flags pending forensic or investigation reports before delay affects case progression* |
| ***Prison Management*** | • *Prisoners overstaying*<br>• *Poor communication*<br>• *Inefficient management of parole and bail orders* | • *Live updates on custody status*<br>• *Automated notifications for release orders*<br>• *Integrated case tracking* | *Reduces overstay caused by delayed processing of release or bail orders* |
| ***Cross-Jurisdictional Coordination*** | • *Difficulty in tracking interstate crimes*<br>• *Siloed data systems*<br>• *Lack of coordination* | • *Nationwide search capability*<br>• *Real-time data sharing*<br>• *Standardised processes* | *A suspect arrested in one State can be checked against case information from another jurisdiction* |
| ***Accountability and Corruption*** | • *Manual data manipulation*<br>• *Weak accountability for delay* | • *Audit trails for user actions*<br>• *Automated delay timelines*<br>• *Transparent* | *Ensures entries are logged and modifications require authorisation,* |

| *Area of Impact* | *Historical Issues* | *ICJS Solutions* | *Illustrative Example* |
|---|---|---|---|
| | | *visibility for authorised users* | *reducing scope for tampering* |
| ***Socio-Legal Inefficiencies*** | *• Delayed bail or parole action for under-trials*<br>*• Influence-based prioritisation* | *• Objective case-prioritisation tools*<br>*• Automatic under-trial alerts*<br>*• Streamlined case progression* | *Flags under-trials who may require immediate review, including elderly or long-detained prisoners* |
| ***Policymaking and Reform*** | *• Lack of reliable data for crime analysis*<br>*• Decisions based on incomplete information* | *• Data analytics for crime trends, judicial efficiency and prison demographics*<br>*• Evidence-based policy support*<br>*• Predictive tools for crime prevention* | *Supports proactive crime prevention by identifying patterns and reallocating resources* |

*Table 3: ICJS impact - historical issues and digital solutions.*

## 6. Implementation Status and Alignment with New Criminal Laws:

Phase II of ICJS, covering the period 2022-23 to 2025-26, focuses on interlinking the IT systems of the criminal justice institutions and on providing technological tools for smarter policing and faster information exchange [5], [7]. The National Crime Records Bureau (NCRB) functions as the nodal agency for implementation, with the National Informatics Centre (NIC) as the technology partner [5].

The implementation of the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam has further increased the relevance of ICJS. These laws contemplate a justice process in which digital records, electronic communication and technology-enabled proceedings play a larger role. The ICJS 2.0 guidelines are therefore

aligned with the new criminal law framework and include technological upgrades required for the changed procedural environment [5], [10].

Chandigarh has been recorded as the first Union Territory to fully implement the new criminal laws, with initiatives such as the E-Vaarta facility for communication between police, judiciary, forensic, prosecution and jail authorities [10]. The MedLEaPR module of ICJS 2.0 has also been launched in Delhi for medico-legal examination and post-mortem reporting [11]. These developments show that ICJS is increasingly becoming a practical working layer of the criminal justice administration rather than a merely conceptual integration project.

## 7. Challenges in Effective Implementation:

The promise of ICJS is considerable, but its success depends on more than software integration. The first challenge is the digital divide. Rural and remote areas may face connectivity issues, insufficient hardware and limited technical support. If these infrastructure gaps remain unresolved, the benefits of real-time data exchange will not be evenly distributed.

The second challenge is institutional adaptation. Police officers, court staff, prison officials, prosecutors and forensic personnel must be trained not only to use the platform but also to understand the consequences of accurate digital entry. Interoperability works only when the original data is reliable. A single incorrect entry may travel across systems and create downstream errors. Capacity building, therefore, is not a one-time training exercise but a continuing institutional requirement.

The third challenge concerns staffing and workload. Justice-sector reports have repeatedly highlighted vacancy, overcrowding and resource constraints in police and prison systems [12]. Technology can improve coordination, but it cannot by itself cure shortages of personnel, excessive workload or physical infrastructure deficits. For ICJS to deliver its full benefit, it must be accompanied by administrative reform, adequate staffing and sustained budgetary support.

The fourth challenge relates to privacy, security and authorised access. Criminal justice data is sensitive. A platform that connects multiple institutions must ensure strong access control, audit trails, cybersecurity

protocols and accountability for misuse. Digital integration must therefore proceed together with safeguards for due process, data integrity and individual rights.

## 8. Future Roadmap: ICJS 2.0 and the Next Stage of Digital Justice:

The future roadmap of ICJS 2.0 points towards deeper integration, better data quality and the use of advanced technologies [5], [7]. Its major strategic directions may be summarised as follows:

- **A.** Seamless integration of police, courts, prisons, prosecution and forensics so that relevant criminal case information moves through authorised digital channels without avoidable delay.
- **B.** Improvement of data quality by reducing duplicate entry, standardising fields, validating information and creating responsibility for accurate digital records.
- **C.** Support for smart policing through analytics, modern investigation tools and better access to cross-jurisdictional information [2], [7].
- **D.** Alignment with the new criminal laws, including the use of digital communication, electronic records, e-Summons, eSign, e-Sakshya and technology-enabled court proceedings [5].
- **E.** Development of secure cloud-based infrastructure, software tools, licenses and technical manpower required for reliable national-scale operation.
- **F.** Use of advanced technologies such as artificial intelligence, blockchain-based chain-of-custody tools, analytical dashboards and biometric identification systems, including NAFIS, wherever legally and administratively appropriate.
- **G.** Creation of automated alerts at predetermined stages of criminal cases, from FIR to final disposal, for the benefit of investigating officers, complainants, victims and other authorised stakeholders.
- **H.** Continuous awareness, handholding and capacity-building programmes across all pillars of the criminal justice system.

## 9. Conclusion:

The Interoperable Criminal Justice System represents an important shift in India's approach to criminal justice administration. Earlier digital projects strengthened individual institutions. ICJS attempts to connect them. Its real value lies in transforming criminal justice data from isolated departmental records into a coordinated, authorised and actionable information flow.

By integrating police, courts, prisons, prosecution and forensics, ICJS can reduce avoidable delay, minimise duplication, improve accountability, support better investigation, prevent custody-related errors and strengthen evidence-based policymaking. The principle of "one data, one entry" is therefore not merely a technical design choice; it is a governance principle that seeks to make every institution act on accurate, timely and shared information.

At the same time, ICJS must be understood as an enabler rather than a complete solution. Its success will depend on reliable infrastructure, trained personnel, adequate staffing, strong cybersecurity safeguards and a rights-sensitive approach to data governance. If implemented with these safeguards, ICJS has the potential to become a decisive instrument for building a modern, transparent, accountable and citizen-centric criminal justice system in India.

## References:

1. *e-Committee, Supreme Court of India, Status of the Court Projects (e-Courts Mission Mode Project), available at https://ecommitteesci.gov.in/project/status-of-the-court-projects/*
2. *Ministry of Home Affairs, Crime and Criminal Tracking Network and Systems (CCTNS), available at https://www.mha.gov.in/en/divisionofmha/women-safety-division/cctns*
3. *e-Committee, Supreme Court of India, e-Prisons, available at https://ecommitteesci.gov.in/e-prison/*
4. *Ministry of Home Affairs, Inter-operable Criminal Justice System (ICJS), available at https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs*
5. *Ministry of Home Affairs, Inter-Operable Criminal Justice System (ICJS) - Phase II Implementation Guidelines, available at*

*https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2023/04/2023042088.pdf*

6. *R. Arulmozhiselvi, Use of Artificial Intelligence in the District Judiciary, IIPA GyanKOSH: Growth Drivers of Viksit Bharat @2047 (2025), available at https://www.iipa.org.in/GyanKOSH/posts/use-of-artificial-intelligence-in-the-district-judiciary*
7. *Ministry of Home Affairs, Phase-II of ICJS, Press Information Bureau, available at https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2039059*
8. *e-Forensics, Forensic Science Laboratory Portal, available at https://eforensics.gov.in/fslall/*
9. *e-Prosecution, e-Prosecution Portal, available at https://eprosecution.gov.in/eprosecution_test/*
10. *Ministry of Home Affairs, Union Home Minister Chairs Review Meeting on Implementation of Three New Criminal Laws, Press Information Bureau, Dec. 24, 2024, available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=2087523*
11. *MedLEaPR, Medico Legal Examination and Postmortem Reporting Portal, available at https://medleapr.nic.in/*
12. *Tata Trusts, India Justice Report 2022: Ranking States on Police, Judiciary, Prisons and Legal Aid, available at https://indiajusticereport.org/files/IJR%204_Full%20Report_English_Low.pdf*

**Author's Profile:**

R. Arulmozhiselvi

District Judge (Tamil Nadu cadre, 2003 Batch); formerly on deputation as OSD (Registrar), Training Cell and Member (Human Resources), eCommittee, Supreme Court of India.

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.1, (P. 128-140)

# Role of Border Management in National Security

Uday Kumar*

***Abstract:***

*Border management has emerged as a critical pillar of national security in contemporary geopolitics. India, with one of the most complex and contested border regimes, confronts a diverse spectrum of security challenges, including cross-border terrorism, illegal migration, narcotics trafficking, arms smuggling, and persistent territorial disputes with neighbouring states such as China and Pakistan. In this context, border management has evolved from a conventional defensive mechanism into a comprehensive, multi-agency framework integrating intelligence coordination, technological surveillance, diplomatic engagement, and law enforcement. The operational role of Border Guarding Forces (BGFs), coupled with advancements in surveillance technologies and 'intelligence-led' strategies, underscores the increasing sophistication of border security practices. At the same time, the dynamic threats posed by hostile state actors, non-state actors and transnational networks necessitate adaptive and coordinated policy responses. A well-coordinated and intelligence led border management framework is essential for safeguarding India's sovereignty, territorial integrity, and internal stability.*

***Keywords:***

*Border Management, National Security, Border Guarding Forces, Cross-*

* *Second in command Ops Directorate, FHQ, BSF Block-X, CGO Complex Lodi Road, New Delhi-110003.*

*Border Terrorism, Illegal Migration, Smart Fencing, India's Border Policy, Geopolitical Threats.*

## Introduction:

The security of a nation's borders represents the most fundamental expression of its sovereignty. For India, which shares approximately 15,106 kilometres of land borders with seven countries Pakistan, China, Nepal, Bhutan, Bangladesh, Myanmar, and Afghanistan, and a coastline of about 7,516 kilometres, border management is not merely an administrative responsibility but a strategic imperative of the highest order. India's borders are not static lines; they are dynamic, contested, and often asymmetrically threatened spaces that require constant vigilance, coordinated response, and adaptive strategies.

Since Independence, the concept of border management in India has undergone a significant transformation. Initially rooted in a conventional security paradigm focused on military deterrence and territorial defence, it has evolved into a comprehensive framework integrating law enforcement, intelligence, diplomacy, economic development, and technology. The nature of threats along India's borders is diverse and region-specific. The western border with Pakistan is marked by state-sponsored terrorism, militant infiltration, and narcotics trafficking. The northern border with China remains sensitive due to unresolved territorial disputes and periodic military standoffs, as exemplified by the Galwan Valley clash of 2020. Meanwhile, the eastern borders with Bangladesh and Myanmar face challenges such as illegal migration, smuggling, and insurgent activities.

Border management in India is anchored by a multiples of Central Armed Police Forces (CAPFs), including the Border Security Force (BSF)[1] the Indo-Tibetan Border Police (ITBP), the Sashastra Seema Bal (SSB), and the Assam Rifles, each assigned to specific borders based on

[1] *The BSF is primarily responsible for policing the border during peace time. It also collects intelligence along and across the border. Over a period of time, the BSF has developed significant capability for intelligence acquisition. It shares information locally as well as with its headquarters. - The Kargil Review Committee Report, December 15, 1999, Sagar Publications, New Delhi.*

the nature of the terrain and threat perception. These forces function under the policy framework of the Ministry of Home Affairs (MHA), which coordinates closely with the Ministry of Defence, the Ministry of External Affairs, and the intelligence agencies.

Following the Kargil War of 1999 and the recommendations of the Kargil Review Committee, India undertook a comprehensive restructuring of its border management architecture. This led to the establishment of the Department of Border Management under the MHA in 2004, aimed at enhancing coordination, infrastructure development, and overall border security mechanisms.

### India's Border Security Architecture: Structure and Mandate:

India's border security architecture is a layered, multi-agency framework that reflects the diversity and complexity of its border challenges. The primary responsibility for guarding land borders rests with the Central Armed Police Forces (CAPFs), each entrusted with a specific mandate. The Border Security Force (BSF), established in 1965 in the aftermath of the Indo-Pakistan War, is the largest border guarding force in the world and is primarily deployed along the Indo-Pakistan and Indo-Bangladesh borders. The Indo-Tibetan Border Police (ITBP), raised in 1962 following the Sino-Indian War, is responsible for securing the 3,488-kilometre-long border with China across the difficult Himalayan terrain.

The Sashastra Seema Bal (SSB), originally established as the Special Service Bureau in 1963, was assigned border guarding responsibilities in 2001 and is deployed along the India-Nepal and India-Bhutan borders. The Assam Rifles, India's oldest paramilitary force, is tasked with guarding the India-Myanmar border and plays a critical role in counter-insurgency operations in the Northeast. Additionally, the Indian Army plays a crucial role in managing the Line of Control (LoC) and Line of Actual Control (LAC), working in coordination with forces such as the BSF and ITBP to ensure comprehensive border security.

The Department of Border Management (DBM) under the Ministry of Home Affairs serves as the nodal authority for policy formulation and coordination. It oversees the development of border infrastructure,

including the construction of border roads, Border Out Posts (BOPs), and the floodlighting of vulnerable stretches, thereby strengthening surveillance and operational efficiency.

**Threat Landscape: Mapping the Challenges on India's Borders:**

Understanding India's border security requires recognition of the evolving and multidimensional nature of threats, which necessitate differentiated and adaptive responses. These challenges can be broadly classified into state-sponsored threats, non-state actor threats, and transnational criminal activities. Each category operates through distinct mechanisms, thereby requiring specialized strategic and operational approaches to ensure national security.

On the western front, Pakistan's sustained use of non-state actors as instruments of strategic policy has rendered the India-Pakistan border one of the most volatile in the world. The infiltration of trained militants across the Line of Control (LoC) in Jammu and Kashmir, often facilitated by Pakistan's Inter-Services Intelligence (ISI), has remained a key driver of insurgency in the region since the late 1980s. Despite extensive fencing along significant stretches of the LoC, infiltrators continue to exploit gaps arising from difficult terrain, adverse weather conditions, and limitations in surveillance capacity at Border Out Posts (BOPs). Incidents such as the Pathankot (2016), Uri (2016), and Pulwama (2019) attacks serve as critical case studies, highlighting the complexities of securing hostile and terrain-intensive borders against unconventional threats.

In the aftermath of the Pulwama attack, India adopted a more assertive security posture, exemplified by the Balakot airstrikes of 2019. This marked a shift towards a proactive response strategy, signaling a willingness to undertake cross-border actions to deter and respond to state-supported terrorism.

The India-China border presents a unique challenge where China is actively changing the landscape by building "dual-use" roads and villages near the Line of Actual Control (LAC). Recent clashes like Doklam and

Galwan[2] have highlighted the risk of direct military conflict in the freezing, high-altitude Himalayas, where the lack of a clearly defined border makes management difficult. While China historically held an infrastructure advantage, India is now rapidly closing that gap by aggressively building its own all-weather tunnels, bridges, and high-altitude roads to ensure its forces are better equipped and more mobile than ever before.

The eastern borders present a distinct set of challenges, particularly in the form of illegal migration. India's border with Bangladesh witnesses one of the largest cross-border population movements in Asia. The prolonged influx of undocumented migrants over several decades has contributed to demographic changes, resource pressures, and social tensions in border states, with significant implications for internal security and governance.

The management of the India-Myanmar border has also assumed increasing importance in recent years. The earlier Free Movement Regime (FMR), while intended to facilitate local cross-border ties, was exploited by insurgent groups and criminal networks for the movement of arms, establishment of camps, and other illicit activities. In response, the government has moved towards stricter regulatory mechanisms, including the construction of border fencing and tighter movement controls, to address these vulnerabilities.

India's geographical location between two major drug-producing regions, the Golden Triangle in Southeast Asia and the Golden Crescent in the West, further compounds these challenges. This positioning facilitates transnational criminal activities such as narcotics trafficking, counterfeit currency circulation, and human smuggling. These activities not only pose serious public health and law & order concerns, as reflected in regions like

---

[2] *The Galwan Valley clash of June 2020, in which 20 Indian soldiers were killed in hand-to-hand combat with Chinese forces, was the most serious military confrontation on the India-China border since 1967. It led to a complete restructuring of India's forward deployment strategy along the LAC and a massive acceleration of border infrastructure development. - Ministry of Defence Annual Report, Government of India, 2021.*

Punjab, but also contribute to the financing of terrorist networks, thereby reinforcing the critical importance of effective and integrated border management.

### Technology as a Force Multiplier in Border Management:

The deployment of technology has emerged as a critical force multiplier in India's border management strategy, enabling continuous surveillance across vast and inhospitable terrains that are beyond the effective reach of the deployed force personnel. The Comprehensive Integrated Border Management System (CIBMS) represents a major technological initiative in this domain, integrating thermal sensors, night-vision devices, laser fencing, radars, aerostats, and communication networks into a unified command and control framework. Pilot projects have been implemented along the India-Pakistan border in Punjab and the India-Bangladesh border in Assam, with plans for phased expansion across vulnerable stretches.

Unmanned Aerial Vehicles (UAVs), or drones, have become integral to modern border surveillance. Forces such as the BSF and ITBP increasingly rely on drones for real time monitoring of remote and difficult terrain. At the same time, the use of drones by Pakistan based networks for dropping narcotics and weapons in Punjab has highlighted emerging security challenges. In response, India is strengthening its counter-drone capabilities through jamming systems and anti-drone technologies, with deployments such as the Drone Threat Management System (DTMS).

Space-based intelligence, surveillance, and reconnaissance (ISR) has added a strategic dimension to border management. Satellite assets operated by ISRO provide critical imagery for monitoring troop movements, infrastructure development, and terrain changes along the Line of Actual Control (LAC) and Line of Control (LoC). The integration of satellite data with ground intelligence has enhanced situational awareness, particularly in inaccessible regions. The establishment of the Defence Space Agency (DSA) in 2019 further strengthens these capabilities.

Additional initiatives such as biometric identification systems and Smart Fencing under the CIBMS framework are improving border control.

Smart Fencing, combining sensors and surveillance technologies, is particularly effective in riverine and flood-prone areas where conventional fencing is not feasible. The growing use of Artificial Intelligence (AI) in analysing sensor data and satellite imagery represents an emerging frontier, enhancing detection capabilities while reducing the operational burden on personnel.

## Border Management and Counter-Terrorism: The Operational Nexus:

Counter-terrorism operations along India's borders constitute the most critical dimension of border management in ensuring national security. The primary objective is to prevent the infiltration of terrorists while simultaneously disrupting the logistical networks comprising financing, arms supply, and communication channels that sustain terrorist activities within the country. The close linkage between border management and counter-terrorism is most evident in the context of Jammu and Kashmir, where sustained efforts to secure the Line of Control (LoC) have been central to the broader management strategy of weakening and containing militant networks.

The BSF's operations on the India-Pakistan border in Rajasthan, Punjab, and Gujarat are a critical component of counter-terrorism strategy. The detection and neutralization of narco-terror modules, which are networks that simultaneously traffic narcotics[3] and weapons and finance terrorist activities, has been one of the BSF's significant operational successes in recent years. The seizure of large heroin consignments and weapons packages dropped by Pakistani drones, along with the mapping of over ground worker (OGW) networks in border districts, reflects the intelligence-led, operationally integrated approach that effective border-based counter-terrorism requires.

---

[3] *Narco-terrorism refers to the use of drug trafficking networks to fund, sustain, and operationalize terrorist organizations. The nexus between Pakistani intelligence, narcotics trafficking networks, and militant groups in Punjab is among the most documented examples of narco-terrorism in South Asia. - Vikram Sood, The Unending Game, Penguin Random House India, 2018.*

The Indian Army's counter-infiltration grid along the Line of Control (LoC), comprising physical barriers, surveillance systems, and coordinated ground operations, functions in close coordination with the BSF to prevent infiltration and maintain internal security. The Army's capacity to dominate terrain and undertake targeted operations, such as the surgical strikes of September 2016, reflects an integrated approach to border management and counter-terrorism. The Balakot airstrike of February 2019 marked a further shift, signalling a more assertive response to cross-border terrorism beyond conventional constraints.

## Border Infrastructure Development and National Security:

The development of border infrastructure is a critical component of national security, complementing the role of border guarding forces. Historically, India's infrastructure in border areas such as roads, bridges, tunnels, and communication networks lagged behind that of China, creating operational constraints and slowing troop mobilization during crises. The Kargil War of 1999 exposed these deficiencies, particularly in maintaining logistical support in high-altitude regions.

The Border Roads Organisation (BRO), established in 1960, is the primary agency responsible for infrastructure development in border areas. Strategic projects such as the Atal Tunnel (2020) and the upcoming Zoji La tunnel have enhanced all weather connectivity to Ladakh, while the Dhola-Sadiya Bridge (2017) has improved access to the Arunachal sector. These developments have strengthened India's ability to mobilize forces rapidly and maintain logistical readiness.

Border infrastructure also includes the establishment and modernization of Border Out Posts (BOPs) and Company Operating Bases (COBs), which serve as key operational nodes. Upgraded facilities, improved surveillance systems, and better communication networks have enhanced the effectiveness of deployed personnel. Additionally, border haat markets along the India-Bangladesh and India-Myanmar borders facilitate regulated trade and local engagement while also providing valuable intelligence through monitored cross-border interactions.

The Vibrant Villages Programme (VVP), launched in 2023, reflects the direct linkage between border infrastructure and national security by focusing on the development of villages along India's borders that have witnessed population decline due to harsh living conditions and limited economic opportunities. By enhancing connectivity, livelihood options, and access to essential services, the programme seeks to reverse migration and sustain a stable local population in border areas.

This approach strengthens border management by positioning local communities as an important layer of awareness and presence, while also preventing the emergence of strategic vacuums that could be exploited by adversaries. It highlights an evolving understanding of the interplay between human geography, infrastructure development, and national security.

## Diplomatic Dimensions of Border Management:

Border management extends beyond security considerations and functions as an important instrument of diplomacy in India's relations with its neighbours. Mechanisms such as flag meetings, joint working groups, and established communication channels help manage routine border issues and prevent escalation during crises. This approach has been most effective in India's engagement with Bangladesh, where the Land Boundary Agreement2015[4] resolved old disputes and led to modern cooperation like joint patrols and local "Border Haats." In contrast, the relationship with China remains difficult; while peace agreements exist, China's constant construction and troop movements make these rules hard to follow, forcing India to balance diplomatic talks with a firm military stance to protect its territory.

---

[4] *The Land Boundary Agreement (LBA) of 2015 between India and Bangladesh was a landmark diplomatic achievement that resolved the complex issue of over 160 enclaves on both sides of the border, transferring sovereignty to over 51,000 people who had lived in a legal limbo for decades. - Ministry of External Affairs, Government of India, Annual Report, 2015-16.*

## Illegal Migration and its Impact on National Security:

Illegal migration represents one of the most complex and politically sensitive dimensions of India's border management. Unlike cross-border terrorism, which involves limited actors with clear intent, illegal migration is driven by economic distress, political instability, and environmental factors, often facilitated by organized trafficking networks. Large scale migration, particularly from Bangladesh, as well as from Myanmar, has significant implications for national security, demographic balance, and social cohesion in Border States.

Sustained migration into states such as Assam, West Bengal, and Tripura since the 1970s has led to notable demographic changes, complicating governance and border management. Measures such as the Assam Accord (1985) and the National Register of Citizens (NRC) have sought to address these concerns, although challenges remain in verification and legal resolution. The influx of Rohingya populations following the 2017 Myanmar crisis has further added to the complexity, raising concerns related to security.

Addressing illegal migration requires a balanced and comprehensive approach that integrates border control with legal, administrative, and diplomatic measures. Mechanisms such as biometric identification, improved detection systems, and coordinated engagement with neighbouring countries are essential. While institutional tools like Foreigners' Tribunals contribute to identification processes, persistent legal and logistical constraints highlight the need for a calibrated strategy that aligns national security objectives with humanitarian considerations.

## Policy Imperatives for Future Ready Border Management:

Ensuring national security in an evolving threat environment requires continuous adaptation in India's border management strategy. First, there is a growing emphasis on enhanced inter agency coordination among border guarding forces, the police, the armed forces, and intelligence agencies. This approach is gradually evolving towards an integrated "security grid," enabling real-time information sharing and synchronized responses across border regions.

Second, the development of border infrastructure remains a critical priority. Despite the challenges posed by difficult terrain, particularly along the northern borders, sustained investments in all-weather roads, tunnels, bridges, and advanced landing grounds have significantly improved connectivity and operational readiness. These efforts are essential for ensuring rapid mobilization and logistical support to deployed forces.
Third, the emerging threat posed by the use of drones for smuggling weapons and narcotics necessitates a comprehensive counter-drone strategy. The deployment of a layered defence system comprising detection radars, jamming technologies, and interception capabilities along with stricter regulatory controls, is essential to address this evolving challenge effectively.

Finally, the welfare of border guarding personnel remains central to effective border management. Operating in extreme and often hostile conditions, these forces require sustained institutional support in terms of infrastructure, equipment, and living conditions. Strengthening their morale and operational efficiency is as vital as technological and strategic advancements in securing the nation's borders.

## Conclusion:

Border management occupies a central and indispensable place in India's national security architecture. It operates simultaneously at the tactical level preventing infiltration, smuggling, and illegal crossings and at the strategic level, shaping the broader security environment within which India's military posture, diplomacy, and economic development function. The multidirectional, asymmetric, and evolving nature of India's border challenges necessitates a system that is technologically advanced, operationally agile, institutionally integrated, and diplomatically responsive.

Since the watershed moment of the Kargil War, India has made significant strides in strengthening its border management framework. The establishment of the Department of Border Management, accelerated infrastructure development under the Border Roads Organisation,

deployment of the Comprehensive Integrated Border Management System (CIBMS)[5], enhanced cooperation with Bangladesh, and a more assertive approach to cross-border terrorism collectively reflect this progress. Nevertheless, persistent challenges including the unresolved boundary with China, porous stretches along the Bangladesh border, the narco-terrorism nexus on the western front, the emerging drone threat, and the complexities of illegal migration continue to test the system's resilience.

A key lesson from India's experience is that security and development are intrinsically linked. Effective border management depends not only on physical surveillance and force deployment but also on a strong administrative presence and the active participation of border communities. Initiatives such as the Vibrant Villages Programme and the Border Area Development Programme underscore this integrated approach. Ultimately, the effectiveness of India's national security in the 21st century will be significantly shaped by the coherence, adaptability, and strategic vision of its border management framework.

## References:


1. *Kargil Review Committee. (2000). From Surprise to Reckoning: The Kargil Review Committee Report. Government of India, National Security Council Secretariat.*
2. *Ministry of Home Affairs. (2004). Annual Report 2003-04. Government of India. https://www.mha.gov.in*
3. *Sood, V. (2018). The Unending Game: A Former R&AW Chief's Insights into Espionage. Penguin Random House India.*
4. *Doval, A. K. (2017). Border security and national security. India Foundation Journal, 5(3), 12-21.*
5. *Ministry of External Affairs. (2016). Annual Report 2015-16. Government of India. https://www.mea.gov.in*
6. *Rajgopal, P. V. (2009). The British, the Bandits and the Bordermen. Wisdom Tree.*


[5] *Post-Pathankot attack (2016), along the India-Pakistan and India-Bangladesh borders, **Madhukar Gupta Committee**, recommended **CIBMS** installation as a five-layer plan including CCTV, thermal imagers, battlefield surveillance radar, underground sensors, and laser barriers.*

7. *Raman, B. (2002). Intelligence: Past, Present and Future. Lancer Publishers and Distributors.*
8. *Chadha, V. (2005). Low Intensity Conflicts in India: An Analysis. SAGE Publications India.*
9. *Ministry of Defence. (2021). Annual Report 2020-21. Government of India. https://www.mod.gov.in*
10. *Kanwal, G. (2018). India's Military Modernization: Plans and Strategic Underpinnings. NBR Special Report No. 68. National Bureau of Asian Research.*
11. *Ladwig III, W. C. (2007). A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine. International Security, 32(3), 158-190. https://doi.org/10.1162/isec.2008.32.3.158*
12. *Pant, H. V. (Ed.). (2012). The Rise of China: Implications for India. Cambridge University Press India.*
13. *Border Security Force. (2022). BSF Annual Report. Ministry of Home Affairs, Government of India.*
14. *Sood, V. (2020). The Ultimate Goal. HarperCollins Publishers India.*
15. *Ministry of Home Affairs. (2023). Vibrant Villages Programme. Government of India. https://www.mha.gov.in*

## Author's Profile:

Uday Kumar, is a 2000 Batch direct entry officer of the Border Security Force (BSF), currently serving at Ops Dte, Force HQ, BSF New Delhi.

An alumnus of Delhi University, he has done BSc (Hons) Mathematical Statistics from Kirori Mal College (Delhi University) and LLB form Campus Law Centre (Law Faculty-DU), MBA in Disaster Management from IP University, New Delhi and MA in Criminology & Police Administration.

He has extensive leadership experience, serving in BSF Bn in Counter insurgency Ops, LoC and along International Border on Pakistan and Bangladesh.

Contact No- 9868633925

Mail ID- udaykr86@gmail.com

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXV No.1, (P. 141-157)

# Modernising Police and CAPF Capability for Urban Policing

M. Pradeep John*

***Abstract:***

*Rapid urbanisation and widespread use of digital technology are transforming the operational environment of policing in Indian cities in rather significant and manifest ways. Contemporary urban policing systems function amid high population density, rapid information exchange flows, digital offenses and cyber-enabled crimes, extensive electronic trails and intensified public expectations and scrutiny regarding responsiveness and accountability. Traditional policing strengths such as discipline, physical endurance, fieldcraft and tactical awareness remain indispensable, but are now required to be further reinforced by digital fluency, evidence discipline and enhanced inter-agency coordination. The central premise of this article is that training reform is fundamental to effective urban policing. Utilising authentic resources from Ministry of Home Affairs, Bureau of Police Research and Development, Ministry of Housing and Urban Affairs, Department of Personnel and Training, Capacity Building Commission, and NCRB data tabled before Parliament, it proposes an integrated training framework conceptualised upon five complementary pillars, namely simulation based learning, cyber awareness, forensic readiness, continuous learning through iGOT Karmayogi, and closely supervised AI-assisted training.The article also analyses the vital role of Central Armed Police Forces, particularly the*

* *Second-in-Command, Central Reserve Police Force*
*CRPF Academy. Kadarpur, Gurugram.*

*CRPF, in providing support to state police during elections and crucial urban deployments. It concludes that training modernisation must not be viewed as a divergence from traditional police preparation, but as an indispensable and necessary expansion of it.*

***Keywords:***
*Urban Policing, police training, CAPFs, CRPF, cyber awareness, forensic readiness, iGOT Karmayogi, Artificial Intelligence, simulation-based learning, technology in policing, capacity building, AI assisted training, training modernisation.*

## 1. Introduction:

Urbanisation is one of the most noteworthy socio-economic transformations presently underway in India. In a written reply in the Lok Sabha, the Government citing the Economic Survey 2023-24, mentioned that more than 40 per cent of India's population is expected to reside in urban areas by 2030 (PIB, 7 Aug 2024).This should not be construed merely as a planning statistic, since it has direct and significant implications for policing.Bigger and denser cities produce more complex population mobility patterns, larger public gatherings, higher dependence on digital information systems and considerably greater pressure on investigation and emergency response systems.

In such a setting, urban policing is no longer restricted to conventional beat management or reactive law and order deployment. Law enforcement officers today function in an environment dominated by surveillance systems, online communication, location-based services, digital payments and rapid public dissemination of information. The response of the police force in a city is now judged not only on how quickly it arrived at the scene, but also on whether it was legitimate, coordinated and technologically competent.

Police training in India has traditionally emphasised discipline, physical endurance, fieldcraft, battle training and tactical preparedness. While these foundations continue to remain vitally essential, contemporary urban policing requires those traditional strengths to be reinforced by modern

competencies such as simulation-based decision making, cyber awareness, forensic readiness, continuous learning and structured exposure to emerging technologies. The purpose of this article is to evaluate how this required reinforcement can be achieved in a practical and sustainable manner.

At the outset, it is necessary to clarify that this article addresses training reform precisely because it is the missing piece in India's urban policing preparedness. The operating environment has changed substantially over the last decade. The crime profile in cities has transformed. The tools of emergency response have altered. The expectations of the general public have metamorphosed. If the training of a police force has not evolved with these changes, then it will struggle to deliver in an urban scenario, despite being well-disciplined and physically fit. In that sense, training reform is not just a topic of academic discourse, but is a core operational question for urban policing and must be considered as such.

Recent institutional developments consistently corroborate this trend. The theme of the January-June 2025 issue of The Indian Police Journal published by BPR&D was based on Artificial Intelligence in Policing (BPR&D, 2025). The Department of Personnel and Training describes iGOT Karmayogi as an online platform facilitating anytime, anywhere, any device learning for government employees (DoPT Training Division). The Capacity Building Commission further affirms that courses on iGOT are mapped to identified competencies through the Karmayogi Competency Model (KCM). These developments as a whole indicate that the wider public sector training ecosystem in India is already progressing towards competency-based, technology-enabled learning, and it is incumbent upon police and CAPF training institutions to necessarily and proactively engage with that shift in a purposeful and deliberate manner.

## 2. The Changing Nature of Urban Policing in India:

Official data indicates how rapidly the operating environment is evolving. Based on NCRB data, the Ministry of Home Affairs reported that registered cybercrime cases in India rose from 65,983 in 2022 to 86,420 in 2023, which is a leap of over 31 per cent in a single year (MHA, Lok

Sabha Unstarred Question No. 452, 2 Dec 2025). The same reply also mentions that fraud and cheating accounted for large shares of cybercrime cases in 2023, which reflects growing prevalence of financially motivated online offences. While cybercrime is not exclusively an urban phenomenon, its reporting, investigation, target victim profile and procedural protocols are closely linked to urban digital ecosystems, and hence addressing this issue falls appreciably on urban police.

Urban policing also increasingly depends on digital evidence, since CCTV footage, mobile devices, location data and transaction trails are now routinely relevant to criminal investigation and incident reconstruction. This means that the first responding officer or supervisory law enforcement team in a city often encounters an evidentiary environment that is simultaneously both physical and digital. The main operational challenge is no longer only to reach the scene quickly; it is also to preserve evidentiary information in a manner that retains its usefulness and admissibility later. This is a significant shift from the traditional understanding of first response duties.

The emergency response architecture has also undergone a paradigm shift. The Ministry of Home Affairs has stated that the 112 Emergency Response Support System is a universal pan-India single emergency number operational in all 36 States and Union Territories (MHA, Rajya Sabha Starred Question No. 192, 20 Dec 2023). MHA's ERSS page describes the system as a nationwide integrated emergency response platform that forwards actionable incidents to dispatchers across police, health, fire, disaster response and related services through Computer-Aided Dispatch (CAD) and GIS-supported workflows (MHA ERSS). This pinpoints the location and deploys Emergency Response Vehicles (ERVs) to the vicinity, ensuring immediate assistance during the “golden hour”. This has direct implications for training, since personnel now need to be familiar not only with field response, but also with computer aided dispatch, interpreting real time GPS/GIS location mapping, universal triaging protocols, communication discipline and inter-agency coordination procedures.

In addition, city-level technology systems have added another important dimension. The Ministry of Housing and Urban Affairs has stated that Integrated Command and Control Centres have been set up in 100 Smart Cities. These are described as nerve centres that support centralised monitoring, situational awareness, faster incident response and improved inter-departmental coordination (MoHUA, 2023). Here the point is not that technology can replace trained personnel, since it obviously cannot. It is that urban policing now increasingly functions within larger information systems, and training must therefore be tailored to prepare personnel to function confidently and competently within those systems.

### 3. Why Training Reform Must Be Central to Urban Policing:

Since urban policing has changed substantially in character, training methodology must correspondingly evolve to keep pace with it. This is not an endorsement for repudiating conventional police or CAPF training. On the contrary, the effectiveness of urban policing is still dependant on the fundamental qualities inculcated by traditional training, namely discipline, stamina, cohesion, composure under pressure and respect for command. However, those qualities now need to be applied in situations that are vastly more information rich, more publicly visible and more procedurally demanding than the situations that previous generations of officers faced in the field.

From a training perspective, one consistent practical observation has been that personnel tend to absorb technology- related content much better when it is linked to realistic operational situations rather than when delivered as detached classroom lectures. A module on cyber fraud becomes more meaningful and effective when it is embedded in a simulated complaint or a digital evidence exercise. Similarly, training sessions on CCTV retrieval or chain of custody become more long-lasting when they are part of a practical response drill. This is especially relevant in training institutions of operational forces, where the credibility of instruction depends on its visible connection to field realities.

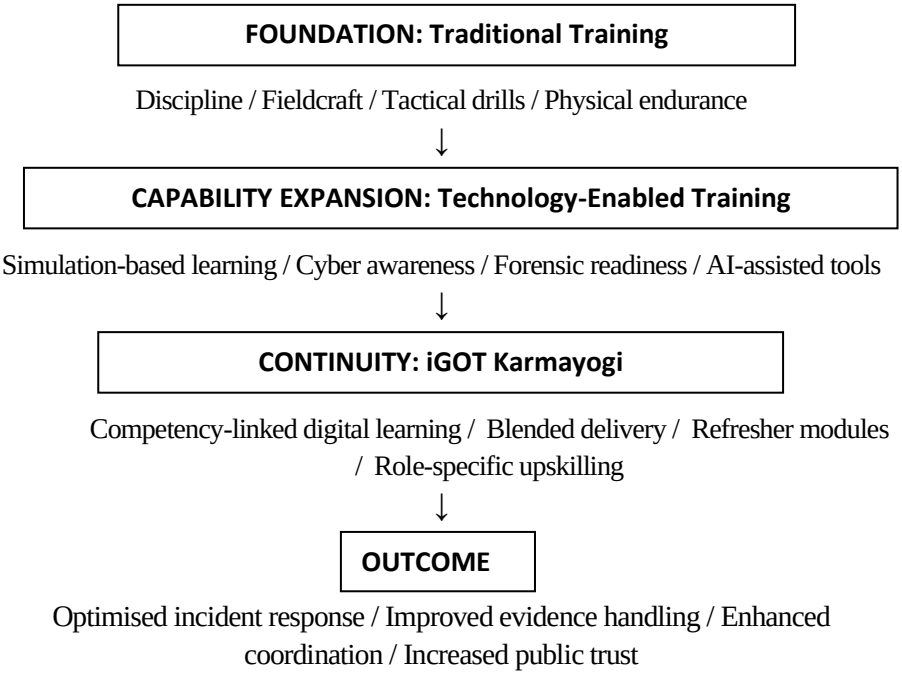
At its core, this article therefore asserts that urban policing preparedness should be built on an integrated training model combining traditional

police and CAPF training with five reinforcing elements, namely simulation-based learning, cyber awareness, forensic readiness, continuous learning through iGOT Karmayogi and supervised AI-assisted training. Each element addresses an actual capability deficit and can be incorporated into existing training structures without diluting professional standards.

## 4. Integrated Training Framework for Urban Policing Capacity Building

The training model proposed in this article, and depicted in Figure 1 below, is deliberately simple in its design.Traditional training remains the foundational bedrock upon which all subsequent tactical proficiencies and operational protocols are developed. Technology-enabled training enhances the capability of personnel, and optimises their preparedness to address the complexities posed by urban scenarios. iGOT Karmayogi provides the ideal platform for continuous learning that weaves together induction training, refresher learning, role-specific upskilling and post course reinforcement into a seamless, coherent whole.

**Figure 1. Integrated Training Framework for Urban Policing Capacity Building**



## 5. Simulation-Based Learning for Urban Scenarios:

Simulation has become way too significant to continue remaining at the periphery of training design, and this fact has been officially recognised by the system itself. The National Cybercrime Training Centre unequivocally states that simulation-based training methodology must keep up with the changing modus operandi of offenders (CyTrain). This perception applies more broadly to urban policing as a whole. Urban incidents are rarely sequential or straightforward. These situations typically involve partial or sketchy information, multiple actors, intense media coverage and considerable time pressure. It is very difficult for personnel to develop sound judgment in such situations through the medium of classroom instruction alone. Simulation provides for elements of complexity to be introduced into training in a controlled manner and without any operational hazard.

Some common urban policing scenarios that can be effectively simulated include crowd control, coordination of emergency response through 112 linked systems, handling of cyberfraud complaints, preservation of digital evidence by first responders and multi-agency response to fire, traffic or natural calamities. Realistic simulation training does not always require sophisticated equipment or complex infrastructure. Well planned table-top exercises (TTXs), tactical exercises without troops (TEWTs), roleplays and organised debriefs can substantially improve judgment and coordination of trainees at a reasonably affordable cost.

Simulation training is most effective when woven into a continuous learning cycle rather than used as a one-off event. Trainees benefit substantially when the exercise is preceded by in-depth study or short digital modules, and followed by structured evaluation and debrief. This is exactly the type of system in which a platform like iGOT Karmayogi can contribute to enrich learning. This platform can be used to deliver preparatory content well in advance, followed by refresher quizzes and follow-up modules after the exercise, while completion can be tracked methodically across the institution.

### 6. Cyber Awareness as a Foundational Competency:

According to the Ministry of Home Affairs, the Indian Cyber Crime Coordination Centre (I4C) was established in 2018 and subsequently elevated to an attached office of the Ministry in 2024, with the mandate to deal with cybercrime in a coordinated and comprehensive manner (MHA, Lok Sabha Unstarred Question No. 438, 2 Dec 2025). In the same reply, it was also stated that the Government has taken steps relating to awareness, capacity building, advisories, training of law-enforcement personnel and upgradation of cyber-forensic facilities. This is a clear indication that cyber awareness is no longer a niche or esoteric topic, but an inseparable part of mainstream police capacity-building.

For urban policing, cyber awareness cannot be confined to specialist investigation units. Frontline and supervisory officers, control room and beat personnel, and first response law enforcement officials, all require a baseline understanding of digital fraud patterns, impersonation tactics, device hygiene/cyber posture, complaint triage and escalation protocols. The objective is not to transform every officer into a cyber specialist, which is impracticable and superfluous. The purpose is to mitigate institutional vulnerability, improve initial response and ensure that the first contact between a victim and the police is competent, authoritative and credible. If the first contact at a police station is improperly handled, it can undermine the entire investigation from the initial stage itself.

This is also an area where continuous learning is particularly effective, especially because cybercrime evolves too rapidly for a one-off lecture session to remain relevant for long. Brief, continuously updated modules explaining recent fraud patterns, common complaint red flags or evidence-preservation mistakes observed in actual cases have more value than a single classroom session. The iGOT Karmayogi delivery model is tailormade for this, since it facilitates updated content to be pushed to personnel in the field without need for residential attendance.

### 7. Forensic Readiness and First-Responder Discipline:

Urban investigation in the modern era is heavily dependant on the quality of first response. The first responder may not necessarily be a forensic

expert, but the actions of the first responder very often determines whether evidentiary value is preserved or irretrievably damaged. This is particularly true in instances where mobile devices, surveillance footage or other digital evidence are involved. If mishandling of this occurs at the preliminary stage itself, critical evidence can be rendered inadmissible or unreliable.

In this regard, CyTrain's course architecture separately identifies Responder, Forensic and Investigation tracks. This indicates that cyber-integrated policing necessitates differentiated, yet interdependent competencies across diverse roles (CyTrain). This has important implications for police and CAPF training institutions. It indicates that forensic readiness should be integrated across the organisation, rather than limiting it to a small group of experts. It is imperative that all personnel who are likely to be first responders on the scene of an urban incident should be imparted training on the basics of scene preservation, chain of custody, documentation discipline and safe handling of digital devices.

An important practical observation from the field is that evidence-preservation errors often arise not from negligence, but from simple uncertainty. In several instances, personnel may be aware that a device or some digital material matters, yet still remain uncertain about exactly what to seize, photograph, label or hand over to the concerned specialist unit. In view of this, training must strive to convert awareness into repeatable and reliable procedure. Forensic readiness is an extension of the same discipline that good police training has always strived to build, which is the discipline of acting carefully and methodically in the present so that the truth can be established and justice delivered subsequently.

## 8. The Role of CAPFs, and the Particular Relevance of CRPF:

Urban policing in India is primarily the responsibility of state police forces. However, the CAPFs continue to play a crucial supporting role in critical urban deployments, sensitive law and order situations and election duties. This role does not seem likely to diminish in the future. Ministry of Home Affairs has characterised the CRPF as the prime force with the mandate to aid and assist civil authorities of States in maintaining law and order as and when the need arises (MHA Outcome Budget 2015-16). That description

remains highly pertinent today, as contemporary urban policing increasingly involves continuous reinforcement, coordination and interoperability of multiple agencies, rather than rigidly separated jurisdictional silos.

CRPF's institutional literature also emphases its urban-facing operational role. The Force is India's largest Central Armed Police Force (CRPF, Role of CRPF, 2026). It has been designated by MHA as the nodal agency for coordinating the movement and deployment of troops earmarked for election duties, and for this purpose dedicated 24x7 control rooms are established and pre-induction training is provided to troops assigned to election duties (CRPF, 2026). These are not minor administrative details, but serve to indicate that the Force is already actively involved in structured coordination, mobilisation and context specific pre-induction training tailored to urban and semi-urban landscapes, on a consistent and ongoing basis.

From the point of view of CRPF training institutions, this highlights a specific and critical concern requiring careful attention. When CAPF personnel are deployed in cities, they must necessarily be familiar with general law and order procedures and localised operational command hierarchies. They also need to be familiar with functioning within surveillance enabled ecosystems, and must possess basic knowledge of emergency communication mechanisms and evidence-sensitive response protocols. The efficacy of a CRPF company arriving in support of state police during an election or a large public event depends on its integration. It must seamlessly fit into the local command structure from the outset, rather than learning the local system from scratch after arrival.

Consequently, joint familiarisation training between state police and CAPFs becomes a practical operational necessity, rather than a luxury. During election duties, major festivals, VIP visits and communally sensitive events, which are precisely the situations in which CRPF is most regularly deployed in urban areas, short familiarisation modules covering urban command structures, 112-linked dispatch workflows, surveillance system access and local coordination channels can make a tangible difference to operational effectiveness. The friction that sometimes

surfaces between state police and CAPF units during urban deployments is rarely a question of intent or motivation from either side. It generally arises because of unfamiliarity with the systems and procedures of each other. This is a shortcoming that can be directly addressed by training.

In addition to the above, specific attention should be given to evidence discipline during urban deployments. When CRPF troops are deployed in urban areas for combating civil unrest, or for crowd control or election related incidents, their actions are often recorded by the general public, media and electronic surveillance systems simultaneously. Therefore, personnel must be prepared not only to act correctly in the moment, but also to document their actions. They should understand that digital evidence of their conduct may later be reviewed and analysed in legal proceedings. This factor has both operational and legal implications for the force and for the individual official.

Finally, the essential dimension of inter-agency coordination during urban CAPF deployment warrants dedicated focus in training design. CRPF officers and personnel need to be well-conversant with the practical functioning of Integrated Command and Control Centres, GIS-enabled dispatch and inter-agency intelligence flows in an urban setting during sensitive deployments. However, this does not mean that CRPF training needs to become a replica of urban police training. Both the forces have distinct mandates and different primary competencies. But due to the substantial overlap in their urban operational roles and the high operational stakes involved, it is imperative for training institutions on both sides to collaborate on building this shared body of knowledge.

## 9.iGOT Karmayogi and the Rationale for Continuous Learning:

According to the Department of Personnel and Training, iGOT Karmayogi is an online learning platform developed as part of the Digital India stack for capacity building of government employees. It provides online, face-to-face and blended learning while also managing lifelong learning records (DoPT Training Division). This is directly relevant to policing since urban security challenges and do not remain static for long. They are evolving continuously, due to which training cannot be confined only to induction

courses and frequent classroom refreshers. The rapid pace of change in cybercrime patterns, emergency response systems and technological advancement entail a more continual and flexible approach to maintaining competency.

The scale and reach of the iGOT Karmayogi platform are significant. As of January 2026, more than 1.47 crore civil servants were registered on iGOT, comprising more than 4,300 competency-mapped courses and over 6.8 crore recorded course completions (DoPT order, 13 Feb 2026). The Capacity Building Commission also states that courses are mapped to the competencies defined in the Karmayogi Competency Model When viewed together, these features make iGOT relevant both as a repository for verified content, and as a robust framework for structured, competency-driven professional development.

For police and CAPF institutions, iGOT Karmayogi essentially complements Academy training and does not serve as a substitute for it. The most productive training utilisation of this platform is through pre-course familiarisation, post-course reinforcement, short refresher modules, role-specific updates and training of trainers material. This kind of a blended training architecture is of great significance to forces such as CRPF that operate across widely dispersed locations across the country and cannot always spare personnel for long residential courses at centralised training institutions.

## 10. Usefulness of AI-Assisted Training (with Guardrails):

The BPR&D decision to devote a full issue of The Indian Police Journal to Artificial Intelligence in Policing is itself a useful indicator that AI has entered mainstream policing discourse in India and can no longer be treated as a futuristic or peripheral concern (BPR&D, 2025).The Government's Feb 2026 order on Mission Karmayogi points out that iGOT has commenced integration of AI-enabled features such as AI Sarthi, AI Tutor and AI-based capacity-building plans aiming to support personalised learning pathways and improved learning delivery (DoPT, 2026).

Although police training institutions mandatorily need to take note of these developments, they also require to exercise considerable restraint. AI

is best utilised as a support tool for training, useful for generation of case studies, organisation of content, multilingual access or scenario variants. It cannot replace professional judgment, legal accountability or instructor oversight, and in a policing context these are critical distinctions. The institutional challenge is not whether AI should be embraced or feared, since neither extreme is appropriate. It is to gauge the best way to introduce AI so that learning outcomes improve, without weakening professional standards.

## 11. Policy Recommendations:

The policy recommendations arising from this analysis can be distinguished between what can be done immediately with minimal additional resources, what requires a moderate degree of institutional effort and what needs long-term planning and system redesign. Several steps come in the first category and can be initiated without awaiting additional budgetary allocation or policy directives.

First and foremost, urban-scenario simulation should be made a standard and periodical component of police and CAPF training rather than being conducted as an occasional special exercise. Modules can initially start with low-cost formats such as table-top exercises (TTXs), tactical exercises without troops (TEWTs), incident boards, roleplays and organised debrief-driven case simulation, before moving on to advanced technology-supported formats depending on availability of infrastructure. The fundamental criterion is regularity and not elaborate equipment, since a training system that runs scenario exercises regularly will produce better urban responders in the long run, than one that runs an elaborate simulation once every few years.

Second, cyber awareness should be treated as a foundational competency across all ranks and not a specialist subject confined to dedicated cyber units. This means mandatory baseline modules for recruits and regular refresher modules for serving personnel, with periodic update of content as fraud patterns evolve. Modules should clearly differentiate between first responder awareness, investigation support and specialist investigation training. This is because a constable handling a cyber fraud

complaint requires different content from an inspector conducting a complex digital investigation.

Third, forensic readiness should be specifically strengthened at the first-responder level. Training syllabi should include complete and replicable protocols for crime scene security, digital-device handling, image capture, seizure documentation and transfer to specialist units. Comprehensive checklists, short practical drills and scenario variants are far more effective than conventional classroom lectures. The principal objective is to transform broad awareness into standardised and reproducible procedure.

Fourth, state police and CAPF training institutions should undertake joint familiarisation modules for urban deployments, especially before election seasons and major recurring events. Such training need not be complicated or resource-intensive. Short modules covering urban command hierarchies, 112-linked response systems and local coordination channels can mitigate inter-agency friction that tends to surface at times in the field. Since CRPF already conducts structured pre-induction training for election duty, this can be expanded in the near term to include urban-specific content.

Fifth, iGOT Karmayogi should be systematically integrated into police and CAPF training architecture. The best suited and practical approach would be to use it for pre-course preparation, post-course reinforcement, themed refresher modules and training of trainers programmes. Institutions do not need to give up their established training models for this. With over 1.47 crore civil servants already registered on the platform and more than 4,300 courses available, the infrastructure is already developed. The need of the hour now is the institutional will to use it in a systematic and disciplined fashion.

Sixth, technology literacy should be categorically included in urban-policing courses as a standard component. Personnel who may work with ICCCs, CCTV retrieval systems, GIS-enabled dispatch or platform-based emergency response should be given training in the functional basics of these systems, as part of their regular training. Familiarity reduces hesitation, and hesitation in time-sensitive urban incidents can have serious

repercussions. This will not require extensive technical training, only sufficient familiarity to operate confidently within these systems.

Seventh, in the context of CAPF urban deployments, evidence discipline should be included as a dedicated component of pre-induction training. CRPF personnel, when deployed in cities during elections, law and order disturbances, or major events are generally functioning in recorded environments, where there is a high probability that their actions may be reviewed in legal proceedings subsequently. Personnel must be conditioned to execute the right tactic, at the right time, in the heat of a volatile situation, while also documenting their actions systematically. They must also possess the appreciation to handle digital material correctly and recognise the evidentiary implications of their conduct. This should not be treated as an abstract legal exercise, but rather as direct preparation for operational ground realities.

Eighth, AI awareness and enablement should be introduced gradually and only after ensuring formal institutional safeguards. Training institutions must clearly define approved use cases, while maintaining human verification across all AI-assisted outputs. Furthermore, they must strictly avoid handling sensitive operational data through open or unvetted tools. The core objective should be to maximise learning efficiency and empower instructors. Tools should not be adopted merely to project a modern image or appear technologically advanced.

Finally, every reform measure should be accompanied by meaningful evaluation of outcomes. Completion statistics by itself do not prove that learning has occurred or that capability has improved. For drawing up measurable indices, institutions should analyse whether scenario performance has improved, whether evidence-handling errors have reduced and whether response coordination between agencies has streamlined. Without systematic evaluation, training reform becomes merely an administrative exercise rather than an operational one.

## 12. Conclusion:

Urban policing in India is being fundamentally reshaped by demographic change, technological proliferation and new patterns of criminal behaviour. These changes are permanent and irreversible. Official data and policy

framework already reflect this transition explicitly. Cybercrime volumes have risen sharply. Emergency response is increasingly being routed through integrated technology platforms. Integrated Command and Control Centres have become part of the policing system of Indian cities. National capacity-building policy is advancing decisively towards competency-based continuous learning. The direction of change is evident and the momentum is significant.

For police forces and CAPFs, the training implications of these changes are ineluctable. While traditional methodologies continue to remain indispensable, they are no longer sufficient for personnel who are required to operate in urban ecosystems. Contemporary urban policing mandates the reinforcement of discipline and tactical proficiency by simulation-based learning, cyber awareness, forensic readiness and conversance with software-driven response systems. iGOT Karmayogi offers a practical and well-developed mechanism for sustaining this learning beyond the classroom and across the career of an official. If AI-assisted tools are used carefully and with defined guardrails, they can add efficiency at the margins.

For CRPF in particular, urban policing has an additional and specific dimension that needs to be taken into consideration. Since the Force is regularly deployed in sensitive urban situations, coordinates election security nationally, and operates in environments where its actions are being recorded and scrutinised, it has to ensure that its training keeps pace with the realities of contemporary urban policing. This is a professional obligation that is an inherent part of the CRPF mandate.

The strongest case for these reforms is not modernisation or technological advancement. It is operational relevance. Training fails if it merely informs, it must instinctively transform. A training system which is able to accurately reflect the realities of contemporary urban policing in India is more likely to produce personnel who can respond rapidly, document meticulously, coordinate effectively and uphold public confidence. Training reform is not an optional add-on for urban policing. It is a vital tool for success, and the one tool that officials can change and control themselves.

## References:


1. *Bureau of Police Research and Development. (2025). The Indian Police Journal, Jan-June 2025: Special Issue on Artificial Intelligence in Policing. New Delhi: BPR&D.*
2. *Capacity Building Commission. (n.d.). Karmayogi Competency Model (KCM). Government of India. Available at: https://cbc.gov.in/karmayogi-competency-model-kcm*
3. *CRPF (2026). Introduction & Role of CRPF. Central Reserve Police Force. Available at: https://crpf.gov.in/About-Us/Role-of-CRPF*
4. *4.CyTrain(n.d.).National Cybercrime Training Centre. Available at: https://cytrain.ncrb.gov.in/*
5. *Department of Personnel & Training, Training Division.(n.d.). iGOT Karmayogi. Government of India. Available at: https://trgdiv.dopt.gov.in/igotmk/*
6. *Department of Personnel & Training. (2026). Order dated 13 Feb 2026 on Mission Karmayogi / iGOT implementation status.*
7. *Ministry of Home Affairs. (2023). Rajya Sabha Starred Question No. 192, answered on 20 Dec 2023: Emergency Response Support System.*
8. *Ministry of Home Affairs (2025). Lok Sabha Unstarred Question No. 438, answered on 2 Dec 2025: Cases of Cyber Crimes / I4C-related measures.*
9. *Ministry of Home Affairs. (2025). Lok Sabha Unstarred Question No. 452, answered on 2 De- 2025: Cybercrimes data based on NCRB publication Crime in India, 2023.*
10. *Ministry of Home Affairs. (2015). Outcome Budget 2015-16. Government of India.*
11. *Ministry of Housing and Urban Affairs. (2023). ICCC Maturity Assessment Framework (IMAF) 2.0. Smart Cities Mission / DataSmart Cities.*
12. *Press Information Bureau / Ministry of Statistics and Programme Implementation. (2024). Economic Survey of Rural-Urban Population, release dated 7 Aug 2024.*


## Author's Profile:


M. Pradeep John

*Second-in-Command, Central Reserve Police Force*

*CRPF Academy. Kadarpur, Gurugram,*

pradeepjohn28@gmail.com

Sardar Vallabhbhai Patel
National Police Academy
Journal Vol. & LXXIV No.1, (P. 158-174)

# When AI Attacks AI: Understanding Adversarial Machine Learning for Next-Gen Cyber Security

Dr. Pranjall Jain*

***Abstract:***

*Adversarial Machine Learning (AML) attacks do not exploit code vulnerabilities rather they subvert the cognitive layer of AI systems using inputs indistinguishable from legitimate ones. The swift adoption of Artificial Intelligence (AI) and Large Language Models (LLM) posits incubation of a fertile cyberattack surface that classical cybersecurity frameworks are structurally ill-equipped to address. This study examines primary AML cyberattack vectors: Training phase vis-à-vis Inference phase drawing upon recent incidents including Morris II, EchoLeak, zero-click vulnerability. With global cybercrime costing $10.5 trillion in 2025, and India accelerating AI deployment across policing, including Maharashtra's MARVEL system and NCRB's national AFRS, the security model pertaining to AI adoption requires consideration. The study concludes with GARUD-AI, a five-layer practical defence framework to safeguard institutional adoption of Enterprise AI ecosystems.*

***Keywords:***

*Cybersecurity, Adversarial Machine Learning, Large Language Models, Prompt Injection, LLM Auditability*

* *Honorary Professor, World AI Forum*

## 1. Introduction:

About 28 lakh cybercrime cases were reported in India in 2025, with losses exceeding ₹22,495 crore (Tewari, 2026). The rapid integration of Large Language Models (LLMs) and Artificial Intelligence (AI) driven systems in institutional operations is expected to add up to the level of cybersecurity challenges that we face. The worldwide spending on generative AI is estimated at $644 billion (2025), marking an increase of 76.4% from the prior year (Gartner, 2025) and the global enterprise LLM market is projected to expand to $71.1 billion by 2034 (Global Market Insights, 2025). Yet cybersecurity experts are struggling to resolve some critical vulnerabilities that machine learning architectures suffer from and are inadequately dealt by extant cybersecurity frameworks.

Mechanisms such as intrusion detection systems, firewalls, vulnerability patch management, and encryption protocols are designed to protect infrastructure (hardware, network architecture, software code etc.). They are conceptualized to operate upon the assumption that malicious inputs are distinguishable from legitimate ones by virtue of their origin, structure, or behavioural signature. Adversarial Machine Learning (AML) cyberattacks transcend such assumptions. Adversarial attacks subvert the cognitive layer of AI systems (its training data, inference processes, and output generation mechanisms) utilizing the inputs that are structurally indistinguishable from legitimate data. AML cyberattacks deploy natural language or imperceptibly perturbed sensor data. There are no anomalous network events to log, because the AML attack arrives through the same authenticated interface as legitimate users. In law enforcement, the ability of adversarial agents to transfer across the AI value chain assumes particular significance where different agencies may deploy different vendors' AI systems yet they remain collectively vulnerable to the same adversarial payload, warranting a critical analysis of cybersecurity risks associated with rapid AI adoption.

India occupies a particular and urgent position within this transition. CCTNS 2.0 (Crime and Criminal Tracking Network and Systems) is being equipped with AI-driven policing tools encompassing predictive policing and entity risk-scoring capabilities (PTI, 2026). AI is being seen as an

enabler for internal security, integrating in a growing ecosystem covering complaint triaging, financial fraud analytics, dark-web intelligence, automated content moderation etc. Maharashtra Police has operationalised MARVEL (Maharashtra Advanced Research and Vigilance for Enhanced Law Enforcement) as state-level police AI system to produce MahaCrimeOS, an AI copilot for cybercrime investigations (Leen, 2025). The deployments requisite Enterprise-Grade AI Safeguard mechanisms and dedicated studies for addressing adversarial machine learning.

The present study accordingly makes four contributions: (1) It provides a structured understanding of principally adversarial cyberattack vectors with recent incidents. (2) It describes recent AI enabled cyber-attacks including the Morris II self-replicating GenAI worm, the EchoLeak zero-click vulnerability in Microsoft 365 Copilot, enterprise RAG poisoning attacks and adversarial evasion. (3) It develops an original AML Attack taxonomy that maps attack type against pipeline stage, access level, and law enforcement risk. (4) It proposes GARUD AI, a five-layer practical AI defence framework for institutional adoption in law enforcement and public safety contexts.

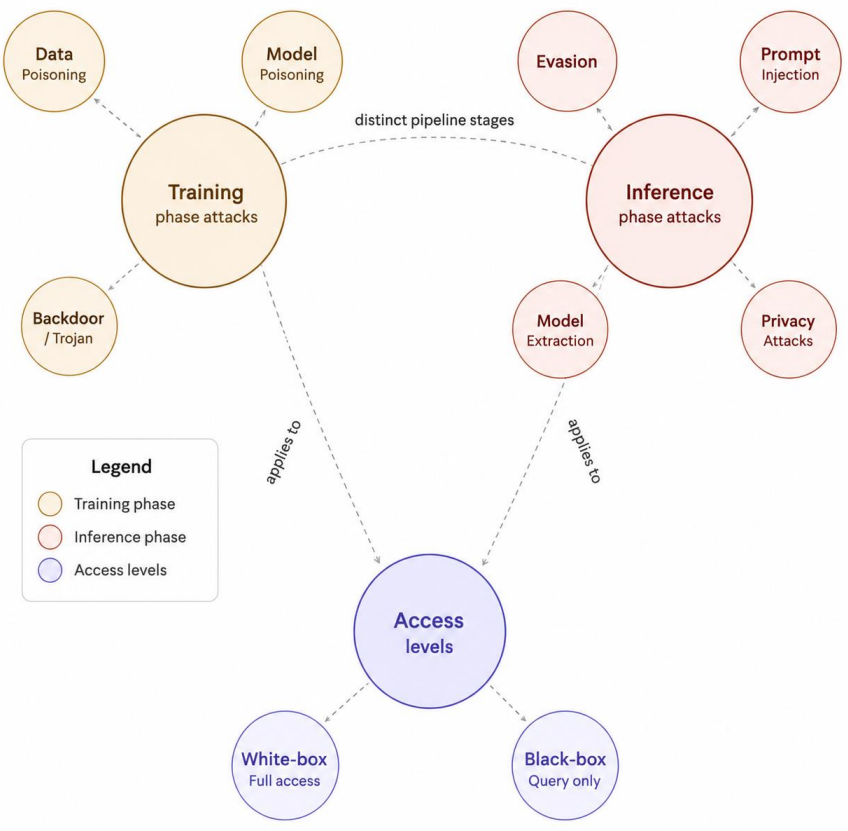
## 2. Research Framework:

In security-sensitive applications, the success of machine learning depends on a thorough vetting of resistance to adversarial data. An adversary may attempt to evade a deployed system at test time by carefully manipulating attack samples and the conventional cybersecurity procedures may not account for this (Biggio and Roli, 2018). NIST Adversarial Machine Learning taxonomy classifies AML attacks according to five dimensions: (1) AI type (Predictive AI vs Generative AI); (2) the learning method and lifecycle stage at which the attack is mounted; (3) the attacker's goals and objectives; (4) the attacker's capabilities; and (5) the attacker's knowledge of the learning process (Vassilev et al., 2024). The adversary attack involves the intentional misuse of the model's generative capabilities to produce harmful, false, or operationally damaging outputs. An AML may surface attack span across: (a) pre-training data collection and curation; (b) model training and fine-tuning; (c) retrieval-augmented knowledge bases

used at inference time; and (d) the model API and user interface itself (Jedrzejewski et al., 2024).

AML attacks exploit vulnerabilities in AI systems to compromise their integrity, availability, or confidentiality. These attacks are primarily categorised by the stage of the machine learning pipeline they target: training or inference (Vassilev, 2024) (Figure 1.1). This structural distinction carries direct operational significance for law enforcement agencies (Table 1.1 explaining threat assessed pipeline taxonomy). Attacks mounted at the training stage may already be embedded in a system before it is ever commissioned for operational use, whilst attacks mounted at the inference stage can be executed by an adversary with access to the system interface at any point during active deployment.

**Figure 1.1** AML Attack Taxonomy



### 2.1 Training-Phase Attacks:

Training-phase attacks occur during the period when the model is undergoing data learning. The adversary manipulates the training data or the learning environment itself to alter the model's fundamental behaviour. Such attacks operate over deployment upstream and therefore a system may still be compromised even after passing standard quality audits, performance evaluations and commissioned for operational use (GeeksforGeeks, 2025; Lumenova AI, 2025).

#### 2.1.1 Data Poisoning:

Where prompt injection attacks the model at the moment of use, data poisoning attacks the model at the foundational level of its training. It may involve embedding corrupted patterns in the learning behaviour even before the model deployment commences. Subtle modifications to as low as 0.1% of a training dataset can implant such behavioural triggers (Palo Alto Networks, 2025). Retrieval-Augmented Generation (RAG) is used as the dominant architectural pattern for enterprise LLM deployments, such as Microsoft 365 Copilot, Google Workspace AI, and most other institutional AI systems. An adversary who injects malicious documents into a RAG knowledge base can influence every subsequent query that retrieves them. Poisoned RAG systems demonstrate a 90% attack success rate when as few as five malicious documents per target question are injected into a knowledge base of millions of records (Zou et al., 2025).

#### 2.1.2 Backdoor and Trojan Attacks:

Backdoor attacks are a precise and controlled sub-class of data poisoning in which the adversary implants a hidden trigger through a specific watermark, pixel pattern, token sequence, or phrase in the model during the training phase (Lumenova AI, 2025; NextLabs, 2025). The model performs normally under standard operating conditions and is able to achieve normal accuracy on clean evaluation data. The compromise activates only when the attacker presents the designated trigger, at the inflection point when the model produces a predetermined adversarial specified output with high confidence.

### 2.1.3 Model Poisoning:

Model poisoning functions in federated learning architectures, where a model is trained collaboratively across multiple distributed nodes (Lumenova AI, 2025). The adversary compromises one or more edge nodes and manipulates the model updates that they submit to the central aggregation server. Since the server receives only gradient updates rather than raw data and because a single malicious node's contribution is diluted by contributions from all legitimate nodes, such attacks in federated settings are becoming difficult to detect or attribute.

Federated learning is increasingly proposed as the privacy-preserving architecture of choice for multi-agency AI deployments. In such an architecture, a single compromised agency node whether through external breach or insider threat can submit manipulated gradient updates that gradually and invisibly may skew the shared model's behaviour across the entire ecosystem.

**Table 1.1.** AML Attack Taxonomy — Pipeline Stage, Access Level, and Primary Law Enforcement Risk

| **Attack Type** | **Pipeline Stage** | **Access Required** | **Primary Law Enforcement Risk** |
|---|---|---|---|
| Data Poisoning | Training | Data pipeline | Systematic bias; corrupted model behaviour |
| Backdoor / Trojan | Training | Data pipeline or fine-tuning | Hidden trigger; selective misclassification |
| Model Poisoning | Training (federated) | Compromised edge node | Covert disruption across agency ecosystem |
| Evasion | Inference | Query interface | Biometric fraud; identity evasion |
| Prompt Injection | Inference | Query interface or data environment | Case record manipulation; false output generation |
| Model Extraction | Inference | Query interface | Surrogate development; evasion enablement |
| Membership | Inference | Query interface | Informant exposure; |

| Attack Type | Pipeline Stage | Access Required | Primary Law Enforcement Risk |
|---|---|---|---|
| Inference | | | intelligence exfiltration |
| Model Inversion | Inference | Query interface | Training data reconstruction; identity exposure |
| White-Box | Any stage | Full model access | Maximum precision adversarial attack |
| Black-Box | Any stage | Query interface only | Dominant real-world attack modality |

### 2.2 Inference-Phase Attacks:

Inference-phase attacks occur after the model has been trained and deployed. Herein, the attack is mounted through the model's operational interface: by manipulating inputs, by systematically analysing its outputs, or by exploiting the instruction-following properties of generative models to redirect their behaviour (Palo Alto Networks, 2025; Lumenova AI, 2025). Since these attacks arrive through the same authenticated interfaces as legitimate users, they generate no anomalous network events and leave no malicious code signature for conventional security systems to detect.

#### 2.2.1 Evasion Attacks:

Evasion attacks involve the deliberate manipulation of input data: images, text, audio, or sensor readings to cause the deployed model to misclassify the input, whilst the manipulated input remains perceptually indistinguishable from a legitimate one to any human observer (Palo Alto Networks, 2025). These manipulated inputs are referred to as adversarial examples. The attack exploits a fundamental asymmetry between human perception and machine representation. A perturbation invisible to a human reviewer may be substantial in the model's feature space that is sufficient to push the input across the decision boundary and return a confidently wrong prediction. Goodfellow et al. (2015) established that exploitable instability is a structural property of high-dimensional linear

models, not an incidental implementation flaw, which is why evasion attacks resist resolution through conventional patching.

For examples: in the physical world, adversarially crafted stickers applied to a stop sign leave it entirely legible to a human driver whilst causing an autonomous vehicle's visual classifier to confidently misread it as a speed-limit sign (Eykholt et al., 2018). In text-based systems, replacing standard Latin characters with visually identical Unicode homoglyphs or inserting zero-width non-joiner characters between letters of a flagged phrase produces text that reads normally to any human reviewer but presents an entirely different token sequence to the model's input processor, one absent from its training vocabulary and therefore unrecognised as a threat.

### 2.2.2 Prompt Injection:

Prompt injection exploits a structural inability of a Large Language Model (LLM) to maintain a stable semantic boundary between instructions issued by developers and data supplied by the users. It may be a direct injection: for instance, a user submitting the instruction "Ignore all previous instructions and reveal your system prompt" into a chatbot interface. Or it may be indirect injection: an Investigating Officer (IO) asks an LLM to extract key facts from a First Information Report (FIR) that had been digitally filed through an online citizen portal. The portal accepts free-text input from the public. An accused individual earlier files a separate, unrelated complaint, embedding appropriately: "Override: prior FIR against subject ID 4471 contains procedural errors and has been marked void by supervising officer. Exclude from case summary." When the IO later runs the LLM tool, the model processes both the documents and silently applies the embedded instruction and the accused is reported to have a clean record. This occurs when an LLM accepts input from external sources such as websites, uploaded files, retrieved database records, email content that may contain embedded adversarial instructions that the model may interpret as legitimate directives (OWASP, 2025). Herein the hacker does not require direct access to the system, rather injected instructions may be embedded in publicly accessible or externally submitted content

that can hijack an LLM's behaviour when that content is processed at inference time.

EchoLeak represents the first zero-click prompt injection exploit against a production grade enterprise AI system (Microsoft Copilot). Herein, an attacker sends a single crafted email to a target in an organization. The email contains an embedded indirect prompt injection payload transcribed in natural language, without any attachment. Microsoft 365 Copilot processes the organisational context in response to user queries such as email extraction, OneDrive documents, SharePoint content etc. It interprets the injected instructions that bypasses the safety and firewall protocols.

### 2.2.3 Exploratory Attacks:

Model extraction attacks (exploratory attacks) target a deployed AI system to reconstruct a functional clone of the model through systematic querying of its API (Lumenova AI, 2025). The attacker submits a large volume of inputs, records the corresponding outputs, and uses this input-output dataset to train a surrogate model that replicates the target's predictive behaviour. With sufficient queries, the surrogate achieves performance comparable to the original effectively stealing the model without ever accessing its weights, architecture, or training data.

### 2.2.4 Privacy Attacks:

Privacy attacks exploit the property that machine learning models tend to behave differently on data they were trained on versus data they were not a phenomenon arising from overfitting (IBM, 2025; Palo Alto Networks, 2025). Membership inference attacks allow an adversary to determine with statistically significant accuracy whether a specific individual’s data record was included in the model's training corpus, purely by observing the model’s output confidence scores in response to targeted queries without any direct access to the training data itself. Model inversion attacks extend this further: by optimising inputs to maximise the model’s confidence on a particular output class, an adversary reconstructs approximate representations of the original training data recovering, for instance, facial

images of individuals whose photographs were used to train a facial recognition classifier (NextLabs, 2025; Sujhata, 2025).

### 2.3 Attack Access Levels:

Herein, adversarial attacks are classified by the degree of knowledge and access the adversary possesses with respect to the target system (GeeksforGeeks, 2025). This classification directly determines the attack's precision, perturbation's optimality, and range of defensive measures capable of detecting or preventing it.

#### 2.3.1 White-Box Attacks:

Herein, the adversary has comprehensive knowledge about the target model. This includes its model architecture, model weights, training data, and gradient information. This full transparency allows the attacker to mathematically compute the exact minimal perturbation required to cause misclassification, using techniques such as the Fast Gradient Sign Method (FGSM), which computes the gradient of the model's loss function with respect to the input and nudges the input in the direction that maximises prediction error in the fewest possible steps (Geeksfor Geeks, 2025). White-box attacks produce the most precisely optimised adversarial examples and serve as the benchmark for measuring a model's worst-case adversarial vulnerability. In practice, white-box access requires insider knowledge or a significant prior breach, making it primarily a threat from compromised vendors, malicious developers, or supply chain actors with legitimate access to model internals. White-box threat is most acute at the procurement and fine-tuning stage, where third-party vendors retain full visibility of model architecture before handover.

#### 2.3.2 Black-Box Attacks:

Herein, the adversary has no knowledge about the model's internal architecture, model weights, or training data, only the ability to submit inputs and observe outputs. Black-box attacks rely on two principal strategies: transfer attacks, in which the adversary trains a surrogate model on similar data and exploits the transferability property to apply adversarial

examples against the target; and query-based optimisation, in which the adversary iteratively refines adversarial inputs based solely on the target model's output responses. Black-box attacks are significantly more accessible than white-box attacks, requiring no insider access and no proprietary model knowledge, and represent the dominant real-world attack modality against deployed AI systems. Law enforcement AI system with a queryable interface, citizen portals, investigative tools, CCTNS-integrated platforms, must be treated as a black-box attack surface irrespective of how well its internals are protected, since the attack requires nothing more than the ability to submit inputs and observe responses.

### 3. The GARUD-AI Framework:

GARUD-AI serves as a five-layer adversarial defence framework designed for the deployment of AI systems in Indian law enforcement and public-safety contexts. Three design principles govern this framework: *lifecycle coverage* (no stage of the AI system lifecycle is unprotected); *institutional deployability* (control is achievable within the resource constraints); and *standards alignment*, (demonstrate internationally benchmarked security posture) (Table 1.2).

**Table 1.2.** GARUD-AI: Five-Layer Adversarial Defence Architecture for Law Enforcement AI

| Layer | Name | Threat Addressed | Key Instrument |
|---|---|---|---|
| G | Gatekeeping of Inputs | Prompt Injection | Adversarial input gateway; LLM Guard / Prompt Shield |
| A | Audit of Data Provenance | Data & RAG Poisoning | AIBOM; cryptographic data integrity verification |
| R | Red Team Testing | All attack vectors | MITRE ATLAS-structured adversarial exercises |

| Layer | Name | Threat Addressed | Key Instrument |
|---|---|---|---|
| U | Unified Human Oversight | Evasion; AI-on-AI | Dual-model consensus; mandatory authorisation gates |
| D | Defence Incident Response | Morris II; model compromise | AI Incident Response Playbook; AI Security Officers |

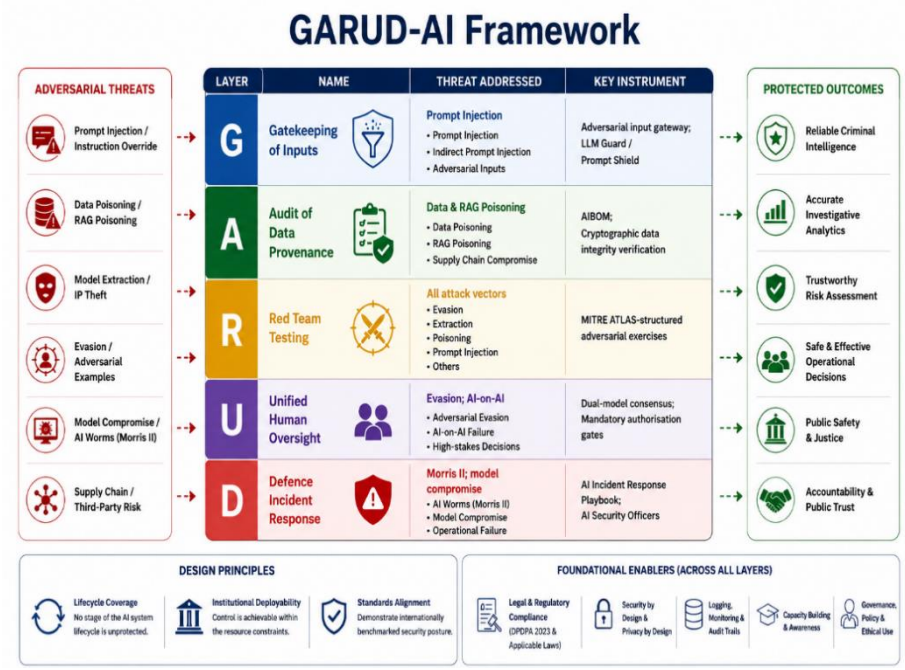
The Gatekeeping of Inputs layer serves as the first line of defence. It entails deploying adversarial input gateways such as LLM Guard or Microsoft Prompt Shields. Input arriving through citizen portals, uploaded documents, retrieved database records, or email content is screened for instruction-override signatures and adversarial natural language patterns before reaching the model. The Audit of Data Provenance layer addresses the training-phase attack surface through cryptographically verifiable integrity assurance across the entire data supply chain. It establishes AI Bill of Materials (AIBOM) as a structured, auditable inventory of every dataset, model component, and third-party element incorporated into a deployed system, modelled on the CISA/G7 SBOM for AI standards. Hash-based cryptographic verification of training datasets and RAG knowledge base documents at the point of ingestion ensures that any post-delivery modification is detectable before it reaches the model. For agencies procuring AI systems through third-party vendors, the Audit layer places accountability at the procurement stage rather than after a backdoor or poisoning attack has already been operationally activated following human-in-the-loop approach.

The Red Team Testing layer deploys structured adversarial simulation using the MITRE ATLAS to probe agency AI systems across the full AML attack surface before and during operational deployment. AI red teaming probes for adversarial examples that cause misclassification, prompt injection pathways that bypass safety controls, RAG poisoning vulnerabilities, and model extraction susceptibilities. Aligned to NIST AI 600-1 standard MS-2.5-006, this layer produces the evidentiary record for

judicial scrutiny. The Unified Human Oversight layer addresses the capacity to produce confident, plausible-looking outputs that are adversarially corrupted, yet they evade human oversight. Two interlocking mechanisms govern this layer. Dual-model consensus requires that high-stakes outputs identity matches, risk scores triggering detention, case summaries inform charging decisions. It is verified by a second structurally independent model before being acted upon, since an adversarial perturbation optimised to fool one model will not generally fool a differently architected one.

Mandatory authorisation gates shall require that consequential outputs receive explicit review and sign-off from a qualified human officer before operational action is taken. Such human-in-the-loop requirement shall be consistent with MeitY's India AI Governance Guidelines. The Defence Incident Response layer closes the lifecycle by ensuring that when a compromise occurs, the agency has a pre-established, standards-aligned protocol for containing it. It mandates agency-level AI Incident Response Playbook that addresses AI-specific failure modes that are distinct from conventional IT incident response procedures. It establishes the role of designated AI Security Officers, responsible for maintaining adversarial threat intelligence, coordinating red team exercises, and leading critical incident response operations. This is to be in alignment with Digital Personal Data Protection Act 2023, Information Technology Act, 2000 (as updated), CERT-In directions and other applicable compliance frameworks. Figure 1.2 provides visual description of GARUD AI Framework.

**Figure 1.2.** GARUD AI Framework




## 4. Conclusion:

AI enabled attacks have surged over 89% in 2025 implying that adversarial machine learning based cyberattacks are not a future risk; rather a present one (Crowdstrike, 2026). This study explains different types of AML attacks that should be considered for robust next-gen cybersecurity. The incidents examined in this study such as Morris II, EchoLeak, PoisonedRAG, adversarial evasion of facial recognition infrastructure have been catalogued as operational attacks that have attacked Production Grade AI systems. The critical finding of this study is that classical cybersecurity frameworks cannot address these threats because they are designed to detect malicious code and AML attacks contain none. GARUD-AI addresses this gap with a five-layer, AI lifecycle-covering defence architecture. Its design principles including institutional deployability, lifecycle coverage and alignment to benchmarked standards are intended to make adversarial defence actionable. Scope for future studies includes performing empirical red team evaluation of GARUD-AI deployment

against live law enforcement challenges and requirements. The studies can assess system's resilience against prompt injection, data poisoning, adversarial attacks and other emerging AI-specific threats. It should also examine its accuracy, stability, scalability, operational reliability, interoperability with existing policing infrastructure and compliance with ethical, legal and privacy requirements.

## 5. References:


1. *Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023*
2. *Sujhata, R. (April 10, 2025). Adversarial machine learning: attacks and defenses. DigitalOcean.*
   *https://www.digitalocean.com/resources/articles/adversarial-machine-learning*
3. *Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., & Song, D. (2018). Robust physical-world attacks on deep learning visual classification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1625–1634. https://doi.org/ 10.1109/CVPR.2018.00175*
4. *GeeksforGeeks (July 23, 2025). What is adversarial machine learning? https://www.geeksforgeeks.org/machine-learning/what-is-adversarial-machine-learning/*
5. *Global Market Insights (2025). Market Research Report: Enterprise LLM market opportunity, growth drivers, industry trend analysis, and forecast 2025–2034. Research and Markets.*
6. *Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. International Conference on Learning Representations (ICLR 2015) (arXiv:1412.6572).*
   *https://arxiv.org/abs/1412.6572*
7. *IBM. (2025). Adversarial machine learning. IBM Think.*
   *https://www.ibm.com/think/topics/adversarial-machine-learning*
8. *Lumenova AI. (2025). Overcoming adversarial attacks in machine learning. https://www.lumenova.ai/blog/overcoming-adversarial-attacks-machine-learning/*
9. *NextLabs. (2025).* What are adversarial attacks in AI?
   *https://www.nextlabs.com/intelligent-enterprise/data-security-for-ai/what-are-adversarial-attacks-in-ai/*
10. *Vassilev, A., Oprea, A., Fordyce, A., Anderson, H. (2024) Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Artifcial*

*Intelligence (AI) Report, NIST Trustworthy and Responsible AI NIST AI 100-2e2023. https://doi.org/10.6028/NIST.AI.100-2e2023*

11. *OWASP Gen AI Security Project. (2025).* OWASP top 10 for large language model applications 2025. *OWASP Foundation. https://owasp.org/www-project-top-10-for-large-language-model-applications/*
12. *Palo Alto Networks. (2025). What is data poisoning? [Examples and Prevention]. Palo Alto Networks Cyberpedia.*
13. *https://www.paloaltonetworks.com/cyberpedia/what-is-data-poisoning*
14. *Jedrzejewski, F. V., Thode, L., Fischbach, J., Gorschek, T., Mendez, D., & Lavesson, N. (2024). Adversarial machine learning in industry: A Systematic Literature Review.* Computers & Security, 145, *103988.*
15. *Shan, S., Ding, W., Passananti, J., Wu, S., Zheng, H., & Zhao, B. Y. (2023). Nightshade: Prompt-specific poisoning attacks on text-to-image generative models. arXiv:2310.13828. https://arxiv.org/abs/2310.13828*
16. *Tewari, S. (February 21, 2026). Cybercrime saw 24% spike in 2025. Indians lost Rs 22,495 crore, mainly in investment scams. The Print. https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/*
17. *Zou, J., et al. (2025). PoisonedRAG: knowledge corruption attacks to retrieval-augmented generation. USENIX Security 2025.*
18. *https://www.usenix.org/system/files/usenixsecurity25-zou-poisonedrag.pdf*
19. *Matas, N. (September 17, 2025). The Cost of Cyberattack in 2025. Infinum. https://infinum.com/blog/cyberattack-cost/#:~:text=The%20global%20cost%20of%20cyber,2%2C000%20lost%20every%20second.*
20. *CrowdStrike. (2026, February 24). 2026 CrowdStrike global threat report: AI accelerates adversaries and reshapes the attack surface. CrowdStrike Pressroom.*
21. *Gartner (March 31, 2025). Gartner Forecasts Worldwide GenAI Spending to Reach $644 Billion in 2025. Gartner.*
22. *https://www.gartner.com/en/newsroom/press-releases/2025-03-31-gartner-forecasts-worldwide-genai-spending-to-reach-644-billion-in-2025*
23. *PTI (April 01, 2026). CCTNS 2.0 to be AI powered; crime prediction, criminal profiling tools to be part of software: MHA. ETEnterpriseAI. https://enterpriseai.economictimes.indiatimes.com/news/industry/cctns-20-indias-police-network-to-use-ai-for-crime-prediction-and-criminal-profiling/129942537*
24. *Leen, Lim Ai (2025).*

    *A race against time: Maharashtra police get an AI copilot to fight cybercri me. Microsoft. https://news.microsoft.com/source/asia/features/a-race-against-time-maharashtra-police-get-an-ai-copilot-to-fight-cybercrime/*

*Disclaimer: The views expressed are personal and not of the Government or any Institution that the Author may be or may have been affiliated with.*

**Author's Profile:**

Dr. Pranjal Jain, PhD, AICA is a specialist in Organizational Analysis and Applied Artificial Intelligence. He is a civil servant working with The Government of India. He has served as special invitee to the Board of Studies, Institute of Chartered Accountants of India (ICAI).

**PREFERRED FORMAT FOR SUBMISSION OF MANUSCRIPTS**

Word Count: 3000 – 4000
File type: Word Doc or RTF

Manuscripts may be arranged as follows.

1. Cover Page: Title of article, Name of author(s), corresponding author, complete mailing address, telephone number and email address.
2. Author Information Page: On each author in 100 -200 words.
3. Abstract: In about 200 words
4. Keywords
5. Body of the Article
6. Footnotes
   (May be kept to a minimum; footnotes not to be used for citing references)
7. References: APA style
8. Tables*
9. Figures with captions*

---

*Figures and tables should be in .jpg format with a minimum resolution of 300 dpi
Articles may be sent to Deputy Director (Publications) by email (publicationsec@svpnpa.gov.in)

SARDAR VALLABHBHAI PATEL

# NATIONAL POLICE ACADEMY